### Contents at a Glance

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Chapter 1</td>
<td>Introduction to Computer Networking</td>
<td>23</td>
</tr>
<tr>
<td>Chapter 2</td>
<td>Media and Connectors</td>
<td>61</td>
</tr>
<tr>
<td>Chapter 3</td>
<td>Networking Components and Devices</td>
<td>99</td>
</tr>
<tr>
<td>Chapter 4</td>
<td>Understanding the TCP/IP Protocol Suite</td>
<td>145</td>
</tr>
<tr>
<td>Chapter 5</td>
<td>TCP/IP Addressing and Routing</td>
<td>185</td>
</tr>
<tr>
<td>Chapter 6</td>
<td>Ethernet Networking Standards</td>
<td>221</td>
</tr>
<tr>
<td>Chapter 7</td>
<td>Wireless Networking</td>
<td>245</td>
</tr>
<tr>
<td>Chapter 8</td>
<td>Wide Area Networking</td>
<td>283</td>
</tr>
<tr>
<td>Chapter 9</td>
<td>OSI Model</td>
<td>325</td>
</tr>
<tr>
<td>Chapter 10</td>
<td>Network Performance and Optimization</td>
<td>349</td>
</tr>
<tr>
<td>Chapter 11</td>
<td>Troubleshooting Procedures and Best Practices</td>
<td>393</td>
</tr>
<tr>
<td>Chapter 12</td>
<td>Command-Line Networking Tools</td>
<td>431</td>
</tr>
<tr>
<td>Chapter 13</td>
<td>Network Management Tools and Documentation Procedures</td>
<td>479</td>
</tr>
<tr>
<td>Chapter 14</td>
<td>Network Access Security</td>
<td>525</td>
</tr>
<tr>
<td>Chapter 15</td>
<td>Security Technologies and Malicious Software</td>
<td>561</td>
</tr>
<tr>
<td>Appendix A</td>
<td>Answers to the Review Questions</td>
<td>605</td>
</tr>
<tr>
<td></td>
<td>Index</td>
<td>639</td>
</tr>
</tbody>
</table>

**Elements on the CD-ROM:**

- Appendix B  Memory Tables
- Appendix C  Memory Tables Answer Key
- Glossary
# Table of Contents

## Introduction  3
- How This Book Helps You  4
  - Exam Objectives and Chapter Organization  4
  - Instructional Features  18
- Network Hardware and Software Requirements  19
- Advice on Taking the Exam  20

### Chapter 1  Introduction to Computer Networking  23
- What Is a Network?  24
- LANs and WANs  25
- Peer-to-Peer Versus Client/Server Networks  28
  - The Peer-to-Peer Networking Model  28
  - Advantages of Peer-to-Peer Networks  29
  - Disadvantages of Peer-to-Peer Networks  30
  - The Client/Server Networking Model  30
- Servers  31
  - Client Computers  32
  - Advantages of Client/Server Networking  32
  - Disadvantages of Client/Server Networking  32
  - Distributed and Centralized Computing  33
- Virtual Private Networks (VPN)  34
  - Components of the VPN Connection  35
  - VPN Pros and Cons  35
- Virtual Local Area Network (VLAN)  36
  - VLAN Membership  37
  - Protocol-Based VLANs  37
  - Port-Based VLANs  38
  - MAC Address-Based VLANs  38
  - VLAN Segmentation  39
- LAN Topologies  40
  - Physical and Logical Topologies  41
  - Bus Topology  41
  - Star Topology  42
  - Ring Topology  44
  - Wired Mesh Topology  45
Wireless Network Topologies 47
  Infrastructure Wireless Topology 47
  Ad Hoc Wireless Networking 48
  Point-to-Point, Point-to-Multipoint, and Mesh-Wireless Topology 48
  Point-to-Point Networks 48
  Point-to-Multipoint 50
  Mesh Networks 50
  Hybrid Topologies 51
Summary 52

Chapter 2  Media and Connectors  61

Networking Media 62
  Media Interference 62
  Data Transmission Rates 63
  Media Length 63
Secure Transmission and Physical Media 64
  Installation and Repair 65
  Simplex, Half-Duplex, and Full-Duplex 65
  Cable Media 66
  Twisted-Pair Cable 67
  Coaxial Cable 69
  Fiber-Optic Cable 70
Media Connectors 72
  RJ Connectors 72
  F-Type Connectors and RG-59/RG-6 Cables 73
  RS-232 Standard 74
  Fiber Connectors 74
  IEEE 1394 (FireWire) 75
  Universal Serial Bus Connectors (USB) 76
  Cable Summary 76
Wiring Standards and Specialized Cable 77
  568A and 568B Wiring Standards 77
  Straight Versus Crossover Cable 78
  Rollover and Loopback Cables 80
Components of Wiring Distribution 80
  Network Cross Connects 81
  Horizontal Cabling 81
Vertical Cable 82
Patch Panels 83
Type 66 and Type 110 Punchdown Blocks 84
MDF and IDF 85
Demarcation Point 86
Verify Wiring Installation and Termination 87
Summary 89

Chapter 3 Networking Components and Devices 99
Common Network Devices 100
Hubs 100
Network Switches 102
Switching Methods 105
Advanced Switch Features 105
Power over Ethernet (PoE) 106
Trunking 106
Port Authentication 107
Working with Hubs and Switches 107
Hub and Switch Ports 107
Hub and Switch Indicator Lights 109
Rack-Mount, Stackable, and Freestanding Devices 109
Managed Hubs and Switches 109
Repeaters 110
Bridges 110
Bridge Implementation Considerations 111
Types of Bridges 114
Routers 114
Gateways 117
Modems 118
Modem Connection Speeds 119
Network Interface Cards (NIC) 120
Types of Network Interfaces 121
Installing Network Cards 123
Media Converters 124
Firewalls 125
DHCP Server 126
Specialized Network Devices 127
  Multilayer and Content Switches 127
  Intrusion Detection and Prevention Systems 128
  Load Balancer 129
  Multifunction Network Devices 129
  DNS Server 129
  Bandwidth Shaper 130
  Proxy Server 131
  CSUs/DSUs 133
  Network Devices Summary 134
Summary 136

Chapter 4 Understanding the TCP/IP Protocol Suite 145
  A Brief Introduction to Protocols 146
    Protocols from the Sending Device 147
    Protocols on the Receiving Device 147
    Internet Protocol (IP) 149
    Transmission Control Protocol (TCP) 149
    User Datagram Protocol (UDP) 150
    File Transfer Protocol (FTP) 151
    Secure Shell (SSH) 152
    Secure File Transfer Protocol (SFTP) 152
    Trivial File Transfer Protocol (TFTP) 153
    Simple Mail Transfer Protocol (SMTP) 153
    Hypertext Transfer Protocol (HTTP) 154
    Hypertext Transfer Protocol Secure (HTTPS) 154
      (POP3/IMAP4) 155
    Telnet 155
    Internet Control Message Protocol (ICMP) 156
    Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol
      (RARP) 156
    Network Time Protocol (NTP) 157
    Network News Transfer Protocol (NNTP) 157
    Secure Copy Protocol (SCP) 158
    Lightweight Directory Access Protocol (LDAP) 158
    Internet Group Management Protocol (IGMP) 158
Domain Name System (DNS) 159

The DNS Namespace 160

Types of DNS Entries 162

DNS in a Practical Implementation 163

Simple Network Management Protocol (SNMP) 163

Components of SNMP 164

SNMP Management Systems 164

SNMP Agents 165

Management Information Bases (MIB) 165

SNMP Communities 166

Dynamic Host Configuration Protocol (DHCP) 167

Transport Layer Security 170

Session Initiation Protocol 170

Real-time Transport Protocol (RTP) 171

TCP/IP Protocol Suite Summary 171

Identifying Common TCP/IP Port Numbers 173

Summary 175

**Chapter 5  TCP/IP Addressing and Routing 185**

Identifying MAC Addresses 186

Understanding IPv4 Addressing Fundamentals 187

General IP Addressing Principles 188

IPv4 Addressing 188

IPv4 Address Types 190

Distributing IPv4 Addresses to the Network 191

Static Addressing 191

Dynamic Addressing 191

Bootstrap Protocol (BOOTP) 191

APIPA and IPv4 192

Broadcast Addresses and “This Network” 193

Classless Interdomain Routing (CIDR) 193

Default Gateways 194

Understanding Subnetting 195

Public and Private IP Address Schemes 198

Private Address Ranges 199

Practical Uses of Public and Private IP Addressing 200

IPv6 Addressing 201
Identifying IPv6 Addresses 201
IPv6 Address Types 202

Differentiating Between Routable and Routing Protocols 204
Routable Protocols 204
Routing Protocols 205

Distance-Vector Routing Protocols 206
Link-State Routing Protocols 208

NAT, PAT, and SNAT 209

Summary 211

Chapter 6 Ethernet Networking Standards 221

Characteristics Specified in the IEEE 802 Standards 223
Speed 223
Access Methods 223
Carrier Sense Multiple Access/Collision Detection 224
CSMA/CA 225
Token Passing 226
Bonding 226
Topology 226
Media 227

Differentiating Between Baseband and Broadband Signaling 227
Baseband 227
Broadband 227

Ethernet Standards 228
10Base2 228
10BaseT 229
10BaseFL 230
Fast Ethernet 230
100BaseTX 231
100BaseT4 231
100BaseFX 231
Fast Ethernet Comparison 231
Gigabit Ethernet 232
1000BaseX 232
1000BaseT 233
10Gigabit Ethernet 234
10GBaseSR/SW 234
Chapter 7  Wireless Networking  245

Understanding Wireless Devices  246
   Wireless Access Point  246
   Wireless Antennas  248
   Antenna Ratings  249
   Types of Wireless Antennas  249

802.11 Wireless Standards  251
   The Magic Behind 802.11n  254
   Wireless Radio Channels  254

Spread Spectrum Technology  257
   Frequency-Hopping Spread Spectrum (FHSS) Technology  257
   Direct-Sequence Spread Spectrum (DSSS) Technology  258
   Orthogonal Frequency Division Multiplexing  258

FHSS, DSSS, OFDM, and 802.11 Standards  258

Beacon Management Frame  259

Configuring and Troubleshooting the Wireless Connection  260
   Configuring Communications Between Wireless Devices  262
   Troubleshooting Wireless Signals  264
   Site Surveys  265
   Troubleshooting AP Coverage  266
   Wireless Troubleshooting Checklist  267

Securing Wireless Networks  268
   Defining Access Control, Authentication, Authorization, and Encryption  268

Wireless Authentication and Encryption Methods  269
   Wired Equivalent Privacy (WEP)  270
   Wi-Fi Protected Access (WPA)  270
   Temporal Key Integrity Protocol (TKIP)  271
   802.1X  272

Securing the Access Point  273

Summary  273
Chapter 8  Wide Area Networking  283

Public and Private Networks  284
  Public Networks  284
    Public Switched Telephone Network (PSTN)  284
    The Internet  285
    Advantages and Disadvantages of Public Networks  286
  Private Networks  286

Switching Methods  287
  Packet Switching  288
    Virtual-Circuit Packet Switching  289
    Datagram Packet Switching  289
  Circuit Switching  290
  Message Switching  290
  Comparing Switching Methods  291

WAN Technologies  292
  X.25  293
  Frame Relay  293
  T-Carrier Lines  295
  T1/E1/J1 Lines  295
  T3 Lines  297
  SONET/OCx Levels  297
  Asynchronous Transfer Mode (ATM)  298
  Integrated Services Digital Network (ISDN)  299
    Basic Rate Interface (BRI)  301
    Primary Rate Interface (PRI)  301
    Comparing BRI and PRI ISDN  301
  WAN Technology Summary  301

Internet Access Technologies  302
  POTS Internet Access  303
  POTS Troubleshooting Procedures  303
  Troubleshooting Poor Connection Speeds  305
  Modem-Specific Troubleshooting  306
  xDSL  307
  Cable Internet Access  310
  Satellite Internet Access  313

Wireless Wide Area Networking  315

Summary  316
Chapter 9  OSI Model  325

OSI Reference Model 101  326
Layer 1: The Physical Layer  328
Layer 2: The Data Link Layer  329
Layer 3: The Network Layer  329
Switching Methods  330
Network Layer Addressing  331
Layer 4: The Transport Layer  331
Connection-Oriented Protocols  332
Connectionless Protocols  332
Flow Control  333
Layer 5: The Session Layer  333
Layer 6: The Presentation Layer  333
Layer 7: The Application Layer  334
OSI Model Summary  334

The Layers at Which Devices Operate  335
Hubs  336
Switches  336
Bridges  336
Routers  336
NICs  336
Wireless Access Points (APs)  337
Summary of the Layers at Which Devices Operate  337

TCP/IP Protocol Suite Summary  337
Summary  340

Chapter 10  Network Performance and Optimization  349

Understanding Uptime  350
Understanding the Risks  352
RAID  353
RAID 0  354
Advantages of RAID 0  354
Disadvantages of RAID 0  355
Recovering from a Failed RAID 0 Array  355
RAID 1  355
Advantages of RAID 1  357
Disadvantages of RAID 1  357
Recovering from a Failed RAID 1 Array  358
RAID 5 358
Advantages of RAID 5 358
Disadvantages of RAID 5 359
Recovering from a RAID 5 Array Failure 359
RAID 10 360
Choosing a RAID Level 361
Hardware and Software RAID 362
Other Fault-Tolerance Measures 363
Link Redundancy 363
Using Uninterruptible Power Supplies 364
Why Use a UPS? 365
Power Threats 365
Using Redundant Power Supplies 366
Server and Services Fault Tolerance 366
Using Standby Servers 366
Server Clustering 367
Preparing for Memory Failures 368
Managing Processor Failures 368
Disaster Recovery 368
Backup Methods 368
Full Backups 369
Incremental Backups 370
Differential Backups 370
A Comparison of Backup Methods 371
Backup Rotation Schedules 371
Offsite Storage 372
Backup Best Practices 373
Hot and Cold Spares 374
Hot Spare and Hot Swapping 374
Cold Spare and Cold Swapping 375
Recovery Sites 375
Cold Site 375
Hot Site 376
Warm Site 376
Network Optimization Strategies 377
QoS 377
Latency-Sensitive High-Bandwidth Applications 378
Chapter 11 Troubleshooting Procedures and Best Practices 393

The Art of Troubleshooting 394
Troubleshooting Servers and Workstations 394
General Troubleshooting Considerations 395
Troubleshooting Methods and Procedures 396
Step 1: Information Gathering—Identify Symptoms and Problems 397
Information from the Computer 397
Information from the User 398
Observation Techniques 399
Effective Questioning Techniques 399
Step 2: Identify the Affected Areas of the Network 399
Step 3: Determine if Anything Has Changed 400
Changes to the Network 400
Changes to the Server 401
Changes to the Workstation 402
Step 4: Establish the Most Probable Cause 402
Step 5: Determine if Escalation Is Necessary 403
Step 6: Create an Action Plan and Solution Identifying Potential Effects 403
Step 7: Implement and Test the Solution 404
Step 8: Identify the Results and Effects of the Solution 405
Step 9: Document the Solution and the Entire Process 406
Troubleshooting the Network 407
Troubleshooting Wiring 407
Where the Cable Is Used 408
Wiring Issues 409
Crosstalk 409
Near-End Crosstalk (NEXT) 409
Far-End Crosstalk (FEXT) 409
Electromagnetic interference (EMI) 409
Attenuation 410
Open Impedance Mismatch (Echo) 410
Shorts 410
Managing Collisions 410
Troubleshooting Infrastructure Hardware 411
Configuring and Troubleshooting Client Connectivity 413
Verifying Client TCP/IP Configurations 413
Setting Port Speeds and Duplex 415
Troubleshooting Incorrect VLANs 416
Identifying Issues That Might Need Escalation 417
Troubleshooting Wireless Issues 418
Troubleshooting Wireless Signals 418
Troubleshooting Wireless Configurations 420
Summary 421

Chapter 12 Command-Line Networking Tools 431
Common Networking Utilities 432
The ping Utility 432
Switches for ping 434
Troubleshooting Steps with ping 435
Ping Error Messages 436
The Destination Host Unreachable Message 437
The Unknown Host Message 438
The traceroute Utility 439
Reviewing tracert Command Printouts 441
The traceroute Command 444
The mtr Utility 445
The arp Utility 445
The ARP Cache 445
Switches for arp 446
The arp Command Printout 447
The arp ping Utility 447
The netstat Utility 448
The netstat Command Printouts 450
netstat -e 450
netstat -a 451
netstat -r 452
netstat -s 453
The nbtstat Utility 454
Chapter 13 Network Management Tools and Documentation Procedures

