Microsoft

CompTIA A+

Exam 220-801
Exam 220-802

Rapid Review

CompTIA AUTHORIZED PARTNER

CompTIA APPROVED QUALITY CONTENT

Darril Gibson

Rapid Review

CompTIA A+ Exams 220-801 and 220-802

Assess your readiness for CompTIA A+ Exams 220-801 and 220-802—and quickly identify where you need to focus and practice. This practical, streamlined guide walks you through each exam objective, providing "need to know" checklists, review questions, tips, and links to further study—all designed to help bolster your preparation.

Reinforce your exam prep with a *Rapid Review* of these objectives:

Exam 220-801:

- PC Hardware
- Networking
- Laptops
- Printers
- Operational Procedures

Exam 220-802:

- Operating Systems
- Security
- Mobile Devices
- Troubleshooting

This book is an ideal complement to the in-depth training of the Microsoft Press *Training Kit* and other exam-prep resources for CompTIA A+ Exams 220-801 and 220-802.

ISBN: 978-0-7356-6682-5

U.S.A. $29.99
Canada $31.99
[*Recommended*]

Certification/CompTIA A+

ABOUT THE AUTHOR

Darril Gibson, MCT, MCSA, MCSE, is a course developer and author of several books. He also holds CISSP, A+, Network+, and Security+ certifications.

Microsoft

Microsoft

CompTIA A+ Rapid Review (Exam 220-801 and Exam 220-802)

Darril Gibson

Copyright © 2013 by Darril Gibson
All rights reserved. No part of the contents of this book may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

ISBN: 978-0-735-66682-5

1 2 3 4 5 6 7 8 9 LSI 8 7 6 5 4 3

Printed and bound in the United States of America.

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Book Support at *mspinput@microsoft.com*. Please tell us what you think of this book at *http://www.microsoft.com/learning/booksurvey*.

Microsoft and the trademarks listed at *http://www.microsoft.com/about/legal/en/us/IntellectualProperty/Trademarks/EN-US.aspx* are trademarks of the Microsoft group of companies. All other marks are property of their respective owners.

The example companies, organizations, products, domain names, email addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

This book expresses the author's views and opinions. The information contained in this book is provided without any express, statutory, or implied warranties. Neither the authors, Microsoft Corporation, nor its resellers, or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

The CompTIA Marks are the proprietary trademarks and/or service marks of CompTIA Properties, LLC used under license from CompTIA Certifications, LLC through participation in the CompTIA Authorized Partner Program. More information about the program can be found at *http://www.comptia.org/certifications/capp/login.aspx*.

Acquisitions and Developmental Editor: Kenyon Brown
Production Editor: Kristen Borg
Editorial Production: nSight, Inc.
Technical Reviewer: Brian Blum
Indexer: BIM Indexing
Cover Design: Karen Montgomery
Cover Composition: Best & Company Design
Illustrator: Rebecca Demarest

Contents at a Glance

Introduction *xxv*

Preparing for the exam *xxx*

PART I EXAM 220-801

Chapter 1 PC hardware 3
Chapter 2 Networking 77
Chapter 3 Laptops 123
Chapter 4 Printers 139
Chapter 5 Operational procedures 159

PART II EXAM 220-802

Chapter 6 Operating systems 181
Chapter 7 Security 247
Chapter 8 Mobile devices 281
Chapter 9 Troubleshooting 299

Index *355*

About the author *379*

Contents

Introduction *xxv*

Preparing for the exam *xxx*

PART I EXAM 220-801

Chapter 1 PC hardware **3**

Objective 1.1: Configure and apply BIOS settings **3**

Exam need to know... **4**

Install firmware upgrades—flash BIOS **4**

BIOS component information **5**

BIOS configurations **6**

Use built-in diagnostics **9**

Monitoring **10**

Can you answer these questions? **11**

Objective 1.2: Differentiate between motherboard components, their purposes, and properties **11**

Exam need to know... **12**

Sizes **12**

Expansion slots **13**

RAM slots **14**

CPU sockets **15**

Chipsets **16**

Jumpers **18**

Power connections and types **18**

Fan connectors **19**

Front panel connectors **19**

Bus speeds **20**

Can you answer these questions? **20**

What do you think of this book? We want to hear from you!

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

microsoft.com/learning/booksurvey

Objective 1.3: Compare and contrast RAM types and features. . 21
Exam need to know... 21
Types 21
RAM compatibility and speed 24
Can you answer these questions? 26
Objective 1.4: Install and configure expansion cards 26
Exam need to know... 26
Sound cards 27
Video cards 27
Network cards 29
Serial and parallel cards 29
USB and FireWire cards 30
Storage cards 30
Modem cards 31
Wireless/cellular cards 32
TV tuner cards 32
Video capture cards 32
Riser cards 33
Can you answer these questions? 33
Objective 1.5: Install and configure storage devices and use appropriate media 33
Exam need to know... 34
Optical drives 34
Combo drives and burners 34
Connection types 35
Hard drives 36
Solid state/flash drives 37
RAID types 37
Floppy drive 39
Tape drive 39
Media capacity 39
Can you answer these questions? 40
Objective 1.6: Differentiate among various CPU types and features and select the appropriate cooling method 40
Exam need to know... 40

Socket types 40
Characteristics 42
Cooling 43
Can you answer these questions? 43
Objective 1.7: Compare and contrast various connection interfaces and explain their purpose 43
Exam need to know... 44
Physical connections 44
Speeds, distances, and frequencies of wireless device connections 48
Can you answer these questions? 49
Objective 1.8: Install an appropriate power supply based on a given scenario 49
Exam need to know... 49
Connector types and their voltages 49
Specifications 50
Dual voltage options 51
Can you answer these questions? 51
Objective 1.9: Evaluate and select appropriate components for a custom configuration, to meet customer specifications or needs 52
Exam need to know... 52
Graphic/CAD/CAM design workstation 52
Audio/Video editing workstation 53
Virtualization workstation 54
Gaming PC 54
Home Theater PC 55
Standard thick client 55
Thin client 56
Home Server PC 56
Can you answer these questions? 57
Objective 1.10: Given a scenario, evaluate types and features of display devices 57
Exam need to know... 57
Types 58
Refresh rates 59
Resolution 59

Native resolution 60
Brightness/lumens 60
Analog vs. digital 60
Privacy/antiglare filters 61
Multiple displays 61
Can you answer these questions? 62

Objective 1.11: Identify connector types and associated cables 62
Exam need to know... 62
Display connector types 62
Display cable types 64
Device connectors and pin arrangements 65
Device cable types 67
Can you answer these questions? 67

Objective 1.12: Install and configure various peripheral devices 68
Exam need to know... 68
Input devices 68
Multimedia devices 71
Output devices 72
Can you answer these questions? 73

Answers 73
Objective 1.1: Configure and apply BIOS settings 73
Objective 1.2: Differentiate between motherboard components, their purposes, and properties 73
Objective 1.3: Compare and contrast RAM types and features 74
Objective 1.4: Install and configure expansion cards 74
Objective 1.5: Install and configure storage devices and use appropriate media 74
Objective 1.6: Differentiate among various CPU types and features and select the appropriate cooling method 74
Objective 1.7: Compare and contrast various connection interfaces and explain their purpose 75
Objective 1.8: Install an appropriate power supply based on a given scenarios 75

