CompTIA® Network+
N10-006 Cert Guide

Keith Barker, CCIE No. 6783
Kevin Wallace, CCIE No. 7945
Contents at a Glance

Introduction xxv

CHAPTER 1 Computer Network Fundamentals 2
CHAPTER 2 The OSI Reference Model 28
CHAPTER 3 Network Components 60
CHAPTER 4 Ethernet Technology 112
CHAPTER 5 IPv4 and IPv6 Addresses 148
CHAPTER 6 Routing IP Packets 198
CHAPTER 7 Wide-Area Networks 230
CHAPTER 8 Wireless LANs 266
CHAPTER 9 Network Optimization 296
CHAPTER 10 Command-Line Tools 326
CHAPTER 11 Network Management 366
CHAPTER 12 Network Security 396
CHAPTER 13 Network Troubleshooting 450
CHAPTER 14 Final Preparation 476
APPENDIX A Answers to Review Questions 486
APPENDIX B Network+ N10-006 Exam Updates 490
APPENDIX C Exam Essentials 494
Glossary 506
Index 533

ON THE DVD:
APPENDIX D Memory Tables
APPENDIX E Memory Table Answer Key
APPENDIX F Study Planner
Table of Contents

Introduction  xxv

Chapter 1  Computer Network Fundamentals  2
  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  8
    CAN  8
    MAN  8
    PAN  9
  Networks Defined by Topology  9
    Physical Versus Logical Topology  9
    Bus Topology  11
    Ring Topology  13
    Star Topology  14
    Hub-and-Spoke Topology  15
    Full-Mesh Topology  17
    Partial-Mesh Topology  18
  Networks Defined by Resource Location  19
    Client/Server Networks  19
    Peer-to-Peer Networks  21
  Real-World Case Study  22
  Summary  23
  Exam Preparation Tasks  23
  Review Questions  25

Chapter 2  The OSI Reference Model  28
  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  37
Specialized Network Devices 90
  VPN Concentrators 90
  Firewalls 91
  DNS Servers 92
  DHCP Servers 94
  Proxy Servers 96
  Content Engines 97
  Content Switches 98

Virtual Network Devices 99
  Virtual Servers 99
  Virtual Routers and Firewalls 100
  Virtual Switches 101
  Virtual Desktops 102
  Other Virtualization Solutions 102
  Cloud Computing 103
  Software-Defined Networking 104

Voice over IP Protocols and Components 104
Real-World Case Study 105
Summary 106
Exam Preparation Tasks 107
Review Questions 109

Chapter 4  Ethernet Technology 112
Foundation Topics 114
  Principles of Ethernet 114
    Ethernet Origins 114
    Carrier Sense Multiple Access Collision Detect 116
    Distance and Speed Limitations 120
  Ethernet Switch Features 122
    Virtual LANs 122
    Switch Configuration for an Access Port 124
    Trunks 125
    Switch Configuration for a Trunk Port 127
    Spanning Tree Protocol 127
    Corruption of a Switch's MAC Address Table 128
    Broadcast Storms 129
    STP Operation 130
Chapter 5  IPv4 and IPv6 Addresses  148

Foundation Topics  150

Binary Numbering  150

Principles of Binary Numbering  150
Converting a Binary Number to a Decimal Number  151
Converting a Decimal Number to a Binary Number  151
Binary Numbering Practice  153
Binary Conversion Exercise 1  153
Binary Conversion Exercise 1: Solution  154
Binary Conversion Exercise 2  154
Binary Conversion Exercise 2: Solution  154
Binary Conversion Exercise 3  154
Binary Conversion Exercise 3: Solution  155
Binary Conversion Exercise 4  155
Binary Conversion Exercise 4: Solution  156

IPv4 Addressing  157

IPv4 Address Structure  157
Classes of Addresses  159
Types of Addresses  161
Unicast  161
Broadcast  161
Multicast  162
Assigning IPv4 Addresses 163
   IP Addressing Components 163
   Static Configuration 164
   Dynamic Configuration 169
   BOOTP 169
   DHCP 169
   Automatic Private IP Addressing 171

Subnetting 172
   Purpose of Subnetting 172
   Subnet Mask Notation 173
   Subnet Notation: Practice Exercise 1 174
   Subnet Notation: Practice Exercise 1 Solution 174
   Subnet Notation: Practice Exercise 2 175
   Subnet Notation: Practice Exercise 2 Solution 175
   Extending a Classful Mask 175
   Borrowed Bits 175
   Calculating the Number of Created Subnets 176
   Calculating the Number of Available Hosts 176
   Basic Subnetting Practice: Exercise 1 177
   Basic Subnetting Practice: Exercise 1 Solution 177
   Basic Subnetting Practice: Exercise 2 178
   Basic Subnetting Practice: Exercise 2 Solution 178
   Calculating New IP Address Ranges 179
   Advanced Subnetting Practice: Exercise 1 182
   Advanced Subnetting Practice: Exercise 1 Solution 182
   Advanced Subnetting Practice: Exercise 2 183
   Advanced Subnetting Practice: Exercise 2 Solution 184
   Additional Practice 185
   Classless Interdomain Routing 186

IP Version 6 187
   Need for IPv6 187
   IPv6 Address Structure 188
   IPv6 Address Types 189
   IPv6 Data Flows 189
   Unicast 189
   Multicast 190
   Anycast 191
Chapter 6  Routing IP Packets  198
Foundation Topics  200
Basic Routing Processes  200
Sources of Routing Information  203
Directly Connected Routes  203
Static Routes  204
Dynamic Routing Protocols  205
Routing Protocol Characteristics  207
Believability of a Route  208
Metrics  208
Interior Versus Exterior Gateway Protocols  209
Route Advertisement Method  210
Distance Vector  210
Link State  212
Routing Protocol Examples  212
Address Translation  214
NAT  214
PAT  217
Multicast Routing  218
IGMP  218
PIM  220
PIM-DM  221
PIM-SM  223
Real-World Case Study  224
Summary  225
Exam Preparation Tasks  226
Review Questions  227

Chapter 7  Wide-Area Networks  230
Foundation Topics  232
WAN Properties  232
WAN Connection Types  232
WAN Data Rates  234
WAN Media Types 235
Physical Media 235
Wireless Media 236
WAN Technologies 237
Dedicated Leased Line 237
T1 238
E1 239
T3 239
E3 239
CSU/DSU 239
Metro Ethernet 240
Point-to-Point Protocol 241
Point-to-Point Protocol over Ethernet 242
Microsoft RRAS 243
Digital Subscriber Line 244
Cable Modem 246
Synchronous Optical Network 247
Satellite 249
Plain Old Telephone Service 251
Integrated Services Digital Network 253
Frame Relay 255
Asynchronous Transfer Mode 256
Multiprotocol Label Switching 259
Overlay Networks 260
Real-World Case Study 261
Summary 261
Exam Preparation Tasks 262
Review Questions 263

Chapter 8 Wireless LANs 266
Foundation Topics 268
Introducing Wireless LANs 268
WLAN Concepts and Components 268
Wireless Routers 268
Wireless Access Point 269
Antennas 270
Frequencies and Channels 273
Contents

CSMA/CA 275
Transmission Methods 276
WLAN Standards 277
802.11a 277
802.11b 277
802.11g 277
802.11n 277
802.11ac 278
802.11x Standard Summary 278
Deploying Wireless LANs 279
Types of WLANs 279
IBSS 279
BSS 280
ESS 280
Mesh Topology 281
Sources of Interference 281
Wireless AP Placement 283
Securing Wireless LANs 284
Security Issues 284
Approaches to WLAN Security 286
Security Standards 288
WEP 288
WPA 289
WPA2 289
Additional Wireless Options 290
Real-World Case Study 290
Summary 291
Exam Preparation Tasks 291
Review Questions 293

Chapter 9 Network Optimization 296
Foundation Topics 298
High Availability 298
High-Availability Measurement 298
Fault-Tolerant Network Design 298
Hardware Redundancy 300
Layer 3 Redundancy 300
Design Considerations for High-Availability Networks 301
High-Availability Best Practices 302
Content Caching 302
Load Balancing 303
QoS Technologies 304
  Introduction to QoS 304
  QoS Configuration Steps 305
  QoS Components 306
  QoS Mechanisms 307
Classification 308
Marking 308
Congestion Management 309
Congestion Avoidance 309
Policing and Shaping 310
Link Efficiency 312
Case Study: SOHO Network Design 313
  Case Study Scenario 313
  Suggested Solution 315
IP Addressing 315
Layer 1 Media 317
Layer 2 Devices 317
Layer 3 Devices 318
Wireless Design 318
Environmental Factors 319
Cost Savings Versus Performance 320
Topology 320
Real-World Case Study 320
Summary 321
Exam Preparation Tasks 322
Review Questions 323
Chapter 10 Command-Line Tools 326
  Foundation Topics 328
  Windows Commands 328
    arp 328
    ipconfig 330
    nbtstat 333
Looking-Glass Sites 375
Speed Test Sites 376
Punch-Down Tool 376
Throughput Tester 376
Time Domain Reflectometer/Optical Time Domain Reflectometer 377
Toner Probe 378
Configuration Management 378
Monitoring Resources and Reports 381
  SNMP 381
  Syslog 385
  Logs 387
  Application Logs 388
  Security Logs 388
  System Logs 389
Real-World Case Study 389
Summary 390
Exam Preparation Tasks 391
Review Questions 392

Chapter 12 Network Security 396
Foundation Topics 398
  Security Fundamentals 398
    Network Security Goals 398
    Confidentiality 398
    Symmetric Encryption 399
    Asymmetric Encryption 400
    Integrity 402
    Availability 403
  Categories of Network Attacks 403
    Confidentiality Attacks 403
    Integrity Attacks 407
    Availability Attacks 409
    Denial of Service 410
    Distributed Denial of Service 410
    TCP SYN Flood 410
    Buffer Overflow 411
    ICMP Attacks 411
Electrical Disturbances 412

Attacks on a System's Physical Environment 413

Physical Controls 414

Defending Against Attacks 414

User Training 414

Patching 415

Security Policies 416

Governing Policy 417

Technical Policies 418

End-User Policies 418

More Detailed Documents 418

Incident Response 419

Vulnerability Scanners 420

Nessus 420

Nmap 421

Honey Pots and Honey Nets 422

Access Control Lists 423

Remote-Access Security 424

Firewalls 426

Firewall Types 426

Firewall Inspection Types 427

Packet-Filtering Firewall 427

Stateful Firewall 428

Firewall Zones 429

Unified Threat Management Firewalls 430

Virtual Private Networks 431

Overview of IPsec with IKEv1 433

IKE Modes and Phases 433

Authentication Header and Encapsulating Security Payload 435

The Five Steps in Setting Up and Tearing Down an IPsec Site-to-Site VPN Using IKEv1 437

