# Contents at a Glance

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>xxvi</td>
<td>Introduction</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Introducing Computer Networks</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>Dissecting the OSI Model</td>
<td>29</td>
</tr>
<tr>
<td>3</td>
<td>Identifying Network Components</td>
<td>59</td>
</tr>
<tr>
<td>4</td>
<td>Understanding Ethernet</td>
<td>107</td>
</tr>
<tr>
<td>5</td>
<td>Working with IP Addresses</td>
<td>139</td>
</tr>
<tr>
<td>6</td>
<td>Routing Traffic</td>
<td>189</td>
</tr>
<tr>
<td>7</td>
<td>Introducing Wide-Area Networks</td>
<td>221</td>
</tr>
<tr>
<td>8</td>
<td>Connecting Wirelessly</td>
<td>257</td>
</tr>
<tr>
<td>9</td>
<td>Optimizing Network Performance</td>
<td>285</td>
</tr>
<tr>
<td>10</td>
<td>Using Command-Line Utilities</td>
<td>315</td>
</tr>
<tr>
<td>11</td>
<td>Managing a Network</td>
<td>357</td>
</tr>
<tr>
<td>12</td>
<td>Securing a Network</td>
<td>385</td>
</tr>
<tr>
<td>13</td>
<td>Troubleshooting Network Issues</td>
<td>437</td>
</tr>
<tr>
<td>14</td>
<td>Final Preparation</td>
<td>461</td>
</tr>
<tr>
<td>A</td>
<td>Answers to Review Questions</td>
<td>469</td>
</tr>
<tr>
<td>B</td>
<td>CompTIA Network+ N10-005 Exam Updates, Version 1.0</td>
<td>473</td>
</tr>
<tr>
<td></td>
<td>Glossary</td>
<td>475</td>
</tr>
<tr>
<td></td>
<td>Index</td>
<td>503</td>
</tr>
<tr>
<td>C</td>
<td>Memory Tables (DVD Only)</td>
<td>3</td>
</tr>
<tr>
<td>D</td>
<td>Memory Table Answer Key (DVD Only)</td>
<td>3</td>
</tr>
</tbody>
</table>
Table of Contents

Introduction  xxvi

Chapter 1  Introducing Computer Networks  3
  Foundation Topics  4
  Defining a Network  4
    The Purpose of Networks  4
    Overview of Network Components  5
  Networks Defined by Geography  7
    LAN  7
    WAN  8
    Other Categories of Networks  9
    CAN  9
    MAN  9
    PAN  9
  Networks Defined by Topology  9
    Physical Versus Logical Topology  10
    Bus Topology  11
    Ring Topology  13
    Star Topology  15
    Hub-and-Spoke Topology  16
    Full-Mesh Topology  18
    Partial-Mesh Topology  19
  Networks Defined by Resource Location  20
    Client-Server Networks  20
    Peer-to-Peer Networks  22
  Summary  24
  Exam Preparation Tasks  25
    Review All the Key Topics  25
    Complete Tables and Lists from Memory  25
    Define Key Terms  25
    Review Questions  26

Chapter 2  Dissecting the OSI Model  29
  Foundation Topics  30
  The Purpose of Reference Models  30
The OSI Model 31
Layer 1: The Physical Layer 33
Layer 2: The Data Link Layer 36
Media Access Control 37
Logical Link Control 37
Layer 3: The Network Layer 39
Layer 4: The Transport Layer 42
Layer 5: The Session Layer 44
Layer 6: The Presentation Layer 45
Layer 7: The Application Layer 46
The TCP/IP Stack 47
Layers of the TCP/IP Stack 47
Common Application Protocols in the TCP/IP Stack 51
Summary 53
Exam Preparation Tasks 54
Review All the Key Topics 54
Complete Tables and Lists from Memory 54
Define Key Terms 55
Review Questions 55

Chapter 3 Identifying Network Components 59
Foundation Topics 60
Media 60
Coaxial Cable 60
Twisted-Pair Cable 62
Shielded Twisted Pair 62
Unshielded Twisted Pair 63
Plenum Versus Non-Plenum Cable 66
Fiber-Optic Cable 66
Multimode Fiber 67
Single-Mode Fiber 68
Cable Distribution 70
Wireless Technologies 73
Network Infrastructure Devices 74
Hubs 74
Bridges 75
Switches 77
Multilayer Switches 83
Routers 84
Infrastructure Device Summary 85
Specialized Network Devices 86
VPN Concentrators 86
Firewalls 87
DNS Servers 88
DHCP Servers 90
Proxy Servers 92
Content Engines 93
Content Switches 94
Virtual Network Devices 95
Virtual Servers 95
Virtual Switches 96
Virtual Desktops 97
Other Virtualization Solutions 98
Voice over IP Protocols and Components 99
Summary 101
Exam Preparation Tasks 102
Review All the Key Topics 102
Complete Tables and Lists from Memory 103
Define Key Terms 103
Review Questions 104

Chapter 4 Understanding Ethernet 107
Foundation Topics 108
Principles of Ethernet 108
Ethernet Origins 108
Carrier Sense Multiple Access Collision Detect 110
Distance and Speed Limitations 113
Ethernet Switch Features 116
Virtual LANs 116
Trunks 118
Spanning Tree Protocol 119
Corruption of a Switch’s MAC Address Table 119
Broadcast Storms 120
STP Operation 122
Link Aggregation 124
Power over Ethernet 126
Port Monitoring 127
User Authentication 129
First-Hop Redundancy 130
Other Switch Features 131
Summary 132
Exam Preparation Tasks 133
Review All the Key Topics 133
Complete Tables and Lists from Memory 133
Define Key Terms 134
Review Questions 134

Chapter 5  Working with IP Addresses 139

Foundation Topics 140
Binary Numbering 140
Principles of Binary Numbering 140
Converting a Binary Number to a Decimal Number 141
Converting a Decimal Number to a Binary Number 141
Binary Numbering Practice 143
Binary Conversion Exercise #1 143
Binary Conversion Exercise #1: Solution 144
Binary Conversion Exercise #2 144
Binary Conversion Exercise #2: Solution 144
Binary Conversion Exercise #3 145
Binary Conversion Exercise #3: Solution 145
Binary Conversion Exercise #4 146
Binary Conversion Exercise #4: Solution 146
IPv4 Addressing 147
IPv4 Address Structure 147
Classes of Addresses 149
Types of Addresses 151
Unicast 151
Broadcast 152
Multicast 152
Assigning IPv4 Addresses 153
IP Addressing Components 154
Static Configuration 154
Dynamic Configuration 159
BOOTP 159
DHCP 160
Automatic Private IP Addressing 161
Subnetting 162
Purpose of Subnetting 162
Subnet Mask Notation 163
Subnet Notation: Practice Exercise #1 165
Subnet Notation: Practice Exercise #1 Solution 165
Subnet Notation: Practice Exercise #2 165
Subnet Notation: Practice Exercise #2 Solution 165
Extending a Classful Mask 166
Borrowed Bits 166
Calculating the Number of Created Subnets 166
Calculating the Number of Available Hosts 167
Basic Subnetting Practice: Exercise #1 167
Basic Subnetting Practice: Exercise #1 Solution 168
Basic Subnetting Practice: Exercise #2 169
Basic Subnetting Practice: Exercise #2 Solution 169
Calculating New IP Address Ranges 170
Advanced Subnetting Practice: Exercise #1 172
Advanced Subnetting Practice: Exercise #1 Solution 172
Advanced Subnetting Practice: Exercise #2 173
Advanced Subnetting Practice: Exercise #2 Solution 174
Additional Practice 176
Classless Inter-Domain Routing 177
IP Version 6 178
Need for IPv6 178
IPv6 Address Structure 178
IPv6 Data Flows 179
Unicast 179
Multicast 180
Anycast 181

Summary 182

Exam Preparation Tasks 183
Review All the Key Topics 183
Complete Tables and Lists from Memory 184
Define Key Terms 184
Review Questions 184

Chapter 6 Routing Traffic 189

Foundation Topics 190
Basic Routing Processes 190
Sources of Routing Information 193
Directly Connected Routes 193
Static Routes 194
Dynamic Routing Protocols 195
Routing Protocol Characteristics 197
Believability of a Route 198
Metrics 198
Interior Versus Exterior Gateway Protocols 199
Route Advertisement Method 200
Distance Vector 200
Link State 202
Routing Protocol Examples 202
Address Translation 204
NAT 204
PAT 206
Multicast Routing 208
IGMP 208
PIM 210
PIM-DM 211
PIM-SM 213
Summary 215
Chapter 7  Introducing Wide-Area Networks  221

Foundation Topics  222

WAN Properties  222
  WAN Connection Types  222
  WAN Data Rates  224
  WAN Media Types  225
     Physical Media  225
     Wireless Media  226

WAN Technologies  227
  Dedicated Leased Line  228
  T1  228
  E1  229
  T3  229
  E3  229
  CSU/DSU  230
  Point-to-Point Protocol  230
  Digital Subscriber Line  234
  Cable Modem  236
  Synchronous Optical Network  237
  Satellite  239
  Plain Old Telephone Service  241
  Integrated Services Digital Network  243
  Frame Relay  245
  Asynchronous Transfer Mode  246
  Multiprotocol Label Switching  249

Summary  250

Exam Preparation Tasks  251
  Review All the Key Topics  251
  Complete Tables and Lists from Memory  251
Chapter 8  Connecting Wirelessly  257

Foundation Topics  258

Introducing Wireless LANs  258
  WLAN Concepts and Components  258
  Wireless Routers  258
  Wireless Access Point  259
  Antennas  260
  Frequencies and Channels  262
  CSMA/CA  265
  Transmission Methods  265
  WLAN Standards  266
    802.11a  266
    802.11b  267
    802.11g  267
    802.11n  267

Deploying Wireless LANs  268
  Types of WLANs  268
    IBSS  269
    BSS  269
    ESS  270
  Sources of Interference  271
  Wireless AP Placement  272

Securing Wireless LANs  273
  Security Issues  273
  Approaches to WLAN Security  275
  Security Standards  277
    WEP  277
    WPA  278
    WPA2  278

Summary  278

Exam Preparation Tasks  279
  Review All the Key Topics  279
  Complete Tables and Lists from Memory  280
Define Key Terms 280
Review Questions 280

Chapter 9 Optimizing Network Performance 285

Foundation Topics 286
High Availability 286
  High-Availability Measurement 286
  Fault-Tolerant Network Design 286
  Hardware Redundancy 288
  Layer 3 Redundancy 288
  Design Considerations for High-Availability Networks 290
  High-Availability Best Practices 290
Content Caching 291
Load Balancing 291

QoS Technologies 292
  Introduction to QoS 292
  QoS Configuration Steps 294
  QoS Components 295
  QoS Mechanisms 296
Classification 296
Marking 297
Congestion Management 298
Congestion Avoidance 298
Policing and Shaping 299
Link Efficiency 301

Case Study: SOHO Network Design 302
  Case Study Scenario 302
  Suggested Solution 304
  IP Addressing 304
  Layer 1 Media 305
  Layer 2 Devices 306
  Layer 3 Devices 307
  Wireless Design 307
  Environmental Factors 308
  Cost Savings Versus Performance 308
  Topology 309
Chapter 10  Using Command-Line Utilities  315

Foundation Topics  316
Windows Commands  316
  arp  316
  ipconfig  318
  nbtstat  321
  netstat  324
  nslookup  326
  ping  328
  route  330
  tracert  334
UNIX Commands  336
  arp  337
  dig and nslookup  340
  host  341
  ifconfig  341
  traceroute  342
  netstat  343
  ping  345
Summary  348
Exam Preparation Tasks  349
  Review All the Key Topics  349
  Complete Tables and Lists from Memory  350
  Define Key Terms  350
  Review Questions  350

Chapter 11  Managing a Network  357

Foundation Topics  358
Maintenance Tools  358
  Bit-Error Rate Tester  358
  Butt Set  359
Cable Certifier 359
Cable Tester 360
Connectivity Software 360
Crimper 360
Electrostatic Discharge Wrist Strap 361
Environmental Monitor 362
Loopback Plug 362
Multimeter 363
Protocol Analyzer 364
Punch-Down Tool 365
Throughput Tester 365
Time Domain Reflectometer/Optical Time Domain Reflectometer 366
Toner Probe 366
Configuration Management 367
Monitoring Resources and Reports 369
    SNMP 369
    Syslog 373
    Logs 375
    Application Logs 376
    Security Logs 376
    System Logs 377
Summary 378
Exam Preparation Tasks 379
    Review All the Key Topics 379
    Complete Tables and Lists from Memory 379
    Define Key Terms 380
    Review Questions 380

Chapter 12  Securing a Network 385
Foundation Topics 386
Security Fundamentals 386
    Network Security Goals 386
    Confidentiality 386
    Integrity 390
    Availability 391
    Categories of Network Attacks 391
Confidentiality Attacks 391
Integrity Attacks 394
Availability Attacks 397
Defending Against Attacks 402
User Training 402
Patching 402
Security Policies 403
Governing Policy 404
Technical Policies 405
End User Policies 405
More Detailed Documents 405
Incident Response 406
Vulnerability Scanners 407
Nessus 407
Nmap 408
Honey Pots and Honey Nets 409
Access Control Lists 410
Remote Access Security 411
Firewalls 413
Firewall Types 413
Firewall Inspection Types 414
Packet-Filtering Firewall 414
Stateful Firewall 415
Firewall Zones 416
Virtual Private Networks 417
Overview of IPsec 419
IKE Modes and Phases 420
Authentication Header and Encapsulating Security Payload 422
The Five Steps in Setting Up and Tearing Down an IPsec Site-to-Site VPN 423
Other VPN Technologies 425
Intrusion Detection and Prevention 425
IDS Versus IPS 426
IDS and IPS Device Categories 427
Detection Methods 427
Deploying Network-Based and Host-Based Solutions 428
Summary 430
Exam Preparation Tasks 431
Review All the Key Topics 431
Complete Tables and Lists from Memory 432
Define Key Terms 432
Review Questions 432

Chapter 13 Troubleshooting Network Issues 437
Foundation Topics 438
Troubleshooting Basics 438
Troubleshooting Fundamentals 438
Structured Troubleshooting Methodology 440
Physical Layer Troubleshooting 443
Physical Layer Troubleshooting: Scenario 444
Physical Layer Troubleshooting: Solution 445
Data Link Layer Troubleshooting 445
Data Link Layer Troubleshooting: Scenario 446
Data Link Layer Troubleshooting: Solution 447
Network Layer Troubleshooting 447
Layer 3 Data Structures 448
Common Layer 3 Troubleshooting Issues 449
Network Layer Troubleshooting: Scenario 451
Network Layer Troubleshooting: Solution 451
Wireless Troubleshooting 452
Wireless Network Troubleshooting: Scenario 454
Wireless Network Troubleshooting: Solution 455
Summary 455
Exam Preparation Tasks 456
Review All the Key Topics 456
Complete Tables and Lists from Memory 456
Define Key Terms 456
Review Questions 457
Chapter 14  Final Preparation  461
  Tools for Final Preparation  461
  Pearson Cert Practice Test Engine and Questions on the DVD  461
    Install the Software from the DVD  462
    Activate and Download the Practice Exam  463
    Activating Other Exams  463
    Premium Edition  463
  Video Training on DVD  464
  Memory Tables  464
  End-of-Chapter Review Tools  465
  Suggested Plan for Final Review and Study  465
  Summary  467

APPENDIX A  Answers to Review Questions  469
APPENDIX B  CompTIA Network+ N10-005 Exam Updates, Version 1.0  473
  Glossary  475
  Index  503

APPENDIX C  Memory Tables (DVD Only)  3
APPENDIX D  Memory Table Answer Key (DVD Only)  3
About the Author

Kevin Wallace, CCIE No. 7945, is a certified Cisco instructor, and he holds multiple certifications, including CCNP, CCNP Voice, CCNP Security, and CCDP, in addition to multiple security and voice specializations. With networking experience dating back to 1989 (and computer experience dating back to 1982), Kevin is a senior technical instructor for SkillSoft. Kevin has been a network design specialist for the Walt Disney World Resort and a network manager for Eastern Kentucky University. Kevin holds a bachelor’s of science degree in electrical engineering from the University of Kentucky. Also, Kevin has authored multiple books for Cisco Press, including Implementing Cisco Unified Communications Voice over IP and QoS (CVOICE), TSHOOT Official Certification Guide, Routing Video Mentor, and TSHOOT Video Mentor. Kevin lives in central Kentucky with his wife (Vivian) and two daughters (Sabrina and Stacie). You can follow Kevin online through the following social-media outlets:

Web page: http://1ExamAMonth.com
Facebook fan page: Kevin Wallace Networking
Twitter: http://twitter.com/kwallaceccie
YouTube: http://youtube.com/kwallaceccie
Network World blog: http://nww.com/community/wallace
iTunes podcast: 1ExamAMonth.com

Dedication

This book is dedicated to my beautiful (inside and out) wife, Vivian. As of this writing, we are 17 years along on our way to forever together.
Acknowledgments

Huge thanks go out to my editor, Brett Bartow, and all the other professionals at Pearson IT Certification. It is my great pleasure to have been associated with you for the past eight years, and I look forward to more exciting projects in the future.