Documentation Management

Wiring Schematics

Physical and Logical Network Diagrams

Physical Network Documentation

Logical Network Documentation

Baselines

Policies, Procedures, Configurations, and Regulations

Policy Documentation

Network Procedure Documentation

Configuration Documentation

Regulations

Monitoring the Network to Identify Performance

Throughput Testing

Port Scanners

Network Testing

Performance Testing

Load Testing

Stress Testing

Logging

Security Logs

Application Logs

System Logs

History Logs

Log Management
Networking Tools 503
   Wire Crimpers 504
   Strippers and Snips 504
   Punchdown Tools 505
   Cable Certifiers 505
   Voltage Event Recorders 506
   Temperature Monitors 506
   Toner Probes 508
   Protocol Analyzer 509
   Media/Cable Testers 509
   Media Testers 510
   TDR 510
   OTDR 510
   Multimeter 511
   Network Qualification Tester 512
   Butt Set 512
   Wireless Detector 512

Summary 513

Chapter 14 Network Access Security 525

Understanding Network Security Threats 526
Security Responsibilities of a Network Administrator 527
Physical and Logical Security 528
   Physical Security 528
   Network Hardware and Server Room Access 529
   Lock and Key 529
   Swipe Card and PIN Access 529
   Biometrics 530
   Hardware Room Best Practices 531
   Logical Security 532

Firewalls 532
   The Purpose and Function of a Firewall 534
   Stateful and Stateless Firewalls 536
   Firewall Methods 536
   Network Layer Firewalls 536
   Circuit-Level Firewalls 537
   Application-Layer Firewalls 537
   Demilitarized Zones 538
Intrusion Detection and Intrusion Prevention Systems 539
Network Access Security 539
Access Control Lists 540
Access Control and MAC Filtering 540
TCP/IP Filtering 540
Port Blocking/Filtering 541
Remote Access Protocols and Services 542
Routing and Remote Access Service (RRAS) 542
SLIP 543
PPP 543
PPPoE 544
Tunneling and Encryption 545
SSL VPNs 546
VPN Concentrators 546
Point-to-Point Tunneling Protocol (PPTP) 547
Layer Two Tunneling Protocol (L2TP) 548
Advantages of L2TP and PPTP 548
Inside IPsec 548
Authentication Headers 549
Encapsulating Security Payloads 549
IPsec Transmission Modes 550
Remote Control Protocols 550
Summary 551

Chapter 15  Security Technologies and Malicious Software 561
Authentication, Authorization, and Accounting (AAA) 562
Authentication 562
Password Policies 562
Password Strength 563
Multifactor Authentication 565
Authentication Tokens 565
Biometrics 565
Multifactor Authentication/Two-Factor Authentication 566
Authorization 566
Accountability 567
RADIUS and TACACS+ 568
RADIUS 568
TACACS+ 570
Understanding Cryptography Keys 570
Kerberos Authentication 572
Public Key Infrastructure  573
Components of a PKI  574
Certificates  575
Certificate Stores  576
Trusts  576
Certificate Authorities (CAs)  577
Public CAs  577
Private CAs  577
Network Access Control  578
Mandatory Access Control (MAC)  578
Discretionary Access Control (DAC)  579
Rule-Based Access Control (RBAC)  579
Role-Based Access Control (RBAC)  579
Remote Authentication Protocols  580
Using Secure Protocols  581
Malicious Software  582
Malware Distribution  583
Malware Payloads  584
More About Viruses  585
More About Trojan Horses and Worms  586
Comparing Malware Types  586
Types of Attacks  587
Denial of Service and Distributed Denial of Service Attacks  587
Other Common Attacks  589
An Ounce of Prevention  590
Maintaining Operating System Software  592
Reasons to Use a Service Pack  593
When to Use a Service Pack  593
How to Apply a Service Pack  594
Server Patches  595
Summary  596

Appendix A  Answers to the Review Questions  605

Index  639

Elements on the CD-ROM:

Appendix B  Memory Tables

Appendix C  Memory Tables Answer Key

Glossary
About the Author

Mike Harwood (MCSE, A+, Network+, Server+, Linux+) has more than 14 years experience in information technology and related fields. He has held a number of roles in the IT field including network administrator, instructor, technical writer, website designer, consultant, and online marketing strategist. Mike has been a regular on-air technology contributor for CBC radio and has coauthored numerous computer books, including the Network+ Exam Cram published by Pearson.
Dedication

This book is dedicated to the grandparents: to Frank and Marlane King whose enthusiasm, support, and sense of adventure make them grandparents a father wants for his daughters, Breanna, Paige, and Delaney; and to Ellen and Stu Jones who are always supportive, wise, and eager to provide the grandchildren with adventures and lifelong memories. And of course to my loving, supportive wife, Linda, who keeps me on track.

Acknowledgments

The creation of a book is not a simple process and requires the talents and dedication from many people to make it happen. With this in mind, I would like to thank the folks at Pearson for their commitment to this project.

Specifically, I would like to say thanks to Betsy Brown for overseeing the project and keeping things moving. A special thanks to Dayna Isley for outstanding editing and focus. Let’s not forget the technical editors Chris Crayton and Tim Warner who checked and rechecked to ensure that the project stayed on target technically—a truly difficult task considering the number of facts presented and the conflicting information that seems to be part of the networking world.

Finally, I am very thankful to my family and friends who once again had to put up with me while I worked my way through another project. Hopefully, a trip to the Magic Kingdom will make it up to you.
About the Reviewers


We Want to Hear from You!

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

As an associate publisher for Que Publishing, I welcome your comments. You can email or write me directly to let me know what you did or didn’t like about this book—as well as what we can do to make our books better.

Please note that I cannot help you with technical problems related to the topic of this book. We do have a User Services group, however, where I will forward specific technical questions related to the book.

When you write, please be sure to include this book’s title and author as well as your name, 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@quepublishing.com
Mail: Dave Dusthimer
Associate Publisher
Pearson Education
800 East 96th Street
Indianapolis, IN 46240 USA
Reader Services

Visit our website and register this book at www.pearsonitcertification.com/title/9780789745590 for convenient access to any updates, downloads, or errata that might be available for this book.
This page intentionally left blank
Introduction

The CompTIA Network+ exam has become the leading introductory-level network certification available today. Network+ is recognized by both employers and industry giants such as Microsoft and Novell as providing candidates with a solid foundation of networking concepts, terminology, and skills. The Network+ exam covers a broad range of networking concepts to prepare candidates for the technologies they are likely to be working with in today’s network environments.

This book is your one-stop shop. Everything you need to know to pass the exam is in here. You do not need to take a class in addition to buying this book to pass the exam. However, depending on your personal study habits or learning style, you might benefit from buying this book and taking a class.

**Exam Preps** are meticulously crafted to give you the best possible learning experience for the particular characteristics of the technology covered and the actual certification exam. The instructional design implemented in the Exam Preps reflects the task- and experience-based nature of CompTIA certification exams. The Exam Preps provide the factual knowledge base you need for the exams but then take it to the next level, with exercises and exam questions that require you to engage in the analytic thinking needed to pass the Network+ exam.

CompTIA recommends that the typical candidate for this exam have a minimum of 9 months experience in network support and administration. In addition, CompTIA recommends that candidates have preexisting hardware knowledge such as CompTIA A+ certification.
How This Book Helps You

This book takes you on a self-guided tour of all the areas covered by the Network+ exam and teaches you the specific skills you need to achieve your certification. The book also contains helpful hints, tips, real-world examples, and exercises.

Exam Objectives and Chapter Organization

Every objective you need to know for the Network+ exam is covered in this book. Table I-1 shows the full list of exam objectives and the chapter in which they are covered. In addition to this table, each chapter begins by specifying the objectives to be covered.

<table>
<thead>
<tr>
<th>Exam Topic</th>
<th>Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 Network Technologies</td>
<td>4</td>
</tr>
<tr>
<td>1.1 Explain the function of common networking protocols</td>
<td>4</td>
</tr>
<tr>
<td>TCP</td>
<td>4</td>
</tr>
<tr>
<td>FTP</td>
<td>4</td>
</tr>
<tr>
<td>UDP</td>
<td>4</td>
</tr>
<tr>
<td>TCP/IP suite</td>
<td>4</td>
</tr>
<tr>
<td>DHCP</td>
<td>4</td>
</tr>
<tr>
<td>TFTP</td>
<td>4</td>
</tr>
<tr>
<td>DNS</td>
<td>4</td>
</tr>
<tr>
<td>HTTP(S)</td>
<td>4</td>
</tr>
<tr>
<td>ARP</td>
<td>4</td>
</tr>
<tr>
<td>SIP (VoIP)</td>
<td>4</td>
</tr>
<tr>
<td>RTP (VoIP)</td>
<td>4</td>
</tr>
<tr>
<td>SSH</td>
<td>4</td>
</tr>
<tr>
<td>POP3</td>
<td>4</td>
</tr>
<tr>
<td>NTP</td>
<td>4</td>
</tr>
<tr>
<td>IMAP4</td>
<td>4</td>
</tr>
<tr>
<td>Telnet</td>
<td>4</td>
</tr>
<tr>
<td>SMTP</td>
<td>4</td>
</tr>
<tr>
<td>SNMP2/3</td>
<td>4</td>
</tr>
<tr>
<td>ICMP</td>
<td>4</td>
</tr>
<tr>
<td>IGMP</td>
<td>4</td>
</tr>
<tr>
<td>TLS</td>
<td>4</td>
</tr>
</tbody>
</table>
1.2 Identify commonly used TCP and UDP default ports

TCP ports:
- FTP — 20, 21
- SSH — 22
- TELNET — 23
- SMTP — 25
- DNS — 53
- HTTP — 80
- POP3 — 110
- NTP — 123
- IMAP4 — 143
- HTTPS — 443

UDP ports:
- TFTP — 69
- DNS — 53
- BOOTPS/DHCP — 67
- SNMP — 161

1.3 Identify the following address formats

IPv6
IPv4
MAC addressing

1.4 Given a scenario, evaluate the proper use of the following addressing technologies and addressing schemes

Addressing technologies:
- Subnetting
- Classful vs. classless (e.g. CIDR, Supernetting)
- NAT
- PAT
- SNAT
- Public vs. private
- DHCP (static, dynamic APIPA)

Addressing schemes:
- Unicast
- Multicast
- Broadcast
1.5 Identify common IPv4 and IPv6 routing protocols

Link state:
- OSPF
- IS-IS

Distance vector:
- RIP
- RIPv2
- BGP

Hybrid:
- EIGRP

1.6 Explain the purpose and properties of routing

IGP vs. EGP
Static vs. dynamic
Next hop
Understanding routing tables and how they pertain to path selection
Explain convergence (steady state)

1.7 Compare the characteristics of wireless communication standards

802.11 a/b/g/n
- Speeds
- Distance
- Channels
- Frequency
Authentication and encryption
- WPA
- WEP
- RADIUS
- TKIP

2.0 Network Media and Topologies
### 2.1 Categorize standard cable types and their properties

**Type:**
- CAT3, CAT5, CAT5e, CAT6
- STP, UTP
- Multimode fiber, single-mode fiber
- Coaxial
  - RG-59
  - RG-6
- Serial
- Plenum vs. Non-plenum

**Properties:**
- Transmission speeds
- Distance
- Duplex
- Noise immunity (security, EMI)
- Frequency

### 2.2 Identify common connector types

- RJ-11
- RJ-45
- BNC
- SC
- ST
- LC
- RS-232

### 2.3 Identify common physical network topologies

- Star
- Mesh
- Bus
- Ring
- Point to point
- Point to multipoint
- Hybrid

### 2.4 Given a scenario, differentiate and implement appropriate wiring standards

- 568A
- 568B
- Straight vs. cross-over
- Rollover
- Loopback
### 2.5 Categorize WAN technology types and properties

**Type:**
- Frame relay
- E1/T1
- ADSL
- SDSL
- VDSL
- Cable modem
- Satellite
- E3/T3
- OC-x
- Wireless
- ATM
- SONET
- MPLS
- ISDN BRI
- ISDN PRI
- POTS
- PSTN

**Properties**
- Circuit switch
- Packet switch
- Speed
- Transmission media
- Distance
2.6 Categorize LAN technology types and properties

Types:
- Ethernet
- 10BaseT
- 100BaseTX
- 100BaseFX
- 1000BaseT
- 1000BaseX
- 10GBaseSR
- 10GBaseLR
- 10GBaseER
- 10GBaseSW
- 10GBaseLW
- 10GBaseEW
- 10GBaseT

Properties
- CSMA/CD
- Broadcast
- Collision
- Bonding
- Speed
- Distance

2.7 Explain common logical network topologies and their characteristics

- Peer to peer
- Client/server
- VPN
- VLAN
### 2.8 Install components of wiring distribution

Vertical and horizontal cross connects  
Patch panels  
66 block  
MDFs  
IDFs  
25 pair  
100 pair  
110 block  
Demarc  
Demarc extension  
Smart jack  
Verify wiring installation  
Verify wiring termination

### 3.0 Network Devices

### 3.1 Install, configure and differentiate between common network devices

Hub  
Repeater  
Modem  
NIC  
Media converters  
Basic switch  
Bridge  
Wireless access point  
Basic router  
Basic firewall  
Basic DHCP server

### 3.2 Identify the functions of specialized network devices

Multilayer switch  
Content switch  
IDS/IPS  
Load balancer  
Multifunction network devices  
DNS server  
Bandwidth shaper  
Proxy server  
CSU/DSU
3.3 Explain the advanced features of a switch
PoE
Spanning tree
VLAN
Trunking
Port mirroring
Port authentication

3.4 Implement a basic wireless network
Install client
Access point placement
Install access point
Configure appropriate encryption
Configure channels and frequencies
Set ESSID and beacon
Verify installation

4.0 Network Management

4.1 Explain the function of each layer of the OSI model
Layer 1 — physical
Layer 2 — data link
Layer 3 — network
Layer 4 — transport
Layer 5 — session
Layer 6 — presentation
Layer 7 — application

4.2 Identify types of configuration management documentation
Wiring schematics
Physical and logical network diagrams
Baselines
Policies, procedures and configurations
Regulations
4.3 Given a scenario, evaluate the network based on configuration management documentation

Compare wiring schematics, physical and logical network diagrams, baselines, policies and procedures and configurations to network devices and infrastructure

Update wiring schematics, physical and logical network diagrams, configurations and job logs as needed

4.4 Conduct network monitoring to identify performance and connectivity issues using the following:

Network monitoring utilities (e.g. packet sniffers, connectivity software, load testing, throughput testers)

System logs, history logs, event logs

4.5 Explain different methods and rationales for network performance optimization

Methods:

- QoS
- Traffic shaping
- Load balancing
- High availability
- Caching engines
- Fault tolerance

Reasons:

- Latency sensitivity
- High bandwidth applications
  - VoIP
  - Video applications
- Uptime

4.6 Given a scenario, implement the following network troubleshooting methodology

Information gathering — identify symptoms and problems

Identify the affected areas of the network

Determine if anything has changed

Establish the most probable cause

Determine if escalation is necessary

Create an action plan and solution identifying potential effects

Implement and test the solution

Identify the results and effects of the solution

Document the solution and the entire process
4.7 **Given a scenario, troubleshoot common connectivity issues and select an appropriate solution**

Physical issues:
- Cross talk
- Nearing crosstalk
- Near End crosstalk
- Attenuation
- Collisions
- Shorts
- Open impedance mismatch (echo)
- Interference

Logical issues:
- Port speed
- Port duplex mismatch
- Incorrect VLAN
- Incorrect IP address
- Wrong gateway
- Wrong DNS
- Wrong subnet mask

Issues that should be identified but escalated:
- Switching loop
- Routing loop
- Route problems
- Proxy arp
- Broadcast storms

Wireless issues:
- Interference (bleed, environmental factors)
- Incorrect encryption
- Incorrect channel
- Incorrect frequency
- ESSID mismatch
- Standard mismatch (802.11 a/b/g/n)
- Distance
- Bounce
- Incorrect antenna placement
5.0 Network Tools

5.1 Given a scenario, select the appropriate command line interface tool and interpret the output to verify functionality
   - Traceroute
   - Ipconfig
   - Ifconfig
   - Ping
   - Arp ping
   - Arp
   - Nslookup
   - Hostname
   - Dig
   - Mtr
   - Route
   - Nbtstat
   - Netstat

5.2 Explain the purpose of network scanners
   - Packet sniffers
   - Intrusion detection software
   - Intrusion prevention software
   - Port scanners

5.3 Given a scenario, utilize the appropriate hardware tools
   - Cable testers
   - Protocol analyzer
   - Certifiers
   - TDR
   - OTDR
   - Multimeter
   - Toner probe
   - Butt set
   - Punch down tool
   - Cable stripper
   - Snips
   - Voltage event recorder
   - Temperature monitor
6.0 Network Security

6.1 Explain the function of hardware and software security devices
Network based firewall
Host based firewall
IDS
IPS
VPN concentrator

6.2 Explain common features of a firewall
Application layer vs. network layer
Stateful vs. stateless
Scanning services
Content filtering
Signature identification
Zones

6.3 Explain the methods of network access security
Filtering:
   ACL
      MAC filtering
      IP filtering
Tunneling and encryption
   SSL VPN
   VPN
   L2TP
   PPTP
   IPSEC
Remote access
   RAS
   RDP
   PPPoE
   PPP
   VNC
   ICA
6.4 Explain methods of user authentication
PKI
Kerberos
AAA
  RADIUS
  TACACS+
Network access control
  802.1x
CHAP
MS-CHAP
EAP

6.5 Explain issues that affect device security
Physical security
Restricting local and remote access
Secure methods vs. unsecure methods
  SSH, HTTPS, SNMPv3, SFTP, SCP
  TELNET, HTTP, FTP, RSH, RCP, SNMPv1/2

6.6 Identify common security threats and mitigation techniques
Security threats
  DoS
  Viruses
  Worms
  Attackers
  Man in the middle
  Smurf
  Rogue access points
  Social engineering (phishing)
Mitigation techniques
  Policies and procedures
  User training
  Patches and updates
This book contains 15 chapters, plus appendixes, as follows:

- **Chapter 1, “Introduction to Computer Networking”**—Introduces some fundamental networking concepts including physical and logical network topologies and their characteristics.