Other VPN Technologies 438

Intrusion Detection and Prevention 439

IDS Versus IPS 439

IDS and IPS Device Categories 440
Detection Methods 440
Signature-Based Detection 440
Policy-Based Detection 441
Anomaly-Based Detection 441
Deploying Network-Based and Host-Based Solutions 442
Real-World Case Study 443
Summary 444
Exam Preparation Tasks 445
Review Questions 447

Chapter 13 Network Troubleshooting 450
Foundation Topics 452
Troubleshooting Basics 452
Troubleshooting Fundamentals 454
Structured Troubleshooting Methodology 454
Physical Layer Troubleshooting 457
Physical Layer Troubleshooting: Scenario 458
Physical Layer Troubleshooting: Solution 459
Data Link Layer Troubleshooting 460
Data Link Layer Troubleshooting: Scenario 461
Data Link Layer Troubleshooting: Solution 461
Network Layer Troubleshooting 462
Layer 3 Data Structures 462
Common Layer 3 Troubleshooting Issues 464
Network Layer Troubleshooting: Scenario 465
Network Layer Troubleshooting: Solution 466
Wireless Troubleshooting 467
Wireless Network Troubleshooting: Scenario 469
Wireless Network Troubleshooting: Solution 469
Specialized Networks 470
Real-World Case Study 470
Summary 471
Exam Preparation Tasks 472
Review Questions 473
Chapter 14  Final Preparation  476

Tools for Final Preparation  477
   Pearson Cert Practice Test Engine and Questions on the DVD  477
   Install the Software from the DVD  478
   Activate and Download the Practice Exam  479
   Activating Other Exams  480
   Premium Edition  480
   Video Training on DVD  480
   Memory Tables  481
   Simulations and Performance-Based Exercises  481
   End-of-Chapter Review Tools  481
   Suggested Plan for Final Review and Study  481
   Strategies for Taking the Exam  483
   Summary  484

APPENDIX A  Answers to Review Questions  486
APPENDIX B  Network+ N10-006 Exam Updates  490
APPENDIX C  Exam Essentials  494
   Glossary  506
   Index  533

ON THE DVD:
APPENDIX D  Memory Tables
APPENDIX E  Memory Table Answer Key
APPENDIX F  Study Planner
About the Authors

**Keith Barker**, CCIE No. 6783, has been working in the information technology (IT) industry since 1985. He currently enjoys creating effective and entertaining video training for CBT Nuggets. He has certified with VMware, Cisco, Juniper, HP, Check Point, Palo Alto, (ISC)², and many others. Keith loves to teach. You can follow Keith online through the following:

Twitter: @KeithBarkerCCIE  
Facebook: Keith Barker Networking  
YouTube: http://youtube.com/Keith6783  
Web page: http://cbtnuggets.com

**Kevin Wallace**, CCIE No. 7945 (R/S and Collaboration), is a Certified Cisco Systems Instructor (CCSI No. 20061) with multiple Cisco professional and associate-level certifications in the R/S, Collaboration, Security, Design, and Data Center tracks. With networking experience dating back to 1989, Kevin has been a network design specialist for the Walt Disney World Resort, an instructor of Cisco courses for Skillsoft, and a network manager for Eastern Kentucky University.

Currently, Kevin owns and operates Kevin Wallace Training, LLC, where he primarily produces video courses and writes books for Cisco Press/Pearson IT Certification (http://kwtrain.com/books).

Kevin holds a bachelor of science degree in electrical engineering from the University of Kentucky, and he lives in central Kentucky with his wife (Vivian) and two daughters (Stacie and Sabrina).

Kevin can be followed on these social media platforms:

Blog: http://kwtrain.com  
Twitter: http://twitter.com/kwallaceccie  
Facebook: http://facebook.com/kwallaceccie  
YouTube: http://youtube.com/kwallaceccie  
LinkedIn: http://linkedin.com/in/kwallaceccie  
Google+: http://google.com/+KevinWallace
Dedication

**Keith:** This book is dedicated to individuals from all backgrounds and experiences who are taking deliberate steps to improve their knowledge, life, and community. May you have measureable success in your journey!

**Kevin:** My contributions to this book are dedicated to you, the reader. The CompTIA Network+ certification can be your first step in a long and rewarding career in networking. May the concepts in this book fuel your passion for continuous learning.
Acknowledgments

Keith Barker:
All the professionals at Pearson IT Certification have been fantastic to work with, including Brett Bartow and Christopher (Chris) Cleveland. Many thanks to all of Pearson IT.

CBT Nuggets has been very supportive of me in all my endeavors. I am grateful on a daily basis for the amazing opportunity that Dan Charbonneau and the CBT Nuggets team represents for both me and the learners around the globe who enjoy CBT Nuggets videos.

Thanks to longtime friend Kevin Wallace for allowing me to work with him on this latest version of book, and for Anthony and Michelle for their sweet tech edits.

Kevin Wallace:
A huge “thank you” goes out to my good friend Keith Barker for taking the lead on this book. Your insight into these technologies is profound, and your enthusiasm is contagious.

Also, I am grateful to work with the team of professionals at Pearson IT Certification. You are all a class act.

As always, I’m thankful to God and His many blessings, not the least of which is my family (my wife, Vivian, and daughters, Sabrina and Stacie).
About the Technical Editors

Michelle Plumb is a full-time Cisco Certified Systems Instructor (CCSI). She has 26-plus years of experience in the field as an IT professional and telecommunications specialist. She maintains a high level of Cisco, Microsoft, and CompTIA certifications, including CCNP Voice, MCSE, CompTIA A+, Network+, Project+, and iNet+. Michelle has been a technical reviewer for numerous books related to the Cisco CCNP Route and Switch, CCNP Voice, and CompTIA course materials. Her main passion is helping others learn these new and exciting technologies. She lives in Phoenix, Arizona, with her husband and two dogs.

Anthony Sequeira, CCIE No. 15626, is a seasoned trainer and author on all levels and tracks of Cisco certification. Anthony formally began his career in the IT industry in 1994 with IBM in Tampa, Florida. He quickly formed his own computer consultancy, Computer Solutions, and then discovered his true passion: teaching and writing about Microsoft and Cisco technologies.

Anthony joined Mastering Computers in 1996 and lectured to massive audiences around the world about the latest in computer technologies. Mastering Computers became the revolutionary online training company KnowledgeNet, and Anthony trained there for many years.

Anthony is currently pursuing his second CCIE in the area of security and then his third Cisco Data Center. When he’s not writing for Cisco Press, Anthony is a full-time instructor at CBT Nuggets.
We Want to Hear from You!

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

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

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

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

Email: feedback@pearsonitcertification.com
Mail: Pearson IT Certification
      ATTN: Reader Feedback
      800 East 96th Street
      Indianapolis, IN 46240 USA

Reader Services

Visit our website and register this book at http://www.pearsonitcertification.com/title/9780789754080 for convenient access to any updates, downloads, or errata that might be available for this book.
Becoming a CompTIA Certified IT Professional is Easy

It’s also the best way to reach greater professional opportunities and rewards.

Why Get CompTIA Certified?

Growing Demand
Labor estimates predict some technology fields will experience growth of over 20% by the year 2020. CompTIA certification qualifies the skills required to join this workforce.

Higher Salaries
IT professionals with certifications on their resume command better jobs, earn higher salaries and have more doors open to new multi-industry opportunities.

Verified Strengths
93% of hiring managers indicate CompTIA certifications are valuable in validating IT expertise, making certification the best way to demonstrate your competency and knowledge to employers.**

Universal Skills
CompTIA certifications are vendor neutral—which means that certified professionals can proficiently work with an extensive variety of hardware and software found in most organizations.

Learn more about what the exam covers by reviewing the following:

- Exam objectives for key study points
- Sample questions for a general overview of what to expect on the exam and examples of question format.
- Visit online forums, like LinkedIn, to see what other IT professionals say about CompTIA exams.

Learn more: Certification.CompTIA.org/networkplus

* Source: CompTIA Annual Information Security Trends study; Info IT end users: Executives Responsible for Security
** Source: 2017 IT Skills and Salary Report by CompTIA Authorized Partner

Pearson VUE Location

Purchase a voucher at a Pearson VUE testing center or at CompTIAstore.com.

- Register for your exam at a Pearson VUE testing center.
- Visit pearsonvue.com/CompTIA to find the closest testing center to you.
- Schedule the exam online. You will be required to enter your voucher number or provide payment information at registration.
- Take your certification exam.

Congratulations on your CompTIA certification!

- Make sure to add your certification to your resume.
- Check out the CompTIA Certification Roadmap to plan your next career move.
CompTIA Network+

The CompTIA Network+ (N10-006) certification exam will test to determine that the successful candidate has the knowledge and skills required to configure, manage and troubleshoot a network that uses Internet Protocol (IP).

It Pays to Get Certified

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

- **The CompTIA Network+ credential**: Proves knowledge of networking features and functions and is the leading vendor-neutral certification for networking professionals.
- **Career pathway**: CompTIA Network+ is the first step in starting a networking career. Hundreds of thousands of 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

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>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>
Steps to Getting Certified and Staying Certified

<table>
<thead>
<tr>
<th>Purchase an exam voucher</th>
<th>Purchase your exam voucher on the CompTIA Marketplace, which is located at <a href="http://www.comptiastore.com/">http://www.comptiastore.com/</a>.</th>
</tr>
</thead>
<tbody>
<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 <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>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/stayCertified.aspx">http://certification.comptia.org/stayCertified.aspx</a>.</td>
</tr>
<tr>
<td>Continuing education</td>
<td></td>
</tr>
</tbody>
</table>

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.

How to Obtain More Information from CompTIA

- **Visit CompTIA online**: Visit http://www.comptia.org to learn more about getting CompTIA certified.

- **Contact CompTIA**: Call 866-835-8020.
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.

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

Goals and Methods

The goal of this book is to assist you in learning and understanding the technologies covered in the Network+ N10-006 blueprint from CompTIA. This also allows you to demonstrate that knowledge by passing the N10-006 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 N10-006 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:** You can find these on the DVD within Appendixes D and E. 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. On the DVD, you will find a flash card application with all the glossary terms separated by chapter, so feel free to use that to study key terms as well.
Exercises: This book comes with 40 performance-based practice exercises that are designed to help you prepare for the hands-on portion of the Network+ exam. These exercises are available on the DVD. Make sure you do the exercises as you complete each chapter and again when you have completed the book and are doing your final preparation.