Objective 1.9: Evaluate and select appropriate components for a custom configuration, to meet customer specifications or needs 75
Objective 1.10: Given a scenario, evaluate types and features of display devices 76
Objective 1.11: Identify connector types and associated cables 76
Objective 1.12: Install and configure various peripheral devices 76

Chapter 2 Networking 77

Objective 2.1: Identify types of network cables and connectors 77
Exam need to know... 78
Fiber 78
Twisted-pair 78
Coaxial 79
Can you answer these questions? 80

Objective 2.2: Categorize characteristics of connectors and cabling 80
Exam need to know... 80
Fiber 80
Twisted-pair 81
Coaxial 82
Can you answer these questions? 82

Objective 2.3: Explain properties and characteristics of TCP/IP 83
Exam need to know... 83
IP class 83
IPv4 vs. IPv6 84
Public vs. private vs. APIPA 85
Static vs. dynamic 86
Client-side DNS 87
DHCP 87
Subnet mask 88
Gateway 89
Can you answer these questions? 90

Objective 2.4: Explain common TCP and UDP ports, protocols, and their purpose 91
Exam need to know... 91
Ports 91
Protocols 92
TCP vs. UDP 93
Can you answer these questions? 94
Objective 2.5: Compare and contrast wireless networking standards and encryption types 94
Exam need to know... 94
Standards 94
Encryption types 96
Can you answer these questions? 96
Objective 2.6: Install, configure, and deploy a SOHO wireless/wired router using appropriate settings 97
Exam need to know... 97
MAC filtering 97
Channels (1–11) 98
Port forwarding, port triggering 98
Built-in networking services 99
Wireless security 100
DMZ 101
Can you answer these questions? 102
Objective 2.7: Compare and contrast Internet connection types and features 102
Exam need to know... 102
Cable and fiber 102
Phone lines 103
Satellite 104
Cellular (mobile hotspot) 105
WiMAX and line of sight wireless Internet service 105
Can you answer these questions? 105
Objective 2.8: Identify various types of networks 106
Exam need to know... 106
LAN 106
WAN 107
PAN 107

MAN 107
Topologies 108
Can you answer these questions? 109

Objective 2.9: Compare and contrast network devices and their functions and features 109
Exam need to know... 109
Hub 110
Switch 110
Router 111
Access point 112
Bridge 113
Modem 113
NAS 113
Firewall 114
VoIP phones 114
Internet appliance 115
Can you answer these questions? 115

Objective 2.10: Given a scenario, use appropriate networking tools 115
Exam need to know... 115
Crimper 116
Multimeter 116
Toner probe 117
Cable tester 117
Loopback plug 118
Punchdown tool 118
Can you answer these questions? 119

Answers 119
Objective 2.1: Identify types of network cables and connectors 119
Objective 2.2: Categorize characteristics of connectors and cabling 119
Objective 2.3: Explain properties and characteristics of TCP/IP 119
Objective 2.4: Explain common TCP and UDP ports, protocols, and their purpose 120

Objective 2.5: Compare and contrast wireless networking standards and encryption types **120**

Objective 2.6: Install, configure, and deploy a SOHO wireless/wired router using appropriate settings **120**

Objective 2.7: Compare and contrast Internet connection types and features **120**

Objective 2.8: Identify various types of networks **120**

Objective 2.9: Compare and contrast network devices and their functions and features **121**

Objective 2.10: Given a scenario, use appropriate networking tools **121**

Chapter 3 Laptops 123

Objective 3.1: Install and configure laptop hardware and components. **123**

Exam need to know... **123**

Expansion options **124**

Hardware/device replacement **125**

Can you answer these questions? **127**

Objective 3.2: Compare and contrast the components within the display of a laptop **128**

Exam need to know... **128**

Types **128**

Wi-Fi antenna connector/placement **129**

Inverter and its function **130**

Backlight **130**

Can you answer these questions? **131**

Objective 3.3: Compare and contrast laptop features. **131**

Exam need to know... **132**

Special function keys **132**

Docking station vs. port replicator **134**

Physical laptop lock and cable lock **135**

Can you answer these questions? **136**

Answers **136**

Objective 3.1: Install and configure laptop hardware and components **136**

Objective 3.2: Compare and contrast the components within the display of a laptop 137
Objective 3.3: Compare and contrast laptop features 137

Chapter 4 Printers 139

Objective 4.1: Explain the differences between the various printer types and summarize the associated imaging process 139
Exam need to know... 139
Laser 140
Inkjet 145
Thermal 147
Impact 147
Can you answer these questions? 148

Objective 4.2: Given a scenario, install, and configure printers 149
Exam need to know... 149
Use appropriate printer drivers for a given operating system 149
Print device sharing 150
Printer sharing 152
Can you answer these questions? 153

Objective 4.3: Given a scenario, perform printer maintenance 154
Exam need to know... 154
Laser 154
Thermal 155
Impact 156
Can you answer these questions? 157

Answers 157
Objective 4.1: Explain the differences between the various printer types and summarize the associated imaging process 157
Objective 4.2: Given a scenario, install, and configure printers 158
Objective 4.3: Given a scenario, perform printer maintenance 158

Chapter 5 Operational procedures 159

Objective 5.1: Given a scenario, use appropriate safety procedures. **159**
Exam need to know... **160**
ESD strap **160**
ESD mats **160**
Self-grounding **161**
Equipment grounding **161**
Personal safety **162**
Compliance with local government regulations **164**
Can you answer these questions? **164**

Objective 5.2: Explain environmental impacts and the purpose of environmental controls **165**
Exam need to know... **165**
MSDS documentation for handling and disposal **165**
Temperature, humidity level awareness, and proper ventilation **166**
Power surges, brownouts, blackouts **166**
Protection from airborne particles **167**
Component handling and protection **168**
Compliance to local government regulations **169**
Can you answer these questions? **169**

Objective 5.3: Given a scenario, demonstrate proper communication and professionalism **170**
Exam need to know... **170**
Use proper language—avoid jargon, acronyms, slang when applicable **170**
Maintain a positive attitude **171**
Listen and do not interrupt the customer **171**
Be culturally sensitive **172**
Avoid distractions **172**
Dealing with difficult customer or situation **172**
Be on time / set and meet expectations **173**
Deal appropriately with customer's confidential materials **174**
Can you answer these questions? **175**

Objective 5.4: Explain the fundamentals of dealing with prohibited content/activity 175
Exam need to know... 175
First response 175
Use of documentation/documentation changes 176
Chain of custody 177
Can you answer these questions? 177
Answers 177
Objective 5.1: Given a scenario, use appropriate safety procedures 177
Objective 5.2: Explain environmental impacts and the purpose of environmental controls 178
Objective 5.3: Given a scenario, demonstrate proper communication and professionalism 178
Objective 5.4: Explain the fundamentals of dealing with prohibited content/activity 178