- **Chapter 2, “Media and Connectors”**—Explores network media, a key network infrastructure component. The chapter includes media types and characteristics, media connectors, wiring standards, specialized wiring, and wiring distribution.

- **Chapter 3, “Networking Components and Devices”**—Covers common networking infrastructure hardware including switches, routers, and more specialized network devices, such as load balancers, multilevel switches, and more.

- **Chapter 4, “Understanding the TCP/IP Protocol Suite”**—Reviews the key individual protocols found within the TCP/IP protocol.

- **Chapter 5, “TCP/IP Addressing and Routing”**—Covers everything TCP/IP including subnetting, addressing, and more for both IPv6 and IPv4. The chapter also includes network routing and routing protocols.

- **Chapter 6, “Ethernet Networking Standards”**—Covers all the aspects of Ethernet networking standards including speeds, access methods, and other characteristics.

- **Chapter 7, “Wireless Networking”**—Reviews wireless networking including the protocols used, access points, characteristics of wireless standards, wireless troubleshooting, and securing wireless communications.

- **Chapter 8, “Wide Area Networking”**—Reviews the technologies used to create wide area networks including standards, WAN implementations, and switching methods.

- **Chapter 9, “OSI Model”**—Reviews the OSI model and maps protocols and network hardware to each level.

- **Chapter 10, “Network Performance and Optimization”**—Looks at disaster recovery, fault tolerant measures, high availability, and quality of service (QoS). It also examines uptime, latency, and high bandwidth applications.

- **Chapter 11, “Troubleshooting Procedures and Best Practices”**—Looks at the art of troubleshooting from isolating the symptoms all the way to finding the solution and documenting the procedures.

- **Chapter 12, “Command-Line Networking Tools”**—Reviews the command-line tools used in networking troubleshooting and procedures and identifies the output from each of the command-line tools.
Chapter 13, “Network Management Tools and Documentation Procedures”—Covers aspects of documentation procedures including wiring schematics and network diagrams; the chapter also reviews some network management tools including packet sniffers, cable testers, toner probes, and more.

Chapter 14, “Network Access Security”—Reviews network security hardware and procedures including firewalls, IDS and IPS, security protocols, and remote access protocols.

Chapter 15, “Security Technologies and Malicious Software”—Covers malicious software including viruses, Trojan horses, and worms. The chapter also explores authentication protocols and secure and unsecure protocols.

The following appendix is printed in the book:

Appendix A, “Answers to the Review Questions”—Includes the answers to all the review questions from Chapters 1 through 15.

The appendixes included on the CD-ROM are

Appendix B, “Memory Tables”—Holds the key tables and lists from each chapter with some of the content removed. You can print this appendix, and as a memory exercise, complete the tables and lists. The goal is to help you memorize facts that can be useful on the exams.

Appendix C, “Memory Tables Answer Key”—Contains the answer key for the exercises in Appendix B.

Glossary—Contains definitions for all the terms listed in the “Define Key Terms” section at the conclusion of Chapter 1–15.

Instructional Features

This book provides multiple ways to learn and reinforce the exam material. Following are some of the helpful methods:

Focus questions—Each chapter ends with a list of questions related to specific exam objectives to keep in mind when preparing for the exam.

Foundation topics—This main section of each chapter covers all the important information related to the exam objectives.

Key topics—An icon marks the tables, figures, and lists you need to memorize.

Key terms—A list of key terms appears at the end of each chapter. Write the definition of each key term, and check your work in the Glossary at the end of the book.
- **Exercises**—Found at the end of the chapters in the “Apply Your Knowledge” section, exercises are performance-based opportunities for you to learn and assess your knowledge.

- **Review questions**—The review questions at the end of each chapter offer an opportunity to test your comprehension of the topics discussed within the chapter.

- **Practice exam**—The CD-ROM accompanying this book includes a practice exam that tests you on all the Network+ exam topics.

### Network Hardware and Software Requirements

As a self-paced study guide, *Network+ Cert Guide* is meant to help you understand concepts that must be refined through hands-on experience. To make the most of your studying, you need to have as much background on and experience with both common operating systems and network environments as possible. The best way to do this is to combine studying with work on actual networks. These networks need not be complex; the concepts involved in configuring a network with only a few computers follow the same principles as those involved in configuring a network that has hundreds of connected systems. This section describes the recommended requirements you need to form a solid practice environment.

To fully practice some of the exam objectives, you need to create a network with two (or more) computers networked together. To do this, you need an operating system. CompTIA maintains that the exam is vendor-neutral, and for the most part, it appears to be. However, if there were a slight tilt in the exam questions, it would be toward Microsoft Windows. Therefore, you would do well to set up a small network using a Microsoft server platform such as Windows servers. In addition, you need clients with operating systems such as Windows Vista, Linux, and Mac. When you actually get into it, you might want to install a Linux server as well because you are most certainly going to work with Linux servers in the real world. The following is a detailed list of the hardware and software requirements needed to set up your network:

- A network operating system such as Windows Server or Linux
- Client operating system software such as Windows XP, Mac OS X, or Linux
- Modern PC offering up-to-date functionality including wireless support
- A minimum 1.5GB of free disk space
- A CD-ROM or DVD drive
- A network interface card (NIC) for each computer system
Network cabling such as Category 5 or higher unshielded twisted-pair
- A two-port (or more) miniport hub to create a test network
- Wireless devices

It’s easy to obtain access to the necessary computer hardware and software in a corporate business environment. It can be difficult, however, to allocate enough time within the busy workday to complete a self-study program. Most of your study time will occur after normal working hours, away from the everyday interruptions and pressures of your regular job.

Advice on Taking the Exam

Keep this advice in mind as you study:

- **Read all the material**—CompTIA has been known to include material that is not expressly specified in the objectives. This book includes additional information that is not reflected in the objectives to give you the best possible preparation for the examination—and for your real-world experiences to come.

- **Complete the exercises in each chapter**—They can help you gain experience in using the specified methodology or approach. CompTIA exams might require task- and experienced-based knowledge and require you to have an understanding of how certain network procedures are accomplished.

- **Use the review questions to assess your knowledge**—Don’t just read the chapter content; use the review questions to find out what you know and what you don’t know. If you struggle, study some more, review, and then assess your knowledge again.

- **Complete the practice exam included on the CD-ROM**—Utilize the practice exam included with this book to assess whether you have retained the information you learned in this book and are prepared to take the exam.

Remember that the primary objective is not to pass the exam but to understand the material. When you understand the material, passing the exam should be simple. Knowledge is a pyramid; to build upward, you need a solid foundation. This book and the Network+ certification are designed to ensure that you have that solid foundation.

Good luck!
This chapter covers CompTIA Network+ objectives 1.7 and 3.4. Upon completion of this chapter, you will be able to answer the following questions:

■ What are the components that create wireless networks?
■ What are the characteristics of 802.11 wireless standards?
■ How is spread spectrum technology used in wireless networking?
■ What is the function of the beacon management frame?
■ What are the factors that cause wireless interference?
■ How can wireless networks be secured?
One of the bigger changes in the networking world since the release of the previous Network+ exam is in wireless networking. Networks of all shapes and sizes incorporate wireless segments. Home wireless networking has also grown significantly in the past few years.

As you know, wireless networking enables users to connect to a network using radio waves instead of wires. Network users within range of a wireless transceiver (transmitter/receiver), known as an access point (AP), can move around an office freely without needing to plug in to a wired infrastructure. The benefits of wireless networking clearly have led to its growth.

Today, wireless local area networks (WLAN) provide a flexible and secure data communications system used to augment an Ethernet LAN or in some cases to replace it altogether. This chapter explores the many facets of wireless networking starting with some of the devices and technologies that make wireless networking possible.
Understanding Wireless Devices

In a common wireless implementation, an AP connects to the wired network from a fixed location using standard cabling. The wireless AP receives and then transmits data between the wireless LAN and the wired network infrastructure.

Client systems communicate with a wireless AP using wireless LAN adapters. Such adapters are built in to, or added to, devices such as PC cards in laptops, PDAs, or desktop computers. Wireless LAN adapters provide the communication point between the client system and the airwaves via an antenna.

This section describes the role of APs and antennas in a wireless network.

Wireless Access Point

*Wireless APs* are both a transmitter and receiver (transceiver) device used for wireless LAN (WLAN) radio signals. An AP is typically a separate network device with a built-in antenna, transmitter, and adapter. APs use the wireless infrastructure network mode to provide a connection point between WLANs and a wired Ethernet LAN. Recall from Chapter 1, “Introduction to Computer Networking,” that wireless networks use the ad-hoc network topology and the infrastructure topology. The ad hoc is a peer-to-peer network design, and the infrastructure topology uses an AP. APs also typically have several ports enabling a way to expand the network to support additional clients.

Depending on the size of the network, one or more APs might be required. Additional APs enable access to more wireless clients and expand the range of the wireless network. Each AP is limited by a *transmissions range*, which is the distance a client can be from an AP and still get a usable signal. The actual distance depends on the wireless standard used and the obstructions and environmental conditions between the client and the AP. Factors affecting wireless transmission ranges are covered later in this chapter. Figure 7.1 shows an example of an AP in a network configuration.

**NOTE:** Wireless Access Points  
An AP can also operate as a bridge connecting a standard wired network to wireless devices or as a router passing data transmissions from one access point to another.

**TIP:** AP Range  
If you use a wireless device that loses its connection, you might be too far away from the AP.
Figure 7.1  APs connect WLANs and a wired Ethernet LAN.

As mentioned, an AP is used in an infrastructure wireless network design. Used in the infrastructure mode, the AP receives transmissions from wireless devices within a specific range and transmits those signals to the network beyond. This network can be a private Ethernet network or the Internet. In infrastructure wireless networking, there can be multiple access points to cover a large area or only a single access point for a small area, such as a single home or small building.

**NOTE: An AP for All Seasons**  Because wireless networks are sometimes deployed in environments other than inside a warm, dry building, some manufacturers offer rugged versions of APs. These devices are sealed against the elements, making them suitable for placement in locations where nonrugged devices would not survive. If you implement a wireless network, consider whether using these rugged devices are warranted.

When working with wireless APs, you need to understand many terms and acronyms. In this section we define some of the more common wireless acronyms you will see both on the exam and in any wireless networking documentation.

- **Service Set Identifier (SSID)**—A network name needed to connect to a wireless AP. It is like a workgroup name used with Windows networking. 802.11 wireless networks use the SSID to identify all systems belonging to the same network. Client stations must be configured with the SSID to be authenticated to the AP. The AP might broadcast the SSID, enabling all wireless clients in the
area to see the SSID of the AP. For security reasons, APs can be configured to not broadcast the SSID or to cloak them. This means that client systems need to be given the SSID name by an administrator instead of it automatically being discovered by the client system.

**NOTE: SSIDs** One element of wireless security involves configuring the AP not to broadcast the SSID name. This configuration is done on the AP.

- **Basic Service Set (BSS)**—Refers to a wireless network that uses a single AP and one or more wireless clients connecting to the AP. Many home offices are an example of a BSS design. The BSS is an example of the infrastructure wireless topology. Wireless topologies were discussed with other network topologies in Chapter 1.

- **Extended Service Set (ESS)**—Refers to two or more BSS sets connected, therefore using multiple APs. The ESS creates WLANs or larger wireless networks and is a collection of APs and clients. Connecting BSS systems enable clients to roam between areas and maintain the wireless connection without having to reconfigure between BSSs.

- **Extended Service Set Identifier (ESSID)**—The ESSID and the SSID are used interchangeably, but there is a difference between the two. The SSID is the name used with BSS networks, and the ESSID is the network name used with an ESS wireless network design. With an ESS, not all APs necessarily use the same name.

- **Basic Service Set Identifier (BSSID)**—Refers to the MAC address of the BSS AP. The BSSID is not to be confused with the SSID, which is the name of the wireless network.

- **Basic Service Area (BSA)**—When troubleshooting or designing wireless networks, the BSA is an important consideration. The BSA refers to the coverage area of the AP. The BSA for an AP depends on many factors, including the strength of the AP antenna, interference in the area, and whether an omnidirectional or directional antenna is used.

**TIP: Know the Acronyms** Several of the acronyms provided in the preceding bulleted list are sure to be on the Network+ exam. Be sure you can identify the function of each before writing the exam.

**Wireless Antennas**

A *wireless* antenna is an integral part of overall wireless communication. Antennas come in many shapes and sizes, with each one designed for a specific purpose. Selecting the right antenna for a particular network implementation is a critical consideration and one that could ultimately decide how successful a wireless network
will be. In addition, using the right antennas can save money on networking costs because you need fewer antennas and access points.

Many small home network adapters and access points come with a nonupgradeable antenna, but higher-grade wireless devices require that you decide which antenna to use. Selecting an antenna takes careful planning and requires an understanding of what range and speed you need for a network. The antenna is designed to help wireless networks do the following:

- Work around obstacles
- Minimize the effects of interference
- Increase signal strength
- Focus the transmission, which can increase signal speed

The following sections explore some of the characteristics of wireless antennas.

**Antenna Ratings**

When a wireless signal is low and influenced by heavy interference, it might be possible to upgrade the antennas to create a more solid wireless connection. To determine the strength of an antenna, we refer to its *gain value*. But how do we determine the gain value?

Consider a huge wireless tower emanating circular waves in all directions. If you could see these waves, you would see the data waves forming a sphere around the tower. The signals around the antenna flow equally in all directions (including up and down). An antenna that does this has a 0dBi gain value and is referred to as an *isotropic antenna*. The isotropic antenna rating provides a base point for measuring actual antenna strength.

An antenna’s gain value represents the difference between the 0dBi isotropic and the power of the antenna. For example, a wireless antenna advertised as a 15dBi antenna is 15 times stronger than the hypothetical isotropic antenna. The higher the decibel figure, the higher the gain.

**NOTE:** dBi

The *dB* in the designation stands for *decibels*, and the *i* references the hypothetical isotropic antenna.

When looking at wireless antennas, remember that a higher gain value means stronger send and receive signals. In terms of performance, the general rule is that every 3dB of gain added doubles the effective power output of an antenna.

**Types of Wireless Antennas**

When selecting an antenna for a particular wireless implementation, you must determine the type of coverage used by an antenna. In a typical configuration, a wire-
less antenna can be either *omnidirectional* or *directional*. The choice between the two depends on the wireless environment.

An omnidirectional antenna is designed to provide a 360-degree dispersed wave pattern. This type of antenna is used when coverage in all directions from the antenna is required. Omnidirectional antennas are good to use when a broad-based signal is required. For example, by providing an even signal in all directions, clients can access the antenna and associated access point from various locations. Because of the dispersed nature of omnidirectional antennas, the signal is weaker overall and therefore accommodates shorter signal distances. Omnidirectional antennas are great in an environment in which there is a clear line of sight between the senders and receivers. The power is evenly spread to all points, making omnidirectional antennas well suited for home and small office applications.