Hands-on Labs: These include matching, drag and drop, and simulations. These hands-on exercises are an important part of this book. In addition to reading this book, you should go through all the exercises included with the book. These interactive hands-on exercises provide examples, additional information, and insight about a vendor’s implementation of the technologies. To perform the labs, simply install the CompTIA Network+ N10-006 Hands-on Lab Simulator Lite software from the DVD.

Practice Exams: This book comes complete with several full length practice exams available to you in the Pearson IT Certification Practice Test software on the DVD. Be sure to run through the questions in Exam Bank 1 as you complete each chapter in study mode. When you have completed the book, take a full practice test using Exam Bank 2-4 questions in practice exam mode to test your exam readiness.

Exam Essentials: This book includes an Exam Essentials appendix that summarizes the key points from every chapter. This review tool is available in both print and an interactive PDF on the DVD. Review these essential exam facts after each chapter and again when you have completed the book. This makes a great review summary that you can mark up as you review and master each concept.

For current information about the CompTIA Network+ certification exam, visit http://certification.comptia.org/getCertified/certifications/network.aspx.

Who Should Read This Book?

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 is also for 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

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

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

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

Download the current exam objectives by submitting a form on the following webpage: http://certification.comptia.org/training/testingcenters/examobjectives.aspx.

Use the practice exam, which is included on this book’s DVD. As you work through the practice exam, use the practice test software reporting features to note the areas where you lack confidence and review those concepts. 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 (N10-006). The following website provides information about registering for the exam: http://certification.comptia.org/training/testingcenters.aspx.

CompTIA Network+ Exam Topics

Table I-1 lists general exam topics (objectives) and specific topics under each general topic (subobjectives) for the CompTIA Network+ N10-006 exam. This table lists the primary chapter in which each exam topic is covered. Note that many objectives and subobjectives are interrelated and are addressed in multiple chapters within the book itself.
<table>
<thead>
<tr>
<th>Chapter</th>
<th>N10-006 Exam Objective</th>
<th>N10-006 Exam Subobjective</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.0 Network architecture</td>
<td>1.1 Explain the functions and applications of various network devices</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.6 Differentiate between common network topologies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.7 Differentiate between network infrastructure implementations</td>
</tr>
<tr>
<td>2</td>
<td>5.0 Industry standards, practices, and network theory</td>
<td>5.1 Analyze a scenario and determine the corresponding OSI layer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.2 Explain the basics of network theory and concepts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.9 Compare and contrast ports and protocols</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.10 Given a scenario, configure and apply the appropriate ports and protocols</td>
</tr>
<tr>
<td>3</td>
<td>1.0 Network architecture</td>
<td>1.3 Install and configure networking services/applications</td>
</tr>
<tr>
<td></td>
<td>5.0 Industry standards, practices, and network theory</td>
<td>1.5 Install and properly terminate various cable types and connectors using appropriate tools</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.10 Identify the basic elements of unified communication technologies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.11 Compare and contrast technologies that support the cloud and virtualization</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.12 Given a set of requirements, implement a basic network</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.7 Given a scenario, install and configure equipment in the appropriate location using best practices</td>
</tr>
<tr>
<td>4</td>
<td>2.0 Network operations</td>
<td>2.6 Given a scenario, configure a switch using proper features</td>
</tr>
<tr>
<td></td>
<td>5.0 Industry standards, practices, and network theory</td>
<td>5.4 Given a scenario, deploy the appropriate wired connectivity standard</td>
</tr>
<tr>
<td>5</td>
<td>1.0 Network architecture</td>
<td>1.8 Given a scenario, implement and configure the appropriate addressing schema</td>
</tr>
<tr>
<td>6</td>
<td>1.0 Network architecture</td>
<td>1.9 Explain the basics of routing concepts and protocols</td>
</tr>
<tr>
<td>Chapter</td>
<td>Section</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>7</td>
<td>1.0</td>
<td>Network architecture</td>
</tr>
<tr>
<td></td>
<td>4.0</td>
<td>Troubleshooting</td>
</tr>
<tr>
<td></td>
<td>1.4</td>
<td>Explain the characteristics and benefits of various WAN technologies</td>
</tr>
<tr>
<td></td>
<td>4.8</td>
<td>Given a scenario, troubleshoot and resolve common WAN issues</td>
</tr>
<tr>
<td></td>
<td>2.0</td>
<td>Network operations</td>
</tr>
<tr>
<td></td>
<td>5.0</td>
<td>Industry standards, practices, and network theory</td>
</tr>
<tr>
<td></td>
<td>2.7</td>
<td>Install and configure wireless LAN infrastructure and implement the appropriate technologies in support of wireless capable devices</td>
</tr>
<tr>
<td></td>
<td>4.3</td>
<td>Given a scenario, troubleshoot and resolve common wireless issues</td>
</tr>
<tr>
<td></td>
<td>5.3</td>
<td>Given a scenario, deploy the appropriate wireless standard</td>
</tr>
<tr>
<td>8</td>
<td>2.0</td>
<td>Network operations</td>
</tr>
<tr>
<td></td>
<td>5.0</td>
<td>Industry standards, practices, and network theory</td>
</tr>
<tr>
<td></td>
<td>2.7</td>
<td>Install and configure wireless LAN infrastructure and implement the appropriate technologies in support of wireless capable devices</td>
</tr>
<tr>
<td></td>
<td>4.3</td>
<td>Given a scenario, troubleshoot and resolve common wireless issues</td>
</tr>
<tr>
<td></td>
<td>5.3</td>
<td>Given a scenario, deploy the appropriate wireless standard</td>
</tr>
<tr>
<td>9</td>
<td>1.0</td>
<td>Network architecture</td>
</tr>
<tr>
<td></td>
<td>1.10</td>
<td>Identify the basic elements of unified communication technologies</td>
</tr>
<tr>
<td>10</td>
<td>4.0</td>
<td>Troubleshooting</td>
</tr>
<tr>
<td></td>
<td>4.6</td>
<td>Given a scenario, troubleshoot and resolve common network issues</td>
</tr>
<tr>
<td>11</td>
<td>2.0</td>
<td>Network operations</td>
</tr>
<tr>
<td></td>
<td>5.0</td>
<td>Industry standards, practices, and network theory</td>
</tr>
<tr>
<td></td>
<td>2.1</td>
<td>Given a scenario, use appropriate monitoring tools</td>
</tr>
<tr>
<td></td>
<td>2.2</td>
<td>Given a scenario, analyze metrics and reports from monitoring and tracking performance tools</td>
</tr>
<tr>
<td></td>
<td>2.3</td>
<td>Given a scenario, use appropriate resources to support configuration management</td>
</tr>
<tr>
<td></td>
<td>5.5</td>
<td>Given a scenario, implement the appropriate policies or procedures</td>
</tr>
<tr>
<td></td>
<td>5.6</td>
<td>Summarize safety practices</td>
</tr>
<tr>
<td></td>
<td>5.8</td>
<td>Explain the basics of change management procedures</td>
</tr>
</tbody>
</table>
12 Network Security
1.0 Network architecture
2.0 Network operations
3.0 Network security
4.0 Troubleshooting

1.2 Compare and contrast the use of networking services and applications
2.4 Explain the importance of implementing network segmentation
2.5 Given a scenario, install and apply patches and updates
3.1 Compare and contrast risk-related concepts
3.2 Compare and contrast common network vulnerabilities and threats
3.3 Given a scenario, implement network hardening techniques
3.4 Compare and contrast physical security controls
3.5 Given a scenario, install and configure a basic firewall
3.6 Explain the purpose of various network access control models
3.7 Summarize basic forensic concepts
3.8 Given a scenario, troubleshoot and resolve common security issues

13 Network Troubleshooting
4.0 Troubleshooting

4.1 Given a scenario, implement a network troubleshooting methodology
4.2 Given a scenario, analyze and interpret the output of troubleshooting tools
4.4 Given a scenario, troubleshoot and resolve common copper cable issues
4.5 Given a scenario, troubleshoot and resolve common fiber cable issues

How This Book Is Organized

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

■ Chapter 1, “Computer Network Fundamentals,” introduces the purpose of computer networks and their constituent components. In addition, networks are categorized by their geography, topology, and resource location.

■ Chapter 2, “The OSI Reference 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, “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, “Ethernet Technology.”** 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, “IPv4 and IPv6 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 IPv4 addressing, the chapter concludes with an introduction to IPv6.

- **Chapter 6, “Routing IP Packets.”** 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 Dynamic NAT (DNAT), Static NAT (SNAT), and Port Address Translation (PAT). Although the primary focus on this chapter is on unicast routing, the chapter concludes with a discussion of multicast routing.

- **Chapter 7, “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, “Wireless LANs.”** In this increasingly mobile world, wireless technologies are exploding in popularity. This chapter discusses the basic operation of WLANs. In addition, WLAN design and security considerations are addressed.
Chapter 9, “Network Optimization.” 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 quality of service (QoS). This chapter allows you to use what you have learned in this and preceding chapters to design a small office/home office (SOHO) network.

Chapter 10, “Command-Line Tools.” 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, “Network Management,” reviews some of the more common tools used to physically maintain a network. The components of configuration management are also presented. 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, “Network Security.” Network security is an issue for most any network, and this chapter covers a variety of network security technologies. You begin by learning 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, virtual private networks (VPNs), intrusion detection systems (IDSs), and intrusion prevention systems (IPSs).

Chapter 13, “Network Troubleshooting.” Troubleshooting network issues is 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 exercises including drag and drop, matching, and simulations as well as a practice exam engine and a collection of a few training videos. Finally, a suggested study plan is presented to assist you in preparing for the CompTIA Network+ exam (N10-006).

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 drag-and-drop, matching, and simulation exercises that are an important part of your preparation for certification. The DVD also includes a practice test and memory tables that you can work through to verify your knowledge of the subject matter. Finally, the DVD contains a few videos that can assist you in mastering the content.
After completion of this chapter, you will be able to answer the following questions:

- How do various wireless LAN 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?
CHAPTER 8

Wireless LANs

The popularity of wireless LANs (WLANs) has exploded over the past decade, allowing users to roam within a WLAN coverage area, 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, smartphones, 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.
Foundation Topics

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 smartphones, 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 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. Many companies offer WiFi as a service, and when in range of an AP, it is also referred to as a *hotspot*, indicating that WiFi is available through the AP.

