



Networking for Home and Small Businesses

CCNA Discovery
Learning Guide



Allan Reid • Jim Lorenz

Networking for Home and Small Businesses

CCNA Discovery Learning Guide

Allan Reid
Jim Lorenz

Cisco Press

800 East 96th Street

Indianapolis, Indiana 46240 USA

Networking for Home and Small Businesses

CCNA Discovery Learning Guide

Allan Reid ▪ Jim Lorenz

Copyright © 2008 Cisco Systems, Inc.

Cisco Press logo is a trademark of Cisco Systems, Inc.

Published by:

Cisco Press

800 East 96th Street

Indianapolis, IN 46240 USA

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Printed in the United States of America

First Printing December 2007

Library of Congress Cataloging-in-Publication data is on file.

ISBN-13: 978-1-58713-209-4

ISBN-10: 1-58713-209-5

Warning and Disclaimer

This book is designed to provide information about the Cisco Networking for Home and Small Businesses CCNA Discovery course. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

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

The opinions expressed in this book belong to the authors and are not necessarily those of Cisco Systems, Inc.

Publisher

Paul Boger

Associate Publisher

Dave Dusthimer

Cisco Representative

Anthony Wolfenden

Cisco Press Program Manager

Jeff Brady

Executive Editor

Mary Beth Ray

Managing Editor

Patrick Kanouse

Development Editors

Dayna Isley, Drew Cupp

Project Editor

Seth Kerney

Copy Editor

Paula Lowell

Technical Editors

Nolan Fretz, Charles Hannon,
Bill Shurbert, Matt Swinford,
Michael Duane Taylor

Editorial Assistant

Vanessa Evans

Book and Cover Designer

Louisa Adair

Composition

Bronkella Publishing

Indexer

Heather McNeill

Proofreader

Mike Henry

This book is part of the Cisco Networking Academy® series from Cisco Press. The products in this series support and complement the Cisco Networking Academy curriculum. If you are using this book outside the Networking Academy, then you are not preparing with a Cisco trained and authorized Networking Academy provider.

For more information on the Cisco Networking Academy or to locate a Networking Academy, please visit www.cisco.com/edu.



Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact: **U.S. Corporate and Government Sales** 1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside the United States please contact: **International Sales** international@pearsoned.com

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through e-mail at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.



Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, IQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)

About the Authors

Allan Reid is the curriculum lead and a CCNA/CCNP instructor at the Centennial College CATC in Toronto, Canada. Allan is a professor in the Information and Communications Engineering Technology department and an instructor and program supervisor for the School of Continuing Education at Centennial College. He has developed and taught networking courses for both private and public organizations and has been instrumental in the development and implementation of numerous certificate, diploma, and degree programs in networking. Allan is also a curriculum developer for the Cisco Networking Academy. Outside of his academic responsibilities, he has been active in the computer and networking fields for more than 25 years and is currently a principal in a company specializing in the design, management, and security of network solutions for small and medium-sized companies. Allan authored the first edition of *WAN Technologies CCNA 4 Companion Guide* (Cisco Press, ISBN: 1-58713-172-2) and *Using a Networker's Journal*, which is a supplement to *A Networker's Journal* (Cisco Press, ISBN: 1-58713-158-7). Most recently, Allan co-authored the CCNA Discovery online academy courses “Networking for Home and Small Businesses” and “Introducing Routing and Switching in the Enterprise” with Jim Lorenz.

Jim Lorenz is an instructor and curriculum developer for the Cisco Networking Academy. Jim co-authored several Cisco Press titles including *Fundamentals of UNIX Companion Guide*, Second Edition (ISBN 1-58713-140-4), *Fundamentals of UNIX Lab Companion*, Second Edition (ISBN 1-58713-139-0), and the third editions of the CCNA Lab Companions. He has more than 20 years' experience in information systems ranging from programming and database administration to network design and project management. Jim has developed and taught computer and networking courses for both public and private institutions. As the Cisco Academy Manager at Chandler-Gilbert Community College in Arizona, he was instrumental in starting the Information Technology Institute (ITI) and developed a number of certificates and degree programs. Most recently, Jim co-authored the CCNA Discovery online academy courses “Networking for Home and Small Businesses” and “Introducing Routing and Switching in the Enterprise” with Allan Reid.

About the Technical Reviewers

Nolan Fretz is currently a college professor in network and telecommunications engineering technology at Okanagan College in Kelowna, British Columbia. He has almost 20 years of experience in implementing and maintaining IP networks and has been sharing his experiences by educating students in computer networking for the past nine years. He holds a master's degree in information technology.

Charles Hannon is an assistant professor of network design and administration at Southwestern Illinois College. He has been a Cisco Certified Academy Instructor (CCAI) since 1998. Charles has a master of arts in education from Maryville University, St. Louis, Missouri, currently holds a valid CCNA certification, and has eight years' experience in Management of Information Systems. Charles' priority is to empower students to become successful and compassionate lifelong learners.

Bill Shurbert is a professor of information technology at New Hampshire Technical Institute, in Concord, New Hampshire. Bill holds a bachelor's degree in technical management from Southern New Hampshire University. He enjoys teaching Cisco CCNA, Wireless, and IT Essentials classes. In his off time, you can find Bill and Joanne, his wife of 25+ years, sailing the waters of Lake Winnepesaukee.

Matt Swinford, associate professor of network design and administration at Southwestern Illinois College, has been an active Cisco Certified Academy Instructor (CCAI) since 1999. Matt is dedicated to fostering a learning environment that produces certified students and quality IT professionals. Matt has a masters of business administration from Southern Illinois University at Edwardsville, Edwardsville, Illinois and currently holds valid CCNP, A+, and Microsoft Certifications.

Michael Duane Taylor is department head of computer information sciences at the Raleigh Campus of ECPI College of Technology. He has more than seven years' experience teaching introductory networking and CCNA-level curriculum and was awarded the Instructor of the Year Award. Previously, Michael was a lab supervisor with Global Knowledge working with router hardware configuration and repair. He holds a bachelor's degree in business administration from the University of North Carolina at Chapel Hill and a masters of science in industrial technology/computer network management from East Carolina University. His certifications include CCNA, CCNP-router, and MCSE.

Acknowledgments

From Allan and Jim:

We want to thank Mary Beth Ray, Dayna Isley, and Drew Cupp with Cisco Press for their help and guidance in putting this book together. We also want to thank the technical editors, Mike Taylor, Bill Shurbert, Nolan Fretz, Charlie Hannon, and Matt Swinford. Their attention to detail and suggestions made a significant contribution to the accuracy and clarity of the content.

We would also like to acknowledge the entire CCNA Discovery development team from Cisco Systems, especially Carole Knieriem and Amy Gerrie for their input, support, and cooperation in the development of the book.

Dedications

This book is dedicated to my children: Andrew, Philip, Amanda, Christopher, and Shaun. You are my inspiration, and you make it all worthwhile. Thank you for your patience and support.

— *Allan Reid*

To the three most important people in my life: my wife Mary, and my daughters, Jessica and Natasha. Thanks for your patience and support.

— *Jim Lorenz*

Contents at a Glance

Introduction xxvi

Part I: Concepts

Chapter 1	Personal Computer Hardware	3
Chapter 2	Operating Systems	41
Chapter 3	Connecting to the Network	61
Chapter 4	Connecting to the Internet Through an ISP	129
Chapter 5	Network Addressing	171
Chapter 6	Network Services	201
Chapter 7	Wireless Technologies	231
Chapter 8	Basic Security	265
Chapter 9	Troubleshooting Your Network	295
Chapter 10	Putting It All Together	325
Appendix	Check Your Understanding and Challenge Questions Answer Key	327

Part II: Labs

Chapter 1	Labs: Personal Computer Hardware	343
Chapter 2	Labs: Operating Systems	361
Chapter 3	Labs: Connecting to the Network	369
Chapter 4	Labs: Connecting to the Internet Through an ISP	295
Chapter 5	Labs: Network Addressing	415
Chapter 6	Labs: Network Services	429
Chapter 7	Labs: Wireless Technologies	439
Chapter 8	Labs: Basic Security	461
Chapter 9	Labs: Troubleshooting Your Network	475
Chapter 10	Capstone Project: Putting It All Together	489
	Glossary	507
	Index	535

Contents

Introduction xxvi

Part I Concepts

Chapter 1	Personal Computer Hardware	3
	Objectives	3
	Key Terms	3
	Personal Computers and Applications	5
	How and Where Computers Are Used	5
	Types of Computer Applications	6
	Types of Computers	7
	Classes of Computers	7
	Servers, Desktops, and Workstations	8
	<i>Servers</i>	8
	<i>Desktops</i>	9
	<i>Workstations</i>	9
	Portable Devices	10
	<i>Laptops</i>	10
	<i>Tablet PC</i>	11
	<i>Pocket PC</i>	11
	<i>PDA</i>	11
	<i>Game Device</i>	12
	<i>Cell Phone</i>	12
	Binary Representation of Data	12
	Representing Information Digitally	12
	Measuring Storage Capacity	13
	Measuring Speed, Resolution, and Frequency	14
	<i>File Transfer Time</i>	15
	<i>Computer Screen Resolution</i>	15
	<i>Analog Frequencies</i>	16
	Computer Components and Peripherals	16
	Computer Systems	16
	Motherboard, CPU, and RAM	17
	<i>Motherboard</i>	17
	<i>Central Processing Unit (CPU)</i>	18
	<i>Random-Access Memory (RAM)</i>	19
	Adapter Cards	20
	<i>Video Cards</i>	21
	<i>Sound Cards</i>	21
	<i>Network Interface Cards (NICs)</i>	21
	<i>Modems</i>	22
	<i>Controller Cards</i>	22

- Storage Devices 22
 - Magnetic Storage* 22
 - Optical Storage* 23
 - Static Memory and Memory Sticks* 24
- Peripheral Devices 24
- Cases and Power Supplies 26
 - Surge Suppressors* 26
 - Uninterruptible Power Supplies* 27

Computer System Components 28

- Safety and Best Practices 28
- Installing Components and Verifying Operation 30
- Installing Peripherals and Verifying Operation 31

Summary 35

Activities and Labs 35

Check Your Understanding 36

Challenge Questions and Activities 39

Chapter 2 Operating Systems 41

Objectives 41

Key Terms 41

Choosing the Operating System 42

- Purpose of an Operating System 42
- Operating System Requirements 46
- Operating System Selection 48

Installing the Operating System 50

- OS Installation Methods 50
- Preparing for OS Installation 50
- Configuring a Computer for the Network 52
- Computer Naming 53
- Network Name and Address Planning 54

Maintaining the Operating System 54

- Why and When to Apply Patches 55
- Applying OS Patches 55
- Application Patches and Updates 56

Summary 58

Activities and Labs 58

Check Your Understanding 59

Chapter 3 Connecting to the Network 61

Objectives 61

Key Terms 61

Introduction to Networking	63
What Is a Network?	63
Benefits of Networking	65
Basic Network Components	65
Computer Roles in a Network	67
Peer-to-Peer Networks	69
Network Topologies	71
Principles of Communication	73
Source, Channel, and Destination	73
Rules of Communication	74
Message Encoding	76
Message Formatting	77
Message Size	79
Message Timing	80
<i>Access Method</i>	80
<i>Flow Control</i>	80
<i>Response Timeout</i>	81
Message Patterns	81
<i>Unicast</i>	81
<i>Multicast</i>	82
<i>Broadcast</i>	82
Communicating on a Wired Local Network	84
Importance of Protocols	84
Standardization of Protocols	85
Physical Addressing	87
Ethernet Communication	88
Hierarchical Design of Ethernet Networks	90
Logical Addressing	91
Access, Distribution, and Core Layers and Devices	92
Building the Access Layer of an Ethernet Network	94
Access Layer	94
Function of Hubs	95
Function of Switches	96
Broadcast Messaging	99
MAC and IP Addresses	101
Address Resolution Protocol (ARP)	101
Building the Distribution Layer of a Network	103
Distribution Layer	103
Function of Routers	105
Default Gateway	107
Tables Maintained by Routers	108
Local-Area Network (LAN)	112
Adding Hosts to Local and Remote Networks	114

- Plan and Connect a Local Network 115**
 - Plan and Document an Ethernet Network 115
 - Prototypes 116
 - Multi-function Device 117
 - Connecting the Linksys Router 119
 - Sharing Resources 121
- Summary 122**
- Activities and Labs 123**
- Check Your Understanding 124**
- Challenge Questions and Activities 127**

Chapter 4 Connecting to the Internet Through an ISP 129

- Objectives 129**
- Key Terms 129**
- The Internet and How We Connect To It 130**
 - Explain What the Internet Is 130
 - Internet Service Providers (ISP) 131
 - The ISP's Relationship with the Internet 132
 - Options for Connecting to the ISP 133
 - ISP Levels of Service 135
- Sending Information Across the Internet 138**
 - Importance of the Internet Protocol (IP) 138
 - How ISPs Handle Packets 139
 - Forwarding Packets Across the Internet 141
- Networking Devices in a NOC 142**
 - Internet Cloud 142
 - Devices in Internet Cloud 142
 - Physical and Environmental Requirements 145
- Cables and Connectors 146**
 - Common Network Cables 147
 - Twisted-Pair Cables 148
 - Coaxial Cable 151
 - Fiber-Optic Cables 152
 - Multimode Fiber 153*
 - Single-Mode Fiber 154*
- Working with Twisted-Pair Cabling 154**
 - Cabling Standards 154
 - UTP Cables 155
 - Unlike Devices 157*
 - Like Devices 157*
 - UTP Cable Termination 158
 - Terminating UTP at Patch Panels and Wall Jacks 159

Cable Testing	160
<i>Attenuation</i>	161
<i>Crosstalk</i>	162
Cabling Best Practices	162

Summary	165
Activities and Labs	166
Check Your Understanding	167
Challenge Questions and Activities	170

Chapter 5 **Network Addressing** **171**

Objectives	171
Key Terms	171
IP Addresses and Subnet Masks	172
Purpose of an IP Address	172
IP Address Structure	172
Parts of an IP Address	174
How IP Addresses and Subnet Masks Interact	175
Types of IP Addresses	177
IP Address Classes and Default Subnet Masks	177
Public and Private IP Addresses	179
Unicast, Broadcast, and Multicast Addresses	180
<i>Unicast</i>	181
<i>Broadcast</i>	181
<i>Multicast</i>	182
How IP Addresses Are Obtained	184
Static and Dynamic Address Assignment	184
<i>Static</i>	184
<i>Dynamic</i>	184
DHCP Servers	185
Configuring DHCP	186
Address Management	188
Network Boundaries and Address Space	188
Address Assignment	189
Network Address Translation	190
Summary	195
Activities and Labs	195
Check Your Understanding	196
Challenge Questions and Activities	199

Chapter 6 **Network Services** **201**

Objectives	201
Key Terms	201

Clients/Servers and Their Interaction 202

- Client/Server Relationship 202
- Role of Protocols in Client/Server Communication 204
 - Application Protocol* 204
 - Transport Protocol* 205
 - Internetwork Protocol* 205
 - Network Access Protocols* 206
- TCP and UDP Transport Protocols 206
 - Using TCP* 206
 - Using UDP* 208
- TCP/IP Port Numbers 208
 - Destination Port* 208
 - Source Port* 208

Application Protocols and Services 209

- Domain Name Service 209
- Web Clients and Servers 211
- FTP Clients and Servers 212
- E-mail Clients and Servers 213
- IM Clients and Servers 215
- Voice Clients and Servers 216
- Port Numbers 217

Layered Model and Protocols 218

- Protocol Interaction 218
- Protocol Operation of Sending and Receiving a Message 219
- Open System Interconnection Model 221

Summary 225

Activities and Labs 226

Check Your Understanding 227

Challenge Questions and Activities 229

Chapter 7 Wireless Technologies 231

Objectives 231

Key Terms 231

Wireless Technology 233

- Wireless Technologies and Devices 233
 - Infrared* 233
 - Radio Frequency (RF)* 234
- Benefits and Limitations of Wireless Technology 235
- Types of Wireless Networks and Their Boundaries 236
 - WPAN* 236
 - WLAN* 236
 - WWAN* 236

Wireless LANs 237

- Wireless LAN Standards 237
- Wireless LAN Components 238

WLANs and the SSID	240
<i>Ad-hoc</i>	240
<i>Infrastructure Mode</i>	240
Wireless Channels	242
Configuring the Access Point	244
<i>Wireless Mode</i>	244
<i>SSID</i>	245
<i>Wireless Channel</i>	246
Configuring the Wireless Client	246
<i>Integrated Wireless Utility Software</i>	246
<i>Standalone Wireless Utility Software</i>	247
Security Considerations on a Wireless LAN	248
Why People Attack WLANs	248
MAC Address Filtering	250
Authentication on a WLAN	251
<i>Open Authentication</i>	251
<i>Pre-shared keys (PSK)</i>	251
<i>Extensible Authentication Protocol (EAP)</i>	252
Encryption on a WLAN	253
<i>Wired Equivalency Protocol (WEP)</i>	253
<i>Wi-Fi Protected Access (WPA)</i>	254
Traffic Filtering on a WAN	254
Configuring an Integrated AP and Wireless Client	255
Planning the WLAN	255
<i>Wireless Standards</i>	255
<i>Installation of Wireless Devices</i>	256
Installing and Securing the AP	257
Backing Up and Restoring Configuration Files	257
Updating the Firmware	258
Summary	260
Activities and Labs	261
Check Your Understanding	262
Challenge Questions and Activities	263
Chapter 8	Basic Security 265
	Objectives 265
	Key Terms 265
	Networking Threats 266
	Risks of Networking Intrusion 266
	Sources of Network Intrusion 267
	<i>External Threats</i> 267
	<i>Internal Threats</i> 267
	Social Engineering and Phishing 268
	<i>Pretexting</i> 268
	<i>Phishing</i> 269
	<i>Vishing</i> 269