My director at SkillSoft, Dan Young, has been super-supportive of my writing efforts, and I extend my gratitude to him.

Thanks to my technical editors, Michelle Plumb and Theodor Richardson. In a book such as this, with all of its terminology, I’m grateful that you guys were looking over my shoulder and pointing out errors.

In the “Dedication” section, I mentioned my wife, Vivian. I once again want to acknowledge her. Being the parents of two teenage daughters can be time-intensive, and she is always willing to take on more than her fair share so that I can immerse myself in writing.

Speaking of our girls, Stacie and Sabrina, I also want to acknowledge you two. I am very proud of the young ladies you are becoming. Your character and your love for God are an inspiration to others.

As I’ve grown in my own personal faith, I’ve discovered that my spiritual gift is teaching. The book you now hold in your hands is a manifestation of that gift. My desire is to be a good steward of that God-given gift. So, with His guidance and continued blessings, I plan to continue demystifying complex concepts to my students and readers.

Albert Einstein once said, “If you can’t explain it simply, you don’t understand it well enough.” My goal for you, the reader, is that you will understand the concepts in this book so well, you will be able to explain them simply to others.
About the Reviewers

Michelle Plumb is a full-time Cisco certified instructor for SkillSoft. Michelle has 22+ years of experience in the field as an IT professional and telephony specialist. She maintains a high level of Cisco, Microsoft, and CompTIA certifications, including A+, Network+, and Project+. Michelle has been a technical reviewer for numerous books related to the Cisco CCNP, CCNP Voice, and CompTIA course material tracks. Michelle currently lives in Phoenix, Arizona, with her husband and two dogs.

Theodor D. Richardson is an author, Choice magazine book reviewer, Online Program Director, and Assistant Professor for a private university. He has served as an Assistant Professor for five years in the area of security and multimedia/web design. Theodor has authored Secure Software Design (Jones and Bartlett Learning, 2012) and Microsoft Office and Beyond (Mercury Learning and Information, 2011). Theodor earned his Ph.D. degree in Computer Science and Engineering from the University of South Carolina in 2006 with a concentration in multimedia and image processing (Graduate Student of the Year 2005). Theodor received an NSF Graduate Research Fellowship and an NSF GK-12 Graduate/K-12 Teaching Fellowship during his graduate studies. He has earned the NSA Graduate Certificate in Information Assurance and Security from the University of South Carolina.
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.

As an Associate Publisher for Pearson Certification, I welcome your comments. You can e-mail or write me directly to let me 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 I cannot help you with technical problems related to the topic of this book. We do have a User Services group, however, where I will forward specific technical questions related to the book.

When you write, please be sure to include this book’s title and author as well as your name, e-mail address, and phone number. I will carefully review your comments and share them with the author and editors who worked on the book.

E-mail:    feedback@pearsonitcertification.com
Mail:    David Dusthimer
         Associate Publisher
         Pearson
         800 East 96th Street
         Indianapolis, IN 46240 USA

Reader Services

Visit our website and register this book at www.pearsonitcertification.com/title/9780789748218 for convenient access to any updates, downloads, or errata that might be available for this book.
CompTIA Network+

The CompTIA Network+ (2011 Edition) certification ensures that the successful candidate has the important knowledge and skills necessary to manage, maintain, troubleshoot, install, operate, and configure basic network infrastructure, describe networking technologies, basic design principles, and adhere to wiring standards and use testing tools.

It Pays to Get Certified

In a digital world, digital literacy is an essential survival skill—Certification proves you have the knowledge and skill to solve business problems in virtually any business environment. Certifications are highly valued credentials that qualify you for jobs, increased compensation, and promotion.

CompTIA Network+ certification held by many IT staff in organizations—21% of IT staff within a random sampling of U.S. organizations within a cross section of industry verticals hold Network+ certification.

- **The CompTIA Network+ credential**—Proves knowledge of networking features and functions and is the leading vendor-neutral certification for networking professionals.

- **Starting Salary**—The average starting salary of network engineers can be up to $70,000.

- **Career Pathway**—CompTIA Network+ is the first step in starting a networking career and is recognized by Microsoft as part of their MS program. Other corporations, such as Novell, Cisco, and HP, also recognize CompTIA Network+ as part of their certification tracks.

- **More than 260,000**—Individuals worldwide are CompTIA Network+ certified.

- **Mandated/recommended by organizations worldwide**—Such as Cisco, HP, Ricoh, the U.S. State Department, and U.S. government contractors such as EDS, General Dynamics, and Northrop Grumman.
How Certification Helps Your Career

IT is Everywhere
IT is ubiquitous, needed by most organizations. Globally, there are over 600,000 IT job openings.

IT Knowledge and Skills Gets Jobs
Certifications are essential credentials that qualify you for jobs, increased compensation, and promotion.

Retain Your Job and Salary
Make your expertise stand above the rest. Competence is usually retained during times of change.

Want to Change Jobs
Certifications qualify you for new opportunities, whether locked into a current job, see limited advancement, or need to change careers.

Stick Out from the Resume Pile
Hiring managers can demand the strongest skill set.

CompTIA Career Pathway
CompTIA offers a number of credentials that form a foundation for your career in technology and allow you to pursue specific areas of concentration. Depending on the path you choose to take, CompTIA certifications help you build upon your skills and knowledge, supporting learning throughout your entire career.
## Steps to Getting Certified and Staying Certified

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review Exam Objectives</td>
<td>Review the certification objectives to make sure you know what is covered in the exam: <a href="http://certification.comptia.org/Training/testingcenters/examobjectives.aspx">http://certification.comptia.org/Training/testingcenters/examobjectives.aspx</a></td>
</tr>
<tr>
<td>Practice for the Exam</td>
<td>After you have studied for the certification, take a free assessment and sample test to get an idea of what type of questions might be on the exam: <a href="http://certification.comptia.org/Training/testingcenters/samplequestions.aspx">http://certification.comptia.org/Training/testingcenters/samplequestions.aspx</a></td>
</tr>
<tr>
<td>Purchase an Exam Voucher</td>
<td>Purchase your exam voucher on the CompTIA Marketplace, which is located at: <a href="http://www.comptiastore.com/">http://www.comptiastore.com/</a></td>
</tr>
<tr>
<td>Take the Test!</td>
<td>Select a certification exam provider and schedule a time to take your exam. You can find exam providers at the following link: <a href="http://certification.comptia.org/Training/testingcenters.aspx">http://certification.comptia.org/Training/testingcenters.aspx</a></td>
</tr>
<tr>
<td>Stay Certified!</td>
<td>Effective January 1, 2011, CompTIA Network+ certifications are valid for three years from the date of certification. There are a number of ways the certification can be renewed. For more information, go to: <a href="http://certification.comptia.org/getCertified/steps_to_certification/stayCertified.aspx">http://certification.comptia.org/getCertified/steps_to_certification/stayCertified.aspx</a></td>
</tr>
</tbody>
</table>

## Join the Professional Community

<table>
<thead>
<tr>
<th>Community</th>
<th>Description</th>
</tr>
</thead>
</table>
| Join IT Pro Community [http://itpro.comptia.org](http://itpro.comptia.org) | The free IT Pro online community provides valuable content to students and professionals.  
Career IT Job Resources:  
- Where to start in IT  
- Career Assessments  
- Salary Trends  
- U.S. Job Board  
Forums on networking, security, computing, and cutting-edge technologies.  
Access to blogs written by industry experts.  
Current information on cutting-edge technologies.  
Access to various industry resource links and articles related to IT and IT careers. |

## Content Seal of Quality

This courseware bears the seal of **CompTIA Approved Quality Content**. This seal signifies this content covers 100% of the exam objectives and implements important instructional design principles. CompTIA recommends multiple learning tools to help increase coverage of the learning objectives.
Why CompTIA?

■ **Global Recognition**—CompTIA is recognized globally as the leading IT non-profit trade association and has enormous credibility. Plus, CompTIA’s certifications are vendor-neutral and offer proof of foundational knowledge that translates across technologies.

■ **Valued by Hiring Managers**—Hiring managers value CompTIA certification, because it is vendor- and technology-independent validation of your technical skills.

■ **Recommended or Required by Government and Businesses**—Many government organizations and corporations either recommend or require technical staff to be CompTIA certified. (For example, Dell, Sharp, Ricoh, the U.S. Department of Defense, and many more.)

■ **Three CompTIA Certifications Ranked in the Top 10**—In a study by DICE of 17,000 technology professionals, certifications helped command higher salaries at all experience levels.

How to Obtain More Information

■ **Visit CompTIA online**—www.comptia.org to learn more about getting CompTIA certified.

■ **Contact CompTIA**—Call 866-835-8020 ext. 5 or email questions@comptia.org.

■ **Join the IT Pro community**—http://itpro.comptia.org to join the IT community to get relevant career information.

■ **Connect with us**—
Introduction

The CompTIA Network+ certification is a popular certification for those entering the computer-networking field. Although many vendor-specific networking certifications are popular in the industry, the CompTIA Network+ certification is unique in that it is vendor-neutral. The CompTIA Network+ certification often acts as a stepping-stone to more specialized and vendor-specific certifications, such as those offered by Cisco Systems.

Notice in your CompTIA Network+ study that the topics are mostly generic, in that they can apply to networking equipment regardless of vendor. However, as you grow in your career, I encourage you to seek specialized training for the equipment you work with on a daily basis.

Goals and Methods

The goal of this book is twofold. The #1 goal of this book is a simple one: to help you pass the N10-005 version of the CompTIA Network+ exam.

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

■ **Opening topics list:** This defines the topics that are covered in the chapter.

■ **Foundation topics:** At the heart of a chapter, this section explains the topics from a hands-on and a theory-based standpoint. This includes in-depth descriptions, tables, and figures that build your knowledge so that you can pass the N10-005 exam. The chapters are each broken into multiple sections.

■ **Key topics:** This indicates important figures, tables, and lists of information that you need to know for the exam. They are sprinkled throughout each chapter and are summarized in table format at the end of each chapter.

■ **Memory tables:** These can be found on the DVD within Appendices C and D. Use them to help memorize important information.

■ **Key terms:** Key terms without definitions are listed at the end of each chapter. Write down the definition of each term, and check your work against the complete key terms in the Glossary.

For current information about the CompTIA Network+ certification exam, you can visit http://certification.comptia.org/getCertified/certifications/network.aspx.
Who Should Read This Book?

The CompTIA Network+ exam measures the necessary competencies for an entry-level networking professional with the equivalent knowledge of at least 500 hours of hands-on experience in the lab or field. This book was written for people who have that amount of experience working with computer networks. Average readers will have connected a computer to a network, configured IP addressing on that computer, installed software on that computer, used command-line utilities (for example, the **ping** command), and used a browser to connect to the Internet.

Readers will range from people who are attempting to attain a position in the IT field to people who want to keep their skills sharp or perhaps retain their job because of a company policy that mandates they take the new exams.

This book also targets the reader who wants to acquire additional certifications beyond the Network+ certification (for example, the Cisco Certified Network Associate [CCNA] certification and beyond). The book is designed in such a way to offer easy transition to future certification studies.

Strategies for Exam Preparation

Strategies for exam preparation vary, depending on your existing skills, knowledge, and equipment available. Of course, the ideal exam preparation would include building and configuring a computer network from scratch. Preferably, the network would contain both Microsoft Windows® and UNIX hosts, at least two Ethernet switches, and at least two routers.

However, not everyone has access to this equipment, so the next best step you can take is to read the chapters in this book, jotting down notes with key concepts or configurations on a separate notepad. For more visual learners, you might consider the Network+ Video Mentor product by Anthony Sequeira, which is available from Pearson IT Certification, where you get to watch an expert perform multiple configurations.

After you read the book, you can download the current exam objectives by submitting a form on the following web page: http://certification.comptia.org/Training/testingcenters/examobjectives.aspx

If there are any areas shown in the certification exam outline that you still want to study, find those sections in this book and review them.
When you feel confident in your skills, attempt the practice exam, which is included on this book’s DVD. As you work through the practice exam, note the areas where you lack confidence and review those concepts or configurations in this book. After you review these areas, work through the practice exam a second time, and rate your skills. Keep in mind that the more you work through the practice exam, the more familiar the questions become, and the practice exam becomes a less accurate judge of your skills.

After you work through the practice exam a second time and feel confident with your skills, schedule the real CompTIA Network+ exam (N10-005). The following website provides information about registering for the exam: http://certification.comptia.org/Training/testingcenters.aspx

To prevent the information from evaporating out of your mind, you should typically take the exam within a week of when you consider yourself ready to take it.

**CompTIA Network+ Exam Topics**

Table I-1 lists general exam topics (objectives) and specific topics under each general topic (subobjectives) for the CompTIA Network+ N10-005 exam. This table also lists the chapter in which each exam topic is covered. Note that some objectives and subobjectives are addressed in multiple chapters.

<table>
<thead>
<tr>
<th>Chapter</th>
<th>N10-005 Exam Objective</th>
<th>N10-005 Exam Subobjective</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (Introducing Computer Networks)</td>
<td>3.0 Network Media and Topologies</td>
<td>3.5 Describe different network topologies.</td>
</tr>
<tr>
<td>2 (Dissecting the OSI Model)</td>
<td>1.0 Network Technologies</td>
<td>1.1 Compare the layers of the OSI and TCP/IP models.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.2 Classify how applications, devices, and protocols relate to the OSI layers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.5 Identify common TCP and UDP default ports.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.6 Explain the function of common network protocols.</td>
</tr>
<tr>
<td>Chapter</td>
<td>N10-005 Exam Objective</td>
<td>N10-005 Exam Subobjective</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>3 (Identifying Network Components)</td>
<td>1.0 Network Technologies</td>
<td>1.7 Summarize DNS concepts and its components.</td>
</tr>
<tr>
<td></td>
<td>2.0 Network Installation and Configuration</td>
<td>1.9 Identify virtual desktop components.</td>
</tr>
<tr>
<td></td>
<td>3.0 Network Media and Topologies</td>
<td>2.3 Explain the purpose and properties of DHCP.</td>
</tr>
<tr>
<td></td>
<td>4.0 Network Management</td>
<td>3.1 Categorize standard media types and associated properties.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.2 Categorize standard connector types based on network media.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.8 Identify components of wiring distribution.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4.1 Explain the purpose and features of various network appliances.</td>
</tr>
<tr>
<td>4 (Understanding Ethernet)</td>
<td>1.0 Network Technologies</td>
<td>1.4 Explain the purpose of routing and switching.</td>
</tr>
<tr>
<td></td>
<td>2.0 Network Installation and Configuration</td>
<td>2.1 Given a scenario, install and configure routers and switches.</td>
</tr>
<tr>
<td></td>
<td>3.0 Network Media and Topologies</td>
<td>3.7 Compare and contrast different LAN technologies.</td>
</tr>
<tr>
<td>5 (Working with IP Addresses)</td>
<td>1.0 Network Technologies</td>
<td>1.3 Explain the purpose and properties of IP addressing.</td>
</tr>
<tr>
<td>6 (Routing Traffic)</td>
<td>1.0 Network Technologies</td>
<td>1.4 Explain the purpose and properties of routing and switching.</td>
</tr>
<tr>
<td></td>
<td>2.0 Network Installation and Configuration</td>
<td>2.1 Given a scenario, install and configure routers and switches.</td>
</tr>
<tr>
<td>7 (Introducing Wide-Area Networks)</td>
<td>3.0 Network Media and Topologies</td>
<td>3.4 Categorize WAN technology types and properties.</td>
</tr>
<tr>
<td>8 (Connecting Wirelessly)</td>
<td>2.0 Network Installation and Configuration</td>
<td>2.2 Given a scenario, install and configure a wireless network.</td>
</tr>
<tr>
<td></td>
<td>3.0 Network Media and Topologies</td>
<td>2.4 Given a scenario, troubleshoot common wireless problems.</td>
</tr>
<tr>
<td></td>
<td>5.0 Network Security</td>
<td>3.3 Compare and contrast different wireless standards.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.1 Given a scenario, implement appropriate wireless security measures.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.4 Explain common threats, vulnerabilities, and mitigation techniques.</td>
</tr>
<tr>
<td>Chapter</td>
<td>N10-005 Exam Objective</td>
<td>N10-005 Exam Subobjective</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>9 (Optimizing Network Performance)</td>
<td>2.0 Network Installation and Configuration</td>
<td>2.6 Given a set of requirements, plan and implement a basic SOHO network.</td>
</tr>
<tr>
<td></td>
<td>4.0 Network Management</td>
<td>4.6 Explain different methods and rationales for network performance optimization.</td>
</tr>
<tr>
<td>10 (Using Command-Line Utilities)</td>
<td>4.0 Network Management</td>
<td>4.3 Given a scenario, use appropriate software tools to troubleshoot connectivity issues.</td>
</tr>
<tr>
<td>11 (Managing a Network)</td>
<td>4.0 Network Management</td>
<td>4.2 Given a scenario, use appropriate hardware tools to troubleshoot connectivity issues.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4.3 Given a scenario, use appropriate software tools to troubleshoot connectivity issues.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4.4 Given a scenario, use the appropriate network resource to analyze traffic.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4.5 Describe the purpose of configuration management documentation.</td>
</tr>
<tr>
<td>12 (Securing a Network)</td>
<td>4.0 Network Management</td>
<td>4.1 Explain the purpose and features of various network appliances.</td>
</tr>
<tr>
<td></td>
<td>5.0 Network Security</td>
<td>5.2 Explain the methods of network access security.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.3 Explain methods of user authentication.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.4 Explain common threats, vulnerabilities, and mitigation techniques.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.5 Given a scenario, install and configure a basic firewall.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.6 Categorize different types of network security appliances and methods.</td>
</tr>
<tr>
<td>13 (Troubleshooting Network Issues)</td>
<td>1.0 Network Technologies</td>
<td>1.8 Given a scenario, implement a given troubleshooting methodology.</td>
</tr>
<tr>
<td></td>
<td>2.0 Network Installation and Configuration</td>
<td>2.4 Given a scenario, troubleshoot common wireless problems.</td>
</tr>
<tr>
<td></td>
<td>3.0 Network Media and Topologies</td>
<td>2.5 Given a scenario, troubleshoot common router and switch problems.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.6 Given a scenario, troubleshoot common physical connectivity problems.</td>
</tr>
</tbody>
</table>
How This Book Is Organized

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

- **Chapter 1, “Introducing Computer Networks.”** introduces the purpose of computer networks and their constituent components. Additionally, networks are categorized by their geography, topology, and resource location.