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 IP Packets,” 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 smartphone) 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.) This is acting as a wireless bridge between the wireless clients connected to the AP and the wired devices connected to the switch in the same Layer 2 domain.

To manage multiple APs, a company will use a Wireless LAN Controller (WLC) for centralized management and control of the APs. A Cisco model 5760 WLC would be an example of a network controller for multiple APs. The protocols used to communicate between an AP and a WLC could be the older Lightweight Access Point Protocol (LWAPP) or the more current Control And Provisioning of Wireless Access Points (CAPWAP). Using a WLC, VLAN pooling can be used to assign IP addresses to wireless clients from a pool of IP subnets and their associated VLANs.

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:

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

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.
- **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.
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 to 2.5-GHz range (commonly referred to as the 2.4-GHz band) or in the 5.725-GHz to 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 with one another. Using wireless survey tools such as AirMagnet from Fluke Networks can provide analysis of what is currently in use, allowing you to set up a new wireless system that does not compete for the same frequencies that are already in use. Those same tools can assist in identifying wireless channel utilization as well in existing and new wireless networks. Regarding channel selection, merely selecting different channels is not sufficient, however, because transmissions on one channel spill over into nearby channels. Site survey tools can collect data to show the relative strength of signals in the areas being serviced by the APs. This output can be color-coded and overlaid on top of the floor plan and is often referred to as a heat map of the wireless signals.

Consider, for example, 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 * 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.
Channel

Figure 8-5  Nonoverlapping Channels in the 2.4 GHz Band

As a reference, Table 8-1 shows the specific frequencies for each of the channels 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>
<tr>
<td>100</td>
<td>5.500**</td>
</tr>
<tr>
<td>104</td>
<td>5.520**</td>
</tr>
<tr>
<td>108</td>
<td>5.540**</td>
</tr>
<tr>
<td>112</td>
<td>5.560**</td>
</tr>
<tr>
<td>116</td>
<td>5.580**</td>
</tr>
<tr>
<td>136</td>
<td>5.680**</td>
</tr>
<tr>
<td>140</td>
<td>5.700**</td>
</tr>
<tr>
<td>149</td>
<td>5.745</td>
</tr>
<tr>
<td>153</td>
<td>5.765</td>
</tr>
<tr>
<td>157</td>
<td>5.785</td>
</tr>
<tr>
<td>161</td>
<td>5.805</td>
</tr>
<tr>
<td>165</td>
<td>5.825</td>
</tr>
</tbody>
</table>

*Must support dynamic frequency selection to prevent interference with RADAR  
**Must be professionally installed

**CSMA/CA**

In Chapter 4, “Ethernet Technology,” 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 the way an Ethernet device listens to an Ethernet segment to determine whether a frame exists on the segment, a WLAN device listens for a transmission on a wireless channel to determine whether it is safe to transmit. In addition, 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 of 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 encode not only 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 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, but 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):** Whereas DSSS uses 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 an 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, 802.11n, and 802.11ac, 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 backward compatible with 802.11b, whereas 802.11g was backward 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 backward 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 is the bonding of two adjacent 20-MHz bands into a 40-MHz band.

The 802.11n high throughput (HT) standard defines modes for ensuring that older a/b/g devices and newer 802.11n devices can avoid collisions with each other.

**802.11ac**

The 802.11ac WLAN standard was published in 2013 and builds on (and is faster and more scalable than) 802.11n. 802.11ac is a 5-GHz only technology that can use wider channels in the 5-GHz band, more spatial streams, and multi-user MIMO (MU-MIMO).

**802.11x Standard Summary**

Table 8-3 acts as a reference to help you contrast the characteristics of the 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>
<tr>
<td>802.11ac</td>
<td>5 GHz</td>
<td>&gt; 3 Gbps (with MU-MIMO and several antennas)</td>
<td>OFDM</td>
<td>Similar to 802.11n operating at 5 GHz</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.

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.

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.
Mesh Topology

A mesh wireless network is a collection of wireless devices that may not use centralized control (decentralized management). The combined wireless coverage range defines the range of the network. This could also be referred to as a mesh cloud. Additional wireless technologies (besides WiFi) could be used to build a mesh wireless topology. This type of network could be used for hosts to communicate with other devices in the mesh, or the network could provide a gateway to the Internet or other networks.

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 to 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 the 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. Concrete walls, metal studs, or even window film could reduce the quality of the wireless network signals.

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 ensure 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. With the increased use of wireless, both coverage and capacity-based planning should be done to provide acceptable goodput. Goodput refers to the number of useful information bits that the network can deliver (not including overhead for the protocols being used). Another factor is the density (ratio of users to APs), which if too high could harm performance of the network. Areas expecting high density would include classrooms, hotels, and hospitals. Device or bandwidth saturation could impact performance.
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.

![Venn Diagram showing channel overlap](image)

**Figure 8-9** 10 Percent to 15 Percent Coverage Overlap in Coverage Areas for Nonoverlapping Channels

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.
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 your network. Fortunately, various 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. Devices like cell phones, laptops, tablets, and gaming and media devices could act as wireless clients as well as be used in a wireless attack as they have potential WiFi access to the network.
Other WLAN security threats include the following:

- **War chalking**: 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 *war chalking*. Figure 8-11 shows common war-chalking symbols.

- **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 his 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 a legitimate AP, the rogue AP is commonly referred to as an evil twin.
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 authentication or provide 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 PSK, as previously described). The PSK could be used as part of a mathematical algorithm to encrypt traffic, such that if an eavesdropper intercepted 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.

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 and a centralized authentication server such as RADIUS 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, but Chapter 4 showed how IEEE 802.1X was used in a wired network. Figure 8-12 shows a wireless implementation of IEEE 802.1X.
IEEE 802.1S 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), EAP-Tunneled Transport Layer Security (EAP-TTLS), 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.

**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.
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.

**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 that 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. WPA2 that uses a centralized server for authenticating users is referred to as *Enterprise* mode. An implementation of WPA2 that uses a configured password or PSK instead of a centralized server is referred to as *Personal* mode.

**Additional Wireless Options**

Other wireless technologies, such as Bluetooth, infrared (IR), and near-field communications (NFC), which are often integrated into smartphones, can also provide connectivity for a personal-area network (PAN) or other short-range networking applications.

**Real-World Case Study**

Acme Inc. hired an outside contractor who specializes in WiFi. The consultants came in and did a needs assessment and performed a wireless site survey. Recommendations were then made about the need for 15 access points in the headquarters office spaces and three access points at each of the remote branch offices. Three wireless LAN controllers, one for each office, will be used to manage the respective access points. The management of the access points through the wireless LAN controllers will be done primarily through the headquarters office using the WAN that is connecting the branch offices to the headquarters office.

Because of the high number of other WiFi access points being used in the same building as the headquarters office, Acme Inc. decided to use the 5-GHz range (due to less competition in that space) and to use 802.11n.

For security, Acme will use WPA2 in conjunction with a RADIUS server. ACME will use Enterprise mode for authentication of each user before allowing them access on the wireless network(s). The RADIUS server is integrated with Microsoft Active Directory so that Acme will not have to re-create every user account; the RADIUS server can check with the Active Directory server to verify user credentials and passwords.

There are separate SSIDs set up that map to the various VLANs and departments that are currently on the wired network. There is also a separate SSID set up as a wireless guest network that has limited access but does provide Internet access for guest users.

Once in place, a site survey was done again to verify the signal strengths and to identify any interference related to the wireless implementation. A heat map was provided to visually represent the signal strengths in the coverage areas in the respective office space.
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>
<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>269</td>
</tr>
<tr>
<td>Figure 8-2</td>
<td>Basic WLAN topology with a wireless access point</td>
<td>270</td>
</tr>
<tr>
<td>List</td>
<td>Antenna selection criteria</td>
<td>271</td>
</tr>
<tr>
<td>Figure 8-3</td>
<td>Omnidirectional antenna coverage</td>
<td>272</td>
</tr>
<tr>
<td>Figure 8-4</td>
<td>Unidirectional antenna coverage</td>
<td>272</td>
</tr>
<tr>
<td>Figure 8-5</td>
<td>Nonoverlapping channels in the 2.4-GHz band</td>
<td>274</td>
</tr>
<tr>
<td>List</td>
<td>Spread spectrum transmission methods</td>
<td>276</td>
</tr>
<tr>
<td>Table 8-3</td>
<td>Characteristics of 802.11 standards</td>
<td>278</td>
</tr>
<tr>
<td>Figure 8-6</td>
<td>Independent basic service set (IBSS) WLAN</td>
<td>279</td>
</tr>
<tr>
<td>Figure 8-7</td>
<td>Basic service set (BSS) WLAN</td>
<td>280</td>
</tr>
<tr>
<td>Figure 8-8</td>
<td>Extended service set (ESS) WLAN</td>
<td>281</td>
</tr>
<tr>
<td>List</td>
<td>Sources of interference</td>
<td>281</td>
</tr>
<tr>
<td>Figure 8-9</td>
<td>10 percent to 15 percent coverage overlap in coverage areas for nonoverlapping channels</td>
<td>281</td>
</tr>
</tbody>
</table>
Complete Tables and Lists from Memory

Print a copy of Appendix D, “Memory Tables” (found on the DVD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix E, “Memory Table Answer Key,” also on the DVD, 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, 802.11ac multiple input, multiple output (MIMO), channel bonding, independent basic service set (IBSS), basic service set (BSS), extended service set (ESS), war chalking, service set identifier (SSID), Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Wi-Fi Protected Access Version 2 (WPA2), Enterprise mode, Personal mode

Complete Chapter 8 Hands-On Lab in Network+ Simulator Lite

- Matching Wireless Standards and Terminology
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
   e. 10
   f. 11
   g. 14
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 extending 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 percent to 10 percent
   b. 10 percent to 15 percent
   c. 15 percent to 20 percent
   d. 20 percent to 25 percent

8. If a WLAN does not require a user to provide 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
Index

Numerics

3DES (Triple DES), 399
10BASE2, 114
10BASE5, 114
10BASE-T, 116
100BASE-T, 122
802.11 standards, 277-278
802.1Q trunking, 126
802.1w, 128
802.1X, 287
1000BASE-X, 122