PART II EXAM 220-802

Chapter 6 Operating systems 181

Objective 1.1: Compare and contrast the features and requirements of various Microsoft Operating Systems 182
Exam need to know... 182
Windows XP Home, Windows XP Professional, Windows XP Media Center, Windows XP 64-bit Professional 182
Windows Vista Home Basic, Windows Vista Home Premium, Windows Vista Business, Windows Vista Ultimate, Windows Vista Enterprise 183
Windows 7 Starter, Windows 7 Home Premium, Windows 7 Professional, Windows 7 Ultimate, Windows 7 Enterprise 185
Features 187
Upgrade paths—differences between in-place upgrades, compatibility tools, Windows upgrade OS advisor 189
Can you answer these questions? 190

Objective 1.2: Given a scenario, install and configure the operating system using the most appropriate method **191**
Exam need to know... **191**
Boot methods **191**
Type of installations **192**
Partitioning **194**
File system types/formatting **195**
Load alternate third-party drivers when necessary **196**
Workgroup vs. domain setup **197**
Time/date/region/language settings **197**
Driver installation, software and windows updates **198**
Factory recovery partition **199**
Can you answer these questions? **199**
Objective 1.3: Given a scenario, use appropriate command line tools **199**
Exam need to know... **200**
Networking **200**
OS **202**
Recovery console **204**
Can you answer these questions? **205**
Objective 1.4: Given a scenario, use appropriate operating system features and tools **205**
Exam need to know... **205**
Administrative **206**
msconfig **208**
Task Manager **209**
Disk Management **210**
Other **213**
Run line utilities **214**
Can you answer these questions? **215**
Objective 1.5: Given a scenario, use Control Panel utilities (the items are organized by "classic view/ large icons" in Windows) **215**
Exam need to know... **215**
Common to all Microsoft operating systems **215**
Unique to Windows XP **219**
Unique to Windows Vista **219**

Unique to Windows 7 **220**
Can you answer these questions? **221**

Objective 1.6: Set up and configure Windows networking on a client/desktop **221**
Exam need to know... **221**
Homegroup, file/print sharing **222**
Workgroup vs. domain setup **223**
Network shares/mapping drives **223**
Establish networking connections **224**
Firewall settings **225**
Proxy settings **226**
Remote desktop **226**
Home vs. Work vs. Public network settings **227**
Configuring an alternative IP address in Windows **228**
Network card properties **228**
Can you answer these questions? **229**

Objective 1.7: Perform preventive maintenance procedures using appropriate tools **229**
Exam need to know... **230**
Best practices **230**
Tools **231**
Can you answer these questions? **232**

Objective 1.8: Explain the differences among basic OS security settings **233**
Exam need to know... **233**
User and groups **233**
Shared files and folders **234**
NTFS vs. share permissions **235**
System files and folders **238**
User authentication **239**
Can you answer these questions? **239**

Objective 1.9: Explain the basics of client-side virtualization . . **239**
Exam need to know... **240**
Purpose of virtual machines **240**
Resource and network requirements **241**
Hypervisor and emulator requirements **242**

Security requirements 242
Can you answer these questions? 243
Answers 243
Objective 1.1: Compare and contrast the features and requirements of various Microsoft Operating Systems 243
Objective 1.2: Given a scenario, install and configure the operating system using the most appropriate method 244
Objective 1.3: Given a scenario, use appropriate command line tools 244
Objective 1.4: Given a scenario, use appropriate operating system features and tools 244
Objective 1.5: Given a scenario, use Control Panel utilities (the items are organized by "classic view/large icons" in Windows) 245
Objective 1.6 Set up and configure Windows networking on a client/desktop 245
Objective 1.7: Perform preventive maintenance procedures using appropriate tools 245
Objective 1.8: Explain the differences among basic OS security settings 245
Objective 1.9: Explain the basics of client-side virtualization 246

Chapter 7 Security 247

Objective 2.1: Apply and use common prevention methods . . 247
Exam need to know... 247
Physical security 248
Digital security 250
User education 251
Principle of least privilege 252
Can you answer these questions? 253
Objective 2.2: Compare and contrast common security threats 253
Exam need to know... 253
Social engineering 254
Malware 254
Rootkits 255

Phishing 255
Shoulder surfing 256
Spyware 257
Viruses 258
Can you answer these questions? 259

Objective 2.3: Implement security best practices to secure a workstation 259
Exam need to know... 259
Setting strong passwords 260
Requiring passwords 261
Restricting user permissions 262
Changing default user names 263
Disabling the Guest account 263
Screensaver required password 264
Disable autorun 264
Can you answer these questions? 265

Objective 2.4: Given a scenario, use the appropriate data destruction/disposal method 265
Exam need to know... 265
Low-level format vs. standard format 266
Hard drive sanitation and sanitation methods 267
Physical destruction 268
Can you answer these questions? 269

Objective 2.5: Given a scenario, secure a SOHO wireless network. 269
Exam need to know... 269
Change default user names and passwords 270
Changing SSID and disabling SSID broadcast 270
Setting encryption 271
Enable MAC filtering 272
Antenna and access point placement 273
Radio power levels 274
Assign static IP addresses 274
Can you answer these questions? 275

Objective 2.6: Given a scenario, secure a SOHO wired network 276

Exam need to know... 276
Common security steps 276
Disabling ports 277
Physical security 278
Can you answer these questions? 278

Answers 278

Objective 2.1: Apply and use common prevention methods 279
Objective 2.2: Compare and contrast common security threats 279
Objective 2.3: Implement security best practices to secure a workstation 279
Objective 2.4: Given a scenario, use the appropriate data destruction/disposal method 280
Objective 2.5: Given a scenario, secure a SOHO wireless network 280
Objective 2.6: Given a scenario, secure a SOHO wired network 280

Chapter 8 Mobile devices 281

Objective 3.1: Explain the basic features of mobile operating systems 281
Exam need to know... 281
Android vs. iOS 282
Screen orientation and calibration 283
GPS and geotracking 284
Can you answer these questions? 284

Objective 3.2: Establish basic network connectivity and configure email 285
Exam need to know... 285
Wireless/cellular data network (enable/disable) 285
Bluetooth 286

What do you think of this book? We want to hear from you!