- **Chapter 2, “Dissecting the OSI Model.”** presents the two network models: the OSI model and the TCP/IP stack. These models categorize various network components from a network cable up to and including an application, such as e-mail. These models are contrasted, and you are given a listing of well-known TCP and UDP port numbers used for specific applications.

- **Chapter 3, “Identifying Network Components.”** A variety of network components are introduced in this chapter. You are given an explanation of various media types, the roles of specific infrastructure components, and the features provided by specialized network devices (for example, a firewall or content switch).

- **Chapter 4, “Understanding Ethernet.”** The most widely deployed LAN technology is Ethernet, and this chapter describes the characteristics of Ethernet networks. Topics include media access, collision domains, broadcast domains, and distance/speed limitations for popular Ethernet standards. Additionally, you are introduced to some of the features available on Ethernet switches, such as VLANs, trunks, STP, link aggregation, PoE, port monitoring, and user authentication.

- **Chapter 5, “Working with IP Addresses.”** One of the most challenging concepts for many CompTIA Network+ students is IP subnetting. This chapter demystifies IP subnetting by reviewing the basics of binary numbering, before delving into basic subnetting and then advanced subnetting. Although most of the focus of this chapter is on IP version 4 (IPv4) addressing, the chapter concludes with an introduction to IP version 6 (IPv6).

- **Chapter 6, “Routing Traffic.”** A primary job of a computer network is to route traffic between subnets. This chapter reviews the operation of routing IP traffic and discusses how a router obtains routing information. One way a router can populate its routing table is through the use of dynamic routing protocols, several of which are discussed in this chapter. Many environments (such as a home network connecting to the Internet via a cable modem) use NAT to convert between private IP addresses inside a network and public IP addresses outside a network. This chapter discusses DNAT, SNAT, and PAT.
Although the primary focus on this chapter is on unicast routing, the chapter concludes with a discussion of multicast routing.

- **Chapter 7, “Introducing Wide-Area Networks.”** Many corporate networks need to interconnect multiple sites separated by large distances. Connections between such geographically dispersed sites make up a WAN. This chapter discusses three categories of WAN connections and contrasts various WAN connection types, based on supported data rates and media types. Finally, this chapter lists characteristics for multiple WAN technologies.

- **Chapter 8, “Connecting Wirelessly.”** In this increasingly mobile world, wireless technologies are exploding in popularity. This chapter discusses the basic operation of WLANs. Additionally, WLAN design and security considerations are addressed.

- **Chapter 9, “Optimizing Network Performance.”** This chapter explains the importance of high availability for a network and what mechanisms help provide a high level of availability. Network performance optimization strategies are addressed, including a section on QoS. Finally, this chapter allows you to use what you have learned in this and preceding chapters to design a SOHO network.

- **Chapter 10, “Using Command-Line Utilities.”** In your daily administration and troubleshooting of computer networks, you need familiarity with various command-line utilities available on the operating systems present in your network. This chapter presents a collection of popular command-line utilities for both Microsoft Windows® and UNIX platforms.

- **Chapter 11, “Managing a Network,”** reviews some of the more common tools used to physically maintain a network. The components of configuration management are also presented. Finally, this chapter discusses some of the network-monitoring tools available to network administrators and what types of information are included in various logs.

- **Chapter 12, “Securing a Network.”** Network security is an issue for most any network, and this chapter covers a variety of network security technologies. You begin by understanding the goals of network security and the types of attacks you must defend against. Then, you review a collection of security best practices. Next, the chapter discusses specific security technologies, including firewalls, VPNs, IDSs, and IPSs.

- **Chapter 13, “Troubleshooting Network Issues.”** Troubleshooting network issues in an inherent part of network administration, and this chapter presents a structured approach to troubleshooting various network technologies. Specifically, you learn how to troubleshoot common Layer 2, Layer 3, and wireless network issues.
Chapter 14, “Final Preparation,” reviews the exam-preparation tools available in this book and the enclosed DVD. For example, the enclosed DVD contains a practice exam engine and a collection of ten training videos presented by the author. Finally, a suggested study plan is presented to assist you in preparing for the CompTIA Network+ exam (N10-005).

In addition to the 13 main chapters, this book includes tools to help you verify that you are prepared to take the exam. The DVD includes a practice test and memory tables that you can work through to verify your knowledge of the subject matter. The DVD also contains ten training videos that cover some of the most fundamental and misunderstood content in the CompTIA Network+ curriculum, specifically the OSI model and IP addressing.
After completion of this chapter, you will be able to answer the following questions:

- How do various wireless LAN (WLAN) technologies function, and what wireless standards are in common use?
- What are some of the most important WLAN design considerations?
- What WLAN security risks exist, and how can those risks be mitigated?
The popularity of wireless LANs (WLAN) has exploded over the past decade, allowing users to roam within a WLAN coverage area, allowing users to take their laptops with them and maintain network connectivity as they move throughout a building or campus environment. Many other devices, however, can take advantage of wireless networks, such as gaming consoles, smart phones, and printers.

This chapter introduces WLAN technology, along with various wireless concepts, components, and standards. WLAN design considerations are then presented, followed by a discussion of WLAN security.
Introducing Wireless LANs

This section introduces the basic building blocks of WLANs and discusses how WLANs connect into a wired local-area network (LAN). Various design options, including antenna design, frequencies, and communications channels are discussed, along with a comparison of today’s major wireless standards, which are all some variant of IEEE 802.11.

WLAN Concepts and Components

Wireless devices, such as laptops and smart phones, often have a built-in wireless card that allows those devices to communicate on a WLAN. But, what is the device to which they communicate? It could be, as one example, another laptop with a wireless card. This would be an example of an ad-hoc WLAN. However, enterprise-class WLANs, and even most WLANs in homes, are configured in such a way that a wireless client connects to some sort of a wireless base station, such as a wireless access point (AP) or a wireless router.

This communication might be done using a variety of antenna types, frequencies, and communication channels. The following sections consider some of these elements in more detail.

Wireless Routers

Consider the basic WLAN topology shown in Figure 8-1. Such a WLAN might be found in a residence whose Internet access is provided by digital subscriber line (DSL) modem. In this topology, a wireless router and switch are shown as separate components. However, in many residential networks, a wireless router integrates switch ports and wireless routing functionality into a single device.
In Figure 8-1, the wireless router obtains an IP address via DHCP from the Internet service provider (ISP). Then, the router uses Port Address Translation (PAT), as described in Chapter 6, “Routing Traffic,” to provide IP addresses to devices attaching to it wirelessly or through a wired connection. The process through which a wireless client (for example, a laptop or a smart phone) attaches with a wireless router (or wireless AP) is called association. All wireless devices associating with a single AP share a collision domain. Therefore, for scalability and performance reasons, WLANs might include multiple APs.

**Wireless Access Point**

Although a wireless access point (AP) interconnects a wired LAN with a WLAN, it does not interconnect two networks (for example, the service provider’s network with an internal network). Figure 8-2 shows a typical deployment of an AP.
The AP connects to the wired LAN, and the wireless devices that connect to the wired LAN via the AP are on the same subnet as the AP (no Network Address Translation [NAT] or PAT is being performed).

**Antennas**

The coverage area of a WLAN is largely determined by the type of antenna used on a wireless AP or a wireless router. Although some lower-end, consumer-grade wireless APs have fixed antennas, higher-end, enterprise-class wireless APs often support various antenna types.

Design goals to keep in mind when selecting an antenna include the following:

- Required distance between an AP and a wireless client
- Pattern of coverage area (for example, the coverage area might radiate out in all directions, forming a spherical coverage area around an antenna, or an antenna might provide increased coverage in only one or two directions)
- Indoor or outdoor environment
- Avoiding interference with other APs

The strength of the electromagnetic waves being radiated from an antenna is referred to as *gain*, which involves a measurement of both direction and efficiency of a transmission. For example, the gain measurement for a wireless AP’s antenna transmitting a signal is a measurement of how efficiently the power being applied to the antenna is converted into electromagnetic waves being broadcast in a specific
direction. Conversely, the gain measurement for a wireless AP’s antenna receiving a signal is a measurement of how efficiently the received electromagnetic waves arriving from a specific direction are converted back into electricity leaving the antenna.

Gain is commonly measured using the $dBi$ unit of measure. In this unit of measure, the $dB$ stands for decibels and the $i$ stands for isotropic. A decibel, in this context, is a ratio of radiated power to a reference value. In the case of dBi, the reference value is the signal strength (power) radiated from an isotropic antenna, which represents a theoretical antenna that radiates an equal amount of power in all directions (in a spherical pattern). An isotropic antenna is considered to have gain of 0 dBi.

The most common formula used for antenna gain is the following:

$$G_{dBi} = 10 \log_{10} (G)$$

Based on this formula, an antenna with a peak power gain of 4 ($G$) would have a gain of 6.02 dBi. Antenna theory can become mathematical (heavily relying on the use of Maxwell’s equations). However, to put this discussion in perspective, generally speaking, if one antenna has 3 dB more gain than another antenna, it has approximately twice the effective power.

Antennas are classified not just by their gain but also by their coverage area. Two broad categories of antennas, which are based on coverage area, are as follows:

- **Omnidirectional**: An omnidirectional antenna radiates power at relatively equal power levels in all directions (somewhat similar to the theoretical isotropic antenna). Omnidirectional antennas, an example of which is depicted in Figure 8-3, are popular in residential WLANs and small office/home office (SOHO) locations.

![Figure 8-3 Omnidirectional Antenna Coverage](image)
■ **Unidirectional**: Unidirectional antennas can focus their power in a specific direction, thus avoiding potential interference with other wireless devices and perhaps reaching greater distances than those possible with omnidirectional antennas. One application for unidirectional antennas is interconnecting two nearby buildings, as shown in Figure 8-4.

![Wireless Access Point with Unidirectional Antenna](image)

**Building A**

**Building B**

**Figure 8-4** Unidirectional Antenna Coverage

Another consideration for antenna installation is the horizontal or vertical orientation of the antenna. For best performance, if two wireless APs communicate with one another, they should have matching antenna orientations, which is referred to as the **polarity** of the antenna.

### Frequencies and Channels

Later in this chapter, you are introduced to a variety of wireless standards, which are all variants of the *IEEE 802.11* standard. As you contrast one standard versus another, a characteristic to watch out for is the frequencies at which these standards operate. Although there are some country-specific variations, certain frequency ranges (or **frequency bands**) have been reserved internationally for industrial, scientific, and medical purposes. These frequency bands are called the **ISM bands**, where ISM derives from industrial, scientific, and medical.

Two of these bands are commonly used for WLANs. Specifically, WLANs can use the range of frequencies in the 2.4 GHz–2.5 GHz range (commonly referred to as the **2.4-GHz band**) or in the 5.725 GHz–5.875 GHz range (commonly referred to as the **5-GHz band**). In fact, some WLANs support a mixed environment, where 2.4 GHz devices run alongside 5-GHz devices.
Within each band are specific frequencies (or channels) at which wireless devices operate. To avoid interference, nearby wireless APs should use frequencies that do not overlap one another. Merely selecting different channels is not sufficient, however, because transmissions on one channel spill over into nearby channels.

As an example, consider the 2.4-GHz band. Here, channel frequencies are separated by 5 MHz (with the exception of channel 14, which has 12 MHz of separation from channel 13). However, a single channel’s transmission can spread over a frequency range of 22 MHz. As a result, channels must have five channels of separation (\(5 \times 5\) MHz = 25 MHz, which is greater than 22 MHz). You can see from Figure 8-5 that, in the United States, you could select nonoverlapping channels of 1, 6, and 11.

![Nonoverlapping Channels in the 2.4 GHz Band](KeyTopic)

**Figure 8-5** Nonoverlapping Channels in the 2.4 GHz Band

**NOTE** Even though some countries use channel 14 as a nonoverlapping channel, it is not supported in the United States.

As a reference, Table 8-1 shows the specific frequencies for each of the channels in the 2.4-GHz band.
Table 8-1  Channel Frequencies in the 2.4-GHz Band

<table>
<thead>
<tr>
<th>Channel</th>
<th>Frequency (GHz)</th>
<th>Recommended as a Nonoverlapping Channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2.412</td>
<td>Yes</td>
</tr>
<tr>
<td>2</td>
<td>2.417</td>
<td>No</td>
</tr>
<tr>
<td>3</td>
<td>2.422</td>
<td>No</td>
</tr>
<tr>
<td>4</td>
<td>2.427</td>
<td>No</td>
</tr>
<tr>
<td>5</td>
<td>2.432</td>
<td>No</td>
</tr>
<tr>
<td>6</td>
<td>2.437</td>
<td>Yes</td>
</tr>
<tr>
<td>7</td>
<td>2.442</td>
<td>No</td>
</tr>
<tr>
<td>8</td>
<td>2.447</td>
<td>No</td>
</tr>
<tr>
<td>9</td>
<td>2.452</td>
<td>No</td>
</tr>
<tr>
<td>10</td>
<td>2.457</td>
<td>No</td>
</tr>
<tr>
<td>11</td>
<td>2.462</td>
<td>Yes</td>
</tr>
<tr>
<td>12</td>
<td>2.467</td>
<td>No</td>
</tr>
<tr>
<td>13</td>
<td>2.472</td>
<td>No</td>
</tr>
<tr>
<td>14</td>
<td>2.484</td>
<td>Yes (not supported in the United States)</td>
</tr>
</tbody>
</table>

The 5-GHz band has a higher number of channels, as compared to the 2.4-GHz band. Table 8-2 lists the recommended nonoverlapping channels for the 5-GHz band in the United States. Note that additional channels are supported in some countries.

Table 8-2  Nonoverlapping Channels in the 5-GHz Band Recommended for Use in the United States

<table>
<thead>
<tr>
<th>Channel</th>
<th>Frequency (GHz)</th>
</tr>
</thead>
<tbody>
<tr>
<td>36</td>
<td>5.180</td>
</tr>
<tr>
<td>40</td>
<td>5.200</td>
</tr>
<tr>
<td>44</td>
<td>5.220</td>
</tr>
<tr>
<td>48</td>
<td>5.240</td>
</tr>
<tr>
<td>52</td>
<td>5.260*</td>
</tr>
<tr>
<td>56</td>
<td>5.280*</td>
</tr>
<tr>
<td>60</td>
<td>5.300*</td>
</tr>
<tr>
<td>64</td>
<td>5.320*</td>
</tr>
</tbody>
</table>
CSMA/CA

In Chapter 4, “Understanding Ethernet,” you learned about Ethernet’s carrier sense multiple access collision detection (CSMA/CD) technology. WLANs use a similar technology called carrier sense multiple access collision avoidance (CSMA/CA). Just as CSMA/CD is needed for half-duplex Ethernet connections, CSMA/CA is needed for WLAN connections, because of their half-duplex operation. Similar to how an Ethernet device listens to an Ethernet segment to determine if a frame exists on the segment, a WLAN device listens for a transmission on a wireless channel to determine if it is safe to transmit. Additionally, the collision avoidance part of the CSMA/CA algorithm causes wireless devices to wait for a random backoff time before transmitting.