Methods of Attack 269

Viruses, Worms, and Trojan Horses 270

Viruses 270

Worms 270

Trojan Horses 271

Denial of Service and Brute Force Attacks 271

Denial of Service Attack 271

Distributed Denial of Service Attack 272

Brute-Force Attack 272

Spyware, Tracking Cookies, Adware, and Pop-Ups 273

Spyware 273

Tracking Cookies 274

Adware 274

Pop-Ups and Pop-Unders 275

Spam 275

Security Policy 276

Common Security Measures 276

Updates and Patches 278

Anti-virus Software 278

Anti-spam 280

Anti-spyware 282

Using Firewalls 283

What Is a Firewall? 283

Using a Firewall 284

Single-Firewall Configuration 285

Two-Firewall Configuration 286

Home Networking Device Firewalls 286

Vulnerability Analysis 287

Best Practices 288

Summary 290

Activities and Labs 291

Check Your Understanding 291

Challenge Questions and Activities 294

Chapter 9 Troubleshooting Your Network 295

Objectives 295

Key Terms 295

Troubleshooting Process 296

Gathering Information 297

Approaches to Troubleshooting 298

Top-Down 298

Bottom-Up 298

Divide-and-Conquer 300

Trial-and-Error 301

Substitution 301

	Using Utilities to Troubleshoot Connectivity Issues	301
	Detecting Physical Problems	301
	<i>Vision</i>	302
	<i>Smell</i>	302
	<i>Touch</i>	302
	<i>Hearing</i>	302
	Software Utilities for Troubleshooting Connectivity	302
	<i>Troubleshooting Using ipconfig</i>	303
	<i>Troubleshooting Using ping</i>	304
	<i>Troubleshooting Using tracert</i>	306
	<i>Troubleshooting Using netstat</i>	307
	<i>Troubleshooting Using nslookup</i>	308
	Common Networking Issues	309
	Connectivity Issues	309
	LED Indicators	310
	<i>Power LED</i>	311
	<i>Status LED</i>	311
	<i>Activity LED</i>	311
	Wired Connectivity Problems	311
	Connectivity Problems in a WLAN	312
	<i>SSID</i>	313
	<i>Authentication</i>	313
	<i>Encryption</i>	313
	DHCP Issues	314
	Troubleshooting the Wireless Router to ISP Connection	315
	Troubleshooting and the Help Desk	316
	Documentation	317
	Using Outside Sources of Help	317
	Using the Help Desk	318
	Summary	320
	Activities and Labs	321
	Check Your Understanding	321
	Challenge Questions and Activities	323
Chapter 10	Putting It All Together	325
	Summary Activity	325
	Activities and Labs	325
Appendix	Check Your Understanding and Challenge Questions Answer Key	327
	Chapter 1	327
	Check Your Understanding	327
	Challenge Questions and Activities	328
	Chapter 2	328
	Check Your Understanding	328

Chapter 3	329
Check Your Understanding	329
Challenge Questions and Activities	330
Chapter 4	331
Check Your Understanding	331
Challenge Questions and Activities	332
Chapter 5	333
Check Your Understanding	333
Challenge Questions and Activities	334
Chapter 6	335
Check Your Understanding	335
Challenge Questions and Activities	336
Chapter 7	336
Check Your Understanding	336
Challenge Questions and Activities	337
Chapter 8	337
Check Your Understanding	337
Challenge Questions and Activities	338
Chapter 9	339
Check Your Understanding	339
Challenge Questions and Activities	339

Part II **Labs**

Chapter 1 **Labs: Personal Computer Hardware** **343**

Lab 1-1: Determining Data Storage Capacity (1.3.2.2)	343
Task 1: Identify the Amount of RAM in a Computer	343
Task 2: Determine the Size of the Hard Disk Drive	344
Task 3: Determine the Free Space and Used Space on the Hard Drive	345
Task 4: Check for Other Storage Devices	346
Task 5: Reflection	347
Lab 1-2: Determining the Screen Resolution of a Computer (1.3.3.4)	348
Task 1: Determine the Current Screen Resolution	348
Task 2: Determine the Maximum Resolution for the Highest Color Quality	349
Task 3: Calculate the Pixels for Current and Maximum Resolution Settings	349
Task 4: Identify the Type of Graphics Card Installed	350
Task 5: Identify the Type of Monitor and Available Refresh Rates	350
Lab 1-3: Installing a Printer and Verifying Its Operation (1.5.3.4)	352
Task 1: Add a Printer	352
Task 2: Verify the Printer Installation	355
Task 3: Download and Install an Updated Printer Driver	356
Task 4: Verify the New Driver Installation	360

Chapter 2 Labs: Operating Systems 361**Lab 2-1: Examining Operating System and Application Versions (2.3.3.2) 361**

Task 1: Determine the Windows XP Version and Revision Number 361

Task 2: Configure Windows XP for Updates 362

Task 3: Determine an Application Version 363

Task 4: Reflection 363

Challenge Lab 2-2: Evaluating an OS Upgrade 363

Task 1: Locate Minimum Requirements for Windows Vista 364

Task 2: Determine the Hardware Information for the Computer Using winmsd.exe 365

Task 3: Determine CPU Type and Amount of RAM Using System Properties 365

Task 4: Determine Hard Disk Capacity and Amount of Free Disk Space Using My Computer Properties 365

Task 5: Check for Other Drives (Floppy, CD-ROM, DVD) 366

Task 6: Verify the Monitor and Graphics Capabilities 366

Task 7: Download and Run Windows Vista Upgrade Advisor 366

Task 8: Reflection 367

Chapter 3 Labs: Connecting to the Network 369**Lab 3-1: Building a Peer-to-Peer Network (3.1.5.3) 369**

Task 1: Diagram the Network 369

Task 2: Document the PCs 370

Task 3: Connect the Ethernet Cable 371

Task 4: Verify Physical Connectivity 371

Task 5: Configure IP Settings 371

Task 6: Verify IP Connectivity Between the Two PCs 372

Task 7: Verify Connectivity Using My Network Places 373

Task 8: (Optional) Re-enable the Firewall 373

Lab 3-2: Determine the MAC Address of a Host (3.3.3.2) 373

Task 1: Open a Windows Command Prompt Window 374

Task 2: Use the ipconfig /all Command 374

Task 3: Locate the MAC (Physical) Address(es) in the Output from the ipconfig /all Command 375

Task 4: Reflection 375

Lab 3-3: Determine the IP Address of a Computer (3.3.6.2) 376

Task 1: Determine the IP Address of the Computer 376

Lab 3-4: IP Addresses and Network Communication (3.5.2.2) 378

Task 1: Connect the PCs to Create a Peer-to-Peer Network 378

Task 2: Verify Physical Connectivity 378

Task 3: Configure IP Settings for the Two PCs 379

Task 4: Verify IP Connectivity Between the Two PCs 379

Task 5: Change IP Address for PC2 380

Task 6: Test Network Connectivity Between the Two PCs 381

Task 7: Change IP Address for PC1 381

Task 8: Test Network Connectivity Between the Two PCs 382

Task 9: (Optional) Re-enable the Firewall 382

Lab 3-5: Connect and Configure Hosts (3.6.4.3) 383

Task 1: Identify Ethernet Ports 383

Task 2: Connect the Cable Between the PC and the Router 384

Task 3: Assign the PCs an IP Address and Default Gateway 384

Task 4: Verify the IP Address Configuration 385

Task 5: Test Connectivity Between the Two PCs 386

Task 6: Configure the NetBIOS Name 386

Task 7: Verify Configuration 387

Task 8: (Optional) Re-enable the Firewall 388

Task 9: Return IP Address and NetBIOS Name to Original Values 388

Task 10: Reflection 389

Lab 3-6: Sharing Resources (3.6.5.3) 390

Task 1: Share a Folder 390

Task 2: Map Network Drives to Provide Quick and Easy Access to Shared Folders 392

Task 3: Verify Work 393

Task 4: Reflection 393

Chapter 4 Labs: Connecting to the Internet Through an ISP 395

Lab 4-1: Tracing Internet Connectivity (4.2.3.3) 395

Task 1: (Optional) Download and Install a Free Program 395

Task 2: Locate Websites 396

Task 3: (Optional) Use Downloaded Visual Trace Route Tool 396

Task 4: Use the tracert Command 397

Task 5: Use the pathping Command 398

Task 6: (Optional) Use the whois Function 398

Task 7: Reflection 399

Lab 4-2: Building Straight-Through and Crossover UTP Cables (4.5.3.2) 400

Part A: Build and Test an Ethernet Straight-Through Patch Cable 401

Task A1: Obtain and Prepare the Cable 401

Task A2: Prepare and Insert the Wires 401

Task A3: Inspect, Crimp, and Reinspect 402

Task A4: Terminate the Other Cable End 403

Task A5: Test the Cable 403

Part B: Build and Test an Ethernet Crossover Cable 403

Task B1: Obtain and Prepare the Cable 403

Task B2: Prepare and Insert the T568A Wires 403

Task B3: Inspect, Crimp, and Reinspect 404

Task B4: Terminate the T568B Cable End 404

Task B5: Test the Cable 404

Task B6: Reflection 405

Lab 4-3: Terminating UTP Cables (4.5.4.4) 406

Task 1: Strip the Sheath 406

Task 2: Position Wires in Data Jack 406

Task 3: Punch Down the Data Jack 407

Task 4: Punch Down the Patch Panel 407

Task 5: Test the Data Jack and Patch Panel Terminations with a Basic Cable Tester (Optional) 408

Task 6: Reflection (Optional) 408

Lab 4-4: Testing UTP Cables (4.5.5.4) 409

Task 1: Set Up the Fluke 620 LAN CableMeter 410

Task 2: Test Cabling Procedure 410

Task 3: Use the Wire Map Meter Function 411

Task 4: Use the Length Meter Function 412

Task 5: Test Data Jack and Patch Panel Terminations for Wire Map, Length, and Miswire (Optional) 412

Task 6: Set Up and Test a Cable Using the Fluke MicroScanner 412

Task 7: Reflection 413

Chapter 5 Labs: Network Addressing 415**Lab 5-1: Using the Windows Calculator with Network Addresses (5.1.4.3) 415**

Task 1: Access Windows Calculator and Determine Mode of Operation 416

Task 2: Convert Between Number Systems 416

Task 3: Convert Host IP Addresses 418

Task 4: Convert Host IP Subnet Masks 418

Task 5: Convert Broadcast Addresses 419

Task 6: Convert IP and MAC Addresses for a Host 420

Task 7: Manipulate Powers of 2 to Determine the Number of Hosts on a Network 421

Task 8: (Optional) Determine the Network Number and Number of Hosts Based on Subnet Mask 421

Task 9: Reflection 422

Challenge Lab 5-2: Exploring IP Address Functions on an Multi-function Device 423

Task 1: View Current IP Settings 423

Task 2: Configure TCP/IP Settings for DHCP 424

Task 3: Connect PCs to the Multi-function Device 424

Task 4: Verify the Physical Connection 424

Task 5: Access the Command Prompt on a Client PC 424

Task 6: Access the Multi-function Device Configuration Through a Web Browser 425

Task 7: Examine the Multi-function Device Configuration 425

Task 8: Connect the Multi-function Device to the Internet 425

Task 9: Verify Connectivity Using the ping Command 426

Task 10: Verify Connectivity Using the tracert Command 427

Task 11: Verify Internet Connectivity 427

Task 12: Determine the Network Boundaries 428

Task 13: Restore All Original Network Connections 428

Task 14: Reflection 428

Chapter 6 Labs: Network Services 429

Lab 6-1: Observing DNS Name Resolution (6.2.1.3) 429

Task 1: Observe DNS Conversion 429

Task 2: Verify DNS Operation Using the nslookup Command 430

Task 3: Identify Mail Servers Using the nslookup Command 431

Task 4: Reflection 432

Lab 6-2: Exploring FTP (6.2.3.3) 433

Task 1: Examine FTP from the Command Prompt 433

Task 2: Use a GUI FTP Client or Web Browser 434

Task 3: (Optional) Use Both an FTP Server and Client 435

Lab 6-3: Configuring an E-mail Client (6.2.4.4) 436

Task 1: Open Microsoft Outlook 436

Task 2: Set Up an E-mail Account 436

Task 3: Enter POP3 E-mail Account Information 436

Task 4: (Optional) Add Another Account or Change an Account 437

Task 5: Reflection 437

Chapter 7 Labs: Wireless Technology 439

Lab 7-1: Configuring a Wireless Access Point (7.2.5.3) 439

Task 1: Verify Connectivity Between the Computer and the Multi-function Device 439

Task 2: Log In to the Multi-function Device and Configure the Wireless Network 440

Task 3: Reflection 441

Lab 7-2: Configuring a Wireless Client (7.2.6.4) 442

Task 1: Install the Wireless NIC Driver 442

Task 2: Connect the Wireless NIC 443

Task 3: Attach to the Wireless Network 443

Task 4: Determine the NIC Driver Version 445

Task 5: Determine If the NIC Driver Is the Most Current 445

Task 6: Verify Connectivity 446

Task 7: Reflection 446

Lab 7-3: Configuring Wireless Security (7.3.5.2) 448

Task 1: Plan the Security for Your Home Network 448

Task 2: Connect a Computer to the Multi-function Device and Log In to the Web-Based Utility 449

Task 3: Change the Linksys Device Password 450

- Task 4: Configure the Wireless Security Settings 451
- Task 5: Configure Encryption and Authentication 452
- Task 6: Configure MAC Address Filtering 454
- Task 7: Reflection 455

Challenge Lab 7-4: Planning the Home or Small Business WLAN 456

- Task 1: Plan the WLAN 456
- Task 2: Use Internet for Research 458
- Task 3: Document Your Findings 459
- Task 4: Reflection 459

Chapter 8 Labs: Basic Security 461

Lab 8-1: Configuring Access Policies and DMZ Settings (8.4.2.4) 461

- Part A: Configuring Access Policies 462
 - Task 1: Build the Network and Configure the Hosts 462*
 - Task 2: Log In to the User Interface 463*
 - Task 3: View Multi-function Device Firewall Settings 463*
 - Task 4: Set Up Internet Access Restrictions Based on IP Address 464*
 - Task 5: Set Up an Internet Access Policy Based on an Application 465*
- Part B: Configuring a DMZ on the Multi-function Device 466
 - Task 1: Set Up a Simple DMZ 466*
 - Task 2: Set Up a Host with Single Port Forwarding 467*
 - Task 3: Restore the Multi-function Device to Its Default Settings 468*

Lab 8-2: Performing a Vulnerability Analysis (8.4.3.2) 469

- Task 1: Download and Install MBSA 470
- Task 2: Build the Network and Configure the Hosts 470
- Task 3: Run MBSA on a Host 471
- Task 4: Select a Computer to Scan 471
- Task 5: View Security Update Scan Results 471
- Task 6: View Windows Scan Results in the Security Report 472
- Task 7: View Desktop Application Scan Results in the Security Report 472
- Task 8: Scan a Server, If Available 472
- Task 9: Uninstall MBSA Using Control Panel Add/Remove Programs 473
- Task 10: Reflection 473

Chapter 9 Labs: Troubleshooting Your Network 475

Lab 9-1: Troubleshooting Using Network Utilities (9.2.7.2) 475

- Task 1: Build the Network and Configure the Hosts 476
- Task 2: Record the Baseline IP Address Information for Computers and Wireless Router 476
- Task 3: Scenario 1—Diagnose Web Server Access 478
- Task 4: Scenario 2—Diagnose Web Server Access 479
- Task 5: Scenario 3—Diagnose FTP Server Access 480
- Task 6: Scenario 4—Diagnose FTP Server Access 480
- Task 7: Scenario 5—Diagnose Telnet Server Access Problem 481

Task 8: Scenario 6—Analyze TCP Connections to Host-A 482

Task 9: Reflection 483

Lab 9-2: Troubleshooting Physical Connectivity (9.3.3.2) 484

Task 1: Build the Network and Configure the Hosts 485

Task 2: Record the Correct Cable Types Used Between Devices 485

Task 3: Record the IP Address Information for the Computers 485

Task 4: Scenario 1 486

Task 5: Scenario 2 486

Task 6: Scenario 3 487

Task 7: Scenario 4 488

Task 8: Reflection 488

Chapter 10 Capstone Project: Putting It All Together 489

Task 1: Gather Information and Determine Customer Requirements 490

AnyCompany Corporation Information Summary 491

Office Floor Plan 493

Interview with the Administrative Manager 494

Task 2: Select the Appropriate Services and Equipment 496

Task 3: Plan the Installation 500

Task 4: Prepare and Present the Proposal 503

Task 5: Install and Configure the Network 503

Task 6: Test and Troubleshoot 505

Task 7: Document and Sign-Off 506

Task 8: Support 506

Glossary 507

Index 535

Icons Used in This Book



Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italics* indicate arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets [] indicate optional elements.
- Braces { } indicate a required choice.
- Braces within brackets [{ }] indicate a required choice within an optional element.

Introduction

Cisco Networking Academy is a comprehensive e-learning program that delivers information technology skills to students around the world. The Cisco CCNA Discovery curriculum consists of four courses that provide a comprehensive overview of networking, from fundamentals to advanced applications and services. The curriculum emphasizes real-world practical application, while providing opportunities for you to gain the skills and hands-on experience needed to design, install, operate, and maintain networks in small to medium-sized businesses, as well as enterprise and service provider environments. The Networking for Home and Small Businesses course is the first course in the curriculum.

Networking for Home and Small Businesses, CCNA Discovery Learning Guide is the official supplemental textbook for the first course in v4.x of the CCNA Discovery online curriculum of the Networking Academy. As a textbook, this book provides a ready reference to explain the same networking concepts, technologies, protocols, and devices as the online curriculum. In addition, it contains all the interactive activities, Packet Tracer activities, and hands-on labs from the online curriculum as well as bonus labs.