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

microsoft.com/learning/booksurvey

Email configuration 287
Can you answer these questions? 288

Objective 3.3: Compare and contrast methods for securing mobile devices 288
Exam need to know... 288
Passcode locks 289
Remote wipes 289
Locator applications 289
Remote backup applications 290
Failed login attempts restrictions 290
Antivirus 291
Patching/OS updates 291
Can you answer these questions? 292

Objective 3.4: Compare and contrast hardware differences in regards to tablets and laptops 292
Exam need to know... 292
No field serviceable parts 292
Typically not upgradable 293
Touch interface 293
Solid state drive 294
Can you answer these questions? 294

Objective 3.5: Execute and configure mobile device synchronization 295
Exam need to know... 295
Types of data to synchronize 295
Software requirements to install the application on the PC 296
Connection types to enable synchronization 296
Can you answer these questions? 297

Answers 297
Objective 3.1: Explain the basic features of mobile operating systems 297
Objective 3.2: Establish basic network connectivity and configure email 297
Objective 3.3: Compare and contrast methods for securing mobile devices 298

Objective 3.4: Compare and contrast hardware differences in regards to tablets and laptops 298
Objective 3.5: Execute and configure mobile device synchronization 298

Chapter 9 Troubleshooting 299

Objective 4.1: Given a scenario, explain the troubleshooting theory 300
Exam need to know... 300
Identify the problem 300
Establish a theory of probable cause 301
Test the theory to determine cause 302
Establish a plan of action to resolve the problem and implement the solution 303
Verify full system functionality and, if applicable, implement preventive measures 303
Document findings, actions, and outcomes 304
Can you answer these questions? 304

Objective 4.2: Given a scenario, troubleshoot common problems related to motherboards, RAM, CPU and power with appropriate tools 304
Exam need to know... 305
Common symptoms 305
Tools 308
Can you answer these questions? 309

Objective 4.3: Given a scenario, troubleshoot hard drives and RAID arrays with appropriate tools 310
Exam need to know... 310
Common symptoms 310
Tools 313
Can you answer these questions? 314

Objective 4.4: Given a scenario, troubleshoot common video and display issues 314
Exam need to know... 314
Common symptoms 315
Can you answer these questions? 318

Objective 4.5: Given a scenario, troubleshoot wired and wireless networks with appropriate tools 318
Exam need to know... 318
Common symptoms 318
Tools 321
Can you answer these questions? 323
Objective 4.6: Given a scenario, troubleshoot operating system problems with appropriate tools 323
Exam need to know... 323
Common symptoms 323
Tools 326
Can you answer these questions? 332
Objective 4.7: Given a scenario, troubleshoot common security issues with appropriate tools and best practices 332
Exam need to know... 332
Common symptoms 332
Tools 335
Best practices for malware removal 337
Can you answer these questions? 338
Objective 4.8: Given a scenario, troubleshoot, and repair common laptop issues while adhering to the appropriate procedures 339
Exam need to know... 339
Common symptoms 339
Disassembling processes for proper reassembly 343
Can you answer these questions? 344
Objective 4.9: Given a scenario, troubleshoot printers with appropriate tools. 344
Exam need to know... 344
Common symptoms 344
Tools 348
Can you answer these questions? 349
Answers 350
Objective 4.1: Given a scenario, explain the troubleshooting theory 350

Objective 4.2: Given a scenario, troubleshoot common problems related to motherboards, RAM, CPU and power with appropriate tools **350**

Objective 4.3: Given a scenario, troubleshoot common problems related to motherboards, RAM, CPU and power with appropriate tools **351**

Objective 4.4: Given a scenario, troubleshoot common video and display issues **351**

Objective 4.5: Given a scenario, troubleshoot wired and wireless networks with appropriate tools **351**

Objective 4.6: Given a scenario, troubleshoot operating system problems with appropriate tools **352**

Objective 4.7: Given a scenario, troubleshoot common security issues with appropriate tools and best practices **352**

Objective 4.8: Given a scenario, troubleshoot, and repair common laptop issues while adhering to the appropriate procedures **352**

Objective 4.9: Given a scenario, troubleshoot printers with appropriate tools **353**

Index *355*

About the author *379*

What do you think of this book? We want to hear from you!

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

microsoft.com/learning/booksurvey

Introduction

This Rapid Review is designed to assist you with studying for the CompTIA A+ exams 220-801 and 220-802. The Rapid Review series is designed for exam candidates who already have a good grasp of the exam objectives through a combination of experience, skills, and study and could use a concise review guide to help them assess their readiness for the exam.

The A+ certification is aimed at an entry-level IT professional who has a minimum of 12 months of hands-on experience with computers. This can be either classroom or lab experience, or on-the-job experience, or a combination of both. To earn the A+ certification, you need to pass two exams:

- CompTIA A+ 220-801 covers the fundamentals of computer technology, installation and configuration of PCs, laptops and related hardware, and basic networking.
- CompTIA A+ 220-802 covers the skills required to install and configure PC operating systems, as well as configuring common features (for example, network connectivity and email) for mobile operating systems Android and Apple iOS.

Successful candidates will have the knowledge required to assemble components based on customer requirements. They can install, configure, and maintain devices, PCs, and software for end users, and they understand the basics of networking and security/forensics. They can provide appropriate customer support by applying appropriate troubleshooting skills to properly and safely diagnose, resolve, and document common hardware and software issues. Successful candidates will also understand the basics of virtualization, desktop imaging, and deployment.

This book will review every concept described in the following exam objective domains from exam 220-801:

- 1.0 PC Hardware
- 2.0 Networking
- 3.0 Laptops
- 4.0 Printers
- 5.0 Operational Procedures

This book will also review every concept described in the following exam objective domains from exam 220-802:

- 1.0 Operating Systems
- 2.0 Security
- 3.0 Mobile Devices
- 4.0 Troubleshooting

This is a Rapid Review and not a comprehensive guide such as the CompTIA A+ Training Kit. The book covers every exam objective on the 220-801 and 220-802 exams but will not necessarily cover every exam question. CompTIA regularly adds new questions to the exam, making it impossible for this (or any) book to provide

every answer. Instead, this book is designed to supplement your existing independent study and real-world experience with the topics.

If you encounter a topic in this book that you do not feel completely comfortable with, you can visit the links described in the text, in addition to researching the topic further by using other websites and by consulting support forums. If you review a topic and find that you don't understand it, you should consider consulting the CompTIA A+ Training Kit from Microsoft Press. You can also purchase practice exams, or you can use the exams available with the Training Kit, to further determine whether you have need further study on particular topics.

> ***NOTE*** **The Rapid Review is designed to assess your readiness for the 220-801 and 220-802 exams. It is not designed as a comprehensive exam preparation guide. If you need that level of training for any or all of the exam objectives covered in this book, we suggest the *CompTIA A+ Training Kit* (ISBN: 9780735662681). The Training Kit provides comprehensive coverage of each exam objective, along with exercises, review questions, and practice tests.**

CompTIA professional certification program

CompTIA professional certifications cover the technical skills and knowledge needed to succeed in a specific IT career. Certification is a vendor-neutral credential. An exam is an internationally recognized validation of skills and knowledge and is used by organizations and professionals around the globe. CompTIA certification is ISO 17024 Accredited (Personnel Certification Accreditation) and, as such, undergoes regular reviews and updates to the exam objectives. CompTIA exam objectives reflect the subject areas in an edition of an exam and result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of a professional with a number of years of experience.

> ***MORE INFO*** **For a full list of CompTIA certifications, go to *http://certification.comptia.org/getCertified/certifications.aspx*.**

Training materials given the CAQC seal have gone through a rigorous approval process to confirm the content meets exam objectives, language standards, necessary hands-on exercises and labs and applicable Instructional Design standards.