Directional antennas are designed to focus the signal in a particular direction. This focused signal enables for greater distances and a stronger signal between two points. The greater distances enabled by directional antennas allow a viable alternative for connecting locations, such as two offices, in a point-to-point configuration.

Directional antennas are also used when you need to tunnel or thread a signal through a series of obstacles. This concentrates the signal power in a specific direction and enables you to use less power for a greater distance than an omnidirectional antenna. Figure 7.2 shows an example of a directional and an omnidirectional antenna beam.

![Directional antenna signal.](image-url)
NOTE: Polarization In the wireless world, polarization refers to the direction that the antenna radiates wavelengths. This direction can either be vertical, horizontal, or circular. Today, vertical antennas are perhaps the most common. As far as configuration is concerned, both the sending and receiving antennas should be set to the same polarization.

Data Rate Versus Throughput
When talking about wireless transmissions, it is important to distinguish between throughput and data rate. From time to time these terms are used interchangeably, but technically speaking, they are different. As shown later in this chapter, each wireless standard has an associated data rate. For instance, the 802.11g wireless standard lists a data rate of up to 54Mbps. This represents the potential maximum data rate at which devices using this standard can send and receive data. However, in network data transmissions, many factors prevent the data rate from reaching this end-to-end theoretical maximum. For instance, data packets include overhead such as routing information, checksums, and error recovery data. Although this might all be necessary, it can impact overall data rate.

The number of clients on the network can also impact the data rate; the more clients, the more collisions. Depending on the network layout, collisions can have a significant impact on end-to-end transmission. Wireless network signals degrade as they pass through obstructions such as walls or doors; the signal speed deteriorates with each obstruction.

All these factors leave us with the actual throughput of wireless data transmissions. Throughput represents the actual transfer rate to expect from wireless transmissions. In practical application, wireless transmissions will be approximately one-half or less of the listed data rate. This means that we could hope for about 20–25Mbps for 802.11g and not the listed rate of 54Mbps. Depending on the wireless setup, the transmission rate could be much less.

802.11 Wireless Standards
802.11 represents the IEEE designation for wireless networking. Several wireless networking specifications exist under the 802.11 banner. The Network+ objectives focus on 802.11, 802.11a, 802.11b, 802.11g, and 802.11n. All these standards use the Ethernet protocol and the CSMA/CA access method.

NOTE: CSMA/CA CSMA/CA defines a media access method for wireless networking. CSMA/CA was discussed in Chapter 6, “Ethernet Networking Standards.”
The 802.11 wireless standards can differ in terms of speed, transmission ranges, and frequency used but are similar in terms of actual implementation. All standards can use either an infrastructure or ad-hoc network design, and each can use the same security protocols. The ad-hoc and infrastructure wireless topologies were discussed in Chapter 1.

The IEEE 802.11 standards include

- **IEEE 802.11**—There were two variations on the initial 802.11 wireless standard. Both offered 1 or 2Mbps transmission speeds and the same radio frequency (RF) of 2.4GHz. The difference between the two was in the way in which data traveled through the RF media. One used frequency hopping spread spectrum (FHSS), and the other used direct sequence spread spectrum (DSSS). These technologies are discussed in the next section. The original 802.11 standards are far too slow for modern networking needs and are now no longer deployed.

- **IEEE 802.11a**—In terms of data rate, the 802.11a standard was far ahead of the original 802.11 standards. 802.11a specifies data rates of up to 54Mbps, but communications typically take place at 6Mbps, 12Mbps, or 24Mbps. 802.11a is not compatible with other wireless standards 802.11b and 802.11g.

- **IEEE 802.11b**—The 802.11b standard provides for a maximum transmission data rate of 11Mbps. However, devices were designed to be backward compatible with previous standards that provided for speeds of 1, 2, and 5.5Mbps. 802.11b offers a transmission range of up to 100ft with 11Mbps data rate and 300ft operating a 1Mbps data rate. 802.11b uses a 2.4GHz RF range and is compatible with 802.11g.

- **IEEE 802.11g**—802.11g is a popular wireless standard today. On average, 802.11g offers wireless transmission over distances of 150 feet and a data rate of 54Mbps compared with the 11Mbps of the 802.11b standard. Like 802.11b, 802.11g operates in the 2.4GHz range and is therefore compatible with it.

- **IEEE 802.11n**—The newest of the wireless standards listed in the Network+ objectives is 802.11n. The goal of the 802.11n standard is to significantly increase throughput in both the 2.4 GHz and the 5 GHz frequency range. The baseline goal of the standard is to reach speeds of 100 Mbps but given the right conditions, it is estimated that the 802.11n data rates might reach a staggering 600 Mbps. In practical operation, 802.11n speeds will be much less.

Table 7.1 highlights the characteristics of the various 802.11 wireless standards.
Table 7.1 802.11 Wireless Standards

<table>
<thead>
<tr>
<th>IEEE Standard</th>
<th>Frequency/ Media</th>
<th>Speed</th>
<th>Topology</th>
<th>Transmission Range</th>
<th>Access Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11</td>
<td>2.4GHz RF</td>
<td>1 to 2Mbps</td>
<td>Ad hoc/ infrastructure</td>
<td>20 feet indoors.</td>
<td>CSMA/CA</td>
</tr>
<tr>
<td>802.11a</td>
<td>5GHz</td>
<td>Up to 54Mbps</td>
<td>Ad hoc/ infrastructure</td>
<td>25 to 75 feet indoors; range can be affected by building materials.</td>
<td>CSMA/CA</td>
</tr>
<tr>
<td>802.11b</td>
<td>2.4GHz</td>
<td>Up to 11Mbps</td>
<td>Ad hoc/ infrastructure</td>
<td>Up to 150 feet indoors; range can be affected by building materials.</td>
<td>CSMA/CA</td>
</tr>
<tr>
<td>802.11g</td>
<td>2.4GHz</td>
<td>Up to 54Mbps</td>
<td>Ad hoc/ infrastructure</td>
<td>Up to 150 feet indoors; range can be affected by building materials.</td>
<td>CSMA/CA</td>
</tr>
<tr>
<td>802.11n</td>
<td>2.4GHz/5GHz</td>
<td>Up to 600Mbps</td>
<td>Ad hoc/ infrastructure</td>
<td>175+ feet indoors; range can be affected by building materials.</td>
<td>CSMA/CA</td>
</tr>
</tbody>
</table>

Want More Wireless?

Wireless developments continue at a rapid pace. Though not specifically outlined in the objectives, IEEE 802.15 and IEEE 802.16 are other wireless standards worth mentioning. 802.15 is a wireless standard specifying characteristics for wireless personal area networks (WPAN). The original 802.15 version specified technologies for WPANs such as those using the Bluetooth standard. Bluetooth is often used to provide wireless links between portable digital devices, including notebook computers, peripherals, cellular telephones, beepers, and consumer electronic devices. 802.16 specifies standards for broadband wireless communications using metropolitan area networks (MAN). The original 802.16 standard identified a fixed point-to-multipoint broadband wireless system operating in the 10–66GHz licensed spectrum. The 802.16a specified non-line-of-sight extensions in the 2–11GHz spectrum, delivering up to 70Mbps at distances up to 31 miles. Known as the WirelessMAN specification, 802.16 standards with faster speeds can accommodate bandwidth demanding applications. Further, the increased range of up to 30 miles provides a true end-to-end solution.

802.16 standards are in a position to take wireless to the next level. Imagine using high-speed wireless links to establish a connection backbone between geographically separate locations. This could replace cumbersome and expensive solutions used today such as T1 or T3 links. Another version of 802.16, 802.16e is expected to enable connections for mobile devices.
The Magic Behind 802.11n

Following on the heels of 802.11g is the 802.11n standard. It is significantly faster and travels greater distances than its predecessor. But how is this done? 802.11n takes the best from the 802.11 standards and mixes in some new features to take wireless to the next level. First among these new technologies is multiple input multiple output (MIMO).

MIMO is unquestionably the biggest development for 802.11n and the key to the new speeds. Essentially, MIMO uses multiplexing to increase range and speed of wireless networking. Multiplexing is a technique that combines multiple signals for transmission over a single line or media. MIMO enables the transmission of multiple data streams traveling on different antennas in the same channel at the same time. A receiver reconstructs the streams that have multiple antennas as well. By using multiple paths, MIMO provides a significant capacity gain over conventional single antenna systems, along with more reliable communication.

In addition to all these improvements, 802.11n enables channel bonding that will essentially double the data rate again. The 802.11b and 802.11g wireless standards use a single channel to send and receive information. With channel bonding, it is possible to use two channels at the same time. As you might guess, the capability to use two channels at once increases performance. It is expected that bonding can help increase wireless transmission rates from the 54Mbps offered with the 802.11g standards to a theoretical maximum of 600Mbps.

**NOTE:** *Channel Surfing*  In wireless networking a single channel is 20MHz in width. When two channels are bonded they are a total of 40MHz. 802.11n systems can use either the 20MHz channels or the 40MHz channel.

Wireless Radio Channels

Radio frequency (RF) channels are important parts of wireless communications. A channel is the band of RF used for the wireless communication. Each IEEE wireless standard specifies the channels that can be used. The 802.11a standard specifies radio frequency ranges between 5.15 and 5.875GHz. In contrast, 802.11b and 802.11g standards operate between the 2.4 to 2.4835GHz range.

**NOTE:** *That Hertz*  Hertz (Hz) is the standard of measurement for radio frequency. Hertz is used to measure the frequency of vibrations and waves, such as sound waves and electromagnetic waves. One hertz is equal to one cycle per second (1Hz). Radio frequency is measured in kilohertz (one thousand cycles per second), megahertz (one million cycles per second), or gigahertz (one billion cycles per second).

As far as channels are concerned, 802.11a has a wider frequency band, enabling more channels and therefore more data throughput. As a result of the wider band,
802.11a supports up to eight nonoverlapping channels. 802.11b/g standards use the smaller band and support only up to three nonoverlapping channels.

It is recommended that the nonoverlapping channels be used for communication. In the United States, 802.11b/g use 11 channels for data communication; three of these—channels 1, 6, and 11—are nonoverlapping channels. Most manufacturers set their default channel to one of the nonoverlapping channels to avoid transmis-
sion conflicts. With wireless devices, you have the option of selecting which chan-
nel your WLAN operates on to avoid interference from other wireless devices that
operate in the 2.4GHz frequency range.

When troubleshooting a wireless network, be aware that overlapping channels can
disrupt the wireless communications. For example, in many environments, APs are
inadvertently placed close together—perhaps two access points in separate offices
located next door to each other or between floors. Signal disruption can result if
channel overlap exists between the access points. The solution is to try to move
the access point to avoid the problem with the overlap, or change channels to one
of the other nonoverlapping channels—for example, switch from channel 6 to
channel 11.

You would typically change the channel of a wireless device only if a channel over-
lap occurs with another device. If a channel must be changed, it must be changed
to another nonoverlapping channel.

**NOTE: Troubleshooting Utilities** When troubleshooting a wireless problem
in Windows, you can use the `ipconfig` command to see the status of IP configura-
tion. Similarly, you can use the `ifconfig` command in Linux. In addition, Linux
users can use the `iwconfig` command to view the state of your wireless network
adapter. Using `iwconfig`, you can view such important information as the link quali-
ty, AP MAC address, data rate, and encryption keys, which can be helpful in ensur-
ing that the parameters within the network are consistent.

**TIP: Channel Separation** IEEE 802.11g/b wireless systems communicate with
each other using radio frequency signals in the band between 2.4GHz and 2.5GHz.
Neighboring channels are 5MHz apart. Applying two channels that enable the
maximum channel separation can decrease the amount of channel cross talk and
provide a noticeable performance increase over networks with minimal channel separation.

Table 7.2 outlines the available wireless channels. When deploying a wireless net-
work, it is recommended that you use channel 1, grow to use channel 6, and add
channel 11 when necessary, because these three channels do not overlap.
Table 7.2  RF Channels for 802.11b/g

<table>
<thead>
<tr>
<th>Channel</th>
<th>Frequency Band</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2412MHz</td>
</tr>
<tr>
<td>2</td>
<td>2417MHz</td>
</tr>
<tr>
<td>3</td>
<td>2422MHz</td>
</tr>
<tr>
<td>4</td>
<td>2427MHz</td>
</tr>
<tr>
<td>5</td>
<td>2432MHz</td>
</tr>
<tr>
<td>6</td>
<td>2437MHz</td>
</tr>
<tr>
<td>7</td>
<td>2442MHz</td>
</tr>
<tr>
<td>8</td>
<td>2447MHz</td>
</tr>
<tr>
<td>9</td>
<td>2452MHz</td>
</tr>
<tr>
<td>10</td>
<td>2457MHz</td>
</tr>
<tr>
<td>11</td>
<td>2462MHz</td>
</tr>
</tbody>
</table>

**NOTE: Why Do They Overlap?** When looking at Table 7.2, remember that the RF channels listed (2412 for channel 1, 2417 for 2, and so on) are actually the center frequency that the transceiver within the radio and access point uses. There is only 5MHz separation between the center frequencies, and an 802.11b signal occupies approximately 30MHz of the frequency spectrum. As a result, data signals fall within about 15MHz of each side of the center frequency and overlap with several adjacent channel frequencies. This leaves you with only three channels (channels 1, 6, and 11 for the United States) that you can use without causing interference between access points.

Table 7.3 shows the channel ranges for 802.11a; 802.11n has the option of using both channels used by 802.11a and b/g.

Table 7.3  RF Channels for 802.11a

<table>
<thead>
<tr>
<th>Channel</th>
<th>Frequency Band</th>
</tr>
</thead>
<tbody>
<tr>
<td>36</td>
<td>5180MHz</td>
</tr>
<tr>
<td>40</td>
<td>5200MHz</td>
</tr>
<tr>
<td>44</td>
<td>5220MHz</td>
</tr>
<tr>
<td>48</td>
<td>5240MHz</td>
</tr>
<tr>
<td>52</td>
<td>5260MHz</td>
</tr>
<tr>
<td>56</td>
<td>5280MHz</td>
</tr>
</tbody>
</table>
**NOTE: War Driving**  
The advent of wireless networking has led to a new phenomenon: *war driving*. Armed with a laptop with an 802.11 capable wireless NIC, it is possible to drive around metropolitan areas seeking out wireless networks. When one is found, users can attempt to gain access to the network over the wireless connection. Such practices are illegal, although little can be done to prevent them other than using the built-in security features of 802.11. The problem is, not many installations use these features. If you are responsible for a network that has a wireless element, be sure to implement all the security features available. Not doing so is tantamount to allowing anyone into your building and letting him use one of your PCs to access the server.

## Spread Spectrum Technology

*Spread spectrum* refers to the manner in which data signals travel through a radio frequency. With spread spectrum, data does not travel straight through a single RF band; this type of transmission is known as *narrowband transmission*. Spread spectrum requires that data signals either alternate between carrier frequencies or constantly change their data pattern. Although the shortest distance between two points is a straight line (narrowband), spread spectrum is designed to trade off bandwidth efficiency for reliability, integrity, and security. Spread spectrum signal strategies use more bandwidth than in the case of narrowband transmission, but the trade-off is a data signal that is clearer and easier to detect. This chapter reviews three types of spread spectrum technologies: frequency hopping, direct sequence, and Orthogonal Frequency Division Multiplexing (OFDM).

### Frequency-Hopping Spread Spectrum (FHSS) Technology

Frequency-Hopping Spread Spectrum (FHSS) requires the use of narrowband signals that change frequencies in a predictable pattern. The term *frequency hopping* refers to hopping of data signals between narrow channels. For example, consider the 2.4GHz frequency band used by 802.11b. This range is divided into 70 narrow channels of 1MHz each. Somewhere between 20 and several hundred milliseconds, the signal hops to a new channel following a predetermined cyclical pattern.

Because data signals using FHSS switch between RF bands, they have a strong resistance to interference and environmental factors. The FHSS signal strategy makes it well suited for installations designed to cover a large geographical area and where the use of directional antennas to minimize the influence of environmental factors is not possible.
FHSS is not the preferred spread spectrum technology for today’s wireless standards. However, FHSS is used for some lesser-used standards and for cellular deployments for fixed Broadband Wireless Access (BWA), where the use of DSSS is virtually impossible because of its limitations.

Direct-Sequence Spread Spectrum (DSSS) Technology

With Direct-Sequence Spread Spectrum (DSSS) transmissions, the signal is spread over a full transmission frequency spectrum. For every bit of data sent, a redundant bit pattern is also sent. This 32-bit pattern is called a chip. These redundant bits of data provide for both security and delivery assurance. Transmissions are safe and reliable because the system sends so many redundant copies of the data, and only a single copy is required to have complete transmission of the data or information. DSSS can minimize the effects of interference and background noise.