This book emphasizes key topics, terms, and activities and provides many alternative explanations and examples as compared with the course. You can use the online curriculum as directed by your instructor and then also use this *Learning Guide's* study tools to help solidify your understanding of all the topics. In addition, the book includes

- Expanded coverage of CCENT/CCNA exam material
- Additional key glossary terms
- Bonus labs
- Additional Check Your Understanding and Challenge questions
- Interactive activities and Packet Tracer activities on the CD-ROM

Goal of This Book

First and foremost, by providing a fresh, complementary perspective of the online content, this book helps you learn all the required materials of the first course in the Networking Academy CCNA Discovery curriculum. As a secondary goal, individuals who do not always have Internet access can use this text as a mobile replacement for the online curriculum. In those cases, you can read the appropriate sections of this book, as directed by your instructor, and learn the topics that appear in the online curriculum. Another secondary goal of this book is to serve as your offline study material to help prepare you for the CCENT and CCNA exams.

Audience for This Book

This book's main audience is anyone taking the first CCNA Discovery course of the Networking Academy curriculum. Many Networking Academies use this textbook as a required tool in the course, while other Networking Academies recommend the *Learning Guides* as an additional source of study and practice materials.

Book Features

The educational features of this book focus on supporting topic coverage, readability, and practice of the course material to facilitate your full understanding of the course material.

Topic Coverage

The following features give you a thorough overview of the topics covered in each chapter so that you can make constructive use of your study time:

- **Objectives:** Listed at the beginning of each chapter, the objectives reference the core concepts covered in the chapter. The objectives match the objectives stated in the corresponding chapters of the online curriculum; however, the question format in the *Learning Guide* encourages you to think about finding the answers as you read the chapter.
- **“How-to” feature:** When this book covers a set of steps that you need to perform for certain tasks, the text lists the steps as a how-to list. When you are studying, the icon helps you easily refer to this feature as you skim through the book.
- **Notes, tips, cautions, and warnings:** These are short sidebars that point out interesting facts, timesaving methods, and important safety issues.
- **Chapter summaries:** At the end of each chapter is a summary of the chapter’s key concepts. It provides a synopsis of the chapter and serves as a study aid.



Readability

The authors have compiled, edited, and in some cases rewritten the material so that it has a more conversational tone that follows a consistent and accessible reading level. In addition, the following features have been updated to assist your understanding of the networking vocabulary:

- **Key terms:** Each chapter begins with a list of key terms, along with a page-number reference from inside the chapter. The terms are listed in the order in which they are explained in the chapter. This handy reference allows you to find a term, flip to the page where the term appears, and see the term used in context. The Glossary defines all the key terms.
- **Glossary:** This book contains an all-new Glossary with more than 350 computer and networking terms.

Practice

Practice makes perfect. This new *Learning Guide* offers you ample opportunities to put what you learn to practice. You will find the following features valuable and effective in reinforcing the instruction that you receive:

- **Check Your Understanding questions and answer key:** Updated review questions are presented at the end of each chapter as a self-assessment tool. These questions match the style of questions that you see in the online course. Appendix A, “Check Your Understanding and Challenge Questions Answer Key,” provides an answer key to all the questions and includes an explanation of each answer.
- **(NEW) Challenge questions and activities:** Additional, and more challenging, review questions and activities are presented at the end of chapters. These questions are purposefully designed to be similar to the more complex styles of questions you might see on the CCNA exam. This section might also include activities to help prepare you for the exams. Appendix A provides the answers.


 Packet Tracer
Activity

- **Packet Tracer activities:** Interspersed throughout the chapters you'll find many activities to work with the Cisco Packet Tracer tool. Packet Tracer allows you to create networks, visualize how packets flow in the network, and use basic testing tools to determine whether the network would work. When you see this icon, you can use Packet Tracer with the listed file to perform a task suggested in this book. The activity files are available on this book's CD-ROM; Packet Tracer software, however, is available through the Academy Connection website. Ask your instructor for access to Packet Tracer.



- **Interactive activities:** These activities provide an interactive learning experience to reinforce the material presented in the chapter.



- **Labs:** This book contains all the hands-on labs from the curriculum plus additional challenge labs for further practice. Part I includes references to the hands-on labs, as denoted by the lab icon, and Part II of the book contains each lab in full. You may perform each lab as you see each lab referenced in the chapter or wait until you have completed the chapter.

A Word About Packet Tracer Software and Activities

Packet Tracer is a self-paced, visual, interactive teaching and learning tool developed by Cisco. Lab activities are an important part of networking education. However, lab equipment can be a scarce resource. Packet Tracer provides a visual simulation of equipment and network processes to offset the challenge of limited equipment. Students can spend as much time as they like completing standard lab exercises through Packet Tracer, and have the option to work from home. Although Packet Tracer is not a substitute for real equipment, it allows students to practice using a command-line interface. This “e-doing” capability is a fundamental component of learning how to configure routers and switches from the command line.

Packet Tracer v4.x is available only to Cisco Networking Academies through the Academy Connection website. Ask your instructor for access to Packet Tracer.

A Word About the Discovery Server CD

The CCNA Discovery series of courses is designed to provide a hands-on learning approach to networking. Many of the CCNA Discovery labs are based on Internet services. Because it is not always possible to allow students access to these services on a live network, the Discovery Server has been developed to provide them.

The Discovery Server CD is a bootable CD developed by Cisco that transforms a regular PC into a Linux server running several preconfigured services for use with the CCNA Discovery labs. The Discovery Server is available from the Academy Connection website *only*. Your instructor can download the CD files from the Instructor Tools section of the Academy Connection website, burn a CD, and show you how to make use of the Server. Hands-on labs that make use of the Discovery Server are identified within the labs themselves.

Once booted, the server provides many services to clients including

- Domain Name Services
- Web Services
- FTP

- TFTP
- Telnet
- SSH
- DHCP
- Streaming Video
- VPN Termination

How This Book Is Organized

This book covers the major topics in the same sequence as the online curriculum for the CCNA Discovery Networking for Home and Small Businesses course. The online curriculum has 10 chapters for this course, so this book has 10 chapters with the same names and numbers as the online course chapters.

To make it easier to use this book as a companion to the course, the major topic headings in each chapter match, with just a few exceptions, the major sections of the online course chapters. However, the *Learning Guide* presents many topics in slightly different order inside each major heading. Additionally, the book occasionally uses different examples than the course. As a result, students get more detailed explanations, a second set of examples, and different sequences of individual topics, all to aid the learning process. This new design, based on research into the needs of the Networking Academies, helps typical students lock in their understanding of all the course topics.

Chapters and Topics

Part I of this book has 10 chapters, as follows:

- **Chapter 1, “Personal Computer Hardware,”** discusses different types of personal computers, how they are used, and the difference between local and network applications. This chapter describes how data is represented and manipulated in a computer system. Also covered is the role of the various computer components and peripherals and the proper way to install and test them.
- **Chapter 2, “Operating Systems,”** introduces the OS, its key components, and user interfaces as well as some of the more common operating systems. It provides an overview of the commercial and GPL software licensing schemes. This chapter presents different options for OS installation and describes the process for upgrading and maintaining the OS. It covers the common types of file systems used with PCs and hard disk partitioning. You will also learn the IP parameters that must be configured to prepare a computer to participate on the network.
- **Chapter 3, “Connecting to the Network,”** introduces communications protocols and describes how communication occurs on an Ethernet network. The main components of an information network are explored as are the roles clients and servers play. In this chapter you will build a peer-to-peer computer network and verify it is functioning. Logical and physical topologies are compared and the layered networking model is introduced. You will learn how hubs, switches, and routers function. Also covered are broadcast and collision domains, ARP, default gateways, and prototyping.
- **Chapter 4, “Connecting to the Internet Through an ISP,”** introduces ISP services, options for connecting to the Internet, and components of an ISP Network Operations Center (NOC). This chapter discusses the Internet Protocol (IP) and how information is sent across the Internet

through an ISP. Other major areas covered by this chapter are the cabling and connectors used for connecting network devices, with focus on Ethernet UTP cables and how they are constructed. You will build Ethernet cables and test them.

- **Chapter 5, “Network Addressing,”** examines the IP address and subnet mask and how they are used on a network. Unicast, multicast, and broadcast IP addresses are introduced as well as the three classes of assignable IP addresses. This chapter covers how IP addresses are obtained, the differences between public and a private addresses, and how network address translation (NAT) functions.
- **Chapter 6, “Network Services,”** builds on the client/server model as it relates to common network services. This chapter describes the TCP and UDP transport protocols, the function of port numbers, and the protocols and applications that use them. Focus is on major Internet services, applications, and protocols including DNS, e-mail, WWW, FTP, and IM. The concept of a protocol stack and how protocols interact on a host when sending and receiving a message are introduced. The purpose of a layered networking model is discussed as are the two major models in use, the Open Systems Interconnect (OSI) and the TCP/IP model.
- **Chapter 7, “Wireless Technologies,”** explores the benefits and limitations of wireless technology and where it is used. This chapter compares the wireless personal-area network (WPAN), wireless local-area network (WLAN), and wireless wide-area network (WWAN). It describes components required to build a WLAN and their functions as well as the current standards for WLANs and how they compare. In this chapter, you will configure parameters on a wireless access point (AP) to allow a wireless client to access network resources. You will also explore techniques available to help secure the WLAN.
- **Chapter 8, “Basic Security,”** introduces networking threats, their characteristics, and different methods of attack. This chapter also describes security procedures and applications that can help prevent attacks and focuses on firewalls, their capabilities, and how a DMZ is structured. You will configure a DMZ and port forwarding with an integrated router device. You will also learn about vulnerability analysis software and how can it help to prevent attacks.
- **Chapter 9, “Troubleshooting Your Network,”** identifies the steps involved in the troubleshooting process and some of the common troubleshooting techniques. Utilities available for troubleshooting connectivity issues are explored. This chapter also covers some of the more common issues with wired and wireless LANs and suggests some possible sources of help when troubleshooting.
- **Chapter 10, “Putting It All Together,”** In this summary activity, you use what you have learned about computer hardware and software, wired and wireless networking components, protocols and applications, and techniques for securing a network to plan and implement a technical solution for a small business.

Part II of this book includes the labs that correspond to each chapter.

This book also includes the following:

- An appendix, **“Check Your Understanding and Challenge Questions Answer Key,”** provides the answers to the Check Your Understanding questions that you find at the end of each chapter. It also includes answers for the Challenge questions and activities that conclude most chapters.
- The **Glossary** provides a compiled list of all the key terms that appear throughout this book plus additional computer and networking terms.

About the CD-ROM

The CD-ROM included with this book provides many useful tools and information to support your education:

Packet Tracer
Activity



- **Packet Tracer Activity files:** These are files to work through the Packet Tracer activities that are referenced throughout the book, as indicated by the Packet Tracer activity icon.
- **Interactive Activities:** The CD-ROM contains the interactive activities referenced throughout the book.
- **OSI Model Overview:** The CD-ROM also contains a brief overview of the OSI model for your reference.
- **Taking Notes:** This section includes a .txt file of the chapter objectives to serve as a general outline of the key topics of which you need to take note. The practice of taking clear, consistent notes is an important skill for not only learning and studying the material but for on-the-job success as well. Also included in this section is “A Guide to Using a Networker’s Journal”; a PDF booklet providing important insight into the value of the practice of using a journal, how to organize a professional journal, and some best practices on what, and what not, to take note of in your journal.
- **IT Career Information:** This section includes a Student Guide to applying the toolkit approach to your career development. Learn more about entering the world of Information Technology as a career by reading two informational chapters excerpted from *The IT Career Builder’s Toolkit*: “Information Technology: A Great Career” and “Breaking into IT.”
- **Lifelong Learning in Networking:** As you embark on a technology career, you will notice that it is ever-changing and evolving. This career path provides new and exciting opportunities to learn new technologies and their applications. Cisco Press is one of the key resources to plug into on your quest for knowledge. This section of the CD-ROM provides an orientation to the information available to you and tips on how to tap into these resources for lifelong learning.

This page intentionally left blank

This page intentionally left blank

Operating Systems

Objectives

Upon completion of this chapter, you will be able to answer the following questions:

- What is the purpose of an OS?
- What role do the shell and kernel play?
- What is the difference between a CLI and GUI interface?
- What is a network redirector?
- What are some of the common operating systems available?
- What is the difference between commercial and GPL software licensing?
- What are the different options for OS installation?
- What is an OS upgrade and how is it performed?
- What is a file system and what types are used with PCs?
- What IP parameters must be configured to prepare a computer to participate on the network?
- How are operating systems maintained?

Key Terms

This chapter uses the following key terms. You can find the definitions in the Glossary.

operating system (OS) page 42

kernel page 43

shell page 43

command-line interface (CLI) page 43

graphical user interface (GUI) page 43

K Desktop Environment (KDE) page 44

multitasking page 44

network client page 45

network operating system (NOS) page 46

GNU Public License (GPL) page 46

UNIX page 46

Linux page 46

total cost of ownership (TCO) page 49

upgrade page 50

virtual machine page 50

file system page 51

File Allocation Table (FAT) 16/32 page 51

New Technology File System (NTFS) page 51

ext2 page 52

ext3 page 52

data loss page 52

network interface card (NIC) page 52

Internet Protocol (IP) page 52

IP address page 52

computer name page 53

patch page 55

How we interact with our computer, and what applications it can run, affects our ability to communicate with others. Computer operating systems enable us to use application software, store information, and join the network. The operating system is the most important program running on a computer. Without it the other programs and features will not operate. In this chapter you will learn about the most popular operating systems, and how to choose the one that will be right for your computer. Part II of this book includes the corresponding labs for this chapter.

Choosing the Operating System

There are a number of operating systems in use with modern computers. Most client computers purchased in a retail outlet come with the operating system preloaded. If a computer is ordered from an online retail outlet, the purchaser frequently has a choice of which OS is installed. Business environments often need to consider other options depending on the intended function of the computer. They may even build their own computers and install the desired OS.

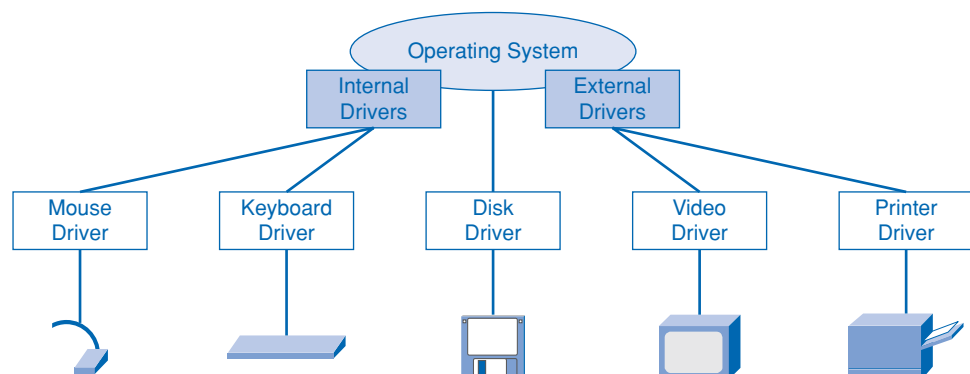
Purpose of an Operating System

System components and peripherals, by themselves, are nothing more than a collection of electronics and mechanical parts. To get these parts to work together to perform a specific task, a special type of computer program, known as an *operating system (OS)*, is required.

Suppose that a user wants to write a report and print it out on an attached printer. A word processing application is required to accomplish this task. Information is entered from the keyboard, displayed on the monitor, saved on the disk drive, and then finally sent to the printer.

In order for the word processing program to accomplish all of this, it must work with the OS, which controls input and output functions. The OS uses specialized software programs known as drivers to interact with the various hardware components. Every major electronic component inside the computer or attached to it requires a driver. These drivers might be integrated into the OS or standalone software modules used by the OS. The OS and its drivers are what accept the information entered from the keyboard, displays it on the monitor, saves it to disk, and sends the document to the printer. As shown in Figure 2-1, the keyboard, mouse, and disk drivers are typically integrated into the OS whereas video and printer drivers are typically external software modules. The entered data is manipulated inside of the computer, stored in RAM, and processed by the CPU. This internal manipulation and processing is also controlled by the OS. All computerized devices, such as servers, desktops, laptops, or handhelds, require an OS in order to function.

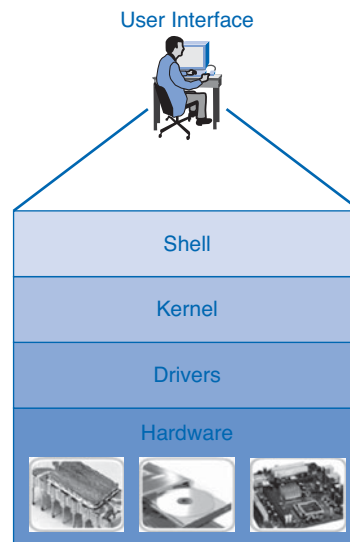
Figure 2-1 Computer Components and OS Drivers



The OS acts like a translator between user applications and the hardware. A user interacts with the computer system through an application, such as a word processor, spreadsheet, or computer game. Application programs are designed for a specific purpose, such as word processing, and know nothing of the underlying electronics. For example, the application is not concerned with how information is entered into the application from the keyboard. The operating system is responsible for the communication between the application and the hardware.

When a computer is powered on, it loads the OS, normally from a permanent storage device, such as a hard disk drive, into RAM. The portion of the OS code that interacts directly with the computer hardware is known as the *kernel*. The portion that interfaces with the applications and user is known as the *shell*. The user can interact with the shell using either the *command line interface (CLI)* or *graphical user interface (GUI)*. Figure 2-2 shows the relationship between the OS shell, the kernel, and the computer hardware.

Figure 2-2 OS Shell, Kernel, and Hardware Relationship



When using the CLI, the user interacts directly with the system in a text-based environment by entering commands on the keyboard at a command prompt. The system executes the command, often providing textual output on the monitor. Figure 2-3 shows the Windows CLI interface command prompt screen with a directory of drive C:\ displayed using the `dir` command.