Transmission Methods

In the previous discussion, you saw the frequencies used for various wireless channels. However, be aware that those frequencies are considered to be the center frequencies of a channel. In actual operation, a channel uses more than one frequency, which is a transmission method called spread spectrum. These frequencies are, however, very close to one another, which results in a narrowband transmission.

The three variations of spread-spectrum technology to be aware of for your study of WLANs include the following:
- **Direct-sequence spread spectrum (DSSS):** Modulates data over an entire range of frequencies using a series symbols called *chips*. A chip is shorter in duration than a bit, meaning that chips are transmitted at a higher rate than the actual data. These chips not only encode the data to be transmitted, but also what appears to be random data. Although both parties involved in a DSSS communication know which chips represent actual data and which chips do not, if a third party intercepted a DSSS transmission, it would be difficult for him to eavesdrop in on the data, because he would not easily know which chips represented valid bits. DSSS is more subject to environmental factors, as opposed to FHSS and OFDM, because of its use of an entire frequency spectrum.

- **Frequency-hopping spread spectrum (FHSS):** Allows the participants in a communication to hop between predetermined frequencies. Security is enhanced, because the participants can predict the next frequency to be used while a third party cannot easily predict the next frequency. FHSS can also provision extra bandwidth by simultaneously using more than one frequency.

- **Orthogonal frequency division multiplexing (OFDM):** While DSSS used a high modulation rate for the symbols it sends, OFDM uses a relatively slow modulation rate for symbols. This slower modulation rate, combined with the simultaneous transmission of data over 52 data streams, helps OFDM support high data rates while resisting interference between the various data streams.

Of these three wireless modulation techniques, only DSSS and OFDM are commonly used in today’s WLANs.

**WLAN Standards**

Most modern WLAN standards are variations of the original IEEE 802.11 standard, which was developed in 1997. This original standard supported a DSSS and a FHSS implementation, both of which operated in the 2.4-GHz band. However, with supported speeds of 1 Mbps or 2 Mbps, the original 802.11 standard lacks sufficient bandwidth to meet the needs of today’s WLANs. The most popular variants of the 802.11 standard in use today are 802.11a, 802.11b, 802.11g, and 802.11n, as described in detail in the following sections.

**802.11a**

The 802.11a WLAN standard, which was ratified in 1999, supports speeds as high as 54 Mbps. Other supported data rates (which can be used if conditions are not suitable for the 54 Mbps rate) include 6, 9, 12, 18, 24, 36, and 48 Mbps. The 802.11a standard uses the 5-GHz band and uses the OFDM transmission method.
Interestingly, 802.11a never gained widespread adoption, because it was not backwards compatible with 802.11b, while 802.11g was backwards compatible.

**802.11b**

The 802.11b WLAN standard, which was ratified in 1999, supports speeds as high as 11 Mbps. However, 5.5 Mbps is another supported data rate. The 802.11b standard uses the 2.4-GHz band and uses the DSSS transmission method.

**802.11g**

The 802.11g WLAN standard, which was ratified in 2003, supports speeds as high as 54 Mbps. Like 802.11a, other supported data rates include 6, 9, 12, 18, 24, 36, and 48 Mbps. However, like 802.11b, 802.11g operates in the 2.4-GHz band, which allows it to offer backwards compatibility to 802.11b devices. 802.11g can use either the OFDM or the DSSS transmission method.

**802.11n**

The 802.11n WLAN standard, which was ratified in 2009, supports a wide variety of speeds, depending on its implementation. Although the speed of an 802.11n network could exceed 300 Mbps (through the use of channel bonding, as discussed later), many 802.11n devices on the market have speed ratings in the 130–150 Mbps range. Interestingly, an 802.11n WLAN could operate in the 2.4 GHz band, the 5-GHz band, or both simultaneously. 802.11n uses the OFDM transmission method.

One way 802.11n achieves superior throughput is through the use of a technology called **multiple input, multiple output** (MIMO). MIMO uses multiple antennas for transmission and reception. These antennas do not interfere with one another, thanks to MIMO’s use of **spatial multiplexing**, which encodes data based on the antenna from which the data will be transmitted. Both reliability and throughput can be increased with MIMO’s simultaneous use of multiple antennas.

Yet another technology implemented by 802.11n is **channel bonding**. With channel bonding, two wireless bands can be logically bonded together, forming a band with twice the bandwidth of an individual band. Some literature refers to channel bonding as **40-MHz mode**, which refers to the bonding of two adjacent 20-MHz bands into a 40-MHz band.

Table 8-3 acts as a reference to help you contrast the characteristics of the 802.11 standards.
### Table 8-3: Characteristics of 802.11 Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Band</th>
<th>Max. Bandwidth</th>
<th>Transmission Method</th>
<th>Max. Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11</td>
<td>2.4 GHz</td>
<td>1 Mbps or 2 Mbps</td>
<td>DSSS or FHSS</td>
<td>20 m indoors/100 m outdoors</td>
</tr>
<tr>
<td>802.11a</td>
<td>5 GHz</td>
<td>54 Mbps</td>
<td>OFDM</td>
<td>35 m indoors/120 m outdoors</td>
</tr>
<tr>
<td>802.11b</td>
<td>2.4 GHz</td>
<td>11 Mbps</td>
<td>DSSS</td>
<td>32 m indoors/140 m outdoors</td>
</tr>
<tr>
<td>802.11g</td>
<td>2.4 GHz</td>
<td>54 Mbps</td>
<td>OFDM or DSSS</td>
<td>32 m indoors/140 m outdoors</td>
</tr>
<tr>
<td>802.11n</td>
<td>2.4 GHz or 5 GHz (or both)</td>
<td>&gt; 300 Mbps (with channel bonding)</td>
<td>OFDM</td>
<td>70 m indoors/250 m outdoors</td>
</tr>
</tbody>
</table>

### Deploying Wireless LANs

When designing and deploying WLANs, you have a variety of installation options and design considerations. This section delves into your available options and provides you with some best practice recommendations.

#### Types of WLANs

WLANs can be categorized based on their use of wireless APs. The three main categories are independent basic service set (IBSS), basic service set (BSS), and extended service set (ESS). An IBSS WLAN operates in an ad-hoc fashion, while BSS and ESS WLANs operate in infrastructure mode. The following sections describe the three types of WLANs in detail.
IBSS

As shown in Figure 8-6, a WLAN can be created without the use of an AP. Such a configuration, called an IBSS, is said to work in an ad-hoc fashion. An ad-hoc WLAN is useful for temporary connections between wireless devices. For example, you might temporarily interconnect two laptop computers to transfer a few files.

![Independent Basic Service Set (IBSS) WLAN](image)

Figure 8-6  Independent Basic Service Set (IBSS) WLAN

BSS

Figure 8-7 depicts a WLAN using a single AP. WLANs that have just one AP are called BSS WLANs. BSS WLANs are said to run in infrastructure mode, because wireless clients connect to an AP, which is typically connected to a wired network infrastructure. A BSS network is often used in residential and SOHO locations, where the signal strength provided by a single AP is sufficient to service all the WLAN’s wireless clients.
Figure 8-7  Basic Service Set (BSS) WLAN

ESS

Figure 8-8 illustrates a WLAN using two APs. WLANs containing more than one AP are called ESS WLANs. Like BSS WLANs, ESS WLANs operate in infrastructure mode. When you have more than one AP, take care to prevent one AP from interfering with another. Specifically, the previously discussed nonoverlapping channels (channels 1, 6, and 11 for the 2.4-GHz band) should be selected for adjacent wireless coverage areas.

Figure 8-8  Extended Service Set (ESS) WLAN
Sources of Interference

A major issue for WLANs is radio frequency interference (RFI) caused by other devices using similar frequencies to the WLAN devices. Also, physical obstacles can impede or reflect WLAN transmissions. The following are some of the most common sources of interference:

- **Other WLAN devices**: Earlier in this chapter, you read about nonoverlapping channels for both the 2.4-GHz and 5-GHz bands. However, if two or more WLAN devices are in close proximity and use overlapping channels, those devices could interfere with one another.

- **Cordless phones**: Several models of cordless phones operate in the 2.4-GHz band and can interfere with WLAN devices. However, if you need cordless phones to coexist in an environment with WLAN devices using the 2.4-GHz band, consider the use of digital enhanced cordless telecommunications (DECT) cordless phones. Although the exact frequencies used by DECT cordless phones vary based on country, DECT cordless phones do not use the 2.4-GHz band. For example, in the United States, DECT cordless phones use frequencies in the range 1.92 GHz–1.93 GHz.

- **Microwave ovens**: Older microwave ovens, which might not have sufficient shielding, can emit relatively high-powered signals in the 2.4-GHz band, resulting in significant interference with WLAN devices operating in the 2.4-GHz band.

- **Wireless security system devices**: Most wireless security cameras operate in 2.4-GHz frequency range, which can cause potential issues with WLAN devices.

- **Physical obstacles**: In electromagnetic theory, radio waves cannot propagate through a perfect conductor. So, although metal filing cabinets and large appliances are not perfect conductors, they are sufficient to cause degradation of a WLAN signal. For example, a WLAN signal might hit a large air conditioning unit, causing the radio waves to be reflected and scattered in multiple directions. Not only does this limit the range of the WLAN signal, but radio waves carrying data might travel over different paths. This multipath issue can cause data corruption.

- **Signal strength**: The range of a WLAN device is a function of the device’s signal strength. Lower-cost consumer-grade APs do not typically allow an administrative adjustment of signal strength. However, enterprise-class APs often allow signal strength to be adjusted to assure sufficient coverage of a specific area, while avoiding interference with other APs using the same channel.
As you can see from this list, most RFI occurs in the 2.4-GHz band as opposed to the 5-GHz band. Therefore, depending on the wireless clients you need to support, you might consider using the 5-GHz band, which is an option for 802.11a and 802.11n WLANs.

**Wireless AP Placement**

WLANs using more than one AP (an ESS WLAN) require careful planning to prevent the APs from interfering with one another, while still servicing a desired coverage area. Specifically, an overlap of coverage between APs should exist to allow uninterrupted roaming from one WLAN cell (which is the coverage area provided by an AP) to another. However, those overlapping coverage areas should not use overlapping frequencies.

Figure 8-9 shows how nonoverlapping channels in the 2.4-GHz band can overlap their coverage areas to provide seamless roaming between AP coverage areas. A common WLAN design recommendation is to have a 10–15 percent overlap of coverage between adjoining cells.

If a WLAN has more than three APs, the APs can be deployed in a honeycomb fashion to allow an overlap of AP coverage areas while avoiding an overlap of identical channels. The example shown in Figure 8-10 shows an approach to channel selection for adjoining cells in the 2.4-GHz band. Notice that cells using the same nonoverlapping channels (channels 1, 6, and 11) are separated by another cell. For
example, notice that none of the cells using channel 11 overlap another cell using channel 11.

![Diagram of nonoverlapping coverage cells for the 2.4-GHz Band](image)

**Figure 8-10** Nonoverlapping Coverage Cells for the 2.4-GHz Band

**NOTE** Although a honeycomb channel assignment scheme can be used for the 5-GHz band, identical channels should be separated by at least two cells, rather than the single cell shown for the 2.4 GHz band.

**Securing Wireless LANs**

WLANs introduce some unique concerns to your network. For example, improperly installed wireless APs are roughly equivalent to putting an Ethernet port in a building’s parking lot, where someone can drive up and access to your network. Fortunately, a variety of features are available to harden the security of your WLAN, as discussed in this section.

**Security Issues**

In the days when dial-up modems were popular, malicious users could run a program on their computer to call all phone numbers in a certain number range. Phone numbers that answered with modem tone became targets for later attacks. This type of reconnaissance was known as *war dialing*. A modern-day variant of war dialing is *war driving*, where potentially malicious users drive around looking for unsecured WLANs. These users might be identifying unsecured WLANs for nefarious purposes or simply looking for free Internet access.
Other WLAN security threats include the following:

- **Warchalking:** Once an open WLAN (or a WLAN whose SSID and authentication credentials are known) is found in a public place, a user might write a symbol on a wall (or some other nearby structure), to let others know the characteristics of the discovered network. This practice, which is a variant of the decades-old practice of hobos leaving symbols as messages to fellow hobos, is called *warchalking*. Figure 8-11 shows common warchalking symbols.

![Figure 8-11  Warchalking Symbols](image)

- **WEP and WPA security cracking:** As discussed later in this chapter, various security standards are available for encrypting and authenticating a WLAN client with an AP. Two of the less secure standards include *Wired Equivalent Privacy* (WEP) and *Wi-Fi Protected Access* (WPA). Although WPA is considered more secure than WEP, utilities are available on the Internet for cracking each of these approaches to wireless security. By collecting enough packets transmitted by a secure AP, these cracking utilities can use mathematical algorithms to determine the *preshared key* (PSK) configured on a wireless AP, with which an associating wireless client must also be configured.

- **Rogue access point:** A malicious user could set up his own AP to which legitimate users would connect. Such an AP is called a *rogue access point*. That malicious user could then use a *packet sniffer* (which displays information about unencrypted traffic, including the traffic’s data and header information) to eavesdrop on communications flowing through their AP. To cause unsuspecting users to connect to the rogue AP, the malicious user could configure the rogue AP with the same *service set identifier* (SSID) as used by a legitimate AP. When a rogue AP is configured with the SSID of legitimate AP, the rogue AP is commonly referred to as an *evil twin*. 
NOTE An SSID is a string of characters identifying a WLAN. APs participating in the same WLAN (in an ESS) can be configured with identical SSIDs. An SSID shared among multiple APs is called an extended service set identifier (ESSID).

Approaches to WLAN Security

A WLAN that does not require any authentication or provide any encryption for wireless devices (for example, a publicly available WLAN found in many airports) is said to be using open authentication. To protect WLAN traffic from eavesdroppers, a variety of security standards and practices have been developed, including the following:

- **MAC address filtering**: An AP can be configured with a listing of MAC addresses that are permitted to associate with the AP. If a malicious user attempts to connect via his laptop (whose MAC address is not on the list of trusted MAC addresses), that user is denied access. One drawback to MAC address filtering is the administrative overhead required to keep an approved list of MAC addresses up-to-date. Another issue with MAC address filtering is that a knowledgeable user could falsify the MAC address of his wireless network card, making his device appear to be approved.

- **Disabling SSID broadcast**: An SSID can be broadcast by an AP to let users know the name of the WLAN. For security purposes, an AP might be configured not to broadcast its SSID. However, knowledgeable users could still determine the SSID of an AP by examining captured packets.

- **Preshared key**: To encrypt transmission between a wireless client and an AP (in addition to authenticating a wireless client with an AP), both the wireless client and the AP could be preconfigured with a matching string of characters (a preshared key [PSK], as previously described). The PSK could be used as part of a mathematical algorithm to encrypt traffic, such that if an eavesdropper intercepted in the encrypted traffic, he would not be able to decrypt the traffic without knowing the PSK. Although using a PSK can be effective in providing security for a small network (for example, a SOHO network), it lacks scalability. For example, in a large corporate environment, a PSK being compromised would necessitate the reconfiguration of all devices configured with that PSK.

NOTE WLAN security based on a PSK technology is called personal mode.
IEEE 802.1X: Rather than having all devices in a WLAN be configured with the same PSK, a more scalable approach is to require all wireless users to authenticate using their own credentials (for example, a username and password). Allowing each user to have his own set of credentials prevents the compromising of one password from impacting the configuration of all wireless devices. IEEE 802.1x is a technology that allows wireless clients to authenticate with an authentication server (typically, a Remote Authentication Dial-In User Service [RADIUS] server).

**NOTE** WLAN security based on IEEE 802.1x is called enterprise mode.

Chapter 4 discussed IEEE 802.1x in detail and described the role of a supplicant, an authenticator, and an authentication server; however, Chapter 4 showed how IEEE 802.1x was used in a wired network. Figure 8-12 shows a wireless implementation of IEEE 802.1x.