As for a comparison between the two, DSSS has the advantage of providing higher security and signal delivery than FHSS, but it is a sensitive technology, affected by many environmental factors.

Orthogonal Frequency Division Multiplexing

Orthogonal Frequency Division Multiplexing (OFDM) is a transmission technique that transfers large amounts of data over 52 separate, evenly spaced frequencies. OFDM splits the radio signal into these separate frequencies and simultaneously transmits them to the receiver. By splitting the signal and transferring over different frequencies, the amount of cross talk interference is reduced. OFDM is associated with 802.11a, 802.11g amendments, and 802.11n wireless standards.

FHSS, DSSS, OFDM, and 802.11 Standards

The original 802.11 standard had two variations, both offering the same speeds but differing in the RF spread spectrum used. One of the original 802.11 standards used FHSS. This 802.11 variant used the 2.4GHz radio frequency band and operated with a 1 or 2Mbps data rate. Since this original standard, wireless implementations have favored DSSS.

The second 802.11 variation uses DSSS and specifies a 2Mbps peak data rate with optional fallback to 1Mbps in noisy environments. 802.11, 802.11b, and 802.11g use the DSSS spread spectrum. This means that the underlying modulation scheme is similar between each standard, enabling all DSSS systems to coexist with 2, 11, and 54Mbps 802.11 standards. As a comparison, it is like the migration from the older 10Mbps Ethernet networking to the more commonly implemented 100Mbps standard. The speed was different, but the underlying technologies were similar, enabling for an easier upgrade.

Table 7.4 provides a comparison of wireless standards and spread spectrum used.
Chapter 7: Wireless Networking

Beacon Management Frame

Within wireless networking is a frame type known as the beacon management frame (beacon). Beacons are an important part of the wireless network because it is their job to advertise the presence of the access point so systems can locate it. Wireless clients automatically detect the beacons and attempt to establish a wireless connection to the AP.

The beacon frame is sent out by the AP in an infrastructure network design. Client stations will send out beacons only if connected in an ad-hoc network design. There are several parts of the beacon frame, all of which are used by the client system to learn about the AP before attempting to join the network. This information includes the following:

- **Channel information**—The channel used by the AP.
- **Supported data rates**—The data transfer rates identified by the AP configuration.
- **SSID**—The name of the wireless network name.
- **Time stamp**—Synchronization information. The time stamp is used by the client system to synchronize its clock with the AP.

These beacons are transmitted from the AP about every 10 seconds. The beacon frames add overhead to the network; therefore, some APs enable you to reduce the amount of beacons sent. With home networks, constant beacon information is not necessary.

Before a client system can attempt to connect to an AP, it must first locate it. There are two methods for AP discovery: passive and active. In passive detection, the client system listens for the beacon frames to discover the AP. After it is detected, the beacon frame provides the information necessary for the system to access the AP.
With active scanning, the client station transmits another type of management frame known as a *probe request*. The probe request goes out from the client system looking for a specific SSID or any SSID within its area. After the probe request is sent, all APs in the area with the same SSID reply with another frame, the *probe response*. The information contained in the probe response is the same information included with the beacon frame. This information enables the client to access the system.

**TIP: Beacon**  Be prepared to identify the role of wireless beacons on the Network+ exam.

### Configuring and Troubleshooting the Wireless Connection

Now that we have reviewed key wireless settings, let’s take a look at an actual wireless connection configuration. Figure 7.3 shows the configuration screen of a wireless access point.

![Figure 7.3 Wireless configuration information.](image)

As you can see from the screen capture, the settings for this wireless router are clearly laid out. For instance, you can see that the wireless connection uses an SSID password of Gigaset602 and wireless channel 11. Each wireless access point might differ in the layout but all have similar configuration options.

The configuration screen on a wireless AP enables you to adjust many settings for troubleshooting or security reasons. This section identifies some of the common settings and terms used on an AP.
SSID—This configuration uses an SSID of Gigaset602. The SSID can be changed in a large network to help identify its location or network segment. For troubleshooting, if a client cannot access a base station, make sure that they are both using the same SSID. Incompatible SSIDs are sometimes found when clients move computers, such as laptops, between different wireless networks. They obtain an SSID from one network, and, if the system is not rebooted, the old SSID won’t enable communication to a different base station.

Channel—This connection is set to use channel 11. To access this network, all systems must use this channel. If needed, the channel can be changed using the drop-down menu. The menu lists channels 1 through 11.

SSID broadcast—In their default configuration, wireless access points typically broadcast the SSID name into the air at regular intervals. This feature of SSID broadcast is intended to enable clients to easily discover the network and roaming between WLANs. The problem with SSID broadcasting is that it makes it a little easier to get around security. SSIDs are not encrypted or protected in any way. Anyone can snoop and get a look at the SSID and attempt to join the network.

Authentication—Typically, you can set three options for the authentication to be used:
- **WEP-open**—The simplest of the three authentications methods because it does not perform any type of client verification. It is a weak form of authentication because there is no proof of identity.
- **WEP-shared**—Requires that a WEP key be configured on both the client system and the access point. This makes authentication with WEP-shared mandatory and therefore more secure for wireless transmission.
- **WPA-PSK**—Wi-Fi Protected Access with Pre-Shared Key (WPA-PSK) is a stronger form of encryption in which keys are automatically changed and authenticated between devices after a specified period of time or after a specified number of packets has been transmitted.

Wireless Mode—To access the network, the client must use the same wireless mode as the AP. Today most users configure the network for 802.11g/n for the faster speeds or a combination of 802.11b/g/n because they are compatible.

DTIM Period—Wireless transmissions can broadcast to all systems; that is, they can send messages to all clients on the wireless network. Multiple broadcast messages are known as multicast or broadcast traffic. Delivery traffic indication message (DTIM) is a feature used to ensure that when the multicast or broadcast traffic is sent, all systems are awake to hear the message. The DTIM setting specifies how often the DTIM message is sent within the beacon frame. The DTIM setting by default is 1. This means that the DTIM message
will be sent with every beacon. If the DTIM is set to 3, every third beacon will include a wake up call.

- **Maximum Connection Rate**—The transfer rate is typically set to Auto by default. This enables the maximum connection speed. However, it is possible to drop the speed down to increase the distance that the signal travels and boost signal strength due to poor environmental conditions.

- **Network Type**—This is where the network can be set to use the ad-hoc or infrastructure network design.

**NOTE:** **Roaming Around** The 802.11 standards enable a wireless client to roam between multiple APs. An AP transmits a beacon signal every so many milliseconds and includes a time stamp for client synchronization and an indication of supported data rates. A client system uses the beacon message to identify the...
strength of the existing connection to an AP. If the connection is too weak, the roaming client attempts to associate itself with a new AP. This enables the client system to roam between distances and APs.

With the association process complete, the authentication process begins. After the devices associate, keyed security measures are applied before communication can take place. On many APs, authentication can be set to either authentication. The default setting is typically open authentication, which enables access with only the SSID and the correct WEP key for the AP. The problem with open authentication is that if you don’t have other protection or authentication mechanisms in place, your wireless network is totally open to intruders. When set to shared-key mode, the client must meet security requirements before communication with the AP can occur.

After security requirements are met, you have established IP-level communication. This means that wireless standard requirements have been met, and Ethernet networking takes over. Basically, a switch occurs between 802.11 to 802.3 standards. The wireless standards create the physical link to the network, enabling regular networking standards and protocols to use the link. This is how the physical cable is replaced, but to the networking technologies there is no difference between regular cable media or wireless media.

Several components combine to enable wireless communications between devices. Each of these must be configured on both the client and the AP:

- **(Extended)Service Set Identifier (SSID/ESSID)**—Whether your wireless network uses infrastructure mode or ad-hoc mode, an SSID is required. The SSID is a configurable client identification that enables clients to communicate to a particular base station. Only client systems configured with the same SSID as the AP can communicate with it. SSIDs provide a simple password arrangement between base stations and clients.

- **Wireless channel**—RF channels are important parts of wireless communications. A channel refers to the band of frequency used for the wireless communication. Each standard specifies the channels that can be used. The 802.11a standard specifies radio frequency ranges between 5.15 and 5.875GHz. In contrast, 802.11b and 802.11g/n standards operate between the 2.4 to 2.4835GHz ranges. Fourteen channels are defined in the IEEE 802.11b/g/n channel set, 11 of which are available in North America.

- **Security features**—IEEE 802.11 provides for security using two methods: authentication and encryption. Authentication refers to the verification of the client system. In the infrastructure mode, authentication is established between an AP and each station. Wireless encryption services must be the same on the client and the AP for communication to occur.
NOTE: Default Settings Wireless devices ship with default SSIDs, security settings, channels, passwords, and usernames. To protect yourself, it is strongly recommended that you change these default settings. Today, many Internet sites list the default settings used by manufacturers with their wireless devices. This information is used by people who want to gain unauthorized access to your wireless devices.

Troubleshooting Wireless Signals

Because wireless signals travel through the atmosphere, they are susceptible to different types of interference than standard wire networks. Interference weakens wireless signals and is therefore an important consideration when working with wireless networking.

Interference is unfortunately inevitable, but the trick is to minimize the levels of interference. Wireless LAN communications are typically based on radio frequency signals that require a clear and unobstructed transmission path.

The following are some factors that cause interference:

- **Physical objects**—Trees, masonry, buildings, and other physical structures are some of the most common sources of interference. The density of the materials used in a building’s construction determines the number of walls the RF signal can pass through and still maintain adequate coverage. Concrete and steel walls are particularly difficult for a signal to pass through. These structures will weaken or at times completely prevent wireless signals.

- **Radio frequency interference**—Wireless technologies such as 802.11b/g use an RF range of 2.4GHz, and so do many other devices, such as cordless phones, microwaves, and so on. Devices that share the channel can cause noise and weaken the signals.

- **Electrical interference**—Electrical interference comes from devices such as computers, refrigerators, fans, lighting fixtures, or any other motorized devices. The impact that electrical interference has on the signal depends on the proximity of the electrical device to the wireless access point. Advances in wireless technologies and in electrical devices have reduced the impact these types of devices have on wireless transmissions.

- **Environmental factors**—Weather conditions can have a huge impact on wireless signal integrity. Lightning, for example, can cause electrical interference, and fog can weaken signals as they pass through.

Many wireless implementations are found in the office or at home. Even when outside interference such as weather is not a problem, plenty of wireless obstacles exist around the office. Table 7.5 highlights a few examples to be aware of when implementing a wireless network indoors.
NOTE: **Wireless and Water**  Water is a major interference factor for 2.4GHz wireless networks because water molecules resonate at the frequency in the 2.4GHz band. Interestingly, microwaves cause water molecules to resonate during cooking, which interferes with 2.4GHz RF.

### Site Surveys

When placing a wireless access point when troubleshooting wireless signals, a wireless site survey is recommended. The wireless site survey is an important first step in the deployment of a wireless network; it enables the administrator to identify the wireless signal coverage area, potential interference area, and channel overlap and helps determine the best place to put an access point. Without the wireless site survey, it is blind placement.

A site survey will often include two key elements: a visual inspection and an RF inspection. A visual inspection of an area helps the administrator identify elements that might limit the propagation of wireless signals. This can include mirrors, concrete walls, metal racks, and more. The visual survey helps isolate the potential location of the AP.

In addition to the visual survey, testing software on laptops and handheld wireless survey devices can be used to test the signal integrity. These devices test for cover-
CompTIA Network+ (N10-004) Cert Guide

age voids, map any signal leakage from your building, discover the existence and
dislocation of rogue access points, channel overlaps, determine effects of neighboring
access points, and more. Without using such a device, it would be impossible to
detect unforeseen wireless deployment problem areas. For this reason, site surveys
are one of the first steps in the deployment of any wireless networks.

Troubleshooting AP Coverage

Like any other network media, APs have a limited transmission distance. This lim-
itation is an important consideration when deciding where an AP should be placed
on the network. When troubleshooting a wireless network, pay close attention to
the distance client systems are from the AP.

When faced with a problem in which client systems cannot consistently access
the AP, you could try moving the AP to better cover the area, but then you might
disrupt access for users in other areas. So what can be done to troubleshoot AP
coverage?

Depending on the network environment, the quick solution might be to throw
money at the problem and purchase another AP, cabling, and other hardware to
expand the transmission area. However, you can try a few options before installing
another wireless AP. The following list starts with the least expensive solution and
progresses to the most expensive:

- **Increase transmission power**—Some APs have a setting to adjust the trans-
mssion power output. By default, most of these settings will be set to the max-
imum output; however, it is worth verifying just in case. As a side note, the
transmission power can be decreased if you try to reduce the dispersion of ra-
dio waves beyond the immediate network. Increasing the power provides
clients stronger data signals and greater transmission distances.

- **Relocate the AP**—When wireless client systems suffer from connectivity prob-
lems, the solution can be as simple as relocating the AP to another location. It
might be that it is relocated across the room, a few feet away, or across the
hall. Finding the right location will likely take a little trial and error.

- **Adjust or replace antennas**—If the AP distance is not sufficient for some net-
work clients, it might be necessary to replace the default antenna used with
both the AP and the client with higher-end antennas. Upgrading an antenna
can make a big difference in terms of transmission range. Unfortunately, not
all APs have replaceable antennas.

- **Signal amplification**—RF amplifiers add significant distance to wireless signals.
An RF amplifier increases the strength and readability of the data transmis-
sion. The amplifier provides improvement of both the received and transmitted
signals, resulting in an increase in wireless network performance.
■ **Use a repeater**—Before installing a new AP, you might first want to think about a wireless repeater. When set to the same channel as the AP, the repeater takes the transmission and repeats it. So, the AP transmission gets to the repeater and then the repeater duplicates the signal and passes it forward. It is an effective strategy to increase wireless transmission distances.

**NOTE: Signal Strength** Wireless signals degrade depending on the construction material used. Signals passing through concrete and steel are particularly weak.

**Wireless Troubleshooting Checklist**

Poor communication between wireless devices has many potential causes. The following is a review checklist of wireless troubleshooting presented in this chapter:

■ **Auto transfer rate**—By default, wireless devices are configured to use the strongest, fastest signal. If you’re experiencing connectivity problems between wireless devices, try using the lower transfer rate in a fixed mode to achieve a more stable connection. For example, you can manually choose the wireless transfer rate and instead of using 11Mbps, the highest rate for 802.11b, try 5.5Mbps, 2Mbps, or 1Mbps. The higher the transfer rate, the shorter the connection distance.

■ **AP placement**—If signal strength is low, try moving the AP to a new location. Moving it just a few feet can make the difference.

■ **Antenna**—The default antenna shipped with wireless devices might not be powerful enough for a particular client system. Better quality antennas can be purchased for some APs, which can boost the distance the signal can go.

■ **Building obstructions**—Wireless RF communications are weakened if they have to travel through obstructions such as metal and concrete.

■ **Conflicting devices**—Any device that uses the same frequency range as the wireless device can cause interference. For example, 2.4GHz phones can cause interference with devices using the 802.11g/n standard.

■ **Wireless channels**—If connections are inconsistent, try changing the channel to another nonoverlapping channel.

■ **Protocol issues**—If an IP address is not assigned to the wireless client, an incorrect SSID or incorrect WEP settings can prevent a system from obtaining IP information.

■ **SSID**—The SSID number used on the client system must match the one used on the AP. Typically, the default SSID assigned is sufficient but might need to be changed if switching a laptop between different WLANs.
Encryption—If encryption is enabled, the encryption type on the client must match what is set up in the AP.

**TIP:** **Troubleshooting** The Network+ exam will likely test knowledge on basic wireless troubleshooting. Be sure to review this section before taking the Network+ exam.

### Securing Wireless Networks

Many strategies and protocols are used to secure LAN and WAN transmissions. What about those network transmissions that travel over the airwaves? In the past few years wireless networking has changed the look of modern networks, bringing with it an unparalleled level of mobility and a host of new security concerns.

Wireless LANs (WLANs) require new protocols and standards to handle security for radio communications. As it stands today, wireless communications represent a significant security concern. When working with wireless, you need to be aware of a few wireless security standards, including Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA-2, and 802.1X. Before we get to describing each, let's define a few terms.

### Defining Access Control, Authentication, Authorization, and Encryption

Wireless security, like all computer security, is about controlling access to data and resources. It is important to understand the difference between authentication, authorization, and access control. Though these terms are sometimes used interchangeably, they refer to distinct steps that must be negotiated successfully to determine whether a particular request for a resource will result in that resource actually being returned. This is true for both a wired and wireless network.