Figure 2-3 Directory of Drive C:\ Using the Windows CLI Command Prompt Window

```

C:\ Command Prompt
C:\>dir
Volume in drive C has no label.
Volume Serial Number is 245C-A1C3

Directory of C:\

09/03/2002  09:59 AM                0 AUTOEXEC.BAT
07/16/2007  03:49 PM                <DIR>         Cisco
10/11/2003  09:33 PM                <DIR>         Cisco-Archive
01/08/2006  04:54 PM                <DIR>         Cisco-Curriculum
02/10/2007  03:38 PM                <DIR>         Cisco-Press
08/26/2005  07:19 PM                <DIR>         CKBrowser
09/03/2002  09:59 AM                0 CONFIG.SYS
04/09/2007  10:07 AM                <DIR>         DELL
04/24/2007  03:46 PM                <DIR>         Documents and Settings
05/22/2007  06:42 PM                <DIR>         Downloads
10/04/2006  06:18 PM                <DIR>         DRIVERS
04/29/2004  02:14 PM                21          dv_trace.log
01/19/2007  12:38 PM                50,804      For_Review.zip
05/22/2007  06:22 PM                517,672    hpfr5100.log
08/04/2006  08:17 AM                1386
03/28/2007  01:41 PM                222        INSTALL.LOG
09/25/2003  09:00 AM                1,217      ipconfig.txt
05/22/2007  12:02 PM                <DIR>         Local Data

```

The GUI allows the user to interact with the system in an environment that uses graphical images, multimedia, and text. Actions are performed by interacting with the images onscreen. GUI is more user friendly than CLI and requires less knowledge of the command structure to utilize the system. For this reason, many individuals rely on the GUI environments. Most operating systems offer both GUI and CLI. Although the GUI is more user friendly, knowing how to work with the CLI is still useful. The GUI depends on the graphics subsystems of the computer to display the high-resolution, multicolor images. If a problem occurs with the graphics hardware or drivers, the CLI might be the only interface available to the user for troubleshooting. Figure 2-4 shows the Windows Explorer GUI interface screen with a directory of drive C:\ displayed by clicking with the mouse.

Figure 2-4 Directory of Drive C:\ Using the Windows Explorer GUI

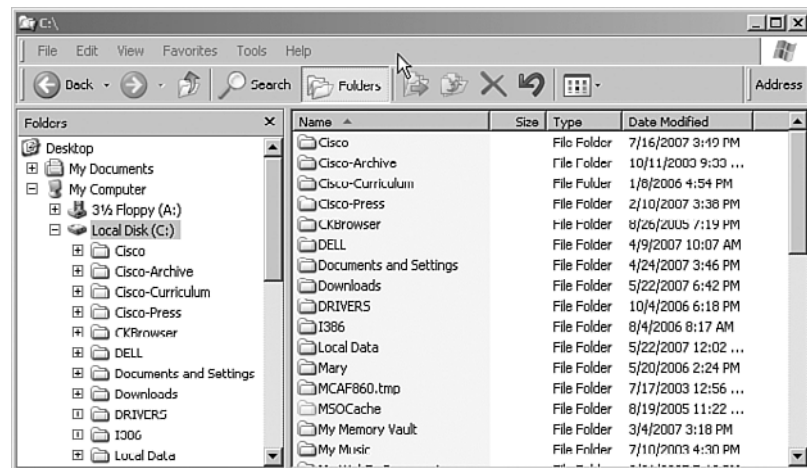
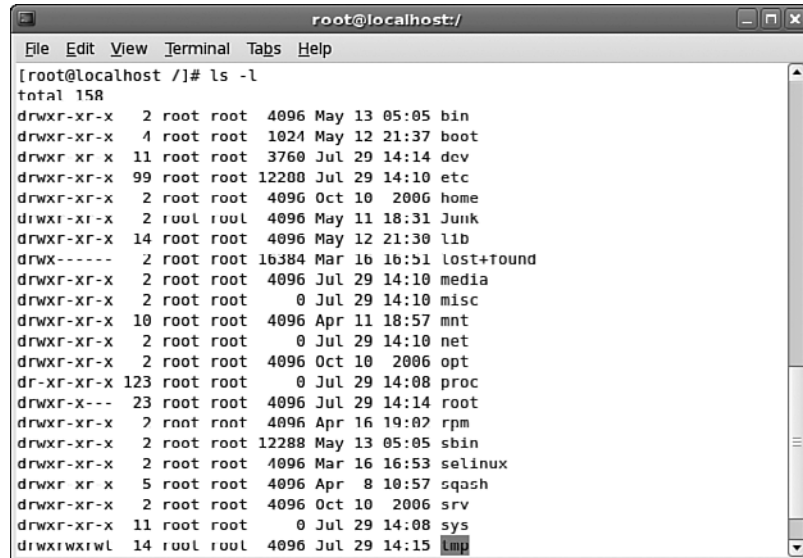


Figure 2-5 shows a Linux CLI terminal window for entering commands. The structure of the file system is displayed using the `ls -l` UNIX command, which is similar to the Windows `dir` command. The `ls -l` command lists directories (also called folders) and files, using the `-l` or “long” option. This option provides additional information for each file and directory. Without the `-l` option, only the directory and filenames would be displayed. With this listing, the name of the directory (or file) is the last entry in blue.

Figure 2-6 shows a Linux GUI window for displaying and managing directories and files. The structure of the file system is displayed using the *K Desktop Environment (KDE)* File Browser application. KDE File Browser is similar to the Windows Explorer application. Notice that directories are referred to as folders in the GUI screen.

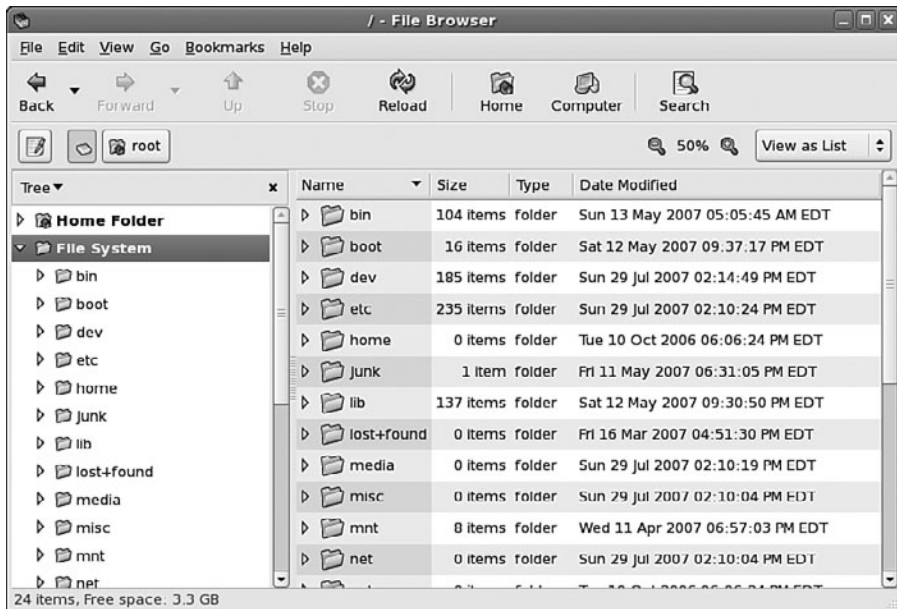
Operating systems have complete control of local hardware resources. They are designed to work with one user at a time. They enable the user to do more than one thing at a time using multiple applications. This capability is known as *multitasking*. The operating system keeps track of which resources are used by which application. A single processor can only manipulate memory to give the impression of multitasking. The CPU is actually giving each application a portion or slice of its processing time. The more applications the system is running, the smaller the time slice for each application. Multiprocessor systems can have multiple independent CPU chips or multiple CPUs on one chip (for example, dual-core). These systems can actually perform multiple tasks simultaneously.

Figure 2-5 Display of File System Directories Using the Linux CLI Terminal Window


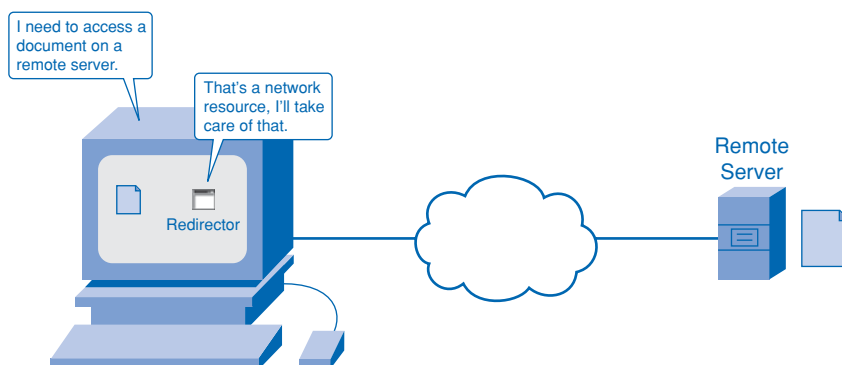
```

root@localhost: /
File Edit View Terminal Tabs Help
[root@localhost /]# ls -l
total 158
drwxr-xr-x  2 root root  4096 May 13 05:05 bin
drwxr-xr-x  4 root root 1024 May 12 21:37 boot
drwxr-xr-x 11 root root 3760 Jul 29 14:14 dev
drwxr-xr-x 99 root root 12200 Jul 29 14:10 etc
drwxr-xr-x  2 root root  4096 Oct 10  2006 home
drwxr-xr-x  2 root root  4096 May 11 18:31 Junk
drwxr-xr-x 14 root root  4096 May 12 21:30 lib
drwx----- 2 root root 16384 Mar 16 16:51 lost+found
drwxr-xr-x  2 root root  4096 Jul 29 14:10 media
drwxr-xr-x  2 root root    0 Jul 29 14:10 misc
drwxr-xr-x 10 root root  4096 Apr 11 18:57 mnt
drwxr-xr-x  2 root root    0 Jul 29 14:10 net
drwxr-xr-x  2 root root  4096 Oct 10  2006 opt
dr-xr-xr-x 123 root root    0 Jul 29 14:08 proc
drwxr-xr-x 23 root root  4096 Jul 29 14:14 root
drwxr-xr-x  2 root root  4096 Apr 16 19:02 rpm
drwxr-xr-x  2 root root 12288 May 13 05:05 sbin
drwxr-xr-x  2 root root  4096 Mar 16 16:53 selinux
drwxr-xr-x  5 root root  4096 Apr  8 10:57 squash
drwxr-xr-x  2 root root  4096 Oct 10  2006 srv
drwxr-xr-x 11 root root    0 Jul 29 14:08 sys
drwxrwxrwl 14 root root  4096 Jul 29 14:15 tmp

```

Figure 2-6 Display of File System Directories Using the Linux KDE File Browser GUI

In order to work with resources that are not directly connected to the computer system, a special piece of software called a *redirector* must be added. Redirectors make it possible to reroute a data request from the OS out of the local machine onto the network to a remote resource. The redirector can either be an integral part of the OS or can be installed separately. With a redirector, the local PC can access remote resources as a *network client*. With a redirector installed, the operating system acquires some of the characteristics of a network operating system (NOS). Figure 2-7 shows the use of the OS redirector when a host needs access to a remote resource on the network. The document being retrieved might appear to the user that it is on the local machine. However, the redirector must send the request out the network interface card (NIC) to contact the remote server and actually retrieve the document.

Figure 2-7 Accessing Remote Network Resources with the Redirector

An operating system that is specifically designed for a network is referred to as a *network operating system (NOS)*. A NOS includes features that allow management of network resources like files, printers, LAN users, and security, and is typically installed on a server. Most network resources appear to the end users as if they were on their local machine, when in reality the NOS is providing the resource to the PC. A true NOS offers complex scheduling and user management software that allows a server to share resources between many users and resources. The client OS with a redirector can access the server NOS resources as if they were directly connected.

Operating System Requirements

Many different operating systems are available. The major groupings are listed here with some examples. Most of these are proprietary commercial offerings.

- **Microsoft Windows:** XP, Vista, and 2003 Server
- **UNIX-Based:** IBM AIX, Hewlett Packard HP-UX, and Sun Solaris
- **BSD:** Free BSD
- **Linux-Based:** Many varieties
- **Macintosh OS X**
- **Non-UNIX Proprietary:** IBM OS/400, z/OS

Although most of these operating systems require the user to purchase and agree to a commercial license, several operating systems are released under a different type of licensing scheme known as the *GNU Public License (GPL)*.

Commercial licenses usually deny end users the ability to modify the program in any way. Windows XP, Mac OS X, and *UNIX* are all examples of commercial OS software.

In contrast, the GPL allows end users to modify and enhance the code, if they desire, to better suit their environment. Some common operating systems released under the GPL include *Linux* and BSD. Refer to Table 2-1 for a comparison of commercially licensed operating systems and those released under GPL.

Table 2-1 Commercial and GPL License Comparison

Criteria	Commercial License	GNU Public License (GPL)
Access	Restrictive in nature and limits what the user can do with the code.	Ensures everyone has full access to the source code and can participate in enhancement of the product.
Cost	Often very expensive depending on deployment (for example, a Windows XP license must normally be purchased for every client machine on a network).	Often released free-of-charge (for example, Linux can be freely installed on as many machines as desired). However, the cost of retraining for a GPL product might exceed the discounted cost of a commercial license.
Development Cycle	Very structured development cycle and changes not quickly available.	Development cycle is less structured and changes are more quickly implemented.
Support	Structured support available for a fee.	Less of a structured support arrangement, often relying on community (user-based) support. Some companies that distribute GPL products provide fee- based support.






Operating systems require a certain amount of hardware resources. These resources are specified by the manufacturer and include such things as

- Amount of RAM
- Hard disk space required
- Processor type and speed
- Video resolution

Manufacturers often specify both a minimum and recommended level of hardware resources. System performance at the minimum specified hardware configuration is usually poor and only sufficient to support the OS and little other functionality. The recommended configuration is usually the better option and is more likely to support standard additional applications and resources. Adding hardware over that recommended, such as another CPU and more RAM, can further improve system performance, but at a significant cost.

To take advantage of all the features provided by an operating system and installed applications, hardware resources such as sound cards, NICs, modems, microphones, and speakers are generally required. Many of the OS developers test various hardware devices and certify that they are compatible with the operating system. Always confirm that the hardware has been certified to work with the operating system before purchasing and installing it. Table 2-2 shows a sample comparison of the minimum amount of hardware needed and the recommended hardware necessary to get the most out of the OS and applications running on the computer.

Table 2-2 Minimum and Recommended OS Requirements

		Minimum	Recommended
CPU		512 Megahertz	1 Gigahertz
RAM		256 Megabytes	1 Gigabyte
Hard drive		40 Gigabytes	80 Gigabytes
Graphics card		800 x 600 pixels	1024 x 768 pixels
Optical drive		CD-ROM	DVD



Interactive Activity 2-1: Software Licensing Scenarios (2.1.2.3)

In this interactive activity, you determine the appropriate type of software licensing for a scenario. Use file ia-2123 on the CD-ROM that accompanies this book to perform this interactive activity.

Operating System Selection

You need to consider many factors before deciding on which OS to use in a given environment.

The first step in selecting an OS is to ensure that the OS being considered fully supports the requirements of the end user. Does the OS support the applications that will be run? Is the security and functionality sufficient for the needs of the users?

Next, conduct research to make sure that sufficient hardware resources are available to support the OS. This includes such basic items as memory, processors, and disk space, as well as peripheral devices such as scanners, sound cards, NICs, and removable storage.

Another consideration is the level of human resources needed to support the OS. In a business environment, a company might limit support to one or two operating systems and discourage, or even disallow, the installation of any other OS. In the home environment, the ready availability of technical support for an OS might be a determining factor. The following are some of the factors that should be considered when selecting an OS:

- Security
- Support
- Politics
- Cost
- Availability

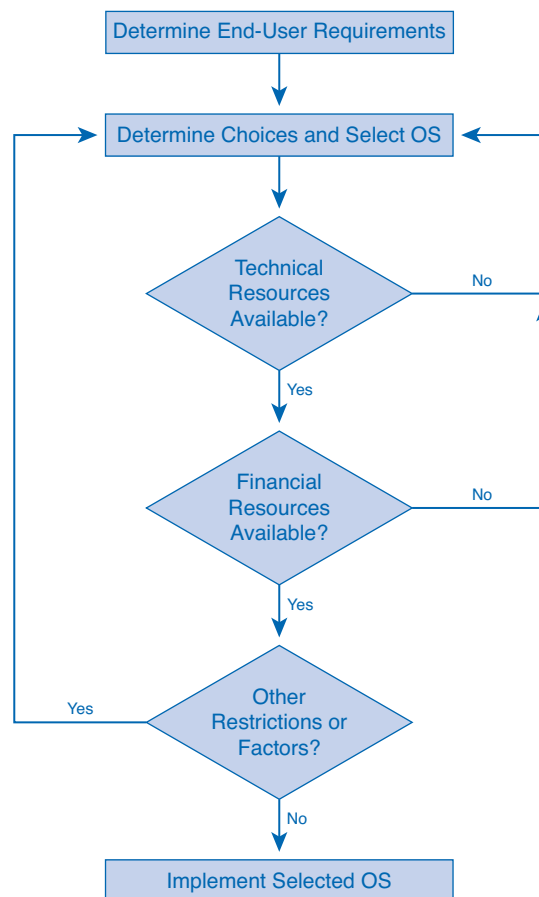
- Resources
- Platform
- Use

When implementing an OS, you should consider *total cost of ownership (TCO)* of the OS in the decision-making process. This not only includes the costs of obtaining and installing the OS, but also all costs associated with supporting it.

Another factor that might come into play in the decision-making process is the availability of the operating system. Some countries and/or businesses have made decisions to support a specific type of OS or might have restrictions barring individuals from obtaining certain types of technologies. In this type of environment, considering a particular OS, regardless of its suitability to the task, might not be possible.

The process for selecting an operating system, as shown in Figure 2-8, must take all of these factors into account.

Figure 2-8 Considerations and Requirements for Selecting an Operating System Process



Installing the Operating System

Most operating systems are installed on a clean hard drive by the manufacturer of the computer system. However, several other options are available depending on the existing operating system installed and the circumstances and goals of the user.