A

A records, 93
AAAA records, 93
acknowledgment messages, 38
ACLs (access control lists), 423-424
activating the practice exam, 479
active hubs, 78
address translation, 214-218
   DNAT, 216
   NAT, 214-216
   PAT, 217-218
   SNAT, 216
anycast addresses, 191
APIPA (Automatic Private IP Addressing), 171-172
APIs (application programming interfaces), 46
application layer (OSI model), 47-48
application layer (TCP/IP stack), 51
   protocols, 51-53
application logs, 388
applications, TCP/IP application layer, 53
APs (access points), 269-270, 283-284
   placement, 283-284
   rogue APs, 285
ARP (Address Resolution Protocol), 81-85
   arp command, 328-330
advanced subnetting practice exercises, 182-186
AES (Advanced Encryption Standard), 399
Aggressive mode (IKE), 434
AH (Authentication Header), 435-436
always on connections, 232
AM (amplitude modulation), 35
analog phones, 104
anomaly-based detection (IDS/IPS), 441
antennas, 270-273
anycast addresses, 191
administrative distance, 208
ADSL (Asymmetric DSL), 244-246
arp command (UNIX), 349-351
ASCII (American Standard Code for Information Interchange), 46
ASPs (application server providers), 103
asset management, 378-379
assigning IPv4 addresses, 163-172
dynamic address assignment, 169-170
static address assignment, 164-168
asymmetric encryption, 400-401
asynchronous bit transmission, 35, 39
ATM (Asynchronous Transfer Mode), 256-258
attacks
availability attacks, 409-414
confidentiality attacks, 403-407
defending against, 414-424
ACLs, 423-424
documentation, 418-419
end-user policies, 418
governing policy, 417
honey pots, 422
incident response, 419-420
Nessus, 420-421
Nmap, 421-422
patching, 415-416
security policies, 416-417
technical policies, 418
user training, 414-415
vulnerability scanners, 420
integrity attacks, 407-409
authentication
open authentication, 286
TFA, 424
Auto-MDIX, 67
autonomous systems, 209
availability, 403
five nines, 127
hardware redundancy, 300
MTTR, 298
six nines, 298
availability attacks, 409-414
B
back reflection, 73
bandwidth, Ethernet, 120-122
baseband, 36
baselining, 379
BECN (backward explicit congestion notification), 256
believability of a route, 208
benefits
of bus topologies, 12
of client/server networks, 20
of full-mesh topologies, 17
of hub-and-spoke topologies, 16
of partial-mesh topologies, 19
of peer-to-peer networks, 22
of ring topologies, 13
of star topologies, 15
best practices for high availability, 302
best-effort QoS, 306
BGP (Border Gateway Protocol), 213-214
bidirectional Telnet sessions, 85-87
binary expressions, 32
binary numbering, 150
converting binary numbers to decimal numbers, 151
converting decimal numbers to binary numbers, 151-153
practice exercises, 153-156
bit error rate testers, 368
bit synchronization, 35
blocking state (STP), 133
BNC (Bayonet Neill-Concelman) connectors, 63
bookshelf analogy of OSI reference model, 30-31
BOOTP, 169
borrowed bits, 175
botnets, 409
BPL (broadband over power lines), 236
BRI (basic rate interface), 253
bridges, 79-80
broadband, 36
BPL, 236
broadcast addresses, 161-162
broadcast domains, 78
broadcast storms, 129-130
BSS (basic service set), 280
buffer overflows, 411
buffering, 44
bus topologies, 11-12
butt sets, 369

C

Cable certifiers, 369
cable distribution systems, 74-76
IDFs, 74-76
MDF, 76
cable management, 379
cable modem, 246-247
cable testers, 370
calculating
bit error rate, 368
number of created subnets, 176
call agents, 104
CANs (Campus-Area Networks), 8
capcitance, 245
capturing packets, 136-137
CAPWAP (Control and Provisioning of Wireless Access Points), 270
CARP (Common Address Redundancy Protocol), 142, 301
case studies
chapter 1, 22-23
chapter 2, 55
chapter 3, 105-106
chapter 4, 143-144
chapter 5, 192
chapter 6, 224-225
chapter 7, 261
chapter 8, 290
chapter 9, 320-321
chapter 10, 359-360
chapter 11, 389-390
chapter 12, 443-444
chapter 13, 470
SOHO network design, 313-320
cost savings versus performance, 320
environmental factors, 319
IP addressing, 315-316
Layer 1 media, 317
Layer 2 devices, 317-318
Layer 3 devices, 318
topology, 320
wireless design, 318-319
categories of UTP cabling, 66
CDMA (Code Division Multiple Access), 236
CE (customer edge) routers, 260
cellular phone technologies, 236-237
change management, 379-380
channels, 273-275
CHAP (Challenge-Handshake Authentication Protocol), 241

characteristics
- of bus topologies, 12
- of client/server networks, 20
- of full-mesh topologies, 17
- of hub-and-spoke topologies, 16
- of LLC sublayer, 38-40
- of MAC sublayer, 37-38
- of network infrastructure devices, 89
- of partial-mesh topologies, 19
- of peer-to-peer networks, 22
- of ring topologies, 13
- of routing protocols, 207-212
  - administrative distance, 208
  - metrics, 208
- of star topologies, 15

cheapernet, 114

CIDR (classless interdomain routing), 186-187

CIR (committed information rate), 256

circuit switching, 41

WAN connections, 233

Cisco Catalyst switches, access port configuration, 124-125

classes of IPv4 addresses, 159-161

classification, 308

clients, 5

client/server networks, 19-21

client-to-site VPNs, 432

cloud computing, 103

CM (configuration management), 378-381

CNAME records, 93

CO (central office), 252

coaxial cable, 62-63, 236

connectors, 63

HFC, 246

collision domains, 79

collisions, 117

commands
- ifconfig, 353-354

UNIX OS commands
- arp, 349-351
- dig, 352-353
- host, 353
- netstat, 355-357
- ping, 357-358
- route, 358-359
- traceroute, 354-355

Windows commands
- arp, 328-330
- ipconfig, 330-333
- nbstat, 333-336
- netstat, 336-338
- nslookup, 338-340
- ping, 340-342
- route, 342-346
- tracert, 346-347

components of networks, 5-6

- bridges, 79-80
- clients, 5
- firewalls, 91
- hubs, 5, 77-78
  - Ethernet, 119
- media, 6
- multilayer switches, 87-88
- routers, 6, 88-89
- servers, 5
- switches, 6, 80-88

  - access port configuration, 124-125
  - ARP requests/replies, 81-85
  - bidirectional Telnet sessions, 85-87
  - content switches, 98-99
management access, 140-141
QoS, 143
trunks, 125-127
VPN concentrators, 90-91
WAN links, 6
CompTIA Network+ Exam, preparing for, 477-476
memory tables, 481
Pearson IT Certification Practice Test engine, 476-478
activating the practice exam, 479
installing, 478-479
strategies for taking exam, 483-484
suggested study plan, 481-483
video training, 480-481
conductors, coaxial cable, 62
confidentiality, 398-399
confidentiality attacks, 403-407
configuring
LACP, 134-135
port mirroring, 138
QoS, 305-306
switches
access ports, 124-125
trunk ports, 127
congestion avoidance, 309-310
congestion management, 309
connectivity software, 370
connectors
coaxial cable, 63
fiber-optic cable, 72
polishing styles, 73
twisted-pair cable, 67-68
content caching, 302
content engines, 97
content switches, 98-99
converged networks, 4
convergence, 207
flapping routes, 210
converting
binary numbers to decimal numbers, 151
decimal numbers to binary numbers, 151-153
CPE (customer premise equipment), 260
CPs (control protocols), 241
CRAM-MD5 (Challenge-Response Authentication Mechanism Message Digest 5), 402
CRC (cyclic redundancy check), 39
crimpers, 370-371
crossover cables, 66-67
CSMA/CA (carrier sense multiple access collision avoidance), 275-276
CSMA/CD (carrier sense multiple access collision detect), 116-120
CSU/DSU (channel service unit/data service unit), 238-240
current state modulation, 34
CWDM (coarse wavelength-division multiplexing), 249

D

data diddling, 408
data flows (IPv6), 189-192
data formatting, 46
data link layer, 37-40
LLC sublayer, 38-40
MAC sublayer, 37-38
troubleshooting, 460-461
data rates, WANs, 234-235
DB-9 connectors, 67
DDNS (dynamic DNS), 94
DDOS (distributed denial-of-service) attacks, 410

decimal numbers, converting to binary numbers, 151-153
dedicated leased lines, 232, 237-238
defending against attacks, 414-424
  ACLs, 423-424
documentation, 418-419
derisk-user policies, 418
governing policy, 417
honey pots, 422
incident response, 419-420
Nessus, 420-421
Nmap, 421-422
patching, 415-416
security policies, 416-417
technical policies, 418
user training, 414-415
vulnerability scanners, 420
delay, 304
demarc, 252
deploying network-based IDS/IPS solutions, 442
DES (Data Encryption Standard), 399
designated ports, 131
devices
  bridges, 79-80
  firewalls, 91
  hubs, 77-78
    Ethernet, 119
  multilayer switches, 87-88
  routers, 88-89
  switches, 80-88
    ARP requests/replies, 81-85
    bidirectional Telnet sessions, 85-87
    content switches, 98-99
    Ethernet, 119-120
  first-hop redundancy, 141-142
  interface diagnostics, 143
  management access, 140-141
  QoS, 143
  trunks, 125-127
  VLANs, 122-124
  virtual network devices, 99-104
    virtual desktops, 102
    virtual routers, 100
    virtual servers, 99-100
  VPN concentrators, 90-91
DHCP (Dynamic Host Configuration Protocol), 53, 94-96, 169-170
diagnosing problems, 452-453
DiffServ (Differentiated Services), 306
dig command, 352-353
directly connected routes, 203-204
disadvantages
  of bus topologies, 12
  of client/server networks, 20
  of full-mesh topologies, 17
  of hub-and-spoke topologies, 16
  of partial-mesh topologies, 19
  of peer-to-peer networks, 22
  of ring topologies, 13
  of star topologies, 15
distance limitations of Ethernet, 120-122
distance-vector routing protocols, 210-212
DMZ (demilitarized zone), 430
DNAT (Dynamic NAT), 216
DNS (Domain Name System), 53
  DDNS, 94
  EDNS, 94
  record types, 93
  URLs, 94
DNS servers, 92-94
FQDNs, 92
hierarchical domain name structure, 92
DOCSIS (Data-Over-Cable Service Interface Specification), 247
documentation, as defense against attacks, 418-419
DoD model. See TCP/IP stack
DoS (denial-of-service) attacks, 410
dot1q, 126
downloading latest version of this book, 491-492
dropped packets, 304
DS0 (Digital Signal 0), 238
DSL (digital subscriber line), 244-246
DSLAM (DSL access multiplexer), 245
DSSS (direct-sequence spread spectrum), 276
DUAL (Diffusing Update Algorithm), 213
DWDM (dense wavelength-division multiplexing), 249
dynamic IPv4 address assignment, 169-170
dynamic routing protocols, 205-207

electrical disturbances as attacks, 412-413
electrostatic discharge wrist straps, 371-372
ELSR (edge label switch routers), 260
EMI (electromagnetic interference), 62
encryption, 46-47, 91
asymmetric encryption, 400-401
symmetric encryption, 399
end-user policies, 418
environmental monitors, 372
error control, 38
ESF (Extended Super Frame), 238
ESP (Encapsulating Security Payload), 435-436
ESS (extended service set), 280
establishing and tearing down IPsec VPNs, 437-438
Ethernet
1000BASE-X, 122
100BASE-T, 122
10BASE2, 114
10BASE5, 114
bandwidth, 120-122
collisions, 117
crossover cables, 66-67
CSMA/CD, 116-120
GBICs, 121
history of, 114-116
hubs, 119
metro Ethernet, 240
PoE, 135-136
PPPoE, 242
switches, 119-120
first-hop redundancy, 141-142
interface diagnostics, 143