Access control refers to any mechanism, software or hardware, used to restrict availability to network resources. To secure a network, it is necessary to determine which users will be granted access to various resources. Access control provides the design strategies necessary to ensure that only permitted users have access to such resources. It is a fundamental concept and forms the basis of a strong and secure network environment.

Although the concept of access control is easily understood, implementing it can be complex. Access to every network resource, including files, folders, hard disks, and Internet access, must be controlled. This is a difficult task in large network environments.

**TIP:** **Access Control** The primary objective of access control is to preserve and protect the confidentiality, integrity, and availability of information, systems, and resources.
Authentication verifies the identity of the computer or user attempting to access a particular resource. Authentication is most commonly done with the presentation of credentials such as a username and a password. More sophisticated identification methods can include the use of the following:

- Smart cards
- Biometrics
- Voice recognition
- Fingerprints

Authorization determines whether the person, previously identified and authenticated, is enabled to access to a particular resource. This is commonly determined through group association; that is, a particular group might have a specific level of security clearance. For instance, a group security policy might enable the school secretaries access to some data while locking students out.

Encryption is the process of encoding the data sent over remote connections, and it involves scrambling the usernames and passwords used to gain access to the remote network. Encryption is the process of encoding data using a mathematical algorithm that makes it difficult for unauthorized users to read the data if they can intercept it. The algorithm is actually a mathematical value known as a key. The key is required to read the encrypted data. Encryption techniques use public and private keys; public keys can be shared, and private keys cannot.

A key is a binary number that has a large number of bits. As you might imagine, the bigger the number or key, the more difficult it is to guess. Today, simple encryption strategies use 40 to 56 bits. On a 40-bit encryption, there are $2^{40}$ possible keys; 56-bit encryption has $2^{56}$ possible keys. That’s a lot of keys. Remember that without the correct key, the data cannot be accessed. Although the number of keys associated with lower-grade encryption might seem amazing, they have been cracked by some high-end, specialized systems. That makes necessary higher-grade encryption: Many online transactions require 128-bit encryption, and other applications support encryption as high as 1,024 bits. (If you have time, try to calculate the key combinations for these higher-grade encryption strategies.)

### Wireless Authentication and Encryption Methods

Now that we have a better idea of what authorization, authentication, and encryption are, we can look at the protocols and methods used to achieve wireless security. As an administrator for a wireless network, you will certainly be using these security features, and you will certainly be asked questions about them on the Network+ exam.
TIP: Wireless Security  The Network+ exam will have questions about wireless security, including WEP and WPA. Be sure you can identify wireless security protocols before taking the exam.

Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) was the first attempt to keep wireless networks safe. WEP was designed to be easy to configure and implement, and originally it was hoped that WEP would provide the same level of security to wireless networks as was available to wired networks. For a time it was the best and only option for securing wireless networks.

WEP is an IEEE standard introduced in 1997 designed for securing 802.11 networks. With WEP enabled, each data packet transmitted over the wireless connection would be encrypted. Originally, the data packet was combined with a secret 40-bit number key as it passed through an encryption algorithm known as RC4. The packet was scrambled and sent across the airwaves. On the receiving end, the data packet passed through the RC4 backward, and the host received the data as it was intended. WEP originally used a 40-bit number key, but later specified 128-bit encryption, making WEP that much more robust.

WEP was designed to provide security by encrypting data from the sending and receiving devices. In a short period of time, however, it was discovered that WEP encryption was not nearly as secure as hoped. Part of the problem was that when the 802.11 standards were written, security was not the major concern it is today. As a result, WEP security was easy to crack with freely available hacking tools. From this point, wireless communication was regarded as a potentially insecure transmission media.

There are two types of WEP security: static and dynamic WEP. Dynamic and static WEP differ in that dynamic WEP changes security keys periodically, or dynamically, making it more secure. Static WEP uses the same security key ongoing. The primary security risks are associated with static WEP, which uses a shared password to protect communications. Security weaknesses discovered in static WEP means that WLANs protected by it are vulnerable to several types of threats. Freely available hacking tools make breaking into static WEP-protected wireless networks a trivial task. Unsecured WLANs are obviously exposed to these same threats as well; the difference being that less expertise, time, and resources are required to carry out the attacks.

Wi-Fi Protected Access (WPA)

Security weaknesses associated with WEP provided administrators with a valid reason to be concerned with wireless security. The need for increased wireless security was important for wireless networking to reach its potential and to bring a sense of confidence for those with sensitive data to use wireless communications. In re-
response, the Wi-Fi Protected Access (WPA) was created. WPA was designed to improve the security weaknesses of WEP and to be backward compatible with older devices using the WEP standard. WPA addressed two main security concerns:

- **Enhanced data encryption**—WPA uses a *temporal key integrity protocol (TKIP)*, which scrambles encryption keys using a hashing algorithm. Then the keys are issued an integrity check to verify that they have not been modified or tampered with during transit.

- **Authentication**—Using the Extensible Authentication Protocol (EAP), WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

WPA was designed to address the security shortcomings of WEP by introducing support for mutual authentication and using the Temporal Key Integrity Protocol (TKIP) for data encryption. TKIP is discussed in the next section. The security features of WPA have been improved upon with WPA2. WPA2 enhances security by using Advanced Encryption Standard (AES) instead of TKIP to secure network traffic making it more secure. AES, also known as Rijndael, is a block cipher encryption standard. AES can create secure keys from 128 bit to 256 bit in length.

**NOTE:** WPA and WPA2  
WPA uses TKIP to secure wireless network traffic whereas WPA2 uses the more secure AES encryption method.

Both WPA and WPA2 are vastly more secure than WEP and, when properly secured, there are no currently known security flaws for either protocol. However, due to the AES protocol, wherever possible it is recommend to use WPA2.

**Temporal Key Integrity Protocol (TKIP)**

As mentioned previously, WEP lacked security. The Temporal Key Integrity Protocol (TKIP) was designed to address the shortcomings of the WEP security protocol. TKIP is an encryption protocol defined in IEEE 802.11i. TKIP was not only designed to increase security but also to use existing hardware, making it easy to upgrade to TKIP encryption.

TKIP is built on the original WEP security standard but enhances it by “wrapping” additional code both at the end and the beginning of the data packet. This additional code modifies the original code for additional security. Because TKIP is based on WEP, it too uses the RC4 stream encryption method, but unlike WEP, TKIP encrypts each data packet with a stronger encryption key than available with regular WEP.

TKIP provides increased security for data communications, but it is far from the final solution. TKIP provides strong encryption for home user and nonsensitive
data, but it might not provide a level of security necessary to protect corporate or more sensitive data while in transmission.

802.1X
802.1X is an IEEE standard specifying port-based network access control. 802.1X was not specifically designed for wireless networks; rather, it provides authenticated access for both wired and wireless networks. Port-based network access control uses the physical characteristics of a switched local area network (LAN) infrastructure to authenticate devices attached to a LAN port and to prevent access to that port in cases where the authentication process fails. There are three main components to the 802.1X framework:

- **Supplicant**—The system or node requesting access and authentication to a network resource.
- **Authenticator**—A control mechanism that enables or denies traffic to pass through a port.
- **Authentication server**—The authentication server validates the credentials of the supplicant trying to access the network or resource.

During a port-based network access control interaction, a LAN port adopts one of two roles: authenticator or supplicant. In the role of **authenticator**, a LAN port enforces authentication before it enables user access to the services that can be accessed through that port. In the role of **supplicant**, a LAN port requests access to the services that can be accessed through the authenticator’s port. An authentication server, which can be either a separate entity or colocated with the authenticator, checks the supplicant’s credentials on behalf of the authenticator. The authentication server then responds to the authenticator, indicating whether the supplicant is authorized to access the authenticator’s services.

The authenticator’s port-based network access control defines two logical APs to the LAN through one physical LAN port. The first logical AP, the **uncontrolled port**, enables data exchange between the authenticator and other computers on the LAN, regardless of the computer’s authorization state. The second logical AP is between an authenticated LAN user and the authenticator.

In a wireless network environment, the supplicant would typically be a network host, the authenticator could be the wireless network switch or AP, and the role of authentication server would be played by a Remote Authentication Dial-In User Service (RADIUS).

RADIUS is a protocol that enables a single server to become responsible for all remote access authentication, authorization, and auditing (or accounting) services. RADIUS functions as a client/server system. The remote user dials in to the remote access server, which acts as a RADIUS client, or network access server.
(NAS), and connects to a RADIUS server. The RADIUS server performs authentication, authorization, and auditing (or accounting) functions and returns the information to the RADIUS client (which is a remote-access server running RADIUS client software); the connection is either established or rejected based on the information received.

Securing the Access Point

Any wireless access point ships with a default configuration that is not secure. Before deploying a wireless network it is important to configure the AP not only with encryption but also to secure other settings to prevent attack. The following checklist identifies some of the settings that can be secured.

- **Changing default AP password**—The wireless AP ships with a generic password. One of the first steps is to change this public password to prevent unauthorized access to the AP.

- **SSID broadcast**—The wireless router is configured to broadcast the SSID to make it easy to find for wireless clients. It is possible to choose not to broadcast the SSID making the network invisible to detection.

- **Disabling DHCP on AP and using Static IP**—Many wireless APs distribute IP information automatically using the DHCP protocol. If someone was trying to access the AP and was successful, DHCP makes it easy for them to get a valid IP address. To help secure the AP, it is possible to disable DHCP and create static IP addresses for each legitimate device connected to it. The static IP would need to be configured on the client workstation.

- **MAC filtering**—Most APs enable for MAC filtering, which is enabling only specified MAC addresses to be authenticated to the AP. There are ways to get around MAC filtering, but the average user would not make the effort to find out how. Each client system connecting to the access point would need to have its MAC address listed in the MAC filter.

Summary

Several wireless standards fall under the 802.11 banner, including 802.11a, 802.11b, 802.11g, and 802.11n. Each of these standards has different characteristics, including speed, range, and RF used. Wireless networks are typically implemented using ad-hoc or infrastructure network design. Many types of interference can weaken the wireless signals, including weather, obstructions such as trees or walls, and RF interference.

Three types of spread spectrum technologies are reviewed in this chapter: frequency hopping, direct sequence, and Orthogonal Frequency Division Multiplexing. Each is associated with a particular wireless networking standard.
Many strategies and protocols secure wireless transmissions, including Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA, AES, and 802.1X. WEP was proven to be insecure but is still widely used. AP uses TKIP to encrypt potentially sensitive data. RADIUS also increases security and acts as an authentication server.

When configuring a wireless network, the client and the AP must be configured with the same characteristics. If the AP uses 802.11a, so must the client. The same holds true for the SSID and the security settings.

### Exam Preparation Tasks

#### Review All the Key Topics

Review the most important topics in the chapter, noted with the key topics icon in the outer margin of the page. Table 7.6 lists a reference of these key topics and the page numbers on which each is found.

<table>
<thead>
<tr>
<th>Key Topic Element</th>
<th>Description</th>
<th>Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 7.1</td>
<td>APs connect WLANs and a wired Ethernet LAN</td>
<td>247</td>
</tr>
<tr>
<td>Figure 7.2</td>
<td>Directional antenna signal</td>
<td>250</td>
</tr>
<tr>
<td>List</td>
<td>802.11 standards</td>
<td>252</td>
</tr>
<tr>
<td>Table 7.1</td>
<td>802.11 wireless standards</td>
<td>253</td>
</tr>
<tr>
<td>Table 7.2</td>
<td>RF Channels for 802.11b/g</td>
<td>256</td>
</tr>
<tr>
<td>Table 7.3</td>
<td>RF Channels for 802.11a</td>
<td>256</td>
</tr>
<tr>
<td>Table 7.4</td>
<td>Comparison of IEEE 802.11 standards</td>
<td>259</td>
</tr>
<tr>
<td>Figure 7.3</td>
<td>Wireless configuration information</td>
<td>260</td>
</tr>
<tr>
<td>Table 7.5</td>
<td>Wireless obstacles found indoors</td>
<td>265</td>
</tr>
<tr>
<td>List</td>
<td>Troubleshooting access points</td>
<td>266</td>
</tr>
<tr>
<td>List</td>
<td>Wireless troubleshooting checklist</td>
<td>267</td>
</tr>
</tbody>
</table>

### Complete the Tables and Lists from Memory

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

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

- 802.11 a/b/g/n
- AES
- AP
- Channels
- Frequency
- Authentication
- Encryption
- Authorization
- WPA
- WPA2
- WEP
- RADIUS
- TKIP
- Omnidirectional antenna
- Directional antenna
- Beaconing
- SSID
- BSS
- ESSID

Apply Your Knowledge

Exercise 7.1 Managing Wireless Security Settings in Windows Vista

You are the network administrator for a large network that has just installed several APs. The APs are configured to use WPA2, but the client stations are not.

In this exercise, you verify the encryption method used for your wireless connection. To complete this exercise, you need a functioning wireless connection.

Estimated time: 5 minutes
Complete the following steps:

1. Right-click the icon for the current wireless network connection, and click Properties.
2. When selected, the Wireless Network Properties window opens. Select the Security tab.
3. From the Security tab, use the drop-down menu to select WPA2.
4. Select OK and the client is configured to use the wireless connection and configured with the WPA2 protocol.

Exercise 7.2 Configuring a Windows XP System to Exclusively Use a Wireless Infrastructure Connection

Configuring and managing wireless connections is an increasing part of the network administrator’s role. Windows XP has built-in wizards and features to make working with wireless as easy as possible. In this exercise, we identify the setting used to determine whether a wireless connection is to be configured as an ad-hoc connection or an infrastructure connection.

This exercise assumes that the system has a wireless adapter installed.

**Estimated time:** 5 minutes

Complete the following steps:

1. In Windows XP, choose Start, Control Panel. (Use the Control Panel in Classic View for this exercise.)
2. From within the Control Panel, double-click the Network Connections Applet to open the Network Connections dialog box.
3. Right-click the wireless connection, and select Properties from the menu screen. This Wireless Network Connection Properties dialog box opens.
4. Select the Wireless Networks tab, and then click the Advanced button on the lower-right side of the dialog box.
5. This displays a small dialog box with three options:
   - Any Available Network (Access Point Preferred)
   - Access Point (Infrastructure) Networks Only
   - Computer-to-Computer (Ad Hoc) Networks Only
6. To configure the XP system to use only an infrastructure wireless connection, select the option button next to the Access Point (Infrastructure) Networks Only option. You need to click Close for the window and click OK for the Wireless Network Connection Properties window. If you click Close and then Cancel, the changes will be dropped.
Review Questions

You can find the answers to these questions in Appendix A.

1. Which of the following wireless protocols operates at 2.4GHz? (Select two.)
   a. 802.11a
   b. 802.11b
   c. 802.11g
   d. 802.11t

2. Under which of the following circumstances would you change the default channel on an access point?
   a. When there is a channel overlap between access points
   b. To release and renew the SSID
   c. To increase the WEP security settings
   d. To decrease WEP security settings

3. A client on your network has had no problem accessing the wireless network, but recently the client moved to a new office. Since the move she cannot access the network. Which of the following is most likely the cause of the problem?
   a. The SSID on the client and the AP are different.
   b. The SSID has been erased.
   c. The client has incorrect WEP settings.
   d. The client system has moved too far away from the access point.

4. Which of the following best describes the function of beacons?
   a. Beacons monitor for wireless security issues.
   b. Beacons advertise the presence of an access point.
   c. Beacons prevent unauthorized access into an AP.
   d. Beacons prevent unauthenticated access into an AP.

5. You have just purchased a new wireless access point that uses no WEP security by default. You change the security settings to use 128-bit encryption. How must the client systems be configured?
   a. All client systems must be set to 128-bit encryption.
   b. The client system will inherit security settings from the AP.
   c. WEP does not support 128-bit encryption.
   d. The client WEP settings have to be set to autodetect.