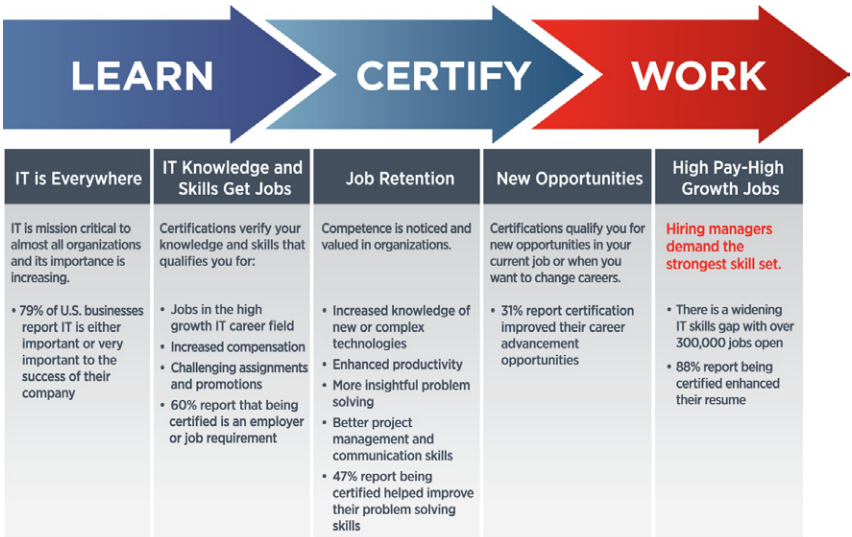
Certification helps your career

Certification can help your career in the following ways:

- The CompTIA A+ credential provides foundation-level knowledge and skills necessary for a career in PC repair and support.
- CompTIA A+ Certified individuals can earn as much as $65,000 per year.
- CompTIA A+ is a building block for other CompTIA certifications such as Network+, Security+ and vendor-specific technologies.
- More than 850,000 individuals worldwide are CompTIA A+ certified.
- Mandated/recommended by organizations worldwide, such as Cisco and HP and Ricoh, the U.S. State Department, and U.S. government contractors such as EDS, General Dynamics, and Northrop Grumman.

It pays to get certified

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



Some of the primary benefits individuals report from becoming A+ certified are:

- More efficient troubleshooting
- Improved career advancement
- More insightful problem solving

Four steps to getting certified and staying certified

If you want to get certified and stay certified, follow these steps:

1. **Review exam objectives** Review the Certification objectives to make sure you know what is covered in the exam. Visit *http://www.comptia.org/certifications/testprep/examobjectives.aspx* for information.
2. **Practice for the exam** After you have studied for the certification, take a free assessment and sample test to get an idea of what type of questions might be on the exam. Go to *http://www.comptia.org/certifications/testprep/practicetests.aspx* for additional information.
3. **Purchase an exam voucher** Purchase exam vouchers on the CompTIA Marketplace, which is located at *www.comptiastore.com*.
4. **Take the test** Select a certification exam provider and schedule a time to take your exam. You can find exam providers at the following link: *http://www.comptia.org/certifications/testprep/testingcenters.aspx*.

Stay certified! Take advantage of continuing education

All new CompTIA A+ certifications will be valid for three years from the date the candidate is certified. After three years, those certifications must be renewed. For more information, go to *http://certification.comptia.org/getCertified/steps_to_certification/stayCertified.aspx*.

How to obtain more information

You can obtain more information about CompTIA in several ways:

- **Visit CompTIA online** Go to *www.comptia.org* to learn more about getting CompTIA certified.
- **Contact CompTIA** Call 866-835-8020 ext. 5 or email *questions@comptia.org*.
- **Join the IT Pro Community** Visit *http://itpro.comptia.org* to join the IT community and get relevant career information.
- Connect with us:
  - **LinkedIn** *http://www.linkedin.com/groups?home=&gid=83900*
  - **Facebook** *http://www.facebook.com/CompTIA*
  - **Twitter** *https://twitter.com/comptia*
  - **Flickr** *http://www.flickr.com/photos/comptia*
  - **YouTube** *http://www.youtube.com/user/CompTIATV*

Support & feedback

The following sections provide information about errata, book support, feedback, and contact information.

Errata

We've made every effort to ensure the accuracy of this book and its companion content. Any errors that have been reported since this book was published are listed on our Microsoft Press site:

http://aka.ms/CompTIARapidReview/errata

If you find an error that is not already listed, you can report it to us through the same page.

If you need additional support, email Microsoft Press Book Support at *mspinput@microsoft.com*.

Please note that product support for Microsoft software is not offered through the addresses above.

We want to hear from you

At Microsoft Press, your satisfaction is our top priority, and your feedback our most valuable asset. Please tell us what you think of this book at:

http://www.microsoft.com/learning/booksurvey

The survey is short, and we read every one of your comments and ideas. Thanks in advance for your input!

Stay in touch

Let's keep the conversation going! We're on Twitter: *http://twitter.com/MicrosoftPress*.

Preparing for the exam

CompTIA certification exams are a great way to build your resume and let the world know about your level of expertise. Certification exams validate your on-the-job experience and product knowledge. Although there is no substitute for on-the-job experience, preparation through study and hands-on practice can help you prepare for the exam. We recommend that you augment your exam preparation plan by using a combination of available study materials and courses. For example, you might use the Rapid Review and another training kit for your "at home" preparation, and take a CompTIA professional certification course for the classroom experience. Choose the combination that you think works best for you.

CHAPTER 2

Networking

The Networking domain covers approximately 27 percent of the A+ 220-801 exam. Almost every computer you'll service will be connected to a network, so it's important to understand some basic networking topics. This includes network cables and connectors, network devices such as routers and switches, wireless connections, and common protocols used to control traffic over a network. Many networks use both wired and wireless connections, along with a router for Internet access. Technicians are often asked to help configure connectivity for different types of networks, and they need to know the functions and features of various devices, along with appropriate networking tools.

This chapter covers the following objectives:

- Objective 2.1: Identify types of network cables and connectors
- Objective 2.2: Categorize characteristics of connectors and cabling
- Objective 2.3: Explain properties and characteristics of TCP/IP
- Objective 2.4: Explain common TCP and UDP ports, protocols, and their purpose
- Objective 2.5: Compare and contrast wireless networking standards and encryption types
- Objective 2.6: Install, configure, and deploy a SOHO wireless/wired router using appropriate settings
- Objective 2.7: Compare and contrast Internet connection types and features
- Objective 2.8: Identify various types of networks
- Objective 2.9: Compare and contrast network devices and their functions and features
- Objective 2.10: Given a scenario, use appropriate networking tools

Objective 2.1: Identify types of network cables and connectors

The first objective in this domain introduces the three most common types of cables used for networks: fiber, twisted-pair, and coaxial. The most important thing you should know for this objective is the types of connectors used with each

type of cable. The next objective builds on these topics requiring you to know the characteristics of the cables.

Exam need to know...

- Fiber
  For example: What types of connectors are used with fiber cable?
- Twisted-pair
  For example: What types of connectors are used with twisted-pair cable? What standards are used when wiring a twisted-pair cable?
- Coaxial
  For example: What are the two common connectors used with coaxial cable?