**Figure 8-12** IEEE 802.1x Security for a WLAN

**NOTE** IEEE 802.1x works in conjunction with an Extensible Authentication Protocol (EAP) to perform its job of authentication. A variety of EAP types exist, including Lightweight Extensible Authentication Protocol (LEAP), EAP-Flexible Authentication via Secure Tunneling (EAP-FAST), EAP-Transport Layer Security (EAP-TLS), Protected EAP–Generic Token Card (PEAP-GTC), and Protected EAP–Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MSCHAPv2). Although these EAP types differ in their procedures, the overriding goal for each EAP type is to securely authenticate a supplicant and provide the supplicant and the authenticator a session key that can be used during a single session in the calculation of security algorithms (for example, encryption algorithms).
Security Standards

When configuring a wireless client for security, the most common security standards from which you can select are as follows:

- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access version 2 (WPA2)

The following sections describe these standards in detail.

WEP

The original 802.11 standard did address security; however, the security was a WEP key. With WEP, an AP is configured with a static WEP key. Wireless clients needing to associate with an AP are configured with an identical key (making this a PSK approach to security). The 802.11 standard specifies a 40-bit WEP key, which is considered to be a relatively weak security measure.

Because a WEP key is a static string of characters, it could be compromised with a brute-force attack, where an attacker attempts all possible character combinations until a match for the WEP key is found. Another concern, however, is that WEP uses RC4 as its encryption algorithm.

RC4 uses a 24-bit initialization vector (IV), which is a string of characters added to the transmitted data, such that the same plain text data frame will never appear as the same WEP-encrypted data frame. However, the IV is transmitted in clear text. So, if a malicious user, using packet-capture software, captures enough packets having the same WEP key, and because the malicious user can see the IV in clear text, he can use a mathematical algorithm (which can be performed with WEP-cracking software found on the Internet) to determine the static WEP key.

Some WEP implementations support the use of a longer WEP key (for example, 128 bits instead of 40 bits), making a WEP key more difficult to crack; however, both the wireless clients and their AP must support the longer WEP key.

NOTE  RC4 (which stands for Ron’s Code or Rivest Cipher, because it was developed by Ron Rivest of RSA Security) is sometimes pronounced arc 4.
WPA

The Wi-Fi Alliance (a nonprofit organization formed to certify interoperability of wireless devices) developed its own security standard, WPA, to address the weaknesses of WEP. Some of the security enhancements offered by WPA include the following:

- WPA operating in enterprise mode can require a user to be authenticated before keys are exchanged.
- In enterprise mode, the keys used between a wireless client and an access point are temporary session keys.
- WPA uses Temporal Key Integrity Protocol (TKIP) for enhanced encryption. Although TKIP does rely on an initialization vector, the IV is expanded from WEP’s 24-bit IV to a 48-bit IV. Also, broadcast key rotation can be used, which causes a key to change so quickly, an eavesdropper would not have time to exploit a derived key.
- TKIP leverages Message Integrity Check (MIC), which is sometimes referred to as Message Integrity Code (MIC). MIC can confirm that data was not modified in transit.

Although not typically written as WPA1, when you see the term WPA, consider it to be WPA version 1 (WPA1). WPA version 2, however, is written as WPA2.

WPA2

In 2004, the IEEE 802.11i standard was approved, and required stronger algorithms for encryption and integrity checking than those seen in previous WLAN security protocols such as WEP and WPA. The requirements set forth in the IEEE 802.11i standard are implemented in the Wi-Fi Alliance’s WPA version 2 (WPA2) security standard. WPA2 uses Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) for integrity checking and Advanced Encryption Standard (AES) for encryption.

Summary

The main topics covered in this chapter are the following:

- Various components, technologies, and terms used in WLANs were identified.
- WLAN design considerations were presented, such as the selection of WLAN standards, bands, and nonoverlapping channels. Potential sources of interference were also identified.
- Some of the security risks posed by a WLAN were described and the technologies available for mitigating those risks were presented.
Exam Preparation Tasks

Review All the Key Topics

Review the most important topics from inside the chapter, noted with the Key Topic icon in the outer margin of the page. Table 8-4 lists these key topics and the page numbers where each is found.

Table 8-4  Key Topics for Chapter 8

<table>
<thead>
<tr>
<th>Key Topic Element</th>
<th>Description</th>
<th>Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 8-1</td>
<td>Basic WLAN topology with a wireless router</td>
<td>259</td>
</tr>
<tr>
<td>Figure 8-2</td>
<td>Basic WLAN topology with a wireless access point</td>
<td>260</td>
</tr>
<tr>
<td>Figure 8-3</td>
<td>Omnidirectional antenna coverage</td>
<td>261</td>
</tr>
<tr>
<td>Figure 8-4</td>
<td>Unidirectional antenna coverage</td>
<td>262</td>
</tr>
<tr>
<td>Figure 8-5</td>
<td>Nonoverlapping channels in the 2.4-GHz band</td>
<td>263</td>
</tr>
<tr>
<td>List</td>
<td>Spread spectrum transmission methods</td>
<td>266</td>
</tr>
<tr>
<td>Table 8-3</td>
<td>Characteristics of 802.11 standards</td>
<td>268</td>
</tr>
<tr>
<td>Figure 8-6</td>
<td>Independent basic service set (IBSS) WLAN</td>
<td>269</td>
</tr>
<tr>
<td>Figure 8-7</td>
<td>Basic service set (IBSS) WLAN</td>
<td>270</td>
</tr>
<tr>
<td>Figure 8-8</td>
<td>Extended service set (ESS) WLAN</td>
<td>270</td>
</tr>
<tr>
<td>List</td>
<td>Sources of interference</td>
<td>271</td>
</tr>
<tr>
<td>Figure 8-9</td>
<td>10–15 percent coverage overlap in coverage areas for nonoverlapping channels</td>
<td>272</td>
</tr>
<tr>
<td>Figure 8-10</td>
<td>Nonoverlapping coverage cells for the 2.4-GHz band</td>
<td>273</td>
</tr>
<tr>
<td>List</td>
<td>Wireless security threats</td>
<td>274</td>
</tr>
<tr>
<td>List</td>
<td>Security standards and best practices</td>
<td>275</td>
</tr>
<tr>
<td>Figure 8-12</td>
<td>IEEE 802.1x security for a WLAN</td>
<td>276</td>
</tr>
</tbody>
</table>
Complete Tables and Lists from Memory

Print a copy of Appendix C, “Memory Tables” (found on the CD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix D, “Memory Table Answer Key,” also on the CD, includes the completed tables and lists so you can check your work.

Define Key Terms

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

- wireless access point (AP)
- wireless router
- decibel (dB)
- omnidirectional antenna
- unidirectional antenna
- carrier sense multiple access collision avoidance (CSMA/CA)
- direct-sequence spread spectrum (DSSS)
- frequency-hopping spread spectrum (FHSS)
- Orthogonal Frequency Division Multiplexing (OFDM)
- 802.11a
- 802.11b
- 802.11g
- 802.11n
- multiple input, multiple output (MIMO)
- channel bonding
- independent basic service set (IBSS)
- basic service set (BSS)
- extended service set (ESS)
- warchalking
- service set identifier (SSID)
- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access version 2 (WPA2)

Review Questions

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

1. What type of antenna, commonly used in wireless APs and wireless routers in SOHO locations, radiates relatively equal power in all directions?
   a. Unidirectional
   b. Yagi
   c. Parabolic
   d. Omnidirectional

2. When using the 2.4-GHz band for multiple access points in a WLAN located in the United States, which nonoverlapping channels should you select? (Choose three.)
   a. 0
   b. 1
   c. 5
   d. 6
3. What technology do WLANs use to determine when they gain access to the wireless media?
   a. SPF
   b. CSMA/CA
   c. RSTP
   d. DUAL

4. What IEEE 802.11 variant supports a maximum speed of 54 Mbps and uses the 2.4-GHz band?
   a. 802.11a
   b. 802.11b
   c. 802.11g
   d. 802.11n

5. Which of the following is used by IEEE 802.11n to achieve high throughput through the use of multiple antennas for transmission and reception?
   a. MIMO
   b. DSSS
   c. FHSS
   d. LACP

6. A WLAN formed directly between wireless clients (without the use of a wireless AP) is referred to as what type of WLAN?
   a. Enterprise mode
   b. IBSS
   c. Personal mode
   d. BSS
7. When extended the range for a 2.4-GHz WLAN, you can use nonoverlapping channels for adjacent coverage cells. However, there should be some overlap in coverage between those cells (using nonoverlapping channels) to prevent a connection from dropping as a user roams from one coverage cell to another. What percentage of coverage overlap is recommended for these adjacent cells?
   a. 5–10 percent  
   b. 10–15 percent  
   c. 15–20 percent  
   d. 20–25 percent

8. If a WLAN does not require a user to provide any credentials to associate with a wireless AP and access the WLAN, what type of authentication is said to be in use?
   a. WEP  
   b. SSID  
   c. Open  
   d. IV

9. WEP’s RC4 approach to encryption uses a 24-bit string of characters added to transmitted data, such that the same plain text data frame will never appear as the same WEP-encrypted data frame. What is this string of characters called?
   a. Initialization vector  
   b. Chips  
   c. Orthogonal descriptor  
   d. Session key

10. What standard developed by the Wi-Fi Alliance implements the requirements of IEEE 802.11i?
    a. TKIP  
    b. MIC  
    c. WEP  
    d. WPA2
This page intentionally left blank
A

A (address) record, 89
AAA (authentication, authorization, and accounting), 412
AAAA (IPv6 address) record, 89
acceptable use policy (AUP), 403
ACL (access control lists), 410-411
action plan, 442
active hubs, 74
active-active NIC redundancy, 288
active-standby NIC redundancy, 288
AD (administrative distance), 198
Adleman, Leonard M., 388
ADSL (asymmetric DSL), 234-236
AES (Advanced Encryption Standard), 387
AH (Authentication Header) protocol, 422
AM (amplitude modulation), 34
analog phone, 100
anomaly-based detection, 428
antennas
  omnidirectional, 261
  orientation of, 262
  overview, 260-261
  unidirectional, 262
anycast transmission, 181
AP (access points)
  rogue access point, 274
troubleshooting, 454
  wireless access point, 259-260
APIPA (Automatic Private IP Addressing), 151, 161-162
application layer
  OSI model, 46-47
  TCP/IP stack, 50-53
application logs (Microsoft Windows), 376
application services, 47
ARIN (American Registry for Internet Numbers), 150
arp command
  UNIX commands, 337-339
  Windows commands, 316-318
asset management, 367
assigning IP addresses, 153-162
asymmetric encryption, 388-390
asynchronous transmissions, 35, 38
ATM (Asynchronous Transfer Mode), 224, 246-248
attacks
  availability attacks
    buffer overflow, 399
    DDoS (distributed denial of service) attack, 398
    DoS (denial of service) attack, 398
    electrical disturbances, 400-401
    environmental threats, 401-402
    ICMP attacks, 399-400
attacks

overview, 397
physical environment, attacks on a system’s, 401-402
ping of death, 399
Smurf attack, 399
TCP SYN flood, 398
categories of, 391-394
confidentiality attacks
dumpster diving, 394
EMI (electromagnetic interference) interception, 394
FTP bounce, 394
overview, 391-392
packet capture, 394
ping sweep and port scan, 394
sending information over covert channels, 394
sending information over overt channels, 394
social engineering, 394
wiretapping, 394
defending against attacks
ACL (access control lists), 410-411
AUP (acceptable use policy), 403
documentation, 405-406
end user policies, 405
governing policy, 404
honey nets, 409
honey pots, 409
incident response, 406
patching, 402-403
security policies, 403-406
technical policies, 405
user training, 402
vulnerability scanners, 407-408
DoS (denial of service) attacks, 391

integrity attacks
botnet, 397
brute force, 396
data diddling, 396
dictionary attack, 397
hijacking a session, 397
keylogger, 396
overview, 393-395
packet capture, 396
password attack, 396-397
salami attack, 395
Trojan horse, 396
trust relationship exploitation, 396
virus, 396
worm, 396

AUP (acceptable use policy), 403
authentication, 372
authentication server, 130
authenticator, 130
availability attacks
buffer overflow, 399
DDoS (distributed denial of service) attack, 398
DoS (denial of service) attack, 398
electrical disturbances, 400-401
environmental threats, 401-402
ICMP attacks, 399-400
overview, 397
physical environment, attacks on a system’s, 401-402
ping of death, 399
Smurf attack, 399
TCP SYN flood, 398
bandwidth
   Ethernet network, 113-114
   physical layer (OSI Layer 1), 35
   WAN (wide-area network), 225
Base-10 numbering system, 140
baseband technologies, 35
baselining, 367
believability of a route, 198
BER (bit error rate), 358
BERT (bit-error rate tester), 358
BGP (Border Gateway Protocol), 199, 203
binary expressions, 32
binary numbering
   conversion from decimal to binary, 141-143
   conversion to decimal, 140-141
   overview, 140
   practice exercises, 143-146
binary representation, 147
bit-error rate tester, 358
blackouts, 400
BNC (Bayonet Neill-Concelman) connector, 61
bookshelf analogy for OSI model, 30-31
BOOTP (Bootstrap Protocol), 159-161
borrowed bits, 166
botnet, 397
BPDU (bridge protocol data units), 124
bridges, 75-77, 85
broadband technologies, 35
broadcast storms, 120-121
broadcast transmission, 152
brownout, 400
brute force, 396
BSS (basic service set), 269
buffer overflow, 399
buffering, 43
bus topology
   advantages of, 13
   characteristics, 13
   disadvantages of, 13
   Ethernet network using shared, 110
   overview, 11-13
butt set, 359

cable
   coaxial cable
      connectors used on, 61
      overview, 60
      RG-6 cable, 61
      RG-58 cable, 61
      RG-59 cable, 61
      types of, 61
   distribution, 70-73
   fiber-optic cable
      connectors for, 69
      multimode fiber (MMF), 67-68
      overview, 66-67
      single-mode fiber (SMF), 68-69
   troubleshooting, 444
   twisted-pair cable
      connectors for, 65
      crossover cable, 65
      fire codes and, 66
      overview, 62
shielded twisted-pair (STP) cable, 62
straight-through cable, 64-65
unshielded twisted-pair (UTP) cable, 63-64
Cat 3 cable, 64
Cat 5 cable, 64
Cat 6 cable, 64
Cat 6a cable, 64
Cat 5e cable, 64
categories of, 64
overview, 63
cable certifier, 360
cable distribution, 70-73
cable management, 368
cable modem, 236-237
cable tester, 360
calculator, subnet, 176
call agent, 100
CAN (campus-area network), 9
CARP (Common Address Redundancy Protocol), 131, 289
carrier sense, 112
carrier sense multiple access collision avoidance (CSMA/CA), 265
carrier sense multiple access collision detect (CSMA/CD), 110-113
case study: SOHO Network Design, 302-309
Cat 3 cable, 64
Cat 5 cable, 64
Cat 6 cable, 64
Cat 6a cable, 64
Cat 5e cable, 64
cellular phone technology for WAN (wide-area network), 227
Challenge-Response Authentication Mechanism Message Digest 5 (CRAM-MD5), 390
change management, 368
channel service unit/data service unit (CSU/DSU), 230
channels (wireless network), 262
CHAP (Challenge-Handshake Authentication Protocol), 231, 412
chassis, 290
CIDR (Classless Inter-Domain Routing), 177
circuit switching, 40
circuit-switched connection, 223
Cisco IOS, 372,
Class A addresses, 149-150
Class B addresses, 149-150
Class C addresses, 149-150
Class D addresses, 149-150
Class E addresses, 149-150
classes of IP addresses, 149-151
classful mask, extending, 166
client, 5
client-server network
advantages of, 21
characteristics of, 21
disadvantages of, 21
overview, 20-22
client-to-site VPN, 418-419
CM (configuration management)
asset management, 367
baselining, 367
cable management, 368
change management, 368
described, 367
network documentation, 368-369
CNAME (canonical name) record, 89
CO (central office), 242
coaxial cable
connectors used on, 61
overview, 60
RG-6 cable, 61
RG-58 cable, 61
RG-59 cable, 61
types of, 61
for WAN, 226
collision detect, 112
collision domain, 75
commands
UNIX
  arp command, 337-339
dig command, 340-341
host command, 341
ifconfig command, 341-342
netstat command, 343-345
nslookup command, 340-341
overview, 336-337
ping command, 345-346
route command, 347-348
traceroute command, 342-343
Windows
  arp command, 316-318
ipconfig command, 318-321
nbstat command, 321-324
netstat command, 324-326
nslookup command, 326-328
overview, 316
ping command, 328-330
route command, 330-334
tracert command, 334-336
Common Address Redundancy Protocol (CARP), 131, 289
companion website, downloading updates from, 472
components (network)
  client, 5
  hub, 6
  media, 6
  overview, 4-5
  router, 6
  server, 5
  switch, 6
  WAN link, 6
confidentiality
  with asymmetric encryption, 388-390
  overview, 386-387
  with symmetric encryption, 387
confidentiality attacks
dumpster diving, 394
EMI (electromagnetic interference) interception, 394
FTP bounce, 394
overview, 391-392
packet capture, 394
ping sweep and port scan, 394
sending information over covert channels, 394
sending information over overt channels, 394
social engineering, 394
wiretapping, 394
configuration (network), 294-295
configuration management. See CM (configuration management)
congestion
  avoidance, 299
  control, 41
  management, 298
connection services, 37-38, 41
connection types for WAN, 222-224
connectivity software, 360
connectors
  coaxial cable, 61
  fiber-optic cable, 69
troubleshooting, 444
twisted-pair cable, 65
contact information included in network documentation, 368
content caching, 93, 291
content engines, 93
content switching, 291
converged networks, 4
convergence (routers), 197
conversion
from binary to decimal, 140-141
from decimal to binary, 141-143
converters, 73
CRAM-MD5 (Challenge-Response Authentication Mechanism Message Digest 5), 390
crimper, 361
crossover cable, 65
crosstalk, 444
CSMA/CA (carrier sense multiple access collision avoidance), 265
CSMA/CD (carrier sense multiple access collision detect), 110-113
CSU/DSU (channel service unit/data service unit), 230
current state modulation, 33