6. You have just been asked to configure the security settings for a new wireless network. You want the setting that offers the greatest level of security. Which of the following would you choose?
   a. WEP-open
   b. WEP-closed
   c. WEP-shared
   d. WEP-unshared
7. Which of the following best describes 802.1X?
   a. Port-based access control
   b. Wireless standard specifying 11Mbps data transfer
   c. Wireless standard specifying 54Mbps data transfer
   d. Integrity-based access control

8. You are installing a wireless network solution and require a standard that can operate using either 2.4GHz or 5GHz frequencies. Which of the following standards would you choose?
   a. 802.11a
   b. 802.11b
   c. 802.11g
   d. 802.11n

9. You are installing a wireless network solution that uses a feature known as MIMO. Which wireless networking standard are you using?
   a. 802.11a
   b. 802.11b
   c. 802.11g
   d. 802.11n

10. In the 802.1X security framework, which of the following best describes the role of supplicant?
    a. To authenticate usernames and passwords
    b. To encrypt usernames and passwords
    c. The system or node requesting access and authentication to a network resource
    d. A control mechanism that enables or denies traffic to pass through a port

11. Which of the following 802.11 standards can use the nonoverlapping channels of 1, 6, or 11? (Select two.)
    a. 802.11a
    b. 802.11b
    c. 802.11g
    d. 802.11h

12. Which of the following wireless security protocols uses TKIP?
    a. WEP-open
    b. WEP-shared
    c. WPA
    d. WPA-shared
13. Which of the following best describes the role of RADIUS?
   a. RADIUS enables a single IP address to become responsible for all remote access authentication.
   b. RADIUS enables a single server to become responsible for all remote access authentication.
   c. RADIUS encrypts all data leaving the AP.
   d. RADIUS encrypts all data leaving the remote system.

14. Which of the following is associated with OFDM?
   a. 802.11n
   b. WEP
   c. WPA
   d. 802.11b

15. A user calls to inform you that she cannot print. Upon questioning her, you determine that she has just been moved from the second floor to the third floor. She connects to the printer via a wireless router on the first floor. You need to allow the user to print but do not want to purchase another AP or disrupt other wireless users. Which of the following might you do?
   a. Move the AP to allow the client system to access the network and therefore the printer.
   b. Search for RF interference on the 2.4GHz range.
   c. Change the channel.
   d. Configure an RF repeater to forward the wireless communications.

16. You are deploying a wireless network and decide you need an antenna that provides a 360-degree dispersed wave pattern. Which of the following antennas would you select?
   a. Multipoint
   b. Unidirectional
   c. Omnidirectional
   d. Dispersal

17. You are working with a wireless network that uses channel 1 (2412MHz). What RF range would be used if you switched to channel 3?
   a. 2417
   b. 2422
   c. 2427
   d. 2408
18. You are the network administrator for a small company. Recently you added two remote clients who access the network through an AP. To increase security you decide you need to keep the network name hidden. Which of the following could you do?
   a. Enable WEP broadcast
   b. Disable WEP broadcast
   c. Enable secure SSID broadcast
   d. Disable SSID broadcast

19. Which of the following wireless standards specifies an RF of 5GHz?
   a. 802.11a
   b. 802.11b
   c. 802.11g
   d. 802.11g

20. What is the maximum network speed defined by the 802.11b standard?
   a. 100Mbps
   b. 5.5Mbps
   c. 11Mbps
   d. 10Mbps
Index

Numerics

2B+D, 301
5-4-3 rule, 229
10 Gigabit Ethernet
   10GBaseER/EW, 235
   10GBaseLR/LW, 235
   10GBaseSR/SW, 234
   10GBaseT, 236
10Base2, 228–229
10BaseFL, 230
10BaseT, 229
100BaseT4, 231
100BaseTX, 231
568A standard, 77
568B standard, 77
802.11 standards, 252–254
802.1X, 272–273
1000BaseT, 234
1000BaseX, 232–233

A

AAA
   accountability, 568
   authentication, 562
      biometrics, 565
      multifactor, 565–566
      password policies, 562–563
   tokens, 565
   authorization, 566
   RADIUS, 568–569
   TACACS+, 570
   access control, 268
   access methods, 223
      CSMA/CA, 225
      CSMA/CD, 224–225
   token passing, 226
   accountability, 568
   ACLs (access control lists), 540–541
   action plan, creating, 403–404
   ad hoc wireless networks, 27
   ad hoc wireless topology, 48
   adapter teaming, 363
   address classes, 189–190
   address resolution, DNS, 160–161
      entry types, 162
         practical implementation of, 163
   address translation, NAT, 210–211
   ADSL (Asymmetric Digital Subscriber Line), 307
   advanced switch features
      PoE, 106
      port authentication, 107
      port mirroring, 106
      trunking, 106
   AES (Advanced Encryption Standard), 271
agents (SNMP), 165
AH (authentication header), 549
antivirus software, 590–591
APIPA (Automatic Private IP Addressing), 192
application layer (OSI model), 334
application logs, 501
application-layer firewalls, 537
applying service packs, 594–595
APs (access points), 246–247
  beacons, 259–260
  configuring, 260–262
  coverage, troubleshooting, 266–267
  OSI layer of operation, 337
  security, 273
  site surveys, 265
  SSIDs, 247
archive bit, 369
ARP, 156–157
arp ping utility, 447–448
arp utility, 445–447
ARPANET, 148
association process, 262
asymmetric encryption, 571
AT commands, 119, 306
ATM, 298–299
attacks, 587, 590
  DoS, 587–589
  preventing, 590–591
attenuation, 64, 410
authentication, 263, 269, 562
  biometrics, 565
  Kerberos, 572–573
  multifactor, 565–566
  password policies, 562–563
  password strength, 563–564
  tokens, 565
authorization, 269, 566

B

backups, 368
  best practices, 373–374
  differential backups, 370
  full backups, 369
  incremental backups, 370
  methods, comparing, 371
  offsite storage, 372–373
  rotation schedules, 371
bandwidth, 63, 223, 312
bandwidth shapers, 130–131
baseband transmission, 227
baselines, 487–488
baud rate, 120
beacons, 259–260
binary numbering system, 188
biometrics, 530–531, 565
blind patching, 594
BNC connectors, 228
bonding, 226
BOOTP, 191
bps rate, 120
BRI (Basic Rate Interface), 301
bridges, 110
  implementing, 111–114
  OSI layer of operation, 336
broadband, 228, 309, 313
broadcast addresses, 193
brouters, 116
BSA, 248
BSS (Basic Service Set), 47, 248
buffering, 333
bus topology, 41–42
butt sets, 512
cable certifiers, 505–506
cable Internet access, 310–312
cable modems, 310
cable testers, 509
cabling
  coaxial, 69–70
  crossover, 78
  fiber-optic, 70–72
  horizontal, 81–82
  loopback, 80
  purchasing, 230
  rollover, 80
  standards, 77
  straight-through, 78
  troubleshooting, 407–411
  twisted-pair, 67–68
  verifying installation, 87–88
  vertical, 82

caching engines, 381–382
call-waiting, troubleshooting, 305
CANS (Controller Area Networks), 27
capturing statistics, 488
CAs (certificate authorities), 577–578
categories of twisted-pair cable, 67
centralized computing, 33
certificates, 575
  CAs, 577–578
  trusts, 576–577
channels, 254–257
checksums, 329
chromatic dispersion, 64
CIDR (classless inter-domain routing), 193
circuit switching, 290, 330
circuit-level firewalls, 537
class=X switch, 463
client/server networking model, 30–33
  client computers, 32
  servers, 31
coaxial cable, 69–70
cold sites, 375
cold spares, 375
cold swapping, 375
collisions, 410
command-line tools
  arp, 445–447
  arp ping, 447–448
  dig, 464, 466
  host, 466
  ifconfig, 460–461
  ipconfig, 457–460
  mtr, 445
  nbtstat, 455–456
  netstat, 448–454
  nslookup, 461–464
  ping, 432–433
    error messages, 437–439
    switches, 434–435
    troubleshooting procedures, 435–436
  route, 466–467
  traceroute, 439–445

communities (SNMP), 166
comparing
  backup methods, 371
  LANs and WANs, 27
  malware types, 586
component baselines, 488
configuration documentation, 490
configuring
  APs, 260–262
  wireless networking, 263
connecting to hotspots, 315–316
connection speed
modems, 119
troubleshooting, 305–306
connection-oriented protocols, 151, 332
connectionless protocols, 333
connectivity, troubleshooting, 413–415
connectors
F-Type, 73
fiber, 74
IEEE 1394, 75
RJ, 72
RS-232 standard, 74
USB, 76
content switches, 127–128
count to infinity, 207
coverage (APs), troubleshooting, 266–267
cross connects, 81
crossover cabling, 78
crosstalk, 63, 409
cryptography, 571
CSMA/CA (carrier sense multiple access/collision avoidance), 225
CSMA/CD (carrier sense multiple access/collision detection), 224–225
CSU/DSU (channel service unit/data service unit), 133
cut-through switching, 105

D
DAC (discretionary access control), 579
data link layer (OSI model), 329
data rate, 63, 251
datagram packet switching, 289–290
DCE (data communication equipment), 295
DDoS attacks, 587–589
decapsulation, 327
decentralized networking, 29
dedicated local bandwidth, 312
default gateways, 194
delivery mechanisms for malware, 583–584
demarcation point, 86–87
development of TCP/IP, 148
DHCP (Dynamic Host Configuration Protocol), 167–170, 191
DHCP servers, 126–127
DHSS, 258
dial-up Internet access, 303–305
differential backups, 370
dig utility, 464–466
directional wireless antennas, 250
disaster recovery
backup methods, 368
  best practices, 373–374
  comparing, 371
differential backups, 370
  full backups, 369
  GFS rotation, 371
  incremental backups, 370
  offsite storage, 372–373
cold sites, 375
hot sites, 376
sites, 375
warm sites, 376
disk mirroring, 355
distance-vector routing protocols, 206–208
distributed computing, 33
distributed parity, 358
DMZ (demilitarized zone), 538
DNAT (Destination Network Address Translation), 211
DNS (Domain Name System), 159–160
  entry types, 162
  practical implementation of, 163
DNS records, 463
DNS servers, 129–130
documentation, 480
  baselines, 487–488
  configuration documentation, 490
  network diagrams, 484
    logical network documentation, 486–487
    physical network documentation, 484–485
  policies, 488–489
  procedures, 489–490
  regulations, 491
  wiring schematics, 481–483
domain names, 161
DoS attacks, 587–589
drop cable, 42
DSL (Digital Subscriber Line), 307–310
DTE (data terminal equipment), 295
DUAL (Diffusing Update Algorithm), 208
dynamic addressing, 191
dynamic WEP, 270

E
  echo, troubleshooting, 410
EGPs (exterior gateway protocols), 209
EIGRP (Enhanced Interior Gateway Routing Protocol), 208
EMI (electromagnetic interference), 62, 409
  encapsulation, 327
  encryption, 263, 269, 545
  enforcing password history, 563
  error detection, 329
  escalation procedures, 403, 417–418
ESP (Encapsulating Security Payload), 549
ESS (Extended Service Set), 47, 248
ESSID (Extended Service Set ID), 248
Ethernet standards
  10Base2, 228–229
  10BaseFL, 230
  10BaseT, 229
  10GBaseER/EW, 235
  10GBaseLR/LW, 235
  10GBaseSR/SW, 234
  10GBaseT, 236
  100BaseFX, 231
  100BaseT4, 231
  100BaseTX, 231
  1000BaseT, 234
  1000BaseX, 232–233

F
  F-Type connectors, 73
  Fast Ethernet, 231
fault tolerance, 290, 351–353
  link redundancy, 363
  RAID, 353, 362
    level, selecting, 361–362
  RAID 0, 354–355
  RAID 1, 355–358
gathering information, 397–399
GFS rotation, 371
Gigabit Ethernet
  • 1000BaseT, 234
  • 1000BaseX, 232–233

H
  • half-duplex transmission, 65, 103
  • half-open connections, 150
  • hardware, troubleshooting, 411–412
  • hardware RAID, 362
  • hardware room best practices, 531–532
  • hierarchical name tree, 166
  • hierarchical star topology, 43
  • high-bandwidth applications
    • video applications, 379
    • VoIP, 378–379
  • history logs, 502
  • hold-down timers, 206
  • horizontal cross connect, 81–82
  • host addresses, 188
  • host command, 466
  • host-based firewalls, 533
  • hot sites, 376
  • hot spare drives, 360
  • hot spares, 374
  • hot swapping, 360, 374
  • hotfixes, 595
  • hotspots, 315–316
  • HTTP (HyperText Transfer Protocol), 151
  • HTTPS (HyperText Transfer Protocol Secure), 154
  • hubs, 100–102
    • indicator lights, 109
managed, 109–110
OSI layer of operation, 336
ports, 107
hybrid networks, 33
hybrid switches, 108
hybrid topologies, mesh, 51
Hz (Hertz), 254

ICMP (Internet Control Message
Protocol), 156
IDCs (insulation displacement
connectors), 84
identifying
IPv6 addresses, 201–202
TCP/IP port numbers, 173–175
identifying problems, 399–400, 402
IDF (intermediate distribution
frame), 85
IEEE 802 standards, 221
access methods, 223
CSMA/CA, 225
CSMA/CD, 224–225
token passing, 226
bonding, 226
speed, 223
IEEE 802.3 standards
10Base2, 228–229
10BaseFL, 230
10BaseT, 229
10GBaseER/EW, 235
10GBaseLR/LW, 235
10GBaseSR/SW, 234
10GBaseT, 236
100BaseFX, 231
100BaseT4, 231
100BaseTX, 231
1000BaseT, 234
1000BaseX, 232–233
IEEE 802.11 standards, 252–253
802.11n, 254
channels, 255–257
IEEE 802.1X, 272–273
IEEE 1394 standard, 75
ifconfig utility, 460–461
IGMP (Internet Group Management
Protocol), 158
IGPs (interior gateway protocols), 209
implementing bridges, 111–114
incremental backups, 370
independent routing, 288
indicator lights, 109
infrastructure wireless topology, 47
installing
media, 65
NICs, 123–124
interference, 62–63, 264–265
Internet access, 24, 285
cable, 310–312
DSL, 307–310
POTS, 303–307
satellite, 313–314
internetworks, 25
IP (Internet Protocol), 149
ipconfig command, 255
ipconfig utility, 457–460
IPS/IDS, 128, 539
IPsec
AH, 549
ESP, 549
transmission modes, 550
IPv4 addressing, 188, 198
APIPA, 192
BOOTP, 191
broadcast addresses, 193
CIDR, 193
classes, 189–190
default gateways, 194
dynamic addressing, 191
private addresses, 199–200
private IP addressing, 200
public IP addressing, 200
static addressing, 191
subnet masks, 190
subnetting, 195–198
IPv6 addressing, 201
address types, 202
addresses, identifying, 201–202
IPX/SPX (Internet Packet
Exchange/Sequenced Packet
Exchange), 146
ISDN (Integrated Services Digital
Network), 299–301
isotropic antenna, 249
iwconfig command, 255

J-K-L

Kerberos authentication, 572–573
keys, 269

L2TP (Layer 2 Transport Protocol), 548
LAN-to-LAN internetworking, 34
LANs, 25, 41
laser standards, 232
latency, 105
latency-sensitive applications
video applications, 379
VoIP, 378–379
Layer 1 (OSI model), 328–329
Layer 2 (OSI model), 329
Layer 3 (OSI model), 330–331
Layer 4 (OSI model), 332–333
Layer 5 (OSI model), 333
Layer 6 (OSI model), 333–334
Layer 7 (OSI model), 334
LDAP (Lightweight Directory Access
Protocol), 158
least privilege concept, 580
linear bus topology, 41–42
link redundancy, 363–364
link-state routing protocols, 208–209
load balancing, 129, 381
load testing, 498
lock and key access, 529
logging, 499, 503
application logs, 501
history logs, 502
security logs, 500–501
system logs, 502
logical network documentation,
486–487
logical security, 532
logical standards, 61
logical topologies, 41
long wavelength laser, 232
loopback cables, 80
LSAs (link-state advertisements), 208
MAC (mandatory access control), 578
MAC address-based VLANs, 39
MAC addresses, 103, 186–187
MAC filtering, 540
malware, 582
attacks
  DoS, 587–589
  preventing, 590–591
distribution, 583–584
payloads, 584
Trojan horses, 586
types of, comparing, 586
viruses, 585–586
worms, 586
man-in-the-middle attacks, 548, 564
managed switches, 109–110
managing processor failures, 368
MANs (Metropolitan Area Networks), 27
MDF (main distribution frame), 85
MDI (medium-dependent interface), 107
MDI-X (medium-dependent interface-crossover), 107, 311
media
cable
  categories, 67–68
  coaxial, 69–70
  fiber-optic, 70–72
  twisted-pair, 67–68
connectors
  F-Type, 73
  fiber, 74
  IEEE 1394, 75
  RJ, 72
  RS-232 standard, 74
  USB, 76
data transmission rates, 63
installing, 65
interference, 62–63
length, 63–64
media converters, 124–125
media testers
  multimeters, 511
  OTDRs, 510
  TDRs, 510
memory failures, 368
mesh topology, 45–47
mesh wireless topology, 50
message switching, 290–291, 330
metrics, 205
MIBs (management information bases), 165–166
MIMO (multiple input multiple output), 254
MMF (multi-mode fiber), 71
modems, 118–119
  AT commands, 306
cable modems, 310
  connection speeds, 119
troubleshooting, 306–307
monitoring the network
  load testing, 498
  logging, 499
    application logs, 501
    history logs, 502
    log management, 503
    security logs, 500–501
    system logs, 502
  performance testing, 498
  port scanners, 495–498
  stress testing, 499
  throughput testing, 493–495
MSAU (multistation access unit), 45
mtr utility, 445
multicast addresses, 203
multicasting, 158
 multifactor authentication, 565–566
multifunction network devices, 129
multilayer switches, 127
multimeters, 511