E1 circuits, 239
E3 circuits, 239
EBCDIC (Extended Binary Coded Decimal Interchange Code), 46
EDNS (Extension Mechanisms for DNS), 94
EGPs (Exterior Gateway Protocols), 209
EIGRP (Enhanced Interior Gateway Routing Protocol), 213
electric power lines, BPL, 236
management access, 140-141
QoS, 143
user authentication, 138-139
VLANs, 122-124
types of, 121-122
Euro-DOCSIS, 247
extending classful masks, 175

F
fault-tolerant network designs, 298-299
F-connectors, 63
FDDI (Fiber Distributed Data Interface), 13
FDM (frequency-division multiplexing), 36
FEP (fluorinated ethylene polymer), 68
FHSS (frequency-hopping spread spectrum), 276
fiber-optic cable, 69-74, 236
connectors, 72
media converters, 74
MMF, 69-71
mode of propagation, 70-71
refractive index, 69-70
PONs, 249
SMF, 71-74
light propagation, 71-72
SONET, 247-249
wavelengths of light, 69
firewalls, 91, 426-431
hardware firewalls, 427
packet-filtering firewalls, 427-428
software firewalls, 426
stateful firewalls, 428
UTM firewalls, 430-431
virtual firewalls, 100
zones, 429-430
first-hop redundancy, 141-142
five nines of availability, 127
flapping routes, 210
flow control, 38, 42
transport layer, 43-44
FM (frequency modulation), 35
forwarding state (STP), 133
FQDNs (fully-qualified domain names), 92
Frame Relay, 255-256
frequencies for wireless networks, 273-275
FRTS (Frame Relay Traffic Shaping), 256
FTP (File Transfer Protocol), 53
full-mesh topologies, 17

G
gain, 271
gateways, 104
GBICs (gigabit interface converters), 121
geographically defined networks
CANs, 8
LANs, 7-8
MANs, 8-9
PANs, 9
WANs, 8
get messages (SNMP), 382
GLBP (Gateway Load Balancing Protocol), 142, 301
goals of network security, 398-403
governing policies, 417
GPC (GNU Privacy Guard), 399
GRE (generic routing encapsulation), 435
guidelines, 419

H
H.323, 45
hardware firewalls, 427
hardware redundancy, 300
HDLC (High-Level Data Link Control), 238
headers, IEEE 802.1Q, 126
HFC (hybrid fiber-coax), 246
hierarchical domain name structure, 92
high availability, 298-303
  best practices, 302
  content caching, 302
  fault-tolerant network designs, 298-299
  load balancing, 303
  MTTR, 298
  network design considerations, 301-302
  redundancy
    hardware redundancy, 300
    Layer 3, 300-301
  six nines, 298
hijacked sessions, 409
history of Ethernet, 114-116
honey pots, 422
host command, 353
host-based firewalls, 426
HSPA+ (Evolved High-Speed Packet Access), 236, 237
HSRP (Hot Standby Router Protocol), 141-142
HTTP (Hypertext Transfer Protocol), 53
HTTPS (Hypertext Transfer Protocol Secure), 53
hub-and-spoke topologies, 15-16
hubs, 5, 77-78
  Ethernet, 119
hybrid networks, 22

I
IANA (Internet Assigned Numbers Authority), 160
IBSS (independent basic service set), 279
ICA (Independent Computer Architecture), 244
ICANN (Internet Corporation for Assigned Names and Numbers), 160
ICMP (Internet Control Message Protocol), 44
ICMP attacks, 411
ICS (Internet connection sharing), 237
identifying root cause of problem, 452
IDFs (intermediate distribution frames), 74-76
IDS (intrusion detection system), 438-442
  anomaly-based detection, 441
  network- and host-based solutions, deploying, 442
  signature-based detection, 440-441
IEEE (Institute of Electrical and Electronics Engineers), 8
IEEE 802.11 standards, 277-278
IEEE 802.1X, 138-139, 287
IEEE 802.3, 114. See also
IEEE 802.3af, 135-136
ifconfig command, 353-354
IGMP (Internet Group Management Protocol), 218-220
IGPs (Interior Gateway Protocols), 209
IKE (Internet Key Exchange), 433-435
IMAP (Internet Message Access Protocol), 53
incident response, 419-420
index of refraction, 69-70
inductance, 245
inside global addresses, 215
inside local addresses, 215
installing Pearson IT Certification Practice Test engine, 478-479
integrity, 402-403
integrity attacks, 407-409
interference, sources of in wireless networks, 281-282
Internet, WAN technologies
ATM, 256-258
cable modem, 246-247
CSU/DSU, 239-240
dedicated leased lines, 237-238
DSL, 244-246
E1, 239
E3, 239
Frame Relay, 255-256
ISDN, 253-254
metro Ethernet, 240
MPLS, 259-260
overlay networks, 260-261
POTS, 251-252
PPP, 241-242
satellite, 249-250
SONET, 247-249
T1, 238
Internet layer (TCP/IP stack), 49-50
IntServ (Integrated Services), 306
IP phones, 104
ipconfig command, 330-333
IPS (intrusion prevention system), 438-442
anomaly-based detection, 441
network- and host-based solutions, deploying, 442
signature-based detection, 440-441
IPsec VPNs, 433-438
AH, 435-436
ESP, 435-436
establishing and tearing down, 437-438
IKE, 433-435
IPv4 addressing, 157-187
address assignment, 163-172
dynamic address assignment, 169-170
static address assignment, 164-168
address classes, 159-161
address structure, 157-159
APIPA, 171-172
available hosts, calculating, 176-177
broadcast addresses, 161-162
CIDR, 186-187
multicast addresses, 162
subnetting, 172-186
borrowed bits, 175
extending classful masks, 175
new IP address ranges, calculating, 179-182
number of created subnets, calculating, 176
practice exercises, 177-179, 182-186
purpose of, 172
subnet mask notation, 173-175
unicast addresses, 161
writing network addresses, 158-159
IPv6 addressing
address structure, 188-189
data flows, 189-192
need for, 187-188
ISAKMP (Internet Security Association and Key Management Protocol), 434
ISDN (Integrated Services Digital Network), 253-254
circuit types, 253
reference points, 254
IS-IS (Intermediate System-to-Intermediate System), 213
isochronous transmission, 38-39

J-K-L

jitter, 304
L2F (Layer 2 Forwarding), 438
L2TP (Layer 2 Tunneling Protocol), 438
LACP (Link Aggregation Control Protocol), 134-135
configuring, 134-135
LANs (local-area networks), 7-8
bridges, 79-80
last-hop routers, 224
Layer 1, 33-37
bandwidth usage, 36
bit synchronization, 35
multiplexing, 36
troubleshooting, 457-459
Layer 2, 37-40
bridges, 79-80
LLC sublayer, 38-40
MAC sublayer, 37-38
STP, 127-132
broadcast storms, 129-130
MAC address table corruption, 128-129
nonroot bridges, 130
port types, 131
root bridges, 130
switches, 6, 80-88
ARP requests/replies, 81-85
bidirectional Telnet sessions, 85-87
troubleshooting, 460-461
Layer 3, 40-42
connection services, 41-42
redundancy, 300-301
route discovery, 41
routers, 88-89
troubleshooting, 462-467
Layer 4, 42-44
flow control, 43-44
Layer 5, 44-46
Layer 6, 46-47
Layer 7, 47-48
layers
of OSI reference model, 31-48
memorizing, 32
of TCP/IP stack, 49-53
LCP (Link Control Protocol), 241-242
LCs (Lucent connectors), 72
LDAP (Lightweight Directory Access Protocol), 53
learning state (STP), 133
LFI (link fragmentation and interleaving), 312-313
light propagation
in MMF, 69-71
in SMF, 71-72
link aggregation, 133-135
LACP, 134-135
link efficiency, 312-313
link-state routing protocols, 212
listening state (STP), 133
LLC (Logical Link Control) sublayer, 38-40
load balancing, 303
load coils, 245
local loop, 252
logging
  application logs, 388
  security logs, 388
  syslog, 385-387
  system logs, 389
logical addressing, 40
logical topologies, 9-11
long STP, 132
looking-glass sites, 375
loopback plugs, 373
LSRs (label switch routers), 260
LTE (Long-Term Evolution), 236

M

MAC address filtering, 286
MAC sublayer, 37-38
Main mode (IKE), 434
malware, 404
man pages, 348
management tools
  bit error rate testers, 368
  butt sets, 369
  cable certifiers, 369
  cable testers, 370
  connectivity software, 370
  crimpers, 370-371
  electrostatic discharge wrist straps, 371-372
  environmental monitors, 372
  looking-glass sites, 375
  loopback plugs, 373
  multimeters, 373-374
  OTDRs, 377
  protocol analyzers, 374-375
  punch-down tools, 376
  speed test sites, 376
  TDRs, 377
  throughput testers, 376
  toner probes, 378
  WiFi analyzers, 375
MANs (metropolitan-area networks), 8-9
marking, 308-309
MAU (media access unit), 9
MDF (main distribution frame), 76
MDI (media-dependent interface), 67
MDIX (media-dependent interface crossover), 67
media, 6, 62-77
  cable distribution systems, 74-76
    IDFs, 74-76
    MDF, 76
  coaxial cable, 62-63
    connectors, 63
  converters, 74
  fiber-optic cable, 69-74
    connectors, 72
    MMF, 69-71
    PONs, 249
    SMF, 71-74
    SONET, 247-249
    wavelengths of light, 69
  twisted-pair cable, 64-68
    connectors, 67-68
    plenum cables, 68
    STP, 64-65
    UTP, 65-68
WANs
  physical media, 235-236
  wireless media, 236-237
wireless, 76-77
memorizing
  layers of OSI reference model, 32
  NAT IP addresses, 216
mesh wireless networks, 281
message switching, 41
metrics, 208
metro Ethernet, 240
MGCP (Media Gateway Control Protocol), 53
Microsoft RRAS (Routing and Remote Access Server), 243-244
mini-GBICs, 121
MMF (multimode fiber), 69-71
  mode of propagation, 70-71
  refractive index, 69-70
mnemonics
  memorizing NAT IP addresses, 216
  memorizing OSI model layers, 32
mode of propagation, 70-71
modulation, 34-35
monitoring ports, 136-138
MPLS (Multiprotocol Label Switching), 259-260
MS-CHAP (Microsoft Challenge-Handshake Authentication Protocol), 242
MTBF (mean time between failures), 298
MTRJ (media termination recommended jack) connectors, 72
MTTR (mean time to repair), 298
multicast addresses, 162
multicast routing, 218-224
  IGMP, 218-220
  PIM, 220-224
multilayer switches, 87-88
multimeters, 373-374
multimode delay distortion, 71
multiplexing, 36
MX records, 93