data diddling, 396
data flows, 179-181
data formatting, 46
data link control (DLC), 36
data link layer (OSI Layer 2)
devices defined by, 39
Logical Link Control (LLC) sublayer, 37-39
Media Access Control (MAC) sublayer, 37
overview, 36-37
troubleshooting, 445-447
data rates, 225
data service unit, 32
Data-Over-Cable Service Interface Specification (DOCSIS), 237
DB-9 connector, 65
dB (decibel) loss, 444
DDNS (dynamic DNS), 90
DDoS (distributed denial of service) attack, 398
dedicated leased lines, 222, 228
default gateway
overview, 154
troubleshooting, 450
default subnet masks, 149
defending against attacks
ACL (access control lists), 410-411
AUP (acceptable use policy), 403
documentation, 405-406
der user policies, 405
governing policy, 404
honey nets, 409
honey pots, 409
incident response, 406
patching, 402-403
security policies, 403-406
technical policies, 405
user training, 402
vulnerability scanners, 407-408
delay, 292
demarc, 242
DEMILITARIZED zone firewalls, 417
DES (Data Encryption Standard), 387
design considerations, 290
designated ports, 122
detection methods, 427-428
device categories, 427
DHCP (Dynamic Host Configuration Protocol)
for IP address assignment, 160-161
overview, 53
servers, 90-92
dictionary attack, 397
DiffServ, 295
dig command, 340-341
digital subscriber lines. See DSL
directly connected routes, 193-194
distance limitations
Ethernet network, 113-114
troubleshooting, 444
distance-vector routing, 200-202
distributed denial of service (DDoS) attack, 398
DLC (data link control), 36
DNAT (dynamic NAT), 206
DNS (Domain Name System)
overview, 53, 154
record types, 89
servers, 88-90
troubleshooting, 450
DNS based Service Discovery (DNS-SD), 162
DOCSIS (Data-Over-Cable Service Interface Specification), 237
documentation
of guidelines, 405
network documentation
  contact information, 368
  network maps, 369
  policies, 369
  wiring schemes, 369
of procedures, 406
for security policies, 405-406
of standards, 405
DoD model. See TCP/IP stack
DoS (denial of service) attacks, 391, 398
dotted-decimal notation for subnetting, 163-164
drops, 292
DSL (digital subscriber lines)
  asymmetric, 234-236
  overview, 234
  symmetric, 236
  very high bit-rate, 236
DSLAM (DSL access multiplexer), 235-236
DSSS (direct-sequence spread spectrum), 266
DUAL (Diffusing-Update Algorithm), 203
dumpster diving, 394
DVD
  activating exams, 463
  contents of, 461-462
  installation of software on, 462
  video training on, 464
dynamic configuration
  (IPv4 addressing), 159-162
dynamic DNS (DDNS), 90
Dynamic Host Configuration Protocol. See DHCP
dynamic NAT (DNAT), 206
dynamic routing, 195-197

E

E1 circuits, 229
E3 circuits, 229
EAP (Extensible Authentication Protocol), 276, 412
EDNS (Extension Mechanism for DNS), 90
EIGRP (Enhanced Interior Gateway Routing Protocol), 203
electric power lines for WAN, 226
electrical disturbances, 400-401
electrical surges, 400
electrostatic discharge wrist strap, 361-362
EMI (electromagnetic interference)
  overview, 60
  troubleshooting, 394
encryption
  AES (Advanced Encryption Standard), 387
  asymmetric, 388-390
  DES (Data Encryption Standard), 387
  overview, 387
  RSA, 388
  symmetric, 387
  3DES (Triple DES), 387
end user policies, 405
enterprise mode, 276
environmental factors, 308
environmental monitor, 362
environmental threats, 401-402
ephemeral ports, 51
error control, 38
ESP (Encapsulating Security Payload) protocol, 422
ESS (extended service set), 270
Ethernet
  bandwidth capacity, 113-114,
  CSMA/CD (carrier sense multiple access collision detect), 110-113
  distance limitations, 113-114
  origins of, 108-109
  overview, 108
  speed limitations, 113-114
  types of, 114-116
Ethernet switches. See switches
Event Viewer, 376-377
Evolved High-Speed Packet Access (HSPA+), 227
exam topics, expansion of most troublesome, 472
Extensible Authentication Protocol (EAP), 276, 412
Extension Mechanism for DNS (EDNS), 90
Exterior Gateway Protocols (EGP), 199
fault-tolerant network design, 286-288
F-connector, 61
FDM (frequency-division multiplexing), 36
FHSS (frequency-hopping spread spectrum), 266
fiber-optic cable
  connectors for, 69
  multimode fiber (MMF), 67-68
  overview, 66-67
  single-mode fiber (SMF), 68-69
  WAN (wide-area network), 226
final preparation
  DVD
    activating exams, 463
    contents of, 461-462
    installation of software on, 462
    video training on, 464
  end-of-chapter review tools, 465
  memory tables, 464-465
  study and review plan, 465-466
fire codes and twisted-pair cable, 66
firewalls, 87
DEMILITARIZED zone, 417
hardware, 414
INSIDE zone, 416
inspection types, 414-415
OUTSIDE zone, 416
overview, 411
packet-filtering, 414-415
software, 414
stateful, 415
types of, 411-414
zones, 416-417
first-hop redundancy, 130-131
flow control, 37, 41-43
FM (frequency modulation), 34
FQDN (fully-qualified domain name), 88-89, 154
Frame Relay, 244-246
Free Kiwi Syslog Server, 375
frequencies, 262
frequency-division multiplexing (FDM), 36
FTP (File Transfer Protocol), 394
full-mesh WAN topology
advantages of, 19
characteristics of, 19
disadvantages of, 19
overview, 18-19

G

gas manipulation as method of attack, 401
gateway, 100
GBIC (Gigabit Interface Converter), 114
government policy, 404
guidelines, documentation of, 405

H

H.323, 45, 50
hardware firewalls, 414
hardware redundancy, 288
hashing, 390
HDLC (High-Level Data Link Control), 228
high-availability
best practices, 290
content caching, 291
content switching, 291
design considerations, 290
fault-tolerant network design, 286-288
hardware redundancy, 288
Layer 3 redundancy, 288-289
load balancing, 291
measurement, 286
overview, 286
hijacking a session, 397
HIPS (host-based intrusion prevention system), 428-429
HMAC (hash-based message authentication code), 390
honey nets, 409
honey pots, 409
host command, 341
host IP address, 148
host-based solutions, 428-429
hosts, calculating number of available, 167
HSPA+ (Evolved High-Speed Packet Access), 227
HSRP (Hot Standby Router Protocol), 131, 288-289
HTTP (Hypertext Transfer Protocol), 53,
HTTPS (Hypertext Transfer Protocol Secure), 53,
hub-and-spoke WAN topology
  advantages of, 16
  characteristics of, 16
  disadvantages of, 16
  overview, 16
hubs
  active, 74
  characteristics of, 85
  disadvantages of, 75
  overview, 6, 74
  passive, 74
  smart, 74
  types of, 74
humidity manipulation as method of attack, 401
hybrid networks, 23

ICANN (Internet Corporation for Assigned Names and Numbers), 150
ICMP (Internet Control Message Protocol), 44, 399-400
ICS (Internet connection sharing), 227
IDF (intermedia distribution frames), 71-72
IDS (intrusion detection system)
  anomaly-based detection, 428
  detection methods, 427-428
  device categories, 427
  IPS compared, 426-427
  network-based solutions, 428-429
  overview, 426
  policy-based detection, 428
  signature-based detection, 427
IEEE (Institute of Electrical and Electronics Engineers), 8
ifconfig command, 341-342
IGMPv1 (Internet Group Management Protocol version 1), 208
IGMPv2 (Internet Group Management Protocol version 2), 209
IGMPv3 (Internet Group Management Protocol version 3), 209
IGP (Interior Gateway Protocols), 199
IKE (Internet Key Exchange) modes, 420
IMAP4 (Internet Message Access Protocol version 4), 53
incident response, 406
Independent Basic Service Set (IBSS), 269
Independent Computing Architecture (ICA), 412
inside global address, 205
inside local address, 205-206
INSIDE zone firewalls, 416
Integrated Services Digital Network. See ISDN
integrity, 372
integrity attacks
botnet, 397
brute force, 396
data diddling, 396
dictionary attack, 397
hijacking a session, 397
keylogger, 396
overview, 393-395
packet capture, 396
password attack, 396-397
salami attack, 395
Trojan horse, 396
trust relationship exploitation, 396
virus, 396
worm, 396
interface diagnostics for switches, 132
interference in WAN, sources of, 271-272
intermedia distribution frames (IDF), 71-72
Intermediate System to Intermediate System (IS-IS), 203
International Organization for Standardization (ISO), 28
Internet Assigned Numbers Authority (IANA), 150
Internet connection sharing (ICS), 227
Internet Control Message Protocol (ICMP), 44
Internet Corporation for Assigned Names and Numbers (ICANN), 150
Internet layer (TCP/IP stack), 48-49
Internetwork Packet Exchange (IPX), 41
IPsec VPN (virtual private networks)

InterNIC (Internet Network Information Center), 150
intrusion detection system. See IDS (intrusion detection system)
IntServ, 295
IP address
case study: SOHO Network Design, 304-305
DHCP server, obtaining IP address information from, 91-92
new IP address range, calculating, 170-176
port numbers and, 51
troubleshooting, 450-452
IP phone, 100
IP routing table, 193
ipconfig command, 318-321
IPS (intrusion prevention system)
anomaly-based detection, 428
detection methods, 427-428
device categories, 427
host-based solutions, 428-429
IDS compared, 426-427
network-based solutions, 428-429
overview, 426
policy-based detection, 428
signature-based detection, 427
IPsec VPN (virtual private networks)
AH (Authentication Header) protocol, 422
ESP (Encapsulating Security Payload) protocol, 422
IKE (Internet Key Exchange) modes, 420
overview, 419-420
steps for setting up and tearing down, 423-424
**IPv4 addressing**

APIPA (Automatic Private IP Addressing), 161-162
assigning addresses, 153-162
binary representation, 147
BOOTP for IP address assignment, 159-161
broadcast transmission, 152
categories of, 151-153
CIDR (Classless Inter-Domain Routing), 177
Class A addresses, 149-150
Class B addresses, 149-150
Class C addresses, 149-150
Class D addresses, 149-150
Class E addresses, 149-150
classes of addresses, 149-151
components of, 154-158
default gateway, 154
default subnet masks, 149
DHCP for IP address assignment, 160-161
dynamic configuration, 159-162
host address, 148
multicast transmission, 152-153
network address, 148-149
overview, 147
private IP networks, 151
route aggregation, 177
server addresses, 154
static configuration, 154-158
structure, 147-149
subnet masks, 154
subnetting,
  borrowed bits, 166
created subnets, calculating number of, 166-167
dotted-decimal notation, 163-164
extending a classful mask, 166
hosts, calculating number of available, 167
new IP address range, calculating, 170-176
octet values, 163-165
overview, 162
practice exercises, 165-176
prefix notation, 163-164
purpose of, 162-163
subnet mask notation, 163-165
unicast transmission, 151

**IPv6 addressing**

anycast transmission, 181
data flows, 179-181
features of, 178
multicast transmission, 180-181
overview, 178
structure of, 178-179
unicast transmission, 179-180

**IPX (Internetwork Packet Exchange), 41**

**ISDN (Integrated Services Digital Network)**

BRI (basic rate interface) circuits, 243
databases, 245
overview, 243-245
PRI (primary rate interface) circuits, 243
reference points, 245
WAN (wide-area network), 243-245

**IS-IS (Intermediate System to Intermediate System), 203**

**ISO (International Organization for Standardization), 28**

isochronous transmissions, 38
Logical Link Control (LLC) sublayer

J

jitter, 292

K

Kerberos, 412
keylogger, 396

L

LACP (Link Aggregation Control Protocol), 289
LAN (local area networks)
  overview, 7
  VLAN Trunking Protocol (VTP), 118
  VLANs (virtual LANs)
    switches, 116-118
    troubleshooting, 446
  WLAN (wireless LAN)
    BSS (basic service set), 269
    channels, 262
    CSMA/CA, 265
    deploying, 268-273
    DSSS (direct-sequence spread spectrum), 266
    ESS (extended service set), 270
    FHSS (frequency-hopping spread spectrum), 266
    frequencies, 262
    IBSS (independent basic service set), 269
    interference, sources of; 271-272
    OFDM (orthogonal frequency division multiplexing), 266
    overview, 258
    security, 273-278
    standards, 266-267
  transmission methods, 265-266
  types of, 268-270
  wireless AP placement, 272-273
  latency, 454
Layer 1 (OSI). See physical layer
Layer 2 (OSI). See data link layer
Layer 2 Tunneling Protocol (L2TP), 425
Layer 3 (OSI). See network layer
Layer 4 (OSI). See transport layer
Layer 5 (OSI). See session layer
Layer 6 (OSI). See presentation layer
Layer 7 (OSI). See application layer
layers in TCP/IP stack
  application layer, 50-53
  described, 47, 50
  Internet layer, 48-49
  network interface layer, 48
  transport layer, 49-50
LC (Lucent) connector, 69
LDAP (Lightweight Directory Access Protocol), 53,
L2F (Layer 2 Forwarding Protocol), 425
LF1 (link fragmentation and interleaving), 301-302
link aggregation, 124-126
Link Aggregation Control Protocol (LACP), 289
link efficiency, 301-302
link-state routing, 202
load balancing, 291
local area network. See LAN
local loop, 242
logical addressing, 40
Logical Link Control (LLC) sublayer
  characteristics of, 37-39
connection services, 37-38
synchronizing transmissions, 38-39
logical topology
overview, 37
physical topology compared, 10-11
logs (Microsoft Windows)
application, 376
overview, 376
security, 376
system, 377
long STP, 124
loopback plug, 362
loops, routing, 200-202
LSA (link-state advertisements), 202
LTE (Long-Term Evolution), 226
L2TP (Layer 2 Tunneling Protocol), 425

M

MAC (media access control) address, 37
filtering, 275
table, corruption of, 119-120
mail exchange (MX) record, 89
maintenance tools
bit-error rate tester, 358
butt set, 359
cable certifier, 360
cable tester, 360
connectivity software, 360
crimper, 361
electrostatic discharge wrist strap, 361-362
environmental monitor, 362
loopback plug, 362
multimeter, 363-364
optical time domain reflectometer, 366
protocol analyzer, 364
punch-down tool, 365
throughput tester, 365
time domain reflectometer, 366
toner probe, 367
MAN (metropolitan-area network), 9, 225
Management Information Base (MIB), 370
maximum transmission unit (MTU)
overview, 203
troubleshooting, 450
MD5 (Message Digest 5), 390
MDF (main distribution frame), 73
MDI (media-dependent interface), 65
MDIX (media-dependent interface crossover)
mDNS (Multicast Domain Name Service), 162
media
cable distribution, 70-73
coaxial cable
connectors used on, 61
overview, 60
RG-6 cable, 61
RG-58 cable, 61
RG-59 cable, 61
types of, 61
converters, 73
fiber-optic cable
connectors for, 69
multimode fiber (MMF), 67-68
overview, 66-67
single-mode fiber (SMF), 68-69
overview, 6, 60
twisted-pair cable
connectors for, 65
crossover cable, 65
fire codes and, 66
overview, 62
shielded twisted-pair (STP) cable, 62
straight-through cable, 64-65
unshielded twisted-pair (UTP) cable, 63-64

wireless technologies, 73-74

**Media Access Control (MAC) sublayer**
characteristics of, 37
logical topology, 37
method of transmitting on the media, 37
physical addressing, 37