OS Installation Methods

An OS is installed in a defined section of the hard disk, called a *disk partition*. Various methods exist for installing an OS. The method selected for installation is based on the system hardware, the OS being installed, and user requirements. Four basic options are available for the installation of a new OS:

- **Clean install:** A clean install is done on a new system or in cases where no *upgrade* path exists between the current OS and the one being installed. It deletes all data on the partition where the OS is installed and requires application software to be reinstalled. A new computer system requires a clean install. A clean install is also performed when the existing OS installation has become damaged in some way.
- **Upgrade:** If you are staying with the same OS platform, doing an upgrade is often possible. With an upgrade, system configuration settings, applications, and data are preserved. It simply replaces the old OS files with the new OS files.
- **Multiboot:** Installing more than one OS on a computer to create a multiboot system is possible. Each OS is contained within its own partition and can have its own files and configuration settings. On startup, the user is presented with a menu to select the desired OS. Only one OS can run at a time and it has full control of the hardware. As an example of multiboot, it is possible to install Windows XP, Windows Server, and Linux all on the same system. This setup can be useful in a test environment where only one PC is available but there is a need to test several different OS and applications.
- **Virtualization:** Virtualization is a technique that is often deployed on servers. It enables multiple copies of an OS to be run on a single set of hardware, thus creating many virtual machines. Each *virtual machine* can be treated as a separate computer. This enables a single physical resource to appear to function as multiple logical resources. This type of approach generally demands more physical resources such as CPU processing and RAM because multiple OSs are running on the same machine.



Interactive Activity 2-2: Operating System Installation Scenarios (2.2.1.2)

In this interactive activity, you determine the appropriate operating system installation technique for each scenario. Use file ia-2212 on the CD-ROM that accompanies this book to perform this interactive activity.

Preparing for OS Installation

A pre-installation checklist helps ensure that the installation process is successful:

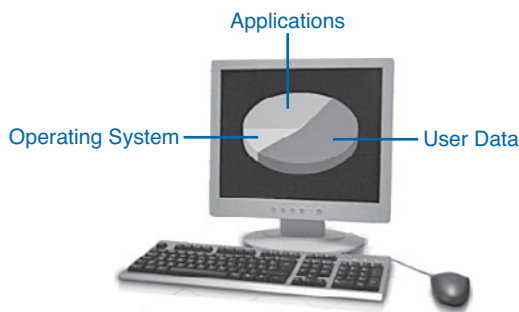


- Step 1.** Verify that all hardware is certified to work with the selected OS. Experienced users can monitor tech blogs to see what problems are being experienced on specific machines/motherboards and so on. This can save the installer time and potential problems.

- Step 2.** Verify that the hardware resources meet or exceed the published minimum requirements.
- Step 3.** Confirm that the appropriate installation medium is available. Due to the file size of current operating systems, they are usually available on both CD and DVD media.
- Step 4.** If the OS is to be installed on a system that already contains data:
- Use system diagnostic tools and utilities to ensure that the current OS installation is in good condition, free of malicious or damaging files and codes.
 - Complete a full backup of all important files.
- Step 5.** If performing a clean install, verify that all application software is available for installation.
- Step 6.** If connecting the computer to a network at this time, verify that the network configuration information is available.
- Step 7.** If this is an end-user computer and a different OS is to be installed, verify that the user has adequate training in the use of the new OS.

Before starting the installation, determining the partition structure that best meets user requirements is necessary. Figure 2-9 depicts hard disk partitioning.

Figure 2-9 Hard Disk Partitioning



One of the techniques available to help protect data is to divide the hard drive into multiple partitions. With a clean install, many technicians prefer to create one partition for data and a separate partition for the OS. This technique enables an OS to be upgraded without the risk of losing data. It also simplifies backup and recovery of data files. Applications might be installed on yet another partition. With all data files on a single partition, backing up only that partition is necessary. The OS and applications can be reinstalled in the event of a system failure.

When installing an OS, determining the type of file system to use is also necessary. A *file system* is the method the OS uses to keep track of the files. Many different file system types exist. Each OS is designed to work with one or more of these file system types and each file system type offers specific advantages:

- **File Allocation Table (FAT) 16/32:** 16- and 32-bit file systems are common with the earlier home versions of Windows OS but do not provide file security. Proprietary.
- **New Technology File System (NTFS):** Developed with Windows NT. A more robust and secure file system available with some newer home versions of Windows such as XP and Vista, and the professional and server version of other Windows OSs. Provide journaling of file system changes. Proprietary.

- **Ext2 and ext3:** Second and third extended file systems. Used primarily with Linux distributions. The ext2 file system supports large files, long filenames, and file security and also provides high-performance lookups. Ext3 adds journaling capabilities to ext2. Both ext2 and ext3 are open source.

Careful consideration should be made to the type of file systems supported by the selected OS and the benefits of each.

Although tools exist to modify the partitioning structure and file system of a hard drive after installation, they should be avoided if possible. Modifying either the file system or partition structure on a hard drive might result in *data loss*. Careful planning can help preserve the integrity of the data.

Configuring a Computer for the Network

After an OS is installed, the computer can be configured to participate in a network. A network is a group of devices, such as computers, that are connected to each other for the purposes of sharing information and resources. Shared resources can include printers, documents, and Internet access connections.

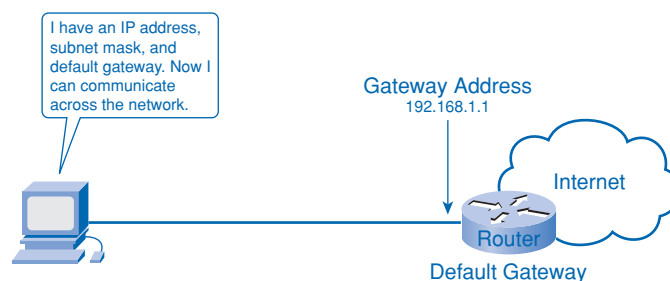
To physically connect to a network, a computer must have a *network interface card (NIC)*. The NIC is a piece of hardware that allows a computer to connect to the network medium. It might be integrated into the computer motherboard or might be a separately installed card.

In addition to the physical connection, some configuration of the operating system is required for the computer to participate in the network. Most modern networks connect to the Internet and use it to exchange information. Each computer on these networks requires an *Internet Protocol (IP)* address, as well as other information, to identify it. The IP configuration contains three parts, which must be correct for the computer to send and receive information on the network. These three parts are

- **IP address:** Identifies the computer on the network.
- **Subnet mask:** Identifies the network on which the computer is connected.
- **Default gateway:** Identifies the device that the computer uses to access the Internet or another network.

In Figure 2-10, the PC must have a NIC installed, usually an Ethernet NIC on modern local networks. It is then configured with an IP address and a subnet mask for the local network it is on. The default gateway entered as part of this configuration is the IP address of the router interface on this local network. All packets that are not destined for local hosts will be sent to the default gateway.

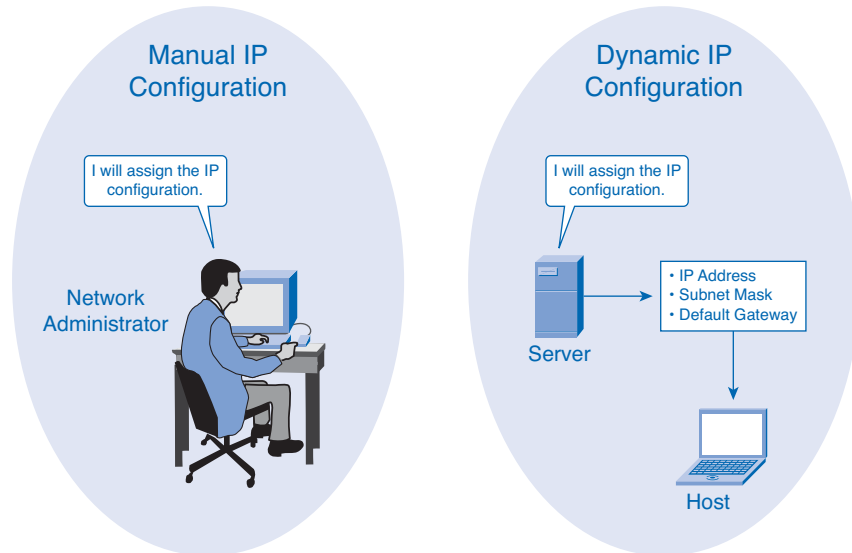
Figure 2-10 Configuration Requirements for Connecting to the Network



IP Address	192.168.1.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1

A computer IP address can be configured manually or assigned automatically by another device, as shown in Figure 2-11.

Figure 2-11 Manual and Dynamic IP Configuration



With manual configuration, the required values are entered into the computer via the keyboard, typically by a network administrator. The IP address entered is referred to as a static address and is permanently assigned to that computer.

Computers can be set up to receive their network configuration dynamically. This feature allows a computer to request an address from a pool of addresses assigned by another device within the network. When the computer is finished with the address it is returned to the pool for assignment to another computer.

Computer Naming

In addition to the IP address, some network operating systems make use of computer names. In this environment each individual system must have a unique name assigned to it.

A **computer name** provides a user-friendly way to identify a computer, making it easier for users to connect to shared resources such as folders and printers on other computers.

The network administrator should determine a logical naming scheme that helps to identify a device's type and/or its location. For example, the name PRT-CL-Eng-01 could represent the first network-attached color laser printer in the Engineering Department.

These names are manually assigned to each device, although some tools do exist to help automate the naming process. A computer description can also be entered when assigning a name to provide additional information on the location or function of the device. Figure 2-12 shows the use of Windows System Properties to enter a computer name.

Figure 2-12 Using Windows System Properties to Name a Computer

Network Name and Address Planning

As a network grows in size and complexity, ensuring that it is well planned, logically organized, and well documented becomes increasingly important.

Many organizations develop conventions for the naming and addressing of computers. These conventions provide guidelines and rules that network support personnel can use when performing these tasks. Computer names must be unique and should have a consistent format that conveys meaningful information. This method can help to determine device type, function, location, and sequence number based on the device name. IP addresses must also be unique to each device.

The use of logical device naming and addressing conventions that are well documented can greatly simplify the tasks of training and network management and can help with troubleshooting when problems arise. Figure 2-13 illustrates a logical naming scheme that can assist the network administration staff.

Figure 2-13 Computer Naming Conventions

Maintaining the Operating System

As operating systems and applications software continue to evolve, users need to keep their systems up to date to ensure they have the latest features and that their systems operate efficiently and are protected against attacks.

Why and When to Apply Patches

After an OS or application is installed, keeping it up to date with the latest patches is important.

A *patch* is a piece of program code that can correct a problem or enhance the functionality of an application program or OS. It is usually provided by the manufacturer to repair a known vulnerability or reported problem. In most cases a patched OS results in a healthier, more stable computer, as shown in Figure 2-14.

Figure 2-14 Operating System Patches



Computers should be continually updated with the latest patches unless a good reason exists not to do so. Sometimes patches negatively impact the operation of another system feature. The impact of the patch should be clearly understood before it is applied. The software manufacturer's website usually provides this information.

Applying OS Patches

Patches to operating systems can be installed in different ways, depending on the OS and the needs of the user. Options for downloading and installing updates include the following:

- **Automatic installation:** The OS can be configured to connect to the manufacturer's website and then download and install minor updates without any user intervention. Updates can be scheduled to occur during times when the computer is on, but not in use.
- **Prompt for permission:** Some users want to have control over which patches are applied. This choice is often the one for users who understand what impact a patch can have on system performance. The system can be configured to notify the end user when a patch is available. The user must then decide whether to download and install the patch.
- **Manual:** Updates that require major pieces of code to be replaced on a system should be run manually. These major updates are often called service packs and are designed to correct problems with an application or OS, and sometimes to add functionality. These service packs usually require the end user to manually connect to a website, download files, and install the update. They can also be installed from a CD available from the manufacturer.

Figure 2-15 shows the Automatic Updates options in Windows System Properties.

Figure 2-15 Windows Automatic Updates**Interactive Activity 2-3: OS Update Options (2.3.2.2)**

In this interactive activity, you determine what type of update the scenario is describing. Use file ia-2322 on the CD-ROM that accompanies this book to perform this interactive activity.

Application Patches and Updates

Applications also require patches and updates. Patches are usually released by the manufacturer to repair a detected vulnerability in the application that could lead to undesirable behavior.

Browsers and office software such as word processors and spreadsheet and database applications are common targets for network attacks. These applications require updates to correct the code that might allow the attack to succeed. The manufacturer might also develop updates that can improve product functionality, at no additional cost.

OS and application patches are generally found through the manufacturer's website. The installation process might request permission to install the update and to verify that any supporting software is present. The installation process might also install any programs that are required to support the update. Web updates can be downloaded to the system from the Internet and installed automatically. Figure 2-16 shows the Internet Explorer Security Warning that is displayed before an update is downloaded and installed.

Figure 2-16 Installing an Update from the Internet

**Lab 2-1: Examining Operating System and Application Versions (2.3.3.2)**

In this lab you will examine the current version of OS and installed applications and determine whether additional patches or updates are available. Refer to the Hands-on lab in Part II of this *Learning Guide*. You may perform this lab now or wait until the end of the chapter.

**Challenge Lab 2-2: Evaluating an OS Upgrade**

In this lab you will evaluate the existing hardware of a Windows XP computer and determine whether it can support an upgrade to Windows Vista. Refer to the Hands-on lab in Part II of this *Learning Guide*. You may perform this lab now or wait until the end of the chapter.

Summary

An operating system (OS) is the most important software in a PC. It is responsible for making all the hardware components and software applications work together. An OS can be installed by the manufacturer, an end user, or a network administrator.

The OS is comprised of a kernel, a shell, and device drivers. The kernel is the main OS program and interacts directly with the hardware through the use of device drivers. The shell interacts with the applications and the user. The user interacts with the shell through the command-line interface (CLI) or a graphical user interface (GUI).

A network operating system (NOS) is a sophisticated OS that allows a computer to share resources among many users and to treat networked resources as if they are directly connected. A NOS includes features that allow management of network resources such as files, printers, LAN users, and security, and is typically installed on a server.

Performing a pre-installation checklist before installing any new OS is important. An OS is installed in a disk partition, which is a defined section of the hard disk. Decide on partition schemes before installing the OS.

Operating systems use various file systems. The most common file systems are Windows FAT 16/32 and NTFS. For Linux they are ext2 and ext3.

To participate in a network, a computer requires a network interface card (NIC) configured with an IP address, subnet mask, and default gateway. The network should be well planned, logically organized, and well documented using standard addressing and naming conventions.

Keeping OS and application software up to date with the latest revisions, upgrades, or patches is important. A patch is a piece of program code that corrects a problem or enhances the functionality of an OS. An OS can be configured to connect automatically to the manufacturer's website and download and install minor updates without any user intervention. Service packs are major updates to an OS or software application. Application software can also require patches and updates to repair a detected vulnerability in the application. Applications patches are generally found through the manufacturer's website.

Part II of this book includes the corresponding labs for this chapter.

Activities and Labs

This summary outlines the activities and labs you can perform to help reinforce important concepts described in this chapter. You can find the activity and Packet Tracer files on the CD-ROM accompanying this book. The complete hands-on labs appear in Part II.



Interactive Activities on the CD-ROM:

Interactive Activity 2-1: Software Licensing Scenarios (2.1.2.3)

Interactive Activity 2-2: Operating System Installation Scenarios (2.2.1.2)

Interactive Activity 2-3: OS Update Options (2.3.2.2)

**Labs in Part II of This Book:**

Lab 2-1: Examining Operating System and Application Versions (2.3.3.2)

Challenge Lab 2-2: Evaluating an OS Upgrade

Check Your Understanding

Complete all the review questions listed here to test your understanding of the topics and concepts in this chapter. The “Check Your Understanding and Challenge Questions Answer Key” appendix lists the answers.

1. A network technician is installing the Linux OS on a computer. What are the most likely file systems she will select from?
2. A network technician needs to install a new operating system on a computer. In order to preserve the data, application, and configuration settings as well as the partitioning already present, which installation method should be used?
 - A. Clean install
 - B. Upgrade
 - C. Multiboot
 - D. Virtualization
3. Allan just purchased a new PC for attachment to an Ethernet local network. What three basic static IP configuration parameters will he need to enter to allow this PC to participate on the network?
4. When developing a naming scheme for a network, which two pieces of information are most beneficial when determining a computer name? (Choose two.)
 - A. Device type
 - B. Location
 - C. Year purchased
 - D. Operating system
 - E. Software installed
5. What is the term used to describe the software added to an OS that allows a user to access remote network resources as if they were local?
6. What portion of operating system code interacts directly with computer hardware?
7. Which two operating systems issued under the GPL allow end users to modify and enhance code? (Choose two.)
 - A. Windows XP
 - B. Mac OS X
 - C. Linux
 - D. BSD
 - E. UNIX

8. What three factors need to be considered when choosing an operating system? (Choose three.)
 - A. The operating system has limited availability.
 - B. The operating system supports end-user requirements.
 - C. Sufficient hardware resources are available.
 - D. Users can provide training on the new software without help.
 - E. Human resources exist to support the product.
 - F. The operating system is backward compatible with MS-DOS.