Fiber

Fiber cable is made of a flexible glass material, and data is sent over the cable as light pulses. There are three primary connectors you'll see with fiber cables.

True or false? An LC is one of the common connectors used with fiber cable.

Answer: *True.* A Lucent Connector (LC) is used with fiber cable.

Some additional connectors commonly used with fiber cable include the following:

- **Square connector (SC)** Just as its name implies, this connector is square shaped. The LC connector is a miniature version of the SC connector.
- **Straight tip (ST)** This is a round connector with a straight tip.

EXAM TIP **Common connectors used with fiber cable are LC, SC, and ST. You should be able to identify each by sight.**

MORE INFO **If you aren't familiar with the different fiber connectors, check out *http://www.bing.com/images*. Enter search words such as fiber connectors, LC connector, SC connector, and ST connector. You can use the same procedure to view pictures for any type connectors introduced in this section. Chapter 19 of the CompTIA A+ Training Kit (Exam 220-801 and Exam 220-802), ISBN-10: 0735662681, covers all of the cable types and connectors in more depth.**

Twisted-pair

Twisted-pair cable includes multiple pairs of wires twisted around each other. These twists are precise and determine the frequency capabilities of the cable. Cables that support higher frequencies allow the cable to transmit more data at a time.

True or false? RJ-11 connectors are used with twisted-pair cables to connect network devices.

Answer: *False.* RJ-45 connectors are used with twisted-pair cables when connecting network devices.

RJ-11 connectors are used with phone-based twisted-pair cables. For example, RJ-11 connectors are used with a plain old telephone system (POTS) modem or even a digital subscriber line (DSL) modem.

> ***MORE INFO*** **Modems can be used for Internet connectivity. Objective 2.7, "Compare and contrast Internet connection types and features," covers various methods of connecting to the Internet, including standard dial-up modems and DSL modems. Twisted-pair cables come in several different categories, such as CAT 5, CAT 6, and so on. These are discussed in Objective 2.2, "Categorize characteristics of connectors and cabling."**

Twisted-pair cables used in networking have four pairs of wires. The colors of each pair are as follows:

- Blue wire and white wire with a blue stripe
- Orange wire and white wire with an orange stripe
- Green wire and white wire with a green stripe
- Brown wire and white wire with a brown stripe

Each wire should be connected to a specific pin on the RJ-45 connector, and there are two standards that can be used—T568A and T568B. When creating a standard cable, both ends should use the same standard. This ensures that the same wire is going to the same pin on each connector.

True or false? A cable wired with the T568A standard on one end and the T568B standard on the other end works as a crossover cable.

Answer: *True.* If different standards are used, certain wires are crossed over and the cable will function as a crossover cable. Crossover cables are used to connect similar devices together, such as two computers or two switches.

> ***EXAM TIP*** **RJ-11 connectors are used for phone lines. RJ-45 connectors are used with network twisted-pair cables. When wiring RJ-45 connectors, you should use either the T568A or T568B standard on both ends of the cable.**

Coaxial

Coaxial cable is commonly used to connect televisions with broadband cable, DVD players, and digital video recorders (DVRs). It isn't used as often with networks, but it has been used in the past.

True or false? F-type screw-on connectors are used with coaxial cable.

Answer: *True.* Coaxial cable uses F-type screw-on or BNC twist-on connectors.

EXAM TIP **The primary connectors used with coaxial cable are BNC or F-type connectors.**

Can you answer these questions?

You can find the answers to these questions at the end of this chapter.

1. What type of cable would an LC connector be used with?
2. What is the difference between an RJ-11 and an RJ-45 connector?
3. What type of cable is used with an F-type connector?

Objective 2.2: Categorize characteristics of connectors and cabling

In this objective, you're expected to know a little more about the cables and connectors introduced in Objective 2.1, "Identify types of network cables and connectors." In addition to being able to recognize the cables and connectors, you also need know about some of their characteristics, such as their speed and transmission limitations.

Exam need to know...

- Fiber
  For example: What is a benefit of fiber cable related to EMI? Which supports the maximum distance—SMF or MMF?
- Twisted-pair
  For example: What category of twisted-pair cable supports 1 Gbps? What is the maximum transmission speed of CAT 3?
- Coaxial
  For example: What is RG-6 cable used for?

Fiber

Fiber cable is more expensive and harder to work with than twisted-pair or coaxial cable. However, it has some significant advantages over other cable types, so it is being used in more and more networks.

True or false? Fiber cable is immune to EMI and RFI.

Answer: *True*. Fiber cable is not susceptible to signal loss from electromagnetic interference (EMI) or radio frequency interference (RFI).

Two common sources of EMI are from electric power cables or fluorescent light fixtures that are too close to signal cables. RFI interference comes from devices transmitting RF signals.

True or false? Data sent on a fiber cable can travel significantly farther than data sent on twisted-pair or coaxial cable.

Answer: *True.* Data sent on single-mode fiber (SMF) can travel the farthest without needing a repeater. Data sent on multi-mode (MMF) fiber can travel farther than data sent on twisted-pair or coaxial cable, but not as far as SMF cable.

For comparison, the maximum distances of different cables without using a repeater are as follows:

- SMF—up to 40 Km
- MMF—up to 2 Km
- Twisted-pair—up to 100 meters
- Coaxial—185 meters or 500 meters, depending on the cable type

NOTE **A repeater receives and retransmits signals; it is used when distances exceed cable limitations. For example, to use twisted-pair cable to connect two devices that are 150 meters apart, you can use a repeater in the middle. One cable run can be about 75 meters and connect to the repeater. The repeater then "repeats" the signal onto the second cable run of about 75 more meters. Neither cable run is more than 100 meters.**

EXAM TIP **Fiber optic cable is immune to EMI and RFI. SMF cable supports the longest cable lengths without repeaters, and MMF cable supports longer cable lengths than twisted-pair and coaxial cable.**

Twisted-pair

Twisted-pair cable comes in many different types and categories. All categories come in both unshielded twisted-pair (UTP) and shielded twisted-pair (STP) versions. The STP version provides some protection against EMI and RFI, but it isn't as effective as fiber cable against this interference.

True or false? If you need to run twisted-pair cable close to fluorescent lights, you should use UTP cable.

Answer: *False.* Fluorescent array lighting is a known source of interference, so STP cable is the best choice.

UTP cable is highly susceptible to signal loss from EMI and RFI. STP cable provides some protection against EMI and RFI, but it isn't as effective as fiber cable.

EXAM TIP **STP protects against EMI and RFI. Use STP cable if you have to run cable near power cables or through a fluorescent lighting array.**

True or false? CAT 5e cable supports a maximum transfer rate of 10 Gbps.

Answer: *False.* CAT 5e cable supports a maximum transfer rate of 1 Gbps.

The maximum transfer rates of various categories are as follows:

- CAT 3—10 Mbps
- CAT 5—100 Mbps

- CAT 5e—1000 Mbps (1 Gbps)
- CAT 6—10 Gbps

EXAM TIP **Ensure that you know the maximum transmission speeds of each of the different cable categories. Even though some of the cable categories are rarely used today, they are specifically listed in the objectives.**

True or false? Plenum rated cable is fire retardant and reduces hazardous fumes from a fire.