**media termination recommended jack (MTRJ) connector**, 69
message switching, 40
metrics, routing, 198-199

metropolitan-area network (MAN), 9, 225

MIB (Management Information Base), 370

Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP), 232, 412

Microsoft Remote Access Server (RAS), 412

Microsoft Routing and Remote Access Server (RRAS), 233-234, 412

MMF (multimode fiber), 67-68

mnemonics for memorizing layers in OSI model, 32
modem, cable, 236-237
monitoring resources and reports
Cisco IOS, 372,
logs (Microsoft Windows)
application, 376

SNMP (Simple Network Management Protocol)
agent, 370
components of, 370
described, 370
GET message, 370
manager, 370
message types, 370
MIB (Management Information Base), 370
security, 371-372
SET message, 370
SNMPv3, 371-372
trap message, 370

syslog,
components, 373-374
described, 373
severity levels, 374-375

MPLS (Multiprotocol Label Switching), 249-250

MS-CHAP (Microsoft Challenge-Handshake Authentication Protocol), 232, 412

MTRJ (media termination recommended jack) connector, 69

MTU (maximum transmission unit)
overview, 203
troubleshooting, 450

Multicast Domain Name Service (mDNS), 162

multicast routing
IGMP (Internet Group Management Protocol), 208-210
overview, 208
PIM (Protocol Independent Multicast), 210-214
  dense mode (PIM-DM), 211-213
  overview, 210
  sparse mode (PIM-SM), 213-214
multicast transmission
IPv4 addressing, 152-153
IPv6 addressing, 180-181
multifactor authentication, 412
multilayer switches, 83-85
multimeter, 363-364
multimode fiber (MMF), 67-68
multiple access, 112
multiple paths of propagation, 454
multiplexing
  frequency-division multiplexing (FDM), 36
  overview, 35
  statistical time-division multiplexing (StatTDM), 36
  time-division multiplexing (TDM), 35
MX (mail exchange) record, 89

N

NaaS (Network as a Service), 98
NAC (Network Admission Control), 130, 412
NAS (network-attached storage) device, 22
NAT (Network Address Translation), 151
  dynamic NAT (DNAT), 206
  inside global address, 205
  inside local address, 205-206
  outside global address, 205
  outside local address, 205
  overview, 204-205
  PAT (Port Address Translation), 206-208
  static NAT (SNAT), 206
native VLAN, 118
nbstat command, 321-324
NCP (Network Control Protocol), 47
Nessus, 407
NetBIOS (Network Basic Input/Output System), 45
netstat command
  UNIX commands, 343-345
  Windows commands, 324-326
network address in IPv4 addressing, 148-149
Network as a Service (NaaS), 98
Network Control Protocol (NCP), 47
network elements, 100
network infrastructure devices,
  bridges
    characteristics of, 85
    overview, 75-77
  hubs
    active, 74
    characteristics of, 85
    disadvantages of, 75
    overview, 74
    passive, 74
    smart, 74
    types of, 74
  overview, 74
  routers
    characteristics of, 85
    overview, 84-85
  switches
    characteristics of, 85
    Layer 2, 77-83
    Layer 3, 83-84
multilayer, 83-85
overview, 77-83

network interface layer (TCP/IP stack), 48

network layer (OSI Layer 3)
connection services, 41
described, 39
devices defined by, 41
logical addressing, 40
route discovery and selection, 40-41
switching, 40
troubleshooting, 447-452

network maps, 369

network sniffer, 127-128

network-based solutions, 428-429

networks
components, 5-6
components of, 4
converged, 4
documentation
contact information, 368
network maps, 369
overview, 368-369
policies, 369
wiring schemes, 369
geography used to define
CAN (campus-area network), 9
LAN, 7
MAN (metropolitan-area network), 9
overview, 7
PAN (personal-area network), 9
WAN, 8
hybrid, 23
overview, 4

purpose of, 4
resource location used to define
client-server networks, 20-22
overview, 20
peer-to-peer networks, 22-23

security goals
availability, 391
confidentiality, 386-390
integrity, 390
overview, 386
topology used to define
bus topology, 11-13
full-mesh topology, 18-19
hub-and-spoke topology, 16
overview, 9-11
partial-mesh topology, 18-20
physical topology versus logical topology, 10-11
ring topology, 12-15
star topology, 14-16

NIC (network interface cards), 287-288

NIDS (network-based intrusion detection system), 428-429

NIPS (network-based intrusion prevention system), 428-429

Nmap, 408

NNTP (Network News Transport Protocol), 53
non-designated ports, 122-124
non-root bridges, 122

nslookup command
UNIX commands, 340-341
Windows commands, 326-328

NTP (Network Time Protocol), 53
octet values, 163-165
OFDM (orthogonal frequency division multiplexing), 266
off-site options for virtual network devices, 98-99
omnidirectional antennas, 261
Open Systems Interconnection model. See OSI model
opens, 444
optical time domain reflectometer (OTDR), 366
optimizing network performance
case study: SOHO Network Design, 302-309
high-availability
best practices, 290
content caching, 291
content switching, 291
design considerations, 290
fault-tolerant network design, 286-288
hardware redundancy, 288
Layer 3 redundancy, 288-289
load balancing, 291
measurement, 286
overview, 286
QoS
best-effort, 295
categories, 295
classification, 296
configuration, 294-295
congestion avoidance, 299
congestion management, 298
DiffServ, 295
IntServ, 295
link efficiency, 301-302
marking, 297
mechanisms, 296-302
overview, 292-294
policing, 299-301
traffic shaping, 299-301
types of quality issues, 292
orientation of antennas, 262
origins of Ethernet network, 108-109
OSI model
application layer (Layer 7), 46-47
bookshelf analogy, 30-31
data link layer (Layer 2)
devices defined by, 39
Logical Link Control (LLC) sublayer, 37-39
Media Access Control (MAC) sublayer, 37
overview, 36-37
mnemonics for memorizing layers in, 32
network layer (Layer 3)
connection services, 41
described, 39
devices defined by, 41
logical addressing, 40
route discovery and selection, 40-41
switching, 40
overview, 30-32
physical layer (Layer 1)
bandwidth usage, 35
bits represented on medium, 33-34
devices defined by, 36
physical layer (OSI Layer 1)

- multiplexing strategy, 35-36
- overview, 33
- physical topology, 34
- synchronizing bits, 35
- wiring standards for connectors and jacks, 34

presentation layer (Layer 6), 45-46
session layer (Layer 5), 44-45
TCP/IP stack compared, 48-50
transport layer (Layer 4)
  - flow control, 43
  - overview, 42
  - protocols, 42

OSPF (Open Shortest Path First), 196, 202-203
OTDR (optical time domain reflectometer), 366
outside global address, 205
outside local address, 205
OUTSIDE zone firewalls, 416

P

- packet capture, 394-396
- packet reordering, 41
- packet switching, 40
- packet-filtering, 414-415
- packet-switched connection, 223
- PAN (personal-area network), 9
- PAP (Password Authentication Protocol), 231
- Pareto, Vilfredo, 220
- Pareto Principle, 220
- partial-mesh topology
  - advantages of, 20
  - characteristics of, 20
  - disadvantages of, 20
  - overview, 18-20
- passive hubs, 74
- password attack, 396-397
- PAT (Port Address Translation), 206-208
- patching, 402-403
- PBX (Private Branch Exchange), 99-100
- PDU (protocol data unit), 32
- Pearson IT Certification Practice Test engine
  - activating exams, 463
  - installation, 462
  - overview, 461
  - practice exam mode use of, 466
  - study mode use of, 466
- peer-to-peer networks
  - advantages of, 23
  - characteristics of, 23
  - disadvantages of, 23
  - overview, 22-23
- performance, optimizing. See optimizing network performance
- permanent virtual circuit (PVC), 246
- personal mode, 275
- physical addressing, 37
- physical environment, attacks on a system's, 401-402
- physical layer (OSI Layer 1)
  - bandwidth usage, 35
  - bits represented on medium, 33-34
  - devices defined by, 36
  - multiplexing strategy, 35-36
  - overview, 33
  - physical topology, 34
  - synchronizing bits, 35
  - troubleshooting, 443-445
  - wiring standards for connectors and jacks, 34
physical media for WAN (wide-area network), 225-226
physical topology
  logical topology compared, 10-11
  overview, 34
PIM (Protocol Independent Multicast), 210
PIM-DM (PIM dense mode), 211-213
PIM-SM (PIM sparse mode), 213-214
ping command
  UNIX commands, 345-346
  Windows commands, 328-330
ping of death, 399
ping sweep and port scan, 394
plenum cabling, 66
PoE (Power over Ethernet), 126-127
pointer (PTR) record, 89
poison reverse feature, 202
policies, documenting, 369
policy-based detection, 428
POP3 (Post Office Protocol version 3), 53
ports
  monitoring, 127-128
  numbers
    for common application layer protocols, 52-53
    ephemeral ports, 51
    and IP addresses, 51
    well-known ports, 51
  roles, 123
  troubleshooting, 446
  types, 122-123
POTS (Plain Old Telephone Service) connection, 241-242
power failure, 446
power fault, 400
power sag, 400
power spikes, 400
PPP (Point-to-Point Protocol), 228, 231-232, 412
PPPoE (Point-to-Point Protocol over Ethernet), 232, 412
PPTP (Point-to-Point Tunneling Protocol) VPN, 425
practice exercises
  binary number conversion to decimal number, 143-144
  binary numbering, 143-146
  decimal number conversion to binary number, 145-146
  subnet mask notation, 165
  subnetting, 165-176
  subnetting (advanced), 172-176
  prefix notation (subnetting), 163-164
Premium Edition eBook and Practice Test, 464
presentation layer (OSI Layer 6), 45-46
preshared keys (PSK), 275
Private Branch Exchange (PBX), 99
private IP networks, 151
problem, defining, 441
procedures, documentation of, 406
protocol analyzer, 364
protocol data unit (PDU), 32
proxy servers, 92-93
PSTN (Public Switched Telephone Network), 241
PTR (pointer) record, 89
punch-down tool, 365
PVC (permanent virtual circuit), 246
Q

QoS (quality of service)
- best-effort, 295
- categories, 295
- classification, 296
- configuration, 294-295
- congestion avoidance, 299
- congestion management, 298
- DiffServ, 295
- IntServ, 295
- link efficiency, 301-302
- marking, 297
- mechanisms, 296-302
- overview, 292-294
- policing, 299-301
- settings, 132
- traffic shaping, 299-301
- types of quality issues, 292

queuing, 298

R

radio frequency interference (RFI), 60, 454
radio technology for WAN, 227
RADIUS (Remote Authentication Dial-In User Service), 412
RARP (Reverse Address Resolution Protocol), 161
RAS (Microsoft Remote Access Server), 412
RC4, 277
RDP (Remote Desktop Protocol), 53, 412
RealVNC, 360
RED (random early detection), 298-299

redundancy, 290

reference models. See also OSI model; TCP/IP stack
- purpose of, 30-31

remote access security
- AAA (authentication, authorization, and accounting), 412
- CHAP (Challenge-Handshake Authentication Protocol), 412
- EAP (Extensible Authentication Protocol), 412
- ICA (Independent Computing Architecture), 412
- IEEE 8021X, 412
- Kerberos, 412
- MS-CHAP (Microsoft Challenge-Handshake Authentication Protocol), 412
- multifactor authentication, 412
- NAC (Network Admission Control), 412
- overview, 411
- PPP (Point-to-Point Protocol), 412
- PPoE (Point-to-Point Protocol over Ethernet), 412
- RADIUS (Remote Authentication Dial-In User Service), 412
- RDP (Remote Desktop Protocol), 412
- RRAS (Microsoft Routing and Remote Access Server), 233-234, 412
- SSH (Secure Shell), 412
- SSO (single sign-on), 412
- TACACS+ (Terminal Access Controller Access-Control System Plus), 412
  - two-factor authentication, 412

Remote Desktop Connection, 360
remote desktop control, 234
remote-access VPN, 418-419
report, creating post-mortem, 442
resolution, verifying problem, 442
resource location used to define networks
client-server networks, 20-22
overview, 20
peer-to-peer networks, 22-23
RFI (radio frequency interference), 60, 454
RG-6 cable, 61
RG-58 cable, 61
RG-59 cable, 61
ring topology
advantages of, 15
characteristics of, 15
disadvantages of, 15
Fiber Distributed Data Interface (FDDI), 14
overview, 12-15
RIP (Routing Information Protocol), 196, 203
Rivest, Ron, 277, 388
RJ-11 connector, 65
RJ-45 connector, 65
RJ-45 jack, 64
rogue access point, 274
root bridges, 122
root ports, 122
route aggregation, 177
route command
UNIX commands, 347-348,
Windows commands, 330-334
routed protocols and routing protocols compared, 197
routers
characteristics of, 85
overview, 6, 40-41, 84-85
wireless, 258-259
routing. See also NAT (Network Address Translation)
administrative distance (AD), 198
advertisement methods, 200-202
believability of a route, 198
BGP (Border Gateway Protocol), 199, 203
convergence, 197
directly connected routes, 193-194
distance-vector, 200-202
dynamic routes, 195-197
EGP (Exterior Gateway Protocols), 199
EIGRP (Enhanced Interior Gateway Routing Protocol), 203
IGP (Interior Gateway Protocols), 199
IP routing table, 193
IS-IS (Intermediate System to Intermediate System), 203
Layer 3 to Layer 2 mapping, 193
link-state, 202
loops, 200-202
metrics, 198-199
multicast
IGMP (Internet Group Management Protocol), 208-210
overview, 208
PIM (Protocol Independent Multicast), 210-214
OSPF (Open Shortest Path First), 196, 202-203
overview, 190-193
protocols, 197-204
RIP (Routing Information Protocol), 196, 203
routed protocols and routing protocols compared, 197
sources of routing information, 193-197
static routes, 194-195
steps for, 190-192
troubleshooting, 447-449
Routing and Remote Access Server
(Microsoft RRAS), 233-234
Routing Information Protocol (RIP), 196, 203
RP (rendezvous point), 213
RRAS (Microsoft Routing and Remote
Access Server), 233-234, 412
RSA encryption, 388
rsh (Remote Shell), 53
RSSI (Received Signal Strength
Indicator), 454
RTP (Real-time Transport Protocol), 100
RTSP (Real Time Streaming
Protocol), 53

S
SaaS (Software as a Service), 98
salami attack, 395
satellite connection for WAN, 227, 239-240
SC connector, 69
SCP (Secure Copy), 53,
SDH (Synchronous Digital Hierarchy), 238
SDSL (symmetric DSL), 236
Secure FTP (SFTP),
Secure Hash Algorithm 1 (SHA-1), 390
Secure Sockets Layer (SSL), 425
security
attack categories, 391-394
authentication, 372
availability attacks
buffer overflow, 399
DDoS (distributed denial of service) attack, 398
DoS (denial of service) attack, 398
electrical disturbances, 400-401
environmental threats, 401-402
ICMP attacks, 399-400
overview, 397
physical environment, attacks on a system's, 401-402
ping of death, 399
Smurf attack, 399
TCP SYN flood, 398
confidentiality attacks
dumpster diving, 394
EMI (electromagnetic interference) interception, 394
FTP bounce, 394
overview, 391-392
packet capture, 394
ping sweep and port scan, 394
sending information over covert channels, 394
sending information over overt channels, 394
social engineering, 394
wiretapping, 394
defending against attacks
ACL (access control lists), 410-411
AUP (acceptable use policy), 403
documentation, 405-406
defining user policies, 405
governing policy, 404
honey nets, 409
honey pots, 409
incident response, 406
patching, 402-403
security policies, 403-406
*technical policies, 405
user training, 402
vulnerability scanners, 407-408
documentation for security policies, 405-406
DoS (denial of service) attacks, 391
encryption, 372
AES (Advanced Encryption Standard), 387
asymmetric, 388-390
DES (Data Encryption Standard), 387
described, 46
overview, 387
RSA, 388
symmetric, 387
3DES (Triple DES), 387
firewalls
DEMILITARIZED zone, 417
hardware, 414
INSIDE zone, 416
inspection types, 414-415
OUTSIDE zone, 416
overview, 411
packet-filtering, 414-415
software, 414
stateful, 415
types of, 411-414
zones, 416-417
hashing, 390
HIPS (host-based intrusion prevention system), 428-429
IDS (intrusion detection system)
anomaly-based detection, 428
detection methods, 427-428
device categories, 427
IPS (intrusion prevention system)
anomaly-based detection, 428
detection methods, 427-428
device categories, 427
host-based solutions, 428-429
IDS compared, 426-427
network-based solutions, 428-429
overview, 426
policy-based detection, 428
signature-based detection, 427
integrity, 372
integrity attacks
botnet, 397
brute force, 396
data diddling, 396
dictionary attack, 397
hijacking a session, 397
keylogger, 396
overview, 393-395
packet capture, 396
password attack, 396-397
salami attack, 395
Trojan horse, 396
trust relationship exploitation, 396
virus, 396
worm, 396
IPS compared, 426-427
network-based solutions, 428-429
overview, 426
policy-based detection, 428
signature-based detection, 427
logs (Microsoft Windows), 376
network security goals
availability, 391
confidentiality, 386-390
integrity, 390
overview, 386
network sniffer, 127-128
NIDS (network-based intrusion detection system), 428-429
NIPS (network-based intrusion prevention system), 428-429
remote access security