9. Jessica's home computer is currently running Windows 98. She wants to convert to Windows Vista but wants to keep her data and applications. She checks the Microsoft website and finds that there is no upgrade path from Windows 98 to Vista. What steps should she take to convert to Vista? (Choose all that apply.)
 - A. Back up her data
 - B. Verify her hardware has enough resources to support Vista
 - C. Reinstall her applications
 - D. Perform a clean install of Vista

10. A network administrator wants to set up the OS update options on the Windows PCs in his network so that he is made aware of updates when they are available but has the opportunity to check what changes the updates contain before downloading and installing them. Which update option does he need to use?
 - A. Prompt for permission
 - B. Automatic installation
 - C. Manual installation

Numbers

- 8-bit bytes, 172
- 8-bit masks, 176
- 10BASE-T cables, 158
- 16-bit masks, 177
- 802.11a standard, 237
- 802.11b standard, 237
- 802.11g standard, 237
- 802.11n standard, 237

A

Accelerated Graphic Port (AGP), 21

acceptable use policies, 277

access

- commercial versus GPL licenses, 47
- remote resources, 45
- servers, 202

access layer (Ethernet), 92, 96-98

- ARP, 101-103
- broadcast messages, 99-100
- hubs, 95-96
- IP addresses, 101
- MAC addresses, 101
- messages, 80
- switches, 96-98

access points. *See* APs

Acknowledgment (DHCP), 187

ACKs (acknowledgments), 244

activity LEDs, 311

ad-hoc networks, 240

adapter cards, 20

- controller cards, 22
- modems, 22
- NICs, 21, 25, 52
- sound, 21
- video, 21

Address Resolution Protocol (ARP), 101-103

addresses

- default gateway, 107-108, 188
- inside global, 192
- inside local, 192

IP

- assigning, 184-190*
- broadcast, 181-182*
- classes, 177-179*
- configuring, 53, 173*
- decimal equivalent, 174*
- dotted-decimal notation, 172*
- dynamic assignment, 184-185*
- function, 172*
- hierarchy, 174-175*
- host connections, 190*
- IPv4, 174*
- local Ethernet networks, 101*
- multicast, 182-183*
- NAT, 190-193*
- network boundaries, 188*
- network connections, 52*
- private, 179-180*
- public, 179*
- structure, 172-174*
- subnet masks interaction, 175-177*
- unicast, 181*
- uniqueness, 139*

logical, 91

MAC, 87

- filtering, 250*
- hexadecimal notation, 99*
- local Ethernet networks, 101*
- tables, 96-97*

physical addressing, 87-88

adware, 274

AGP (Accelerated Graphic Port), 21

American Standard Code for Information Interchange (ASCII), 12**analog frequencies, 16****antennas (WLANs), 239****anti-spam software, 280-281****anti-spyware, 282****anti-virus software, 278-280****APIPA (Automatic Private IP Addressing), 180****appliance-based firewalls, 283****application protocols**

client/server systems, 204

DNS, 209-210

e-mail clients/servers, 213-215

FTP clients/servers, 212

IM clients/servers, 215

port numbers, 217-218

VoIP clients/servers, 216

web clients/servers, 211

applications. See software; utilities**applying patches, 55****approaches to troubleshooting, 298**

bottom-up, 298

divide-and-conquer, 300

substitution, 301

top-down, 298

trial-and-error, 301

APs (access points), 239

client associations, 252

configuring, 244

*channels, 246**SSIDs, 245**wireless modes, 244*

WLANs, 239, 257

ARP (Address Resolution Protocol), 101-103**ASCII (American Standard Code for Information Interchange), 12****assigning**

channels (WLANs), 242

IP addresses, 184-190

*DHCP configuring, 186-188**DHCP servers, 185-186**dynamic, 184-185**static, 184***asymmetric services, 136-137****attacks (security)**

normal operations, 271

*brute-force, 272**Denial of Service, 271-272**Distributed Denial of Service, 272*

risks, 266

social engineering, 268-269

software, 270

*signs, 279**Trojan horses, 271**viruses, 270**worms, 270*

sources, 267-268

spam, 275

types of threats, 266

user information collection, 273

*adware, 274**cookies, 274**pop-ups/pop-unders, 275**spyware, 273*

WLANs, 248-250

attenuation, 161**authentication**

policies, 277

troubleshooting, 313

WLANs, 251

*EAP, 252**open, 251**pre-shared keys, 251***Automatic Private IP Addressing (APIPA), 180****availability of operating systems, 49**

B**back-side bus (BSB), 19****backbone connections, 132**

backing up configuration files, 257-258

bandwidth

- fiber-optic cables, support, 152
- WLANs, 256

baseband transmission, 85

baseline Linksys router, 120

Basic Service Sets (BSSs), 239

binary digits, 172

binary format, 12

BIOS (basic input output system), 6

bits, 12

blade servers, 8

Blu-ray disks, 23

Bluetooth, 234

bottom-up troubleshooting, 298

boundaries (network), 188

braids (coax), 151

bridges, 239

broadband, 133

broadcasts

- addresses, 181-182
- domains, 99
- Ethernet, 90
- local networks, 99-100
- messages, 82-84
- replying, 99
- sending, 99

brute-force attacks, 272

BSB (back-side bus), 19

BSD operating system, 46

BSSs (Basic Service Sets), 239

buffers (fiber-optic cables), 152

bus topologies, 72

business class ISP service, 135

businesses

- critical services, 8
- software, 6
- requirements, 325

busses, 19-21

bytes, 12

C

Cable Modem Termination System (CMTS), 142

cable modems, 135

cables

- 10BASE-T, 158
- best practices, 162-164
- Category 3, 148-150
- Category 5, 150
- Category 6, 150
- Category 7, 150
- certifiers, 160
- coaxial, 148, 151-152
- common, 147-148
- crossover, 156
- fiber-optic, 14, 147-148
 - bandwidth support, 152*
 - buffers, 152*
 - circuits, 152*
 - cladding, 152*
 - components, 152*
 - core, 152*
 - jackets, 152*
 - multimode, 153*
 - single-mode, 154*
 - strengthening material, 152*
- managing, 163
- metal, 14, 147
- shorts, 161
- straight-through, 156
- structured, 163
- successful termination, 162-163
- testing, 160-163
 - attenuation, 161*
 - continuity, 161*
 - crosstalk, 162*
 - opens, 161*
 - reversed-pair faults, 161*
 - shorts, 161*
 - split-pair faults, 161*
 - tools, 160-161*
- troubleshooting, 311-312

- twisted pair, 148-151
 - like devices, 157-158*
 - standards, 154-155*
 - T568A/T568B wiring schemes, 155-156*
 - termination, 158-159*
 - unlike devices, 157*
- careers in networking, 325**
- Carrier Sense, Multiple Access with Collision Avoidance (CSMA/CA), 243**
- Carrier Sense, Multiple Access with Collision Detection (CSMA-CD), 86**
- cases (computers), 26**
- catastrophic failures, 28**
- Category 3 cables, 148-150**
- Category 5 cables, 148-150**
- Category 6 cables, 150**
- Category 7 cables, 150**
- CDMA (Code Division Multiple Access), 236**
- CD-Rs (CD-Recordable), 23**
- CD-RWs (CD-Read/Write), 23**
- CDs (compact discs), 23**
- cell modem ISPs, 134**
- cell phones, 12**
- cells (WLANs), 239**
- central processing units (CPUs), 8, 18-19**
- channels**
 - communication, 74
 - wireless APs, 246
 - WLANs, 242-244
 - ACKs, 244*
 - assigning, 242*
 - CSMA/CA, 243*
 - RTS/CTS, 243*
- choosing**
 - operating systems, 48-49
 - storage devices, 24
- Cisco ISR (integrated services router), 119**
- cladding (fiber-optic cables), 152**
- Class A addresses, 178**
- Class B addresses, 178**
- Class C addresses, 178**
- Class D addresses, 178**
- Class E addresses, 178**
- classes**
 - computers, 7-8
 - IP addresses, 177-179
- classless systems (IP addresses), 177**
- clean installs, 50**
- cleaning computers, 28**
- Clear to Send (CTS), 243**
- CLI (command-line interface), 43-44**
- client/server systems**
 - Domain Name Service, 209-210
 - e-mail clients/servers, 213-215
 - client configuration, 214*
 - composing messages, 213*
 - Outlook, configuring, 215*
 - POP3/IMAP4 charts, 214*
 - FTP clients/servers, 212
 - IM clients/servers, 215
 - port numbers, 217-218
 - protocols, 204
 - application, 204*
 - internetwork, 205*
 - network access, 206*
 - transport, 205-208*
 - relationships, 202-203
 - services, 203
 - TCP/IP port numbers, 208
 - VoIP clients/servers, 216
 - web browser/web server example, 203
 - web clients/servers, 211
- clients**
 - associations with APs, 252
 - e-mail, 213-215
 - composing messages, 213*
 - configuring, 214*
 - Outlook, configuring, 215*
 - POP3/IMAP4 charts, 214*
 - FTP, 212
 - as hosts, 68
 - IM, 215

- multiple, supporting, 68
- server relationships, 68
- VoIP, 216
- web, 211
- web pages, displaying, 203
- wireless, configuring, 239, 246
 - integrated software*, 246
 - standalone software*, 247-248

clouds (Internet), 142

- physical/environmental requirements, 145-146
- sdevic, 142-144

CMTS (Cable Modem Termination System), 142

coaxial cables, 148, 151-152

Code Division Multiple Access (CDMA), 236

collision domains

- hubs, 95
- switches, 98

command-line interface (CLI), 43-44

commercial OS licenses, 46-47

communication

- channels, 74
- computers, 75
- destinations, 74
- Ethernet, 88-89
- human, 74
- Internet, 138-141
- messages
 - encapsulation*, 77-78
 - encoding*, 76
 - flow control*, 80
 - formatting*, 77-78
 - patterns*, 81-84
 - size*, 79-80
 - timing*, 80-81
- physical addressing, 87-88
- protocols, 75-76
- rules, 74-76
- sources, 74

compact discs (CDs), 23

components

- coaxial cables, 151
- computers
 - adapter cards*, 20-22
 - catastrophic failures*, 28
 - CPUs*, 18-19
 - drivers*, 30
 - hot-swapping*, 28
 - installing*, 29-31
 - motherboards*, 17-20
 - RAM*, 19-20
 - static electricity*, 28-29
 - storage devices*, 22-24
- fiber-optic cables, 152
- integrated routers, 118
- networks, 65-67
 - hosts*, 65-66
 - media*, 65
 - networking devices*, 65-66
 - peripherals*, 65
- WLANs, 238-240

composing e-mail messages, 213

computers

- adapter cards, 20
 - controller cards*, 22
 - modems*, 22
 - NICs*, 21
 - sound*, 21
 - video*, 21
- application software, 5
- cases, 26
- catastrophic failures, 28
- cleaning, 28
- communication, 75
- components, installing, 29-31
- CPUs, 18-19
- customizing, 5, 16-17
- data
 - digital information*, 12
 - storage capacities*, 13
 - transmission*, 14-16
- drivers, 30

- dust, 28
- firmware, 6
- functions, 5
- hardware, 5
 - as hosts, 68
- hot-swappable components, 28
- mass-produced, 16-17
- motherboards, 17-20
- multiple clients, supporting, 68
- naming, 53-54
- network configuration, 52-53
- operating systems, 5
 - applications and hardware communication*, 43
 - availability*, 49
 - BSD*, 46
 - choosing*, 48-49
 - CLI*, 43-44
 - defined*, 5
 - drivers*, 42
 - function*, 42
 - GUI*, 44
 - hardware certification*, 47
 - hardware resources, controlling*, 44
 - kernel*, 43
 - licensing*, 46-47
 - Linux*, 44-46, 68
 - Mac*, 46
 - Microsoft*, 70
 - multitasking*, 44
 - non-UNIX proprietary*, 46
 - NOS*, 46
 - patches*, 55
 - redirectors*, 45
 - requirements*, 10-13, 46-48
 - shell*, 43
 - total cost of ownership*, 49
 - UNIX*, 46, 68
 - Windows*, 46
- peripherals, 24-25
 - functionality*, 33
 - installing*, 31-33
 - legacy*, 33
- power supplies
 - surge suppressors*, 26
 - uninterruptible*, 27
- RAM, 19-20
- safety precautions, 29
- static electricity, 28-29
- storage devices
 - choosing*, 24
 - magnetic*, 22-23
 - optical*, 23
 - static memory*, 24
- types
 - classes*, 7-8
 - desktops*, 9
 - mainframes*, 8
 - portable*, 10-12
 - servers*, 8-9
 - workstations*, 9
- work areas, 28
- working inside, 28
- conductors (coax)**, 152
- configuration files**, 257-258
- configuring**
 - APs, 244
 - channels*, 246
 - SSIDs*, 245
 - wireless modes*, 244
 - computers for networks, 52-53
 - DHCP, 186-188
 - e-mail clients, 214
 - firewalls
 - home networking devices*, 286-287
 - multi*, 286
 - single*, 285
 - IP addresses, 53, 173
 - Outlook, 215
 - wireless clients
 - integrated software*, 246
 - standalone software*, 247-248
- connections**
 - hosts to IP addresses, 190
 - Internet backbone, 132

ISPs

- broadband, 133*
- cable modems, 135*
- cell modems, 134*
- leased lines, 133*
- speeds, 135*

Linksys integrated routers, 119-120

troubleshooting, 309

- Internet, 315-316*
- ipconfig, 303-304*
- netstat, 307-308*
- nslookup, 308-309*
- physical problems, 301-302*
- ping, 304-305*
- software utilities, 302*
- tracert, 306-307*
- wired networks, 311-312*
- WLANs, 312-314*

content filtering (ISPs), 136

continuity tests, 161

controller cards, 22

converged networks, 64

cookies, 274

core (fiber-optic cables), 152

core layer (Ethernet), 93

costs

- CD/DVD devices, 23
- commercial versus GPL licenses, 47
- total cost of ownership, 49
- wireless devices, 235
- WLANs, 256

CPUs (central processing units), 8, 18-19

crossover cables, 156

crosstalk, 148, 162

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), 243

CSMA-CD (Carrier Sense, Multiple Access with Collision Detection), 86

CTS (Clear to Send), 243

customizing computers, 5, 16-17

D

daemons, 68

data

- digital representation, 12
- loss/manipulation threats, 52, 266
- storage. *See also* RAM
 - capacities, 13*
 - choosing, 24*
 - magnetic, 22-23*
 - optical, 23*
 - static memory, 24*
- transmission, 14
 - analog frequencies, 16*
 - file size, 14*
 - interference, 149*
 - media, 14*
 - resolution, 15*
 - transfer time, 15*
 - units of measure, 15*

datagrams

- forwarding, 141
- handling, 139-140
- headers, 139
- importance, 138-139
- RFCs, 138
- routing, 105
- size, 139
- tracing, 141

DDoS (Distributed Denial of Service) attacks, 272

de facto standard, 85

dedicated networks, 64

default gateways, 107-108, 188

default routes, 109

demilitarized zone (DMZ), 284

Denial of Service (DoS) attacks, 271-272

desktop computers, 9

destinations

- communication, 74
- port numbers, 208

DHCP (Dynamic Host Configuration Protocol), 184

- acknowledgment, 187
- configuring, 186-188

- Discover message, 187
 - offers, 187
 - ranges, 187
 - requests, 187
 - servers, 185-186, 204
 - troubleshooting, 314
 - dial-up ISPs, 134**
 - digital subscriber line (DSL), 134**
 - digital versatile/video discs (DVDs), 23**
 - disks**
 - Blu-ray, 23
 - CDs, 23
 - drives, 25
 - DVDs, 23
 - floppy, 23
 - hard drives, 22
 - partitions, 50
 - disruption of service threats, 266**
 - Distributed Denial of Service (DDoS) attacks, 272**
 - distribution layers (Ethernet), 92, 103-104**
 - default gateway, 107-108
 - hosts, adding, 114-115
 - LANs, 112
 - routers, 105-107
 - routing tables, 108-112
 - divide-and-conquer troubleshooting, 300**
 - DMZ (demilitarized zone), 284**
 - DNS (Domain Name Service), 209-210**
 - documentation for troubleshooting, 317**
 - domains, 209**
 - broadcast, 99
 - collision
 - hubs*, 95
 - switches*, 98
 - DoS (Denial of Service) attacks, 271-272**
 - dotted-decimal notation, 172**
 - drivers**
 - installing, 30
 - operating systems, 42
 - drives**
 - disks, 25
 - flash, 24-25
 - floppy, 23
 - hard, 22, 51
 - optical, 48
 - tape, 23
 - DSL (digital subscriber line), 134**
 - DSLAM (DSL Access Multiplexer), 142**
 - dual-core processors, 19**
 - dust, 28**
 - DVD-Rs (DVD-Recordable), 23**
 - DVD-RWs (DVD-Read/Write), 23**
 - DVDs (digital versatile/video discs), 23**
 - Dynamic Host Configuration Protocol. *See* DHCP**
 - dynamic IP addresses, 184-185**
-
- ## E
-
- EAP (Extensible Authentication Protocol), 252**
 - echo replies, 305**
 - echo requests, 305**
 - electromagnetic waves, 233**
 - electromagnetic interference (EMI), 148**
 - electromagnetic spectrum, 233**
 - electrostatic discharge (ESD), 28-29**
 - e-mail**
 - accounts, 135
 - clients
 - composing messages*, 213
 - configuring*, 214
 - Outlook, configuring*, 215
 - POP3/IMAP4 charts*, 214
 - servers, 203, 213-215
 - spam, 275
 - virus hoax, 281
 - EMI (electromagnetic interference), 148**
 - encapsulation, 77-78**
 - encoding messages, 76**
 - encryption**
 - troubleshooting, 313
 - WLANs, 253-254
 - environmental requirements, 145-146**
 - ESD (electrostatic discharge), 28-29**

ESSs (Extended Service Sets), 240**Ethernet**

- access layer, 92-95
 - ARP, 101-103*
 - broadcast messages, 99-100*
 - hubs, 95-96*
 - IP addresses, 101*
 - MAC addresses, 101*
 - switches, 96-98*
- broadcasts, 90
- communication, 88-89
- core layer, 93
- distribution layer, 92, 103-104
 - default gateway, 107-108*
 - hosts, adding, 114-115*
 - LANs, 112*
 - routers, 105-107*
 - routing tables, 108-112*
- evolution, 86-87
- frames, 88-89
- hierarchical design, 90-91
- integrated routers, 117-119
 - Cisco ISR, 119*
 - components, 118*
 - Linksys, 119-120*
- IP traffic, managing, 92-93
- logical addressing, 91
- physical addressing, 87-88
- planning, 115-116
- protocol
 - local networks, 84-85*
 - standardization, 85-87*
- prototyping, 116-117
- resources, sharing, 121
- shared Ethernet networks, 86
- speeds, 86
- switched, 86

ext2/ext3 file systems, 52**Extended Service Sets (ESSs), 240****extended star topologies, 72****Extensible Authentication Protocol (EAP), 252****Extensible HTML (XHTML), 211****Extensible Markup Language (XML), 211****external security threats, 267****F****failures, catastrophic, 28****FAT (File Allocation Table) 16/32, 51****FDDs (floppy drives), 23****FEXT (far-end crosstalk), 162****fiber-optic cables, 14, 147-148**