N

NAT (Network Address Translation), 210–211
nbtstat utility, 455–456
NetBEUI (NetBIOS Extended User Interface), 146
netstat utility, 448, 450–454
network access control
DAC, 579
MAC, 578
RBAC, 579

network access security
ACLs, 540–541
port blocking/filtering, 541–542

network addresses, 188

network administrators, responsibilities of, 527

network devices
bandwidth shapers, 130–131
bridges, 110–114
content switches, 127–128
CSUs/DSUs, 133
DHCP servers, 126–127
DNS servers, 129–130
firewalls, 125–126, 532–533
application-layer, 537
circuit-level, 537
DMZs, 538
network layer, 536–537
purpose of, 534–535
stateful/stateless, 536
gateways, 117–118
hubs, 100–102
indicator lights, 109
managed, 109–110
IPS/IDS, 128
LED indicators, 122
load balancers, 129
media converters, 124–125
modems, 118–119
multifunction network devices, 129
multilayer switches, 127
NICs, 120–124
OSI layer operation, 336–337
proxy servers, 131–133
repeaters, 110
routers, 114–117
switches, 102–103
full-duplex connections, 104
indicator lights, 109
managed, 109–110
PoE, 106
port authentication, 107
port mirroring, 106
switching methods, 105
trunking, 106
troubleshooting, 411–412

network diagrams
logical network documentation, 486–487
physical network documentation, 484–485

network layer (OSI model), 330–331

network layer firewalls, 537

network management, 492–493

network optimization

caching engines, 381–382
load balancing, 381
QoS, 377–380

network qualification testers, 512
network-based firewalls, 533
networking tools
butt sets, 512
cable certifiers, 505–506
cable testers, 509
media testers
multimeters, 511
OTDRs, 510
TDRs, 510
network qualification testers, 512
protocol analyzers, 509
punchdown tools, 505
snips, 504
temperature monitors, 506–507
toner probes, 508
voltage event recorders, 506
wire crimpers, 504
wire strippers, 504
wireless detectors, 512
networks
client/server networking model, 30–33
demarcation point, 86–87
peer-to-networking model, 28–30
VLANs, 36–37
MAC address-based, 39
membership, 37
port-based, 38
segmentation, 40
VPNs, 35–36
newsgroups, 157
NEXT (near-end crosstalk), 409
NICs (network interface cards), 120–121
installing, 123–124
LED indicators, 122
OSI layer of operation, 337
NID (Network Interface Device), 87
NNTP (Network News Transfer Protocol), 158
nslookup utility, 461–464
NTP (Network Time Protocol), 157
O
OCx (Optical Carrier) levels, 298
OFDM (orthogonal frequency-division multiplexing), 258
offsite backup storage, 372–373
omnidirectional wireless antennas, 250
operating systems
server patches, 595–596
service packs, 593–595
OSI model
application layer, 334
data link layer, 329
network layer, 330–331
physical layer, 328–329
presentation layer, 333–334
session layer, 333
transport layer, 332–333
OSI reference model, 326
devices, layer of operation, 336–337
encapsulation, 327
OTDRs (optical time-domain reflectometers), 510
overlapping channels, 255
P
packet switching, 288, 330
datagram packet switching, 289–290
virtual-circuit packet switching, 289
packets, 328
PADs (packet assemblers/disassemblers), 293
PANs (Personal Area Networks), 27
partial-octet subnetting, 196
password attacks, 589
passwords, 562–564
patch panels, 83, 505
payloads (malware), 584
peer-to-peer networking model, 28–30
performance
    testing, 498
    uptime, 350–352
physical layer (OSI model), 328–329
physical media, 61
physical network documentation, 484–485
physical security, 528–529
    biometrics, 530–531
    hardware room best practices, 531–532
    lock and key access, 529
    PIN access, 530
    swipe cards, 530
physical topologies, 41
PIN access, 530
ping, 156, 432–433
    error messages, ping command, 437–439
    switches, 434–435
    troubleshooting procedures, 435–436
Ping of Death, 588
PKI (public key infrastructure), 573–574
    certificates, 575
        CAs, 577–578
        trusts, 576–577
plenum cables, 65
PoE (Power over Ethernet), 106
polarization, 251
policies, 488–489
POP3/IMAP4, 155
port authentication, 107
port blocking/filtering, 541–542
port mirroring, 106
port numbers, identifying, 173–175
port scanners, 495–498
port speeds, setting, 415
port-based VLANs, 38
ports, 107
POTS (plain-old telephone service), 303–304
    connection speed, troubleshooting, 305–306
    modems, troubleshooting, 306–307
PPPoE (Point-to-Point Protocol over Ethernet), 544
PPP (Point-to-Point Protocol), 543–544
PPTP (Point-to-Point Tunneling Protocol), 547
presentation layer (OSI model), 333–334
preventing
    attacks, 590–591
    routing loops, 207
PRI (Primary Rate Interface), 301
private address ranges, 199–200
private addressing, 200
private CAs, 577
private networks, 198, 286–287
probable cause, establishing, 402
probe requests, 260
probe responses, 260
procedures, 489–490
processor failures, managing, 368
protocol analyzers, 509
protocol suites, 146
protocols
connection-oriented, 332
connectionless, 333
on receiving device, 147
routable, 204–205
routing protocols, 205
distance-vector, 206–208
link-state, 208–209
on sending device, 147
proxy servers, 131–133
PSTN (public switched telephone network), 284
PtMP (Point-to-Multipoint Protocol)
wireless topology, 50
PtP (Peer-to-Peer) wireless topology, 48
public CAs, 577
public IP addressing, 200
public networks, 198, 286
Internet, 285
PSTN, 284
punchdown tools, 84–85, 505

Q-R

QoS, 377–380
rack-mount devices, 109
RADIUS (Remote Authentication Dial In User Service), 272, 568–569
RADSL (Rate-Adaptive Digital Subscriber Line), 308
RAID (Redundant Array of Inexpensive Disks), 353
level, selecting, 361–362
RAID 0, 354–355
RAID 1, 355–358
RAID 5, 358–360
RAID 10, 360
RARP (Reverse Address Resolution Protocol), 156–157
rate adaptive DSL, 308
ratings of wireless antennas, 249
RBAC (role-based access control), 579
RBAC (rule-based access control), 579
reassociation, 262
recovery sites
cold sites, 375
hot sites, 376
warm sites, 376
regulations, 491
remote access protocols
PPP, 543–544
RRAS, 542
SLIP, 543
remote authentication protocols, 580–581
remote control protocols, 550
repeaters, 110
reserved IPv6 addresses, 204
responsibilities of network administrators, 527
RF channels, 254–257
RFB (remote frame buffer) protocol, 550
RFCs (Requests For Comments), 148
RG-6 cables, 73
RG-59 cables, 73
ring topology, 44
RIPv2, 208
RJ connectors, 72
rollover cables, 80
routable protocols, 204–205
route command, 466–467
route selection, 331
routers, 114–117, 336
routing loops, 207
routing protocols, 205
  distance-vector, 206, 208
  link-state, 208–209
RRAS (Routing and Remote Access Service), 542
RS-232 standard, 74
RTP (Real-time Transport Protocol), 171

S

satellite Internet access, 313–314
SCP (Service Control Point), 158
SDSL (Symmetric Digital Subscriber Line), 307
secure protocols, 581
security
  AAA
    accountability, 568
    authentication, 562–566
    authorization, 566
    RADIUS, 568–569
    TACACS+, 570
ACLS, 540–541
authentication, Kerberos, 572–573
broadband, 313
cryptography, 571
firewalls, 532–533
  application-layer, 537
  circuit-level, 537
  DMZs, 538
  network layer, 536–537
  purpose of, 534–535
  stateful/stateless, 536
  hardware room best practices, 531–532
  IPS/IDS, 128, 539
IPsec
    AH, 549
    ESP, 549
    transmission modes, 550
logical security, 532
network access control
  DAC, 579
  MAC, 578
  RBAC, 579
physical security, 528
  biometrics, 530–531
  lock and key access, 529
  PIN access, 530
  swipe cards, 530
PKI, 573–578
port blocking/filtering, 541–542
wireless networks, 268–269
  802.1X, 272–273
  APs, 273
  TKIP, 271–272
  WEP, 270
  WPA, 270–271
security logs, 500–501
segmentation, 40
selecting RAID level, 361–362
server clustering, 367–368
server failover, 366
server farms, 381
server patches, 595–596
servers, troubleshooting, 394–395
service packs, 593–595
session layer (OSI model), 333
SFTP (SSH File Transfer Protocol), 152–153
shared bandwidth, 312
short wavelength laser, 232
shorts, troubleshooting, 410
signal regeneration, 64
signaling
   baseband, 227
   broadband, 228
simplex transmission, 65
SIP (Session Initiation Protocol), 170
site local addresses, 203
site surveys, 265
SLIP (Serial Line Internet Protocol), 543
SMF (single mode fiber), 71
Smurf attacks, 588
SNAT (Source Network Address Translation), 211
snips, 504
SNMP (Simple Network Management Protocol), 153, 163–164
   agents, 165
   communities, 166
   management systems, 165
   MIBs, 165–166
social engineering, 589
software gateways, 117
software RAID, 362
solutions
   documenting, 406–407
   implementing, 404–406
SONET (Synchronous Optical Networking), 297–298
source-route bridges, 114
speed of IEEE 802 networks, 223
spread spectrum
   DHSS, 258
   FHSS, 257
   OFDM, 258
   technologies, comparing, 258
SSH (Secure Shell), 152
SSIDs (Service Set IDs), 247, 263
SSL (Secure Sockets Layer) VPNs, 546
STA (Spanning Tree Algorithm), 112
stackable devices, 109
standby servers, 366–367
star topology, 42, 44
stateful/stateless firewalls, 536
static addressing, 191
static WEP, 270
store-and-forward switching, 291
STP (Spanning Tree Protocol), 67, 114
straight-through cabling, 78
stress testing, 499
subnet masks, 188–190
subnetting, 195–198, 331
SVCs (switched virtual circuits), 289
swipe cards, 530
switches, 102–103
   advanced features, 106–107
   arp command, 446
   content, 127–128
   full-duplex connections, 104
   indicator lights, 109
   managed, 109–110
   multilayer, 127
   OSI layer of operation, 336
   ports, 107
switching, 105
   circuit switching, 290
   message switching, 290–291
   packet switching, 288–290
symmetric encryption, 546, 571
SYN flooding, 150, 588
system baselines, 488
system logs, 502
T-carrier lines, 295
   T1/E1/J1, 296–297
   T3 lines, 297
TACACS+ (Terminal Access Controller Access-Control System Plus), 570
TCP (Transmission Control Protocol), 149–150
TCP/IP, 171, 337, 339–340
   ARP, 156–157
development of, 148
   DHCP, 167–170
   DNS, 159–161
      entry types, 162
      practical implementation of, 163
   FTP, 151
   HTTP, 154
   HTTPS, 154
   ICMP, 156
   IGMP, 158
   IP, 149
   LDAP, 158
   MAC addresses, 186–187
   NNTP, 158
   NTP, 157
   POP3/IMAP4, 155
   port numbers, identifying, 173–175
   RARP, 156–157
   RTP, 171
   SCP, 158
   SFTP, 152–153
   SIP, 170
   SNMP, 153, 163–164
      agents, 165
      communities, 166
   SSH, 152
   TCP, 149–150
   Telnet, 155
   TFTP, 153
   TLS, 170
   UDP, 150
TCP/IP filtering, 540
TDM (time-division multiplexing), 227
TDRs (time-domain reflectometers), 510
Telnet, 155
temperature monitors, 506–507
termination, 87–88
TFTP (Trivial File Transfer Protocol), 153
thin client computing, 550
throughput
   testing, 493–495
   versus data rate, 251
timeouts, 150
TKIP (Temporal Key Integrity Protocol), 271–272
TLS (Transport Layer Security), 170
token passing, 226
tokens, 565
toner probes, 508
tools. See networking tools
topologies
   bus, 41–42
   hybrid, 51
   mesh, 45, 47
   ring, 44
   star, 42–44
wireless
  *ad hoc, 48*
  *infrastructure wireless, 47*
  *mesh wireless, 50*
  *PtMP wireless, 50*
  *PtP wireless, 48*
traceroute utility, 439–445
tracert command, 441–443
traffic shaping, 379–380
translational bridges, 114
transmission range, 246
transparent bridges, 114
transport layer (OSI model), 332–333
traps, 164
Trojan horses, 586
troubleshooting
  action plan, creating, 403–404
  AP coverage, 266–267
  connectivity, 413–415
  DSL, 309–310
  escalation procedures, 403, 417–418
  general considerations, 395–396
  identifying affected areas, 399–402
  information gathering, 397–399
  infrastructure hardware, 411–412
  Internet access
    *cable Internet, 311–312*
    *POTS, 304–307*
    *satellite Internet access, 314*
  probable cause, establishing, 402
  servers, 394–395
  solution, documenting, 406–407
  solution, implementing, 404–406
  VLANs, 416–417
wireless networks
  *incorrect configurations, 420–421*
  *interference, 264–265*
  *signals, 418–420*
  wiring, 407–411
workstations, 394–395
trunking, 106
trusts, 576–577
tunneling, 34, 545
  *L2TP, 548*
  *PPTP, 547*
twisted-pair cable, 67–68
two-way satellite systems, 314
type 110 punchdown block, 84–85
type 66 punchdown block, 84–85

U

UDP (User Datagram Protocol), 150
unicast addresses, 203
UPSs (uninterruptible power supplies), 364–366
uptime, 350–352
USB connectors, 76
UTP (unshielded twisted pair), 67

V

V standards, 120
verifying wiring installation, 87–88
vertical cross connect, 81–82
video applications, 379
virtual-circuit packet switching, 289
viruses, 585–586
VLANs (virtual LANs), 36
  *MAC address-based, 39*
  *membership, 37*
  *port-based, 38*
  *segmentation, 40*
  *troubleshooting, 416–417*
VNC (virtual network computing), 550
VoIP, 378–379
voltage event recorders, 506
VPN concentrators, 546
VPNs (virtual private networks), 35–36, 285, 545–546

W

WANs, 27
ATM, 298–299
circuit switching, 290
Frame Relay, 293–295
ISDN, 299–300
BRI, 301
PRI, 301
message switching, 290–291
packet switching, 288–289
datagram packet switching, 289–290
virtual-circuit packet switching, 289
SONET, 297–298
T-carrier lines, 295
T1/E1/J1, 296–297
T3, 297
X.25, 293
war driving, 257
warm sites, 376
warm swapping, 375
WEP (Wired Equivalent Privacy), 270
windowing, 333
wire crimpers, 504
wire strippers, 504
wireless antennas
directional, 250
omnidirectional, 250
polarization, 251
ratings, 249
wireless detectors, 512
wireless networking
APs
configuring, 260–262
site surveys, 265
association process, 262
authentication process, 263
beacons, 259–260
IEEE 802.11 standards, 252–254
incorrect configurations,
troubleshooting, 420–421
interference, troubleshooting, 264–265
RF channels, 254–257
security, 268–269
802.1X, 272–273
APs, 273
configuring, 263
TKIP, 271–272
WEP, 270
WPA, 270–271
signals, troubleshooting, 418–420
spread spectrum
DHSS, 258
FHSS, 257
OFDM, 258
topologies
ad hoc wireless, 48
infrastructure wireless, 47
mesh, 50
PtMP wireless, 50
PtP wireless, 48
troubleshooting checklist, 267–268
war driving, 257
WirelessMAN specification, 253
wiring, troubleshooting, 407–411
wiring closets, 85
wiring schematics, 481–483
WISP (wireless Internet service provider), 315
WLANs (wireless LANs), 315
  APs, 246–247
  wireless antennas
    directional, 250
    omnidirectional, 250
    ratings, 249
workstations, troubleshooting, 394–395
worms, 586
WPA (Wi-Fi Protected Access), 270–271
WWANs (wireless wide area networks), 315–316

X-Y-Z

X.25, 293

Zeroconf (Zero Configuration), 193
zombies, 587