N
NaaS (network as a service), 102
NAC (Network Admission Control), 139
NAS (network-attached storage), 21
NAT (Network Address Translation), 214-216
nbstat command, 333-336
Nessus, 420-421
NetBEUI (NetBIOS Extended User Interface), 46
NetBIOS (Network Basic Input/Output System), 45
netstat command, 336-338
netstat command (UNIX), 355-357
network interface layer (TCP/IP stack), 49
network layer, 40-42
  connection services, 41-42
  logical addressing, 40
  route discovery, 41
  switching, 40-41
  troubleshooting, 462-467
network sniffers, 136-137
network-based IDS/IPS solutions, deploying, 442
networks
  CANs, 8
  client/server networks, 19-21
  components, 5-6
    bridges, 79-80
    clients, 5
    hubs, 5, 77-78
    media, 6
multilayer switches, 87-88
routers, 6, 88-89
server, 5
switches, 6, 80-88
VPNs converters, 90-91
WAN links, 6
converged networks, 4
DNS servers, 92-94
FQDNs, 92
hierarchical domain name structure, 92
documentation, 380-381
fault-tolerant designs, 298-299
firewalls, 91
high availability, design considerations, 301-302
hybrid networks, 22
LANs, 7-8
MANs, 8-9
media, 62-77
cable distribution systems, 74-76
diagram cable, 62-63
converters, 74
fiber-optic cable, 69-74
twisted-pair cable, 64-68
OSI reference model, bookshelf analogy, 30-31
PANs, 9
peer-to-peer networks, 21-22
purpose of, 4
SCADA networks, 470
security, goals of, 398-403
software defined networking, 104
specialized networks, troubleshooting, 470
topologies, 9-19
bus topologies, 11-12
full-mesh topologies, 17
hub-and-spoke topologies, 15-16
logical topologies, 9-11
partial-mesh topologies, 18-19
physical topologies, 9-11
ring topologies, 13
star topologies, 14-15
WANs, 8
ATM, 256-258
cable modem, 246-247
connection types, 232-234
CSU/DSU, 239-240
data rates, 234-235
dedicated leased lines, 237-238
DSL, 244-246
EI, 239
E3, 239
Frame Relay, 255-256
ISDN, 253-254
metro Ethernet, 240
MPLS, 259-260
overlay networks, 260-261
physical media, 235-236
POTS, 251-252
PPP, 241-242
satellite connections, 249-250
SONET, 247-249
T1, 238
wireless media, 236-237
next-hop addresses, 205
NFS (Network File System), 21
NIC (network interface card), 6
MDI, 67
Nmap, 421-422
NNTP (Network News Transport Protocol), 53
nondesignated ports, 131-133
nonplenum cables, 68
nonroot bridges, 130
nonstatistical anomaly detection (IDS/IPS), 441
nslookup command, 338-340
NTP (Network Time Protocol), 53

O
octets, 157
OFDM (orthogonal frequency-division multiplexing), 276
omnidirectional antennas, 271
OOB (out-of-band) management, 140-141
open authentication, 286
OSI reference model
application layer, 47-48
bookshelf analogy, 30-31
data link layer, 37-40
  LLC sublayer, 38-40
  MAC sublayer, 37-38
  troubleshooting, 460-461
network layer, 40-42
  connection services, 41-42
  logical addressing, 40
  route discovery, 41
  switching, 40-41
  troubleshooting, 462-467
physical layer, 33-37
  bandwidth usage, 36
  bit synchronization, 35
  multiplexing, 36
  troubleshooting, 457-459
presentation layer, 46-47
session layer, 44-46
transport layer, 42-44
  flow control, 43-44

OSPF (Open Shortest Path First), 213
OTDRs (optical time domain reflectometers), 377
outside global addresses, 215
outside local addresses, 215
overlay networks, 260-261

P
P (provider) routers, 260
packet shapers, 256
packet switching, 40
  WAN connections, 233-234
packet-filtering firewalls, 427-428
packets, 32
  capturing, 136-137
  dropped packets, 304
  reordering, 42
PANs (personal-area networks), 9
PAP (Password Authentication Protocol), 241
parameters
  arp command, 328
  arp command (UNIX), 350
  ipconfig command, 330
  nbstat command, 334
  netstat command, 336
  netstat command (UNIX), 355
  ping command, 340
  ping command (UNIX), 357
  route command, 342
  route command (UNIX), 358
parity bits, 39
partial-mesh topologies, 18-19
passive hubs, 78
password attacks, 408-409
PAT (Port Address Translation), 217-218
patching, 415-416
PathPing Windows tool, 348
PBX (private branch exchange), 103-104
PPDIOO (prepare, plan, design, implement, operate, and optimize), 378-379
PDUs (protocol data units), 32
PE (provider edge) routers, 260
Pearson IT Certification Practice Test engine, 476-478
activating the practice exam, 479
installing, 478-479
peer-to-peer networks, 21-22
PGP (pretty good privacy), 399
physical environment, attacks on, 413-414
physical layer, 33-37
bandwidth usage, 36
bit synchronization, 35
multiplexing, 36
troubleshooting, 457-459
physical media, WANs, 235-236
physical topologies, 9-11
PIM (Protocol Independent Multicast), 220-224, 223-224
PIM-DM (Protocol Independent Multicast-Dense Mode), 221-223
PIM-SM (Protocol Independent Multicast-Sparse Mode), 223-224
ping command, 340-342
ping command (UNIX), 357-358
placement of APs, 283-284
plenum cables, 68
PoE (Power over Ethernet), 135-136
poison reverse, 212
policing, 310-312
polishing styles of fiber connectors, 73
PONs (passive optical networks), 249
POP3 (Post Office Protocol version 3), 53
port forwarding, 214
port numbers, 52
ports
access ports, configuring, 124-125
link aggregation, 133-135
LACP, 134-135
mirroring, 138
monitoring, 136-138
STP, 131
trunk ports, configuring, 127
POTS (plain old telephone service), 251-252
PPP (Point-to-Point Protocol), 241-242
Microsoft RRAS, 243-244
PPPoE, 242
PPTP (Point-to-Point Tunneling Protocol), 438
practice exercises
binary numbering, 153-156
subnetting, 177-179
preparing for CompTIA Network+ Exam, 477-476
memory tables, 481
Pearson IT Certification Practice Test engine, 476-478
activating the practice exam, 479
installing, 478-479
strategies for taking exam, 483-484
suggested study plan, 481-483
video training, 480-481
presentation layer, 46-47
preshared keys, 286
preventing routing loops, 212
PRI (primary rate interface), 253
problem diagnosis, 452-453
procedures, 419
protocol analyzers, 374-375
protocols. See also
CPs, 241
TCP/IP application layer, 51-53
proxy servers, 96-97
prune messages (PIM-DM), 221
PTR records, 93
punch-down tools, 376
purpose
of networks, 4
of reference models, 30-31
of subnetting, 172
PVC (polyvinyl chloride), 68

Q
QoS (quality of service), 143, 304-313
best-effort, 306
classification, 308
configuring, 305-306
congestion avoidance, 309-310
congestion management, 309
delay, 304
IntServ, 306
jitter, 304
link efficiency, 312-313
marking, 308-309
packet drops, 304
policing, 310-312
shaping, 310-312
Quick mode (IKE), 434