- bandwidth support, 152
- buffers, 152
- circuits, 152
- cladding, 152
- components, 152
- core, 152
- jackets, 152
- multimode, 153
- single-mode, 154
- strengthening material, 152

fields (Ethernet frames), 89**File Allocation Table (FAT) 16/32, 51****file system types, 51-52****File Transfer Protocol (FTP), 204**

- clients, 212
- servers, 204, 212

files

- configuring, 257-258
- size, 14
- storage, 135
- transfer time, 15

filtering

- applications, 283
- content, 136
- MAC addresses, 250
- packets, 283
- traffic, 254
- websites, 283

firewalls, 283

- appliance-based, 283
- application/website filtering, 283
- DMZ, 284
- home networking devices, 286-287
- integrated, 284
- intranets, 284

- multi-configuration, 286
- NAT, 283
- overview, 283-284
- packet filtering, 283
- personal, 284
- server-based, 284
- single configuration, 285
- stateful packet inspection, 283
- vulnerability analysis, 287-288

FireWire, 33**firmware**

- defined, 6
- updates, 258

flash drives, 24-25**floppy drives, 23****flow control (messages), 80****formatting messages, 77-78****forwarding IP packets, 141****frames (Ethernet), 78, 88-89****FSB (front-side bus), 19****FTP (File Transfer Protocol), 204**

- clients, 212
- servers, 204, 212

functionality

- components, testing, 31
- computers, 5
- hubs, 95-96
- IP addresses, 172
- networks, 65
- operating systems, 42
- peripherals, 33
- routers, 105-107
- switches, 96-98
 - collision domains, 98*
 - MAC address table, 96-97*

F-UTP (shielded cables), 149

G**gaming devices, 12****gateways (default), 107-108****GB (gigabytes), 13****general-use software, 6****Global System for Mobile Communication (GSM), 236****GPL (GNU Public License), 46-47****graphic cards, 21****graphical user interface (GUI), 43-44****graphics resolution, 15****grounding straps, 28****GSM (Global System for Mobile Communication), 236****GUI (graphical user interface), 43-44**

H**hackers, 266****handling IP packets, 139-140****hard drives, 22, 51****hardware**

- adapter cards, 20

- controller cards, 22*

- modems, 22*

- NICs, 21, 25, 52*

- sound, 21*

- video, 21*

- application communication, 43

- cables, 147-148

- 10BASE-T, 158*

- best practices, 162-164*

- Category 3, 148-150*

- Category 5, 150*

- Category 6, 150*

- Category 7, 150*

- coaxial, 148-152*

- common, 147-148*

- crossover, 156*

- fiber-optic. See fiber-optic cables*

- managing, 163*

- metal, 14, 147*

- shorts, 161*

- straight-through, 156*

- structured, 163*

- successful termination, 162-163*

testing, 160-163
troubleshooting, 311-312
twisted pair. See twisted pair cables
 certification, 47
 CPUs, 18-19
 defined, 5
 Internet clouds, 142-144
 motherboards, 17
 CPUs, 18-19
 RAM, 19-20
 peripheral devices, 24-25
 physical/environmental requirements, 145-146
 RAM, 19-20
 installing, 30
 requirements, 19
 system, 20
 resources
 controlling, 44
 required, 47
 servers, 8
 storage devices, 22
 choosing, 24
 magnetic, 22-23
 optical, 23
 static memory, 24
 wireless
 infrared, 233-234
 radio frequency, 234-235
 WLANs, installing, 256
HDDs (hard disk drives), 22, 51
headers (IP), 139, 220
help desk, 318-319
hertz, 16
hexadecimal notation, 99
hierarchy
 Ethernet, 90-91
 IP addresses, 174-175
 protocols, 218
 topologies, 72
Hoaxbusters website, 281
hoaxes, 281

home networks

Internet cloud hardware, 142-144
 ISP service, 135
 physical/environmental requirements, 145-146

hosts, 65-66

availability, calculating, 177
 clients, 68
 computers, 68
 IP address connections, 190
 local/remote networks, 114-115
 servers, 68

hot-swapping components, 28**hotspots, 235****HTML (Hypertext Markup Language), 211****HTTP (Hypertext Transfer Protocol), 204, 211****HTTPS (secure HTTP), 211****hubs**

collision domains, 95
 functions, 95-96
 switches, compared, 96

human communication, 74**IAB (Internet Architecture Board), 131****IANA (Internet Assigned Numbers Authority), 131****IBSS (Independent Basic Service Set), 240****ICANN (Internet Corporation for Assigned Names and Numbers), 217****IDCs (insulation displacement connectors), 159****identification policies, 277****identity thefts, 266****IEEE (Institute of Electrical and Electronic Engineer), 85****IETF (Internet Engineering Task Force), 131****IM (instant messaging), 215****IMAP (Internet Message Access Protocol), 214****IMAP4 (Internet Message Access Protocol version 4), 214****inbound NAT, 193****incident handling procedures, 277****Independent Basic Service Set (IBSS), 240**

Industrial, Scientific, and Medical (ISM) bands, 234**industry software, 6****Infoplease website, 131****information thefts, 266****infrared (IR) technology, 233****Infrared Direct Access (IrDA), 233****infrastructure mode (WLANs), 240-242****input peripherals, 24****inside global addresses, 192****inside local addresses, 192****installing**

APs, 257

components, 29-31

drivers, 30

operating systems, 50

*clean, 50**file system types, determining, 51-52**multiboot, 50**pre-installation checklists, 50-51**upgrades, 50**virtualization, 50*

peripherals, 31-33

*legacy, 33**ports, 32-33**steps, 33*

RAM, 30

wireless hardware, 256

instant messaging (IM), 215**Institute of Electrical and Electronic Engineers (IEEE), 85****insulation displacement connectors (IDCs), 159****insulators (coax), 152****integrated firewalls, 284****integrated routers, 117**

Cisco ISR, 119

components, 118

Linksys, 119-120

local networks, 118-119

integrated services router (ISR), 119**integrated wireless utility software, 246****interference**

data transmission, 149

twisted-pair cables, 148

internal security threats, 267**International Organization for Standardization (ISO), 221****Internet**

backbone connections, 132

broadband, 133

clouds, 142-144

connectivity, troubleshooting, 315-316

development/management websites, 131

IAB, 131

IANA, 131

IETF, 131

Internet Society (ISOC), 130-131

IP packets

*forwarding, 141**handling, 139-140**headers, 139**importance, 138-139**RFCs, 138**size, 139**tracing, 141*

IRTF, 131

ISPs, 131

*broadband, 133**cable modems, 135**cell modems, 134**connection options, 133-135**connectivity, troubleshooting, 315-316**dial-up, 134**DSL, 134**Internet backbone connections, 132**IXPs, 132**leased lines, 133-135**levels of service, 135-137**modems, 133**POPs, 132**satellite, 135*

overview, 130

physical/environmental requirements, 145-146

Internet Architecture Board (IAB), 131

Internet Assigned Numbers Authority (IANA), 131

Internet Corporation for Assigned Names and Numbers (ICANN), 217

Internet Engineering Task Force (IETF), 131

Internet Exchange Points (IXPs), 132

Internet Message Access Protocol (IMAP), 214

Internet Message Access Protocol version 4 (IMAP4), 214

Internet Protocol. *See* IP

Internet Research Task Force (IRTF), 131

Internet service providers. *See* ISPs

internetwork protocol, 205

interoperability of Wi-Fi, 238

intranet firewalls, 284

intrusion threats

risks, 266

social engineering, 268

phishing, 269

pretexting, 268

vishing, 269

sources, 267-268

types, 266

IP (Internet Protocol), 52, 138, 205

addresses. *See* IP addresses

client/server systems, 205

datagram, 105

headers, 220

packets

forwarding, 141

handling, 139-140

headers, 139

importance, 138-139

RFCs, 138

routing, 105

size, 139

tracing, 141

telephone, 136

traffic, 92-93

version 4 (IPv4), 174

version 6 (IPv6), 174

IP addresses

assigning

DHCP configuration, 186-188

DHCP servers, 185-186

dynamic, 184-185

static, 184

broadcast, 181-182

classes, 177-179

configuring, 53, 173

decimal equivalent, 174

dotted-decimal notation, 172

function, 172

hierarchy, 174-175

host connections, 190

IPv4, 174

local Ethernet networks, 101

multicast, 182-183

NAT, 190-193

back at source, 193

destination replies, 193

inbound, 193

outbound NAT, 192

overloaded, 191

packet generation, 192

network boundaries, 188

network connections, 52

private, 179-180

public, 179

structure, 172-174

subnet masks interaction, 175-177

unicast, 181

uniqueness, 139

ipconfig utility, 303-304

IPv4 (IP version 4), 174

IPv6 (IP version 6), 174

IR (infrared) technology, 233

IrDA (Infrared Direct Access), 233

IRTF (Internet Research Task Force), 131

ISM (Industrial, Scientific, and Medical) bands, 234

ISO (International Organization for Standardization), 221

ISOC (Internet Society), 130-131

ISPs (Internet service providers), 131

- broadband, 133
- cable modems, 135
- cell modems, 134
- connections
 - options, 133-135*
 - troubleshooting, 315-316*
- dial-up, 134
- DSL, 134
- Internet backbone connections, 132
- IXPs, 132
- leased lines, 133-135
- levels of service, 135-137
- modems, 133
- POPs, 132
- satellite, 135

IXPs (Internet Exchange Points), 132**J – K****jackets (fiber-optic cables), 152****KB (kilobytes), 13****kbps (thousands of bits per second), 15****kernel, 43****keyboards, 25****kilo, 13****L****LANs (local-area networks), 112**

- Ethernet, 84-85
 - broadcasts, 90*
 - communication, 88-89*
 - frames, 88-89*
 - hierarchical designs, 90-91*
 - IP traffic, managing, 92-93*
 - layers. See layers (Ethernet)*
 - logical addressing, 91*

- physical addressing, 87-88*
- standardization, 85-87*

hosts, adding, 114-115

integrated routers, 117-119

- Cisco ISR, 119*

- components, 118*

- Linksys, 119-120*

local Ethernet network, 112

planning, 115-116

protocols

- importance, 84-85*

- standardization, 85-87*

prototyping, 116-117

resources, sharing, 121

switches, 86

wireless

- APs, configuring, 244-246*

- authentication, 251-252*

- bandwidth, 256*

- channels, 242-244*

- clients, configuring, 246-248*

- connectivity, troubleshooting, 313-314*

- costs, 256*

- encryption, 253-254*

- MAC address filtering, 250*

- planning, 255-258*

- security attacks, 248-250*

- traffic filtering, 254*

- war driving, 249*

- war walking, 249*

laptops, 10**layered models**

- OSI, 221-223

- protocols, 218-219

- TCP/IP, 219-221

layers (Ethernet)

- access, 92-95

- ARP, 101-103*

- broadcast messages, 99-100*

- hubs, 95-96*

- IP addresses, 101*

- MAC addresses, 101*

- switches, 96-98*

core, 93
 distribution, 92, 103-104
 default gateway, 107-108
 hosts, adding, 114-115
 LANs, 112
 routers, 105-107
 routing tables, 108-112

leased lines (ISPs), 133-135

LEDs (light-emitting diodes), 119, 310-311

legacy devices, 33

levels of service (ISPs), 135-137

licensing (operating systems), 46-47

light-emitting diodes (LEDs), 119

Linksys integrated routers, 119-120

Linux, 46

 CLI Terminal Window, 44
 daemons, 68

local applications, 6-7

local-area networks. *See* LANs

logical addressing (Ethernet), 91

logical topologies, 71

loopback addresses, 180

losing data, 52

M

MAC (Media Access Control) addresses, 87

 filtering, 250
 hexadecimal notation, 99
 local Ethernet networks, 101
 tables, 96-97

Mac operating systems, 46

magnetic storage devices, 22-23

mainframes, 8

maintenance

 applications, 56
 operating systems, 55

managing

 cables, 163
 IP traffic, 92-93

mass-produced computer systems, 16-17

MB (megabytes), 13

Mbps (millions of bits per second), 15

McAfee Virus Hoaxes website, 281

measuring storage capacities, 13

Media Access Control. *See* MAC addresses

media, 65

megabytes (MB), 13

memory. *See* RAM

mesh topologies, 72

messages

 broadcast, 99-100
 encapsulation, 77-78
 encoding, 76
 formatting, 77-78
 patterns, 81
 broadcast, 82-84
 multicast, 82
 unicast, 81
 sending/receiving, 219-221
 size, 79-80
 timing, 80
 access method, 80
 flow control, 80
 responses, 81

metal cables, 14, 147

Microsoft

 operating systems, 70
 Outlook, configuring, 215
 Windows, 46

millions of bits per second (Mbps), 15

mobile phone networks, 63

mobility of WLANs, 235

modems, 25

 defined, 14
 ISPs, 133
 overview, 22

monitors, 25

motherboards, 17

 CPUs, 18-19
 RAM, 19-20

mounting CPUs, 19

mouse, 25

multiboot installations, 50

multicast addresses, 182-183

multicasting (communication), 82

multicore processors, 19

multi-function devices. *See* integrated routers

multimeters, 161

multimode fiber, 153

multiprocessor systems, 19

multitasking, 44

N

names

computers, 53-54

domains, 209

NAT (Network Address Translation), 190-192

back at source, 193

destination replies, 193

firewalls, 283

inbound, 193

IP addresses, 193

outbound NAT, 192

overloaded, 191

packet generation, 192

near-end crosstalk (NEXT), 162

netstat utility, 307-308

network access protocols, 206

Network Address Translation. *See* NAT

network applications, 6-7

network interface cards (NICs), 21, 25, 52

network numbers, 177

network operating system (NOS), 46

Network Operations Center (NOC), 139

networks

advantages, 65

components, 65-67

hosts, 65-66

media, 65

networking devices, 65-66

peripherals, 65

computers, configuring, 52-53

converged, 64

dedicated, 64

defined, 63

devices, 65-66

functions, 65

monitoring tools, 297

peripherals, 24

topologies, 71-73

types, 63

New Technology File System (NTFS), 51

NEXT (near-end crosstalk), 162

NICs (network interface cards), 21, 25, 52

NOC (Network Operations Center), 139

non-UNIX proprietary operating systems, 46

non-volatile storage, 22

magnetic, 22-23

optical, 23

static memory devices, 24

NOS (network operating system), 46

notebooks, 10

nslookup utility, 308-309

NTFS (New Technology File System), 51

O

octets, 172

offers (DHCP), 187

office suites, 6

open authentication (WLANs), 251

Open System Interconnection (OSI), 221-223

opens, 161

operating systems

applications and hardware communication, 43

availability, 49

BSD, 46

choosing, 48-49

CLI, 43-44

defined, 5

drivers, 42

function, 42

GUI, 44

hardware

certification, 47

resources, controlling, 44

installing, 50
clean, 50
file system types, determining, 51-52
multiboot, 50
pre-installation checklists, 50-51
upgrades, 50
virtualization, 50

kernel, 43

licensing, 46-47

Linux, 44-46, 68

Mac, 46

Microsoft, 70

multitasking, 44

non-UNIX proprietary, 46

NOS, 46

patches, 55

redirectors, 45

requirements, 10-13, 46-48

shell, 43

total cost of ownership, 49

UNIX, 46, 68

Windows, 46

optical storage devices, 23, 48

OSI (Open System Interconnection), 221-223

outbound NAT, 192

Outlook, configuring, 215

output peripherals, 24

outside sources of help, 317-318

overloaded NAT, 191

P

packets

broadcast, 181

echo replies, 305

echo requests, 305

filtering, 283

IP
forwarding, 141
handling, 139-140
headers, 139
importance, 138-139
RFCs, 138
routing, 105

size, 139

tracing, 141

NAT

back at source, 193

destination replies, 193

inbound NAT, 193

outbound NAT, 192

packet generation, 192

stateful inspection, 283

unicast, 181

parallel ports, 32

partitioning

disks, 50

hard drives, 51

passphrases (WEP), 253

password policies, 277

PAT (Port Address Translation), 191

patches

applications, 56

operating systems, 55

panels, 159

security policies, 278

patterns (messages), 81

broadcast, 82-84

multicast, 82

unicast, 81

PCs (personal computers), 9

PDA's (personal digital assistants), 11

PDU's (protocol data units), 88

peer-to-peer networks, 69-70

peripherals, 24-25, 65

functionality, 33

installing, 31

legacy, 33

ports, 32-33

steps, 33

personal computers (PCs), 9

personal digital assistants (PDAs), 11

personal firewalls, 284

personal home pages, 135

phishing, 269

physical addressing, 87-88

physical connectivity problems, 301-302**physical requirements, 145-146****physical topologies, 71-73****picture element (pixels), 15-16****ping of death, 272****ping utility, 141, 304-305****pixels, 15-16****planning**

local networks, 115-116

WLANs, 255

*APs installation/security, 257**configuration backup, 257-258**firmware updates, 258**hardware installations, 256**standards, 255-256***Pocket PCs, 11****PoE (Power over Ethernet), 155****points of presence (POPs), 132****policies (security), 276**

acceptable use, 277

anti-spam, 280-281

anti-spyware, 282

anti-virus software, 278-280

goals, 277

identification/authentication, 277

incident handling procedures, 277

passwords, 277

procedures, 277

remote access, 277

tools/applications, 277

updates/patches, 278

POP3 (Post Office Protocol), 214**POPs (points of presence), 132****pop-unders, 275****pop-ups, 275****Port Address Translation (PAT), 191****portable computing devices, 10**

cell phones, 12

gaming devices, 12

laptops, 10

PDAs, 11

Pocket PCs, 11

Tablet PCs, 11

ports

AGP, 21

FireWire, 33

forwarding, 287

numbers

*client/server systems, 217-218**TCP/IP, 208*

parallel, 32

peripheral installations, 32-33

private, 217

PS/2, 32

registered, 217

RJ-11, 32

RJ-45, 33

serial, 32

USB, 32

VGA, 32

well-known, 217

Post Office Protocol (POP3), 214**power LEDs, 311****power networks, 63****Power over Ethernet (PoE), 155****power supplies (computers), 26**

surge suppressors, 26

uninterruptible, 27

pre-installation checklists, 50-51**pre-shared keys (PSKs), 251****pretexting, 268****printers, 25****private IP addresses, 179-180. See also NAT****private ports, 217****procedures (security), 277****processing cores (CPUs), 19****protocol data units (PDUs), 88****protocols**

application

*clients/servers, 204**DNS, 209-210**e-mail clients/servers, 213-215**FTP clients/servers, 212**IM clients/servers, 215**port numbers, 217-218*