AAA (authentication, authorization, and accounting), 412
CHAP (Challenge-Handshake Authentication Protocol), 412
EAP (Extensible Authentication Protocol), 412
ICA (Independent Computing Architecture), 412
IEEE 8021X, 412
Kerberos, 412
MS-CHAP (Microsoft Challenge-Handshake Authentication Protocol), 412
multifactor authentication, 412
NAC (Network Admission Control), 412
overview, 411
PPP (Point-to-Point Protocol), 412
PPPoE (Point-to-Point Protocol over Ethernet), 412
RADIUS (Remote Authentication Dial-In User Service), 412
RAS (Microsoft Remote Access Server), 412
RDP (Remote Desktop Protocol), 412
RRAS (Microsoft Routing and Remote Access Server), 412
SSH (Secure Shell), 412
SSO (single sign-on), 412
TACACS+ (Terminal Access Controller Access-Control System Plus), 412
two-factor authentication, 412

SNMP (Simple Network Management Protocol), 371-372
user authentication, 129-130
VPN (virtual private networks)

client-to-site, 418-419
IPSec, 419-424
L2F (Layer 2 Forwarding Protocol), 425
L2TP (Layer 2 Tunneling Protocol), 425
overview, 418-419
PPTP (Point-to-Point Tunneling Protocol), 425
remote-access, 418-419
site-to-site, 418-419
SSL (Secure Sockets Layer), 425
TLS (Transport Layer Security), 425

WLAN (wireless LAN)

enterprise mode, 276
IEEE 802.1X, 276
MAC address filtering, 275
overview, 273
personal mode, 275
preshared keys (PSK), 275
rogue access point, 274
SSID broadcast, disabling, 275
standards, 277-278
warchalking, 274
WEP, 277
WEP cracking, 274
WPA, 278
WPA2, 278
WPA cracking, 274

security policies, 403-406

Seifert, Rich, 31
server
  addresses, 154
authentication server, 130
client-server network
  advantages of, 21
  characteristics of, 21
  disadvantages of, 21
  overview, 20-22
DHCP servers, 90-92
DNS (Domain Name System) servers, 88-90
Free Kiwi Syslog Server, 375
Microsoft RRAS (Routing and Remote Access Server), 233-234
overview, 5
proxy servers, 92-93
RAS (Microsoft Remote Access Server), 412
RRAS (Microsoft Routing and Remote Access Server), 412
virtual servers, 95-96
service advertisement, 47
service discovery protocols, 162
Service Location Protocol (SLP), 162
Session Initiation Protocol (SIP), 100
session layer (OSI Layer 5), 44-45
sessions
  described, 44
  maintaining, 44
  setting up, 44
  tearing down, 45
SET message, 370
severity levels, 374-375
SFTP (Secure FTP)
SHA-1 (Secure Hash Algorithm 1), 390
Shamir, Adi, 388
shielded twisted-pair (STP) cable, 62
shorts, 444
signal strength, 454
signature-based detection, 427
Simple Service Discovery Protocol (SSDP), 162
single-mode fiber (SMF), 68-69
SIP (Session Initiation Protocol), 100
site-to-site VPN, 418-419
smart hubs, 74
smart jack, 242
SMF (single-mode fiber), 68-69
SMTP (Simple Mail Transfer Protocol), 53
Smurf attack, 399
SNMP (Simple Network Management Protocol)
  agent, 370
  components of, 370
described, 370
  GET message, 370
  manager, 370
  message types, 370
  MIB (Management Information Base), 370
  security, 371-372
  SET message, 370
  SNMPv3, 371-372
  trap message, 370
SNMPv3, 371-372
SNTP (Simple Network Time Protocol), 53
SOA (start of authority) record, 89
social engineering, 394
Software as a Service (SaaS), 98
software firewalls, 414
SONET (Synchronous Optical Network), 238-239
sources of routing information, 193-197
specialized network devices
content engines, 93
content switches, 94-95
DHCP servers, 90-92
DNS (Domain Name System) servers, 88-90
firewalls, 87
overview, 86
proxy servers, 92-93
VPN concentrators, 86-87
speed limitations for Ethernet network, 113-114
split horizon feature, 202
splitting pairs in a cable, 444
SPS (standby power supply), 401
SPT (shortest path tree), 214
SPX (Sequenced Packet Exchange), 42
SSDP (Simple Service Discovery Protocol), 162
SSH (Secure Shell), 53, 412
SSID (service set identifier), 274-275
SSID broadcast, disabling, 275
SSL (Secure Sockets Layer), 425
SSO (single sign-on), 412
ST (straight tip) connector, 69
stack, OSI. See OSI model
star topology
advantages of, 16
characteristics of, 16
disadvantages of, 16
overview, 14-16
stateful firewalls, 415
static addressing, 154-158
static NAT (SNAT), 206
static routing, 194-195
statistical time-division multiplexing
(StatTDM), 36
steganography, 394
STP (spanning tree protocol)
designated ports, 122
long STP, 124
non-designated ports, 122-124
non-root bridges, 122
overview, 119-120
port costs, 123-124
port roles, 123
port types, 122-123
root bridges, 122
root ports, 122
straight-through cable, 64-65
structured methodology for troubleshooting
create action plan, 442
define problem, 441
hypothesize probable cause, 441
implement action plan, 442
report, creating post-mortem, 442
test hypothesis, 441
verify problem resolution, 442
study and review plan, 465-466
subnet calculator, 176
subnet masks
notation, 163-165
overview, 154
troubleshooting, 450
subnetting
borrowed bits, 166
created subnets, calculating number of, 166-167
dotted-decimal notation, 163-164
extending a classful mask, 166
hosts, calculating number of available, 167
new IP address range, calculating, 170-176
octet values, 163-165
overview, 162
practice exercises, 165-176
prefix notation, 163-164
purpose of, 162-163
subnet mask notation, 163-165
supplicant, 130
SVC (switched virtual circuit), 246
switches
broadcast storms, 120-121
characteristics of, 85
features, 116-132
first-hop redundancy, 130-131
interface diagnostics, 132
Layer 2, 77-83
Layer 3, 83-84
link aggregation, 124-126
MAC address table, corruption of, 119-120
MAC filtering, 132
multilayer, 83-85
overview, 6, 77-83
PoE (Power over Ethernet), 126-127
port monitoring, 127-128
QoS (quality of service) settings, 132
STP (spanning tree protocol)
designated ports, 122
long STP, 124
non-designated ports, 122-124
non-root bridges, 122
overview, 119-120
port costs, 123-124
switching
circuit, 40
described, 40
message, 40
network layer (OSI Layer 3), 40
packet, 40
The Switch Book (Seifert), 31
symmetric DSL (SDSL), 236
symmetric encryption, 387
synchronizing bits, 35
synchronizing transmissions
asynchronous, 38
described, 38
isochronous, 38
synchronous, 35, 39
Synchronous Digital Hierarchy (SDH), 238
syslog
components, 373-374
described, 373
severity levels, 374-375
system logs (Microsoft Windows), 377
T
T1 circuits, 228-229
T3 circuits, 229
TACACS+ (Terminal Access Controller Access-Control System Plus), 412
TCP (Transmission Control Protocol), 42, 49-50
TCP SYN flood, 398
TCP/IP stack
  application layer protocols, common, 51-53
  layers in
    application layer, 50-53
    described, 47, 50
    Internet layer, 48-49
    network interface layer, 48
    transport layer, 49-50
  OSI model compared, 48-50
  overview, 47
TDM (time-division multiplexing), 35
TDR (time domain reflectometer), 366
tearing down sessions, 45
technical content, 472
technical policies, 405
telco, 242
Telecommunications Industry Association/Electronic Industries Alliance (TIA/EIA), 62
Telnet, 53,
temperature manipulation as method of attack, 401
tethering, 227
TFTP (Trivial File Transfer Protocol), 53,
throughput tester, 365
TIA/EIA-568 standard, 62
TIA/EIA-568-A standard, 62
TIA/EIA-568-B standard, 62
time domain reflectometer, 366
tip and ring, 242
TKIP (Temporal Key Integrity Protocol), 278
TLS (Transport Layer Security), 425
Token Ring networks, 110
toner probe, 367
topology used to define networks
  bus topology, 11-13
  full-mesh topology, 18-19
  hub-and-spoke topology, 16
  overview, 9-11
  partial-mesh topology, 18-20
  physical topology versus logical topology, 10-11
  ring topology, 12-15
  star topology, 14-16
traceroute command, 342-343
tracert command, 334-336
traffic filtering, 132
traffic shaping, 299-301
transition modulation, 34
Transmission Control Protocol (TCP), 42, 49-50
transmission methods for wireless networks, 265-266
transport layer (OSI Layer 4)
  flow control, 43
  overview, 42
  protocols, 42
transport layer (TCP/IP stack), 49-50
transposed Tx/Rx leads, 444
trap message, 370
Trojan horse, 396
troubleshooting
  cable, 444
  cable placement, 444
  connectors, 444
crosstalk, 444
data link layer (Layer 2), 445-447,
dB (decibel) loss, 444
default gateway, 450
distance limitations exceeded, 444
DNS configuration, 450
IP address, duplicate, 450
IP address, invalid, 451-452
Layer 2 loop, 446
module, bad, 446
MTU (maximum transmission unit),
mismatched, 450
network layer (Layer 3), 447-452
opens, 444
overview, 438-439, 452-455
physical layer (Layer 1), 443-445
port configuration, 446
power failure, 446
routing protocols, 447-449
shorts, 444
splitting pairs in a cable, 444
steps for, 439
structured methodology for
create action plan, 442
define problem, 441
hypothesize probable cause, 441
implement action plan, 442
overview, 440
report, creating post-mortem, 442
test hypothesis, 441
verify problem resolution, 442
subnet mask, 450
switches, 127-128
transposed Tx/Rx leads, 444
VLAN configuration, 446
wireless networks,
  AP placement, incorrect, 454
  latency, 454
  misconfiguration of wireless parameters, 454
  multiple paths of propagation, 454
  overview, 452-455
  RFI (radio frequency interference), 454
  signal strength, 454
trunks, 118-119
trust relationship exploitation, 396
TTL (Time-to-Live) value, 49
twisted-pair cable
  connectors for, 65
crossover cable, 65
fire codes and, 66
overview, 62
shielded twisted-pair (STP) cable, 62
straight-through cable, 64-65
unshielded twisted-pair (UTP) cable, 63-64
two-factor authentication, 412

UDP (User Datagram Protocol), 42, 50
unicast transmission
  IPv4 addressing, 151
  IPv6 addressing, 179-180
unidirectional antennas, 262
UNIX commands
  arp command, 337-339
dig command, 340-341
host command, 341
ifconfig command, 341-342
netstat command, 343-345
nslookup command, 340-341
overview, 336-337
ping command, 345-346
route command, 347-348
traceroute command, 342-343

**UPS (uninterruptable power supply), 401**

uptime, 286

**user authentication**

authentication server, 130
authenticator, 130
overview, 129-130
supplicant, 130
switches, 129-130

**user training, 402**

**UTP (unshielded twisted-pair) cable, 63-64, 226**

Cat 3 cable, 64
Cat 5 cable, 64
Cat 6 cable, 64
Cat 6a cable, 64
Cat 5e cable, 64
categories of, 64

**V**

**VDSL (very high bit-rate DSL), 236**

vendor codes, 37

**virtual desktops, 97**

**virtual network devices, 95-99**

**virtual PBX, 99-100**

**virtual servers, 95-96**

**virtual switches, 96-97**

**virus, 396**

**VLAN Trunking Protocol (VTP), 118**

**VLANs (virtual LANs)**

switches, 116-118
troubleshooting, 446

**Voice over IP (VoIP)**

analog phone, 100
call agent, 100
gateway, 100
IP phone, 100
network elements, 100
overview, 99-100
PBX (Private Branch Exchange), 100
RTP (Real-time Transport Protocol), 100
SIP (Session Initiation Protocol), 100

**VoIP network elements,**

**VPN (virtual private networks),**

client-to-site, 418-419
described, 86
IPsec, 419-424

\[AH (Authentication Header) protocol, 422\]

\[ESP (Encapsulating Security Payload) protocol, 422\]

\[IKE (Internet Key Exchange) modes, 420\]

overview, 419-420

steps for setting up and tearing down, 423-424

L2F (Layer 2 Forwarding Protocol), 425

L2TP (Layer 2 Tunneling Protocol), 425

overview, 418-419

PPTP (Point-to-Point Tunneling Protocol), 425

remote-access, 418-419

site-to-site, 418-419

SSL (Secure Sockets Layer), 425

TLS (Transport Layer Security), 425

**VPN concentrators, 86-87**
VTP (VLAN Trunking Protocol), 118
vulnerability scanners, 407-408

W–X

WAN (wide-area network),
ATM (Asynchronous Transfer Mode), 224, 246-248
bandwidths for, 225
cable modem, 236-237
cellular phone technology for, 227
circuit-switched connection, 223
coaxial cable for, 226
connection types, 222-224
CSU/DSU, 230
data rates, 225
dedicated leased lines, 222, 228
described, 220
DSL (digital subscriber lines)
  asymmetric, 234-236
  overview, 234
  symmetric, 236
  very high bit-rate, 236
E1 circuits for, 229
E3 circuits for, 229
electric power lines for, 226
fiber-optic cable for, 226
Frame Relay, 244-246
HSPA+ technology for, 227
ISDN (Integrated Services Digital
  Network), 243-245
media types, 225-227
Microsoft RRAS (Routing and Remote
  Access Server), 233-234
MPLS (Multiprotocol Label
  Switching), 249-250
overview, 8
packet-switched connection, 223
physical media for, 225-226
POTS (Plain Old Telephone Service)
  connection, 241-242
PPP (Point-to-Point Protocol), 231-232
PPPoE (Point-to-Point Protocol over Ethernet), 232
radio technology for, 227
satellite connection, 227, 239-240
SONET networks, 238-239
T1 circuits for, 228-229
T3 circuits for, 229
UTP (unshielded twisted pair) cabling
  for, 226
WiMAX technology for, 227
wireless media for, 226-227
warchalking, 274
well-known ports, 51
WEP (Wired Equivalent Privacy), 274, 277
WiMAX (Worldwide Interoperability
  for Microwave Access), 227
windowing, 43
Windows commands
  arp command, 316-318
  ipconfig command, 318-321
  nbstat command, 321-324
  netstat command, 324-326
  nslookup command, 326-328
  overview, 316
  ping command, 328-330
  route command, 330-334
  tracert command, 334-336
wireless access point, 259-260. See also antennas
wireless AP placement, 272-273
wireless design (case study: SOHO Network Design), 307-308
wireless media for WAN (wide-area network), 226-227
wireless networks
  BSS (basic service set), 269
  channels, 262
  CSMA/CA, 265
  deploying, 268-273
  DSSS (direct-sequence spread spectrum), 266
  ESS (extended service set), 270
  FHSS (frequency-hopping spread spectrum), 266
  frequencies, 262
  IBSS (independent basic service set), 269
  interference, sources of, 271-272
  OFDM (orthogonal frequency division multiplexing), 266
  overview, 258
  security
    enterprise mode, 276
    IEEE 802.1X, 276
    MAC address filtering, 275
    overview, 273
    personal mode, 275
    preshared keys (PSK), 275
    rogue access point, 274
    SSID broadcast, disabling, 275
    standards, 277-278
    warclicking, 274
    WEP, 274, 277
    WPA, 274, 278
    WPA2, 278
  standards, 266-267
  transmission methods, 265-266
troubleshooting,
  AP placement, incorrect, 454
  latency, 454
  misconfiguration of wireless parameters, 454
  multiple paths of propagation, 454
  overview, 452-455
  RFI (radio frequency interference), 454
  signal strength, 454
  types of, 268-270
  wireless AP placement, 272-273
wireless routers, 258-259. See also antennas
wireless technologies, 73-74
Wireshark, 127, 364
wiretapping, 394
wiring schemes, documenting, 369
wiring standards for connectors and jacks, 34
WLAN. See wireless networks
worm, 396
WPA (Wi-Fi Protected Access), 274, 278

Z

Zero Configuration (Zeroconf), 162