R
radio-based WAN technologies, 237
Rapid Spanning Tree, 128
RDP (Remote Desktop Protocol), 53
real-world case studies
chapter 1, 22-23
chapter 2, 55
chapter 3, 105-106
chapter 4, 143-144
chapter 5, 192
chapter 6, 224-225
chapter 7, 261
chapter 8, 290
chapter 9, 320-321
chapter 10, 359-360
chapter 11, 389-390
chapter 12, 443-444
chapter 13, 470
records, DNS, 93
redundancy
hardware redundancy, 300
Layer 3, 300-301
reference models, 30-31. See also
reference points (ISDN), 254
refractive index, 69-70
remote desktop control, 244
remote-access security, 424
reordering packets, 42
representing binary data, 34-35
resource location-defined networks, 19-22
client/server networks, 19-21
peer-to-peer networks, 21-22
RFI (radio frequency interference), 62
RG-58 cable, 63
RG-59 cable, 63
RG-6 cable, 63
ring topologies, 13
RIP (Routing Information Protocol), 213
RJ-11 connectors, 67
RJ-45 connectors, 67
rogue APs, 285
root domains, 92
root ports, 131
route command, 342-346
route command (UNIX), 358-359
routed protocols, 207
routers, 6, 88-89
CE routers, 260
ELSRs, 260
last-hop routers, 224
LSRs, 260
P routers, 260
PE routers, 260
virtual routers, 100
wireless routers, 268-269
routing, 200-203. See also
coreference, 207
flapping routes, 210
next-hop addresses, 205
sources of information, 203-207
directly connected routes, 203-204
static routes, 204-205
sources of routing information, dynamic routing protocols, 205-207
routing loops, preventing, 212
routing protocols
autonomous systems, 209
characteristics, 207-212
administrative distance, 208
metrics, 208
distance-vector routing protocols, 210-212
dynamic routing protocols, 205-207
EGPs, 209
IGPs, 209
link-state routing protocols, 212
and routed protocols, 207
RPs (rendezvous points), 223
rsh (Remote Shell), 53
RTP (Real-time Transport Protocol), 53, 104
RTSP (Real Time Streaming Protocol), 53
S
SaaS (software as a service), 103
salami attacks, 408
satellite WAN connections, 237
SC connectors, 72
SCADA (supervisory control and data acquisition) networks, 470
SCP (Secure Copy), 53
SDH (Synchronous Digital Hierarchy), 248
SDSL (Symmetric DSL), 246
security
attacks
availability attacks, 409-414
confidentiality attacks, 403-407
defending against, 414-424
integrity attacks, 407-409
authentication
open authentication, 286
TFA, 424
availability, 403
confidentiality, 398-399
encryption, 46-47, 91
  asymmetric encryption, 400-401
  symmetric encryption, 399
firewalls, 91, 426-431
  hardware firewalls, 427
  packet-filtering firewalls, 427-428
  software firewalls, 426
  stateful firewalls, 428
  UTM firewalls, 430-431
  virtual firewalls, 100
  zones, 429-430
IDS/IPS, 438-442
  anomaly-based detection, 441
  signature-based detection, 440-441
integrity, 402-403
remote-access security, 424
VPNs, 431-438
  client-to-site VPNs, 432
  IPsec VPNs, 433-438
  site-to-site VPNs, 431
wireless networks, 284-290
  rogue APs, 283-284
  WEP, 288-289
  WPA, 289
  WPA2, 289-290
security levels (SNMP), 383-384
security logs, 388
segments
  TCP, 50-51
  UDP, 51
Seifert, Rich, 31
sequence numbering, 50-51
servers, 5
  DHCP servers, 94-96
  DNS servers, 92-94
  FQDNs, 92
  hierarchical domain name structure, 92
proxy servers, 96-97
virtual servers, 99-100
session layer, 44-46
set messages (SNMP), 382
severity levels (syslog), 386
SF (Super Frame), 238
SFTP (Secure FTP), 53
shaping, 310-312
shim headers, 259
Shortest Path Bridging, 128
signature-based detection (IDS/IPS), 440-441
single points of failure, 298
SIP (Session Initiation Protocol), 53, 104
site-to-site VPNs, 431
six nines, 298
SLIP (Serial Line Internet Protocol), 244
smart hubs, 78
smart jacks, 252
SMB (Server Message Block), 53
SMF (single-mode fiber), 71-74
  light propagation, 71-72
SMTP (Simple Mail Transfer Protocol), 53
SNAT (Static NAT), 216
SNMP (Simple Network Management Protocol), 53, 381-385
  messages, 382-383
  security levels (SNMP), 383-384
SNTP (Simple Network Time Protocol), 53
SOA records, 93
social engineering, 404
software defined networking, 104
software firewalls, 426
SOHO network design, case study, 313-320
- cost savings versus performance, 320
- environmental factors, 319
- IP addressing, 315-316
- Layer 1 media, 317
- Layer 2 devices, 317-318
- Layer 3 devices, 318
- topology, 320
- wireless design, 318-319

SONET (Synchronous Optical Network), 247-249
- source distribution trees, 221
- sources of routing information, 203-207
  - directly connected routes, 203-204
  - dynamic routing protocols, 205-207
  - static routes, 204-205
- specialized networks, troubleshooting, 470
- speed limitations of Ethernet, 120-122
- speed test sites, 376
- split horizon, 212
- spread spectrum technologies, 276
- SPT (shortest path tree) switchover, 224
- SSH (Secure Shell), 53
  - switch management access, 140-141
- SSL (Secure Sockets Layer), 438
- ST (straight tip) connectors, 72
- standards, 419
- star topologies, 14-15
- state transition modulation, 34-35
- stateful firewalls, 428
- static IPv4 address assignment, 164-168
- static routes, 204-205
- statistical anomaly detection (IDS/IPS), 441

StatTDM (statistical TDM), 36
- store-and-forward networks, 41
- STP (shielded twisted pair), 64-65
- STP (Spanning Tree Protocol), 127-132
  - broadcast storms, 129-130
  - MAC address table corruption, 128-129
  - nonroot bridges, 130
  - port costs, 132
  - port types, 131
  - root bridges, 130
- structure of IPv4 addresses, 157-159
- structured troubleshooting methodology, 454-456
- subnet mask, 158
- subnetting, 172-186
  - available hosts, calculating, 176-177
  - borrowed bits, 175
  - extending classful masks, 175
  - new IP address ranges, calculating, 179-182
  - number of created subnets, calculating, 176
  - practice exercises, 177-179, 182-186
  - purpose of, 172
  - subnet mask notation, 173-175
- supplicants, 139
- The Switch Book, 31
- switches, 6, 80-88
  - access port configuration, 124-125
  - ARP requests/replies, 81-85
  - bidirectional Telnet sessions, 85-87
  - content switches, 98-99
  - Ethernet, 119-120
  - first-hop redundancy, 141-142
  - interface diagnostics, 143
  - management access, 140-141
ports
  * link aggregation, 133-135
  * mirroring, 138
  * monitoring, 136-138
QoS, 143
STP, 127-132
  * broadcast storms, 129-130
  * MAC address table corruption, 128-129
  * nonroot bridges, 130
  * port types, 131
  * root bridges, 130
trunks, 125-127
user authentication, 138-139
VLANs, 122-124
  * VTP, 124
switching, 40-41
symmetric encryption, 399
synchronous bit transmission, 35, 39
syslog, 385-387
system logs, 389

T

T1 circuits, 238
TCP (Transmission Control Protocol), 43
  * segments, 50-51
TCP SYN floods, 410
TCP/IP stack, 49-53
  * application layer, 51
  * network interface layer, 49
  * transport layer, 50-51
TDM (time-division multiplexing), 36
TDRs (time domain reflectometers), 377
tearing down IPsec VPNs, 437-438
technical policies, 418
telcos, 252
Telnet, 53
tethering, 236
TFA (two-factor authentication), 424
TFTP (Trivial File Transfer Protocol), 53
thinnet, 114
TIA/EIA-568 standard, 64
tip and ring, 252
TLS (Transport Layer Security), 438
Token Ring, 9-11, 13
toner probes, 378
topologies, 9-19
  * bus topologies, 11-12
  * full-mesh topologies, 17
  * hub-and-spoke topologies, 15-16
  * logical topologies, 9-11
  * partial-mesh topologies, 18-19
  * physical topologies, 9-11
  * ring topologies, 13
  * star topologies, 14-15
traceroute command, 354-355
tracert command, 346-347
traffic shaping, 310-312
transport layer (OSI model), 42-44
  * flow control, 43-44
transport layer (TCP/IP stack), 50-51
trap messages (SNMP), 383
troubleshooting
  * data link layer, 460-461
  * identifying root cause of problem, 452
  * network layer, 462-467
  * physical layer, 457-459
  * problem diagnosis, 452-453
  * structured troubleshooting methodology, 454-456
  * wireless networks, 467-470
trunks, 125-127
trust relationship exploitation, 408
twisted-pair cable, 64-68
connectors, 67-68
plenum cables, 68
STP, 64-65
UTP, 65-68
categories, 66
crossover cables, 66-67

UDP (User Datagram Protocol), 43
segments, 51
unicast addresses, 161
unidirectional antennas, 272
UNIX OS commands
arp, 349-351
dig, 352-353
host, 353
ifconfig, 353-354
man pages, 348
netstat, 355-357
ping, 357-358
route, 358-359
traceroute, 354-355
URLs (uniform resource locators), 94
UTM (unified threat management)
firewalls, 430-431
UTP (unshielded twisted-pair) cable,
15, 65-68, 235
categories, 66

crossover cables, 66-67

V

VCs (virtual circuits), 255
VDLS (Very High Bit-Rate DSL), 246
vendor code, 38
versions of IGMP, 218-219
video training for CompTIA Network+
Exam, 480-481
virtual desktops, 102
virtual network devices, 99-104
cloud computing, 103
virtual desktops, 102
virtual servers, 99-100
VLANs, 122-124
VTP, 124
VNC (virtual network computing), 244
VoIP (Voice over IP), 104
voltage, current state modulation, 34
VPN concentrators, 90-91
VPNs (virtual private networks), 90,
431-438
client-to-site VPNs, 432
IPsec VPNs, 433-438
AH, 435-436
ESP, 435-436
establishing and tearing down,
437-438
IKE, 433-435
site-to-site VPNs, 431
VRRP (Virtual Router Redundancy
Protocol), 142, 301
VTP (VLAN Trunking Protocol), 124
vulnerability scanners, 420
WAN links, 6
WANs (wide-area networks), 8
   ATM, 256-258
   cable modem, 246-247
   connection types, 232-234
   CSU/DSU, 239-240
   data rates, 234-235
   dedicated leased lines, 237-238
   DSL, 244-246
   E1, 239
   E3, 239
   Frame Relay, 255-256
   ISDN, 253-254
      circuit types, 253
         reference points, 254
   metro Ethernet, 240
   MPLS, 259-260
   overlay networks, 260-261
   physical media, 235-236
   POTS, 251-252
   PPP, 241-242
      Microsoft RRAS, 243-244
      PPPoE, 242
   satellite connections, 249-250
   SONET, 247-249
   T1, 238
   wireless media, 236-237
war chalking, 285
wavelengths of light in fiber-optic cable, 69
well-known ports, 52
WEP (Wired Equivalent Privacy), 288-289
Wi-Fi analyzers, 375

WiMAX (Worldwide Interoperability for Microwave Access), 237
windowing, 43
Windows commands
   arp, 328-330
   ipconfig, 330-333
   nbstat, 333-336
   netstat, 336-338
   nslookup, 338-340
   ping, 340-342
   route, 342-346
   tracert, 346-347
wireless networks, 76-77
   antennas, 270-273
   APs, 269-270, 283-284
      placement, 283-284
      rogue APs, 283-284
   channels, 273-275
   CSMA/CA, 275-276
   frequencies, 273-275
   IEEE 802.11 standards, 277-278
   interference, sources of, 281-282
   media, 236-237
   mesh topology, 281
   security, 284-290
      WEP, 288-289
      WPA, 289
      WPA2, 289-290
   spread spectrum technologies, 276
   troubleshooting, 467-470
   war chalking, 285
   wireless routers, 268-269
WLANs
   BSS, 280
   ESS, 280
   IBSS, 279
Wireshark, 136-137
wiretapping, 404
WLANs (wireless LANs)
  BSS, 280
  ESS, 280
  IBSS, 279
  security, 286-288
WPA (WiFi Protected Access), 289
WPA2 (WiFi Protected Access version 2), 289-290
WPANs (wireless PANs), 9
writing network addresses, 158-159

X-Y-Z

zero-day attacks, 441
zones, 429-430