- VoIP clients/servers*, 216
 - web clients/servers*, 211
 - ARP, 101-103
 - client/server systems, 204
 - application*, 204
 - internetwork*, 205
 - network access*, 206
 - transport*, 205-208
 - communication, 75-76
 - DHCP, 184
 - Acknowledgment*, 187
 - configuring*, 186-188
 - Discover message*, 187
 - offers*, 187
 - ranges*, 187
 - requests*, 187
 - EAP, 252
 - Ethernet
 - broadcasts*, 90
 - communication*, 88-89
 - evolution*, 86-87
 - frames*, 88-89
 - hierarchical design*, 90-91
 - integrated routers*, 117-120
 - IP traffic, managing*, 92-93
 - layers*. See *layers (Ethernet)*
 - local networks*, 84-85
 - logical addressing*, 91
 - physical addressing*, 87-88
 - planning*, 115-116
 - prototyping*, 116-117
 - resources, sharing*, 121
 - shared Ethernet networks*, 86
 - speeds*, 86
 - standardization*, 85-87
 - switched*, 86
 - hierarchy, 218
 - HTTP, 204, 211
 - HTTPS, 211
 - IMAP, 214
 - IMAP4, 214
 - interaction in layered models, 218-219
 - IP, 52, 138, 205
 - addresses*. See *IP addresses*
 - client/server systems*, 205
 - datagram*, 105
 - headers*, 220
 - packets*, 138-141
 - telephone*, 136
 - traffic*, 92-93
 - version 4 (IPv4)*, 174
 - version 6 (IPv6)*, 174
 - local networks
 - importance*, 84-85
 - standardization*, 85-87
 - OSI model, 221-223
 - POP3, 214
 - SMTP, 213
 - TCP, 205
 - client/server systems*, 206-207
 - port numbers*, 217-218
 - TCP/IP, 208, 219-221
 - UDP
 - client/server systems*, 206-208
 - port numbers*, 217-218
 - web server stack, 218
 - WEP, 253
 - WPA, 254
 - prototyping local networks, 116-117**
 - PS/2 ports, 32**
 - PSKs (pre-shared keys), 251**
 - PSTN (public switched telephone network), 216**
 - public IP addresses, 179**
 - public switched telephone network (PSTN), 216**
- ## Q – R
-
- quad-core processors, 19**
 - rack-mounted servers, 8**
 - radio frequency (RF), 234-235**
 - radio frequency interference (RFI), 148**
 - RADIUS (Remote Authentication Dial-in User Service), 252**

RAM (random-access memory), 8, 19-20

- installing, 30
- requirements, 19
- system, 20

ranges (DHCP), 187**receiving messages, 219-221****redirectors, 45****regional Internet registry (RIR), 139****registered ports, 217****reliability (WLANs), 235****remote access policies, 277****Remote Authentication Dial-in User Service (RADIUS), 252****remote network hosts, adding, 114-115****remote resources, accessing, 45****replying, broadcast messages, 99****Request for Comments (RFCs), 138**

- 1918 private address space, 179
- website, 138

RFI (radio frequency interference), 148**Request to Send (RTS), 243****requests (DHCP), 187****requirements**

- business, 325
- operating systems, 10-13, 46-48
- optical drives, 48
- physical/environmental, 145-146
- RAM, 19

resources

- hardware
 - controlling, 44*
 - required, 47*
- remote, 45
- sharing, 121

responses (messages), 81**restoring configuration files, 257-258****reversed-pair faults, 161****RF (radio frequency), 234-235****RFCs (Request for Comments), 138**

- 1918 private address space, 179
- website, 138

RFI (radio frequency interference), 148**ring topologies, 72****RIR (regional Internet registry), 139****RJ-11 ports, 32****RJ-45 ports, 33****routers, 105**

- functionality, 105-107
- integrated, 117
 - Cisco ISR, 119*
 - components, 118*
 - Linksys, 119-120*
 - local networks, 118-119*
- interfaces, 112
- routing tables
 - default routes, 109*
 - forwarding messages to remote hosts, 110*
 - local Ethernet network, 108-112*
 - sending messages to default gateway, 111*
 - sending messages to hosts on another network, 110*
- wireless modes, 244

routing tables

- default routes, 109
- forwarding messages to remote hosts, 110
- local Ethernet network, 108-112
- sending messages
 - default gateway, 111*
 - hosts on another network, 110*

RTS (Request to Send), 243**rules of communication, 74-76****S****safety precautions, 29****satellite ISPs, 135****scalability (WLANs), 235****scanners, 25****ScTP (screened twisted-pair), 149****ScTP (shielded cables), 149****security**

- APs, 257
- brute-force, 272
- Denial of Service, 271-272
- Distributed Denial of Service, 272
- firewalls, 283
 - appliance-based, 283*
 - application/website filtering, 283*

- DMZ, 284
- home networking devices, 286-287
- integrated, 284
- intranets, 284
- multi-configuration, 286
- NAT, 283
- overview, 283-284
- packet filtering, 283
- personal, 284
- server-based, 284
- single configuration, 285
- stateful packet inspection, 283
- vulnerability analysis, 287-288
- policies, 276
 - acceptable use, 277
 - anti-spam, 280-281
 - anti-spyware, 282
 - anti-virus software, 278-280
 - goals, 277
 - identification/authentication, 277
 - incident handling procedures, 277
 - passwords, 277
 - procedures, 277
 - remote access, 277
 - tools/applications, 277
 - updates/patches, 278
- recommended practices, 288
- software attacks, 270
 - signs, 279
 - Trojan horses, 271
 - viruses, 270
 - worms, 270
- spam, 275
- threats
 - risks, 266
 - social engineering, 268-269
 - sources, 267-268
 - types, 266
- user information collection, 273
 - adware, 274
 - cookies, 274
 - pop-ups/pop-unders, 275
 - spyware, 273
- WLANs, 236
 - attacks, 248-250
 - authentication, 251-252
 - encryption, 253-254
 - MAC address filtering, 250
 - traffic filtering, 254
 - war driving, 249
 - war walking, 249
- segments, 207**
- selecting. See choosing**
- sending messages, 99, 219-221**
- serial ports, 32**
- server-based firewalls, 284**
- server-based networks, 69**
- servers, 8-9**
 - accessing, 202
 - blade, 8
 - browser relationships, 203
 - client relationships, 68
 - DHCP, 204
 - configuring, 187
 - IP addresses, assigning, 185-186
 - troubleshooting, 314
 - DNS, 209-210
 - e-mail, 203, 213-215
 - FTP, 204, 212
 - hardware, 8
 - as hosts, 68
 - IM, 215
 - overview, 8
 - rack-mounted, 8
 - services, 8
 - spam blockers, 280
 - standalone, 8
 - Telnet, 203
 - VoIP, 216
 - web, 204, 211, 218
- Service Set Identifiers. See SSIDs**
- service-level agreements (SLAs), 135**
- services**
 - asymmetric, 136-137
 - business critical, 8
 - client/server systems, 203

- ISPs, 135-137
- servers, 8
- symmetric, 136-137
- web hosting, 135
- sharing**
 - bandwidth, 95
 - Ethernet networks, 86
 - resources, 121
- shell, 43**
- shielded cables, 149**
- shorts, 161**
- Simple File Sharing, 121**
- Simple Mail Transfer Protocol (SMTP), 213**
- single-mode fiber, 154**
- site surveys (WLANs), 256**
- size**
 - Ethernet frames, 89
 - files, 14
 - IP packets, 139
 - messages, 79-80
- SLAs (service-level agreements), 135**
- small business networks**
 - Internet cloud hardware, 142-144
 - physical/environmental requirements, 145-146
- small office/home office (SOHO) networks, 65**
- SMTP (Simple Mail Transfer Protocol), 213**
- social engineering, 268**
 - phishing, 269
 - pretexting, 268
 - vishing, 269
- software. *See also* utilities**
 - anti-spam, 280-281
 - anti-spyware, 282
 - anti-virus, 278-280
 - application, 5
 - attacks, 270
 - signs*, 279
 - Trojan horses*, 271
 - viruses*, 270
 - worms*, 270
 - business/industry, 6
 - connectivity, troubleshooting, 302
 - ipconfig*, 303-304
 - netstat*, 307-308
 - nslookup*, 308-309
 - ping*, 304-305
 - tracert*, 306-307
 - filtering, 283
 - general-use, 6
 - hardware, communicating, 43
 - integrated wireless utility, 246
 - local, 6-7
 - network, 6-7
 - office suites, 6
 - patches, 56
 - security, 277
 - standalone wireless utility, 247-248
- SOHO (small office/home office) networks, 65**
- sound cards, 21**
- sources**
 - communication, 74
 - intrusion threats, 267-268
 - port numbers, 208
- spam, 275, 280-281**
- speed**
 - CPUs, 19
 - Ethernet, 86
 - file transfers, 15
 - ISPs, 135
- SPI (stateful packet inspection), 283**
- split-pair faults, 161**
- spyware, 273, 282**
- SSIDs (Service Set Identifiers), 240**
 - APs, configuring, 245
 - broadcast feature, 249
 - security attacks, 249
 - troubleshooting, 313
 - WLANs, 240-242
- standalone servers, 8**
- standalone wireless utility software, 247-248**
- standards**
 - protocols, 85-87
 - twisted pair cables, 154-155
 - WLANs, 237-238, 255-256

star topologies, 72
STAs, 239
stateful packet inspection (SPI), 283
static electricity, 28-29
static IP addresses, 184
static memory devices, 24
status LEDs, 311
storage
 capacities, 13
 devices, 22
 choosing, 24
 magnetic, 22-23
 optical, 23
 static memory, 24
 files, 135
 peripherals, 24
STP (shielded twisted-pair), 149
straight-through cables, 156
strengthening material (fiber-optic cables), 152
structure, 172-174
 cables, 163
 troubleshooting, 300
subnet masks
 8-bit masks, 176
 16-bit masks, 177
 host availability, calculating, 177
 IP addresses
 classes, 177-179
 interaction, 175-177
substitution troubleshooting, 301
support
 commercial versus GPL licenses, 47
 multiple clients, 68
surge suppressors, 26
switches
 collision domains, 98
 Ethernet, 86
 functions, 96-98
 hubs, compared, 96
 LANs, 86
 MAC address table, 96-97

symmetric services, 136-137
synchronous floods, 271
systems
 custom-assembled, 16-17
 mass-produced, 16-17
 RAM, 20
 resources, 31

T

T568A/T568B wiring scheme, 155-156

tables

ARP, 101-103
 routing
 default routes, 109
 forwarding messages to remote hosts, 110
 local Ethernet network, 108-112
 sending messages to default gateway, 111
 sending messages to hosts on another network, 110

Tablet PCs, 11

tape drives, 23

TB (terabytes), 13

TCO (total cost of ownership), 49

TCP (Transmission Control Protocol), 205

client/server systems, 206-207
 layered model, 219-221
 port numbers, 217-218

TCP/IP (Transmission Control Protocol/Internet Protocol)

layered model, 219-221
 port numbers, 208

technologies (wireless), 233

benefits, 235
 infrared, 233-234
 limitations, 235-236
 radio frequency, 234-235
 security, 236

telephone networks, 64

television networks, 64

Telnet servers, 203

terabytes (TB), 13

termination of cables, 162-163

- coax, 151
- UTP, 158-159

testing

- cables, 160-163
 - attenuation, 161*
 - continuity, 161*
 - crosstalk, 162*
 - opens, 161*
 - reversed-pair faults, 161*
 - shorts, 161*
 - split-pair faults, 161*
 - tools, 160-161*

- components, 31
- peripherals, 33

thousands of bits per second (kbps), 15**threats (security)**

- brute-force, 272
- Denial of Service, 271-272
- Distributed Denial of Service, 272
- normal operations, 271
- risks, 266
- social engineering, 268
 - phishing, 269*
 - pretexting, 268*
 - vishing, 269*
- software attacks, 270
 - signs, 279*
 - Trojan horses, 271*
 - viruses, 270*
 - worms, 270*
- sources, 267-268
- spam, 275
- types, 266
- user information collection, 273
 - adware, 274*
 - cookies, 274*
 - pop-ups/pop-unders, 275*
 - spyware, 273*

timing messages, 80

- access method, 80
- flow control, 80
- responses, 81

tools

- cable testing, 160-161
- networking monitoring, 297
- ping utility, 141
- security, 277
- traceroute utility, 141

top-down troubleshooting, 298**topologies, 71-73****total cost of ownership (TCO), 49****traceroute utility, 141****tracert utility, 306-307****tracing IP packets, 141****traffic**

- filtering, 254
- IP, 92-93

trailers, 220**Transmission Control Protocol. *See* TCP****Transmission Control Protocol/Internet Protocol. *See* TCP/IP****transmitting data, 14, 86**

- analog frequencies, 16
- file size, 14
- interference, 149
- media, 14
- resolution, 15
- transfer time, 15
- units of measure, 15

transport protocols, client/server systems, 205-208**trial-and-error troubleshooting, 301****Trojan horses, 271****troubleshooting**

- approaches, 298
 - bottom-up, 298*
 - divide-and-conquer, 300*
 - substitution, 301*
 - top-down, 298*
 - trial-and-error, 301*
- connectivity, 309
 - Internet, 315-316*
 - ipconfig, 303-304*
 - netstat, 307-308*

nslookup, 308-309
physical problems, 301-302
ping, 304-305
software utilities, 302
tracert, 306-307
wired networks, 311-312
WLANs, 312-314

documentation, 317
 help desk, 318-319
 information, gathering, 297
 LEDs, 310-311
 outside sources of help, 317-318
 overview, 296
 steps, 296
 structured, 300

twisted pair cables, 148-151

like devices, 157-158
 standards, 154-155
 T568A/T568B wiring schemes, 155-156
 termination, 158-159
 unlike devices, 157

types

busses, 19
 computers
 classes, 7-8
 desktops, 9
 mainframes, 8
 portable, 10-12
 servers, 8-9
 workstations, 9
 file systems, 51-52
 intrusion threats, 266
 networks, 63
 wireless networks, 236

U

UDP

client/server systems, 206-208
 port numbers, 217-218

unicast addresses, 81, 181

UNII (Unlicensed National Information Infrastructure) bands, 234

uninterruptible power supplies (UPSs), 27

unit of measure (UOM), 13

UNIX, 46, 68

unshielded twisted-pair (UTP), 149-150

unterminated UTP cable, 156

UOM (unit of measure), 13

updates

firmware, 258
 operating systems, 50
 security policies, 278

UPSs (uninterruptible power supplies), 27

USB memory keys, 24

USB ports, 32

US-Cert website, 280

utilities. *See also* software

connectivity, troubleshooting, 302
ipconfig, 303-304
netstat, 307-308
nslookup, 308-309
ping, 141, 304-305
tracert, 141
tracert, 306-307

UTP (unshielded twisted-pair), 149-150

like devices, 157-158
 T568A/T568B, 155-156
 termination, 158-159
 unlike devices, 157
 unterminated, 156

V

VGA ports, 32

video cards, 21

video on demand, 136

virtual machines, 50

virtualization (operating systems), 50

viruses, 270

anti-virus software, 278-280
 hoaxes, 281
 ISPs, scanning, 136

vishing, 269

VoIP (Voice over IP), 216

W

wall jacks, 159

war driving, 249

war walking, 249

wavelengths, 233

web browsers, 203

web clients, 211

web hosting services (ISPs), 135

web servers, 204, 211

protocol stack, 218

web browser relationships, 203

websites

filtering, 283

Hoaxbusters, 281

IAB, 131

IANA, 131

ICANN, 217

IETF, 131

Infoplease, 131

Internet management/development, 131

IRTF, 131

ISOC, 131

McAfee Virus Hoaxes, 281

RFCs, 138

US-Cert, 280

well-known ports, 217

WEP (Wired Equivalency Protocol), 253

Wi-Fi (Wireless Fidelity), 237

Alliance, 238

Protected Access (WPA), 254

Windows

CLI, 43

Explorer GUI, 44

operating systems, 46

Simple File Sharing, 121

wire maps, 161

Wired Equivalency Protocol (WEP), 253

wired network connectivity, troubleshooting, 311-312

wireless clients, 239

Wireless Fidelity. See Wi-Fi

wireless networks

benefits, 235

LANs. *See* WLANs

limitations, 235-236

media, 14

security, 236

technologies

infrared, 233-234

radio frequency, 234-235

technologies, 233

types, 236

wireless personal-area networks (WPANs), 236

wireless wide-area networks (WWANs), 236

WLANs (wireless LANs)

APs, configuring, 244

channels, 246

SSIDs, 245

wireless modes, 244

bandwidth, 256

channels, 242-244

ACKs, 244

assigning, 242

CSMA/CA, 243

RTS/CTS, 243

clients, configuring, 246

integrated software, 246

standalone software, 247-248

components, 238-240

connectivity, troubleshooting, 313-314

costs, 256

planning, 255

APs installation/security, 257

configuration backup, 257-258

firmware updates, 258

hardware installations, 256

standards, 255-256

security

attacks, 248-250

authentication, 251-252

encryption, 253-254

MAC address filtering, 250

traffic filtering, 254

war driving, 249

war walking, 249

site surveys, 256

SSIDs, 240

ad-hoc, 240

infrastructure mode, 240-242

standards, 237-238

work areas, 28

working inside computers, 28

workstations, 9

worms, 270

WPA (Wi-Fi Protected Access), 254

WPANs (wireless personal-area networks), 236

wrist grounding straps, 28

WWANs (wireless wide-area networks), 236

X

XHTML (Extensible HTML), 211

XML (Extensible Markup Language), 211

Notes