Answer: *True*. Plenum rated cable should be used when cable is run through a plenum. It is fire retardant and reduces hazardous fumes from a fire.

A plenum, or plenum space, is the open space where heated and/or air conditioned air is forced through a building. Cables are commonly routed through these plenum spaces. The standard jacket covering used for cables is made of polyvinyl chloride (PVC), and it will emit toxic fumes if it burns. PVC cable should never be used in a plenum space because the toxic fumes are sent through the building from the heating and ventilation system.

EXAM TIP **Plenum-rated cable should be used when cable is routed through plenums. PVC cable emits toxic fumes, but plenum-rated cable is fire retardant.**

Coaxial

The two types of coaxial cable mentioned in the objectives are RG-6 and RG-59. RG-6 cable commonly uses an F-type screw-on connector, and RG-59 normally uses a BNC twist-on connector, although both cable types can use either connector.

True or false? RG-6 cable is commonly used for cable television distribution and supports the transmission of both analog and digital data.

Answer: *True*. RG-6 supports both analog and digital data.

RG-59 supports analog or digital data, although it is susceptible to high-frequency losses, so it is not used for cable television transmissions. Cable TV companies often provide Internet access through the same cable used for television channels. RG-6 cable is often used for these connections. When customers subscribe to broadband Internet in addition to cable television, a splitter is used to send one output to televisions and another output to a cable modem for the Internet connection.

EXAM TIP **RG-6 and RG-59 are two types of coaxial cable. RG-6 is used with broadband cable connections and supports both analog and digital transmissions.**

Can you answer these questions?

You can find the answers to these questions at the end of this chapter.

1. Which cable type supports the longest cables without a repeater?

2. What is the maximum transfer rate supported by CAT 6 cables?
3. What type of data is transmitted on RG-6 cable?

Objective 2.3: Explain properties and characteristics of TCP/IP

The primary protocol suite used on networks is Transmission Control Protocol/Internet Protocol (TCP/IP), and it includes several underlying protocols. You aren't expected to be an expert on everything related to TCP/IP, but you do need to be able to identify and explain many basic characteristics. This includes the class of an IP address, differences between IPv4 and IPv6, differences between private and public addresses, and differences between statically and dynamically assigned IP addresses. You should also know about basic services provided on a network.

Exam need to know...

- IP class
  For example: What class is 192.168.1.6? What class is 172.16.6.3?
- IPv4 vs. IPv6
  For example: How many bits does an IPv6 address use? How are IPv6 addresses displayed?
- Public vs. private vs. APIPA
  For example: What are the ranges of private IP addresses? When is an APIPA address used?
- Static vs. dynamic
  For example: Which method (static or dynamic) results in more IP address conflicts?
- Client-side DNS
  For example: What does DNS provide for a client?
- DHCP
  For example: What does DHCP provide for a client?
- Subnet mask
  For example: How is the subnet mask used with an IP address?
- Gateway
  For example: What is the difference between a gateway and a router?

IP class

Classful IP addresses are in certain predefined ranges. When you know the class of an IP address, you automatically know its subnet mask.

True or false? An address of 10.20.30.88 is a Class C address.

Answer: *False.* This address is a Class A address.

The class of an address is identified by the first number in the address. For example, in the 10.20.30.88 address, the first number is 10, which indicates that it

is a Class A address. This also tells you that it has a subnet mask of 255.0.0.0. The ranges of each type of address are as follows:

- Class A—1 to 126 (subnet mask 255.0.0.0)
- Class B—128 to 191 (subnet mask 255.255.0.0)
- Class C—192 to 223 (subnet mask 255.255.255.0)

EXAM TIP **Given an IP address, you should be able to identify if it is a Class A, Class B, or Class C IP address. Similarly, if you're given a specific class such as Class C, you should be able to identify all the IP addresses in a list that are in that class.**

MORE INFO **The Wikipedia article titled "Classful Network" includes more details on classful IP addresses, including specifically how many networks each supports and how many IP addresses can be used on each network. You can access it here: *http://en.wikipedia.org/wiki/Classful_network*.**

IPv4 vs. IPv6

IPv4 addresses use 32 bits and are displayed in dotted decimal format, such as 192.168.1.1. IPv6 addresses use 128 bits and are displayed in hexadecimal format separated by colons, like this: FC00:0000:0000:0000:042A:0000:0000:07F5.

True or false? The following two IPv6 addresses are identical: FC00::42A:0:0:7F5 and FC00:0000:0000:0000:042A:0000:0000:07F5.

Answer: *True*. IPv6 addresses can omit leading zeroes and use zero compression to shorten the way the address is displayed without changing the actual address.

IPv6 addresses use 32 hexadecimal characters. Each hexadecimal character represents four bits for a total of 128 bits (4 × 128).

MORE INFO **Hexadecimal characters include the numbers 0 to 9 and the characters A to F. The following page shows how decimal, hexadecimal, and binary numbers compare side by side: *http://blogs.getcertifiedgetahead.com/comparing-decimal-hexadecimal-and-binary/*.**

The IPv6 address is often represented as eight groups of four hexadecimal characters separated by colons. For example, in the IPv6 address of FC00:0000:0000:0000:042A:0000:0000:07F5, FC00 is one group of four hexadecimal characters, and the next group is 0000.

To understand how leading zeros are omitted, imagine you have 120 dollars. It could be represented as 0120 dollars, and it's still the same amount of money. However, we typically omit the leading zeros with money, and you can do the same thing with IPv6 addresses. The following example address is shown with leading zeros omitted: FC00:0:0:0:42A:0:0:7F5.

Trailing zeros are never omitted. For example, 120 dollars and 12 dollars are not the same amount of money. Similarly, FC00 is the not the same hexadecimal number as FC.

Zero compression is also used with IPv6 addresses. Instead of displaying groups of zeros, you can use a double colon to replace one or more such zero-value groups. For example, either of the following two IPv6 addresses represents the same address:

- FC00::042A:0000:0000:07F5
- FC00:0000:0000:0000:042A::07F5

An IPv6 address has eight groups of four hexadecimal characters. When you see a double colon, you can replace it with enough missing groups to get eight groups.

For example, in the first address, FC00::042A:0000:0000:07F5, five groups are showing (FC00, 042A, 0000, 0000, and 07F5), so you know that the double colon represents three groups of zeros (0000, 0000, and 0000).

In the second address, FC00:0000:0000:0000:042A::07F5, you can see six groups (FC00, 0000, 0000, 0000, 042A, and 07F5), so you know that the double colon represents two groups of zeros (0000 and 0000).

You cannot use two double colons in any IPv6 address. For example, if you did this FC00::042A::07F5, you would see that three groups are showing (FC00, 042A, and 07F5), indicating that five groups are missing. However, there's no way to tell how many groups should be used for each double colon. It could be FC00:0000:0000:042A:0000:0000:0000:07F5 or FC00:0000:0000:0000:042A:0000:0000:07F5.

Both methods of omitting leading zeros and zero compression can be combined. For example, FC00:0000:0000:0000:042A:0000:0000:07F5 can be shortened to FC00::42A:0:0:7F5.

EXAM TIP **IPv4 addresses use 32 bits and are commonly represented in dotted decimal format. IPv6 addresses use 128 bits and are commonly represented in hexadecimal format with eight groups of four hexadecimals. IPv6 addresses can be simplified by omitting leading zeroes in each group and using zero compression. With zero compression, a single string of zeroes is represented with a double colon.**

MORE INFO **IPv6 uses ::1 instead of 127.0.0.1 as the loopback address. Chapter 21 of the CompTIA A+ Training Kit (Exam 220-801 and Exam 220-802), ISBN-10: 0735662681, provides more detailed information about IPv6.**

Public vs. private vs. APIPA

IP addresses used on the Internet are public IP addresses. IP addresses used on internal networks are private IP addresses. Automatic Private IP Addressing (APIPA) addresses are randomly selected private addresses that always start with 169.254.

True or false? An IP address of 172.16.10.5 is a public address.

Answer: *False.* This is a private IP address.

Private IP addresses are formally defined in Request for Comments (RFC) 1918, with the following ranges:

- 10.0.0.0 through 10.255.255.255 (Class A private IP addresses)
- 172.16.0.0 through 172.31.255.255 (Class B private IP addresses)
- 192.168.0.0 through 192.168.255.255 (Class C private IP addresses)

EXAM TIP **Given an IP address, you should be able to identify whether it is a public IP address or a private IP address. Similarly, you should be able to identify all the IP addresses in a list that are either public or private.**

True or false? If you see a computer with an IP address of 169.254.6.3, you know that it was unable to get an IP address from a DHCP server.

Answer: *True*. An address starting with 169.254 is an APIPA address, and Dynamic Host Configuration Protocol (DHCP) clients can assign themselves an APIPA address if a DHCP server isn't available.

In many networks, administrators configure a DHCP server to provide clients with an IP address and other TCP/IP configuration information such as a subnet mask, a default gateway, and the address of a DNS server. If the DHCP server doesn't respond to the request for this information, the DHCP client assigns itself an APIPA address.

EXAM TIP **APIPA addresses always start with 169.254 and are assigned only when a DHCP client does not get a reply from a DHCP server for an IP address.**

Static vs. dynamic

IP addresses can be statically assigned or dynamically assigned. A statically assigned address has been manually entered by a person, and a dynamically assigned address has been assigned through a service on the network or on the computer.

True or false? Statically assigned IP addresses often result in IP address conflicts.

Answer: *True*. When IP addresses are manually assigned, it's easy to assign the same IP address to two or more systems on the network, resulting in an IP address conflict.

IP address conflicts adversely affect the network communication of at least one client on the network and sometimes both. If you statically assign an IP address to one Windows-based computer named Win7 on a network and then later assign the same IP address to another Windows-based computer, the second computer recognizes the conflict and won't use the IP address. The Win7 computer continues to operate without problems, but the second computer can't communicate on the network.

However, printers aren't that smart. If you statically assign an IP address to a printer that was previously assigned to the Win7 computer, it adversely affects both the printer and the computer. Both will have network connectivity problems.

EXAM TIP **Statically assigned IP addresses require more labor and are more prone to IP address conflicts. Even when an organization takes extra time to document which IP addresses are assigned to every computer in the network, technicians can incorrectly enter an address, causing a conflict.**

MORE INFO **Dynamically assigned addresses are typically assigned by a DHCP server (covered in the DHCP section). They can also be assigned by services running on the computer. For example, an APIPA address (starting with 169.254) can be assigned by the computer when a DHCP server doesn't respond.**

Client-side DNS

The primary purpose of a Domain Name System (DNS) server is to resolve computer and host names to IP addresses. DNS is used on the Internet and on internal networks.

True or false? DNS maps user-friendly names to network resources.

Answer: *True*. A DNS server stores computer names and their assigned IP address on a network.

Clients are configured with the IP address of a DNS server for name resolution purposes. Clients can query the DNS server by sending the user-friendly name of any host on the network (also called a host name), and the DNS server responds with the IP address. For example, when a user enters the user-friendly name of *www.bing.com* in the URL for a web browser, the user's computer queries DNS for the IP address of *www.bing.com* without any additional user intervention. Users don't need to memorize IP addresses but instead need only to remember names.

EXAM TIP **Clients need to be configured with an accurate IP address of a DNS server, and the DNS server provides name resolution services. That is, clients can query the DNS server with the user-friendly name of a network resource, and the DNS server provides the IP address of the network resource.**

NOTE **A host name is combined with a domain name to create a fully qualified domain name (FQDN). For example, in *www.bing.com*, *www* is the host name and *bing.com* is the domain name. Because web servers commonly use *www* as a server name, you often do not need to add *www*. For example, if you enter *bing.com* as the URL, it's automatically changed to *www.bing.com*.**

DHCP

Dynamic Host Configuration Protocol (DHCP) is a protocol that often runs on a DHCP server in a network. In small networks, routers often include DHCP, eliminating the need for a server to run DHCP.

True or false? DHCP assigns IP addresses to hosts on a network.

Answer: *True*. DHCP dynamically assigns IP addresses and other TCP/IP configuration to hosts within a network.

DHCP can assign much more than just the IP address, but assigning the IP address is a primary purpose. Other information commonly assigned by DHCP includes the following:

- Subnet mask
- Default gateway
- DNS server address

NOTE **DHCP servers track which IP addresses are assigned to computers in the network so that the same IP addresses are not assigned to more than one client. They also have the ability to detect whether an IP address is already assigned within the network and, if so, can choose an alternate IP address to give to a client.**

EXAM TIP **The primary purpose of DHCP is to dynamically assign IP addresses and other TCP/IP configuration information to DHCP clients. DHCP clients that do not receive an IP address from DHCP assign themselves an APIPA address starting with 169.254.**

Subnet mask

IPv4 addresses are matched with a subnet mask. For example, a Class C address of 192.168.1.5 has a subnet mask of 255.255.255.0. You don't always see the subnet mask, but it is being used.

True or false? The subnet mask defines what portion of an IP address is the network ID and what portion is the host ID.

Answer: *True*. IP addresses have two parts (the network ID and the host ID), and the subnet mask is used to differentiate the two.

Both IP addresses and subnet masks are composed of 32 bits. They are typically presented as four decimal numbers divided by dots (also known as dotted decimal notation), but they can also be represented in binary. For example, consider the IP address of 192.168.1.5 with a subnet mask of 255.255.255.0. Both can be represented in binary as follows:

- `192.168.1.5 = 1100 0000.1010 1000.0000 0001.0000 0101`
- `255.255.255.0 = 1111 1111.1111 1111.1111 1111.0000 0000`

NOTE **Numbers are easier to comprehend when they are grouped. For example 1,234,567,890 is easier to read and understand than 1234567890. Both are the same number, but it is easier to see that it is more than 1 million when grouping is used. Similarly, bytes are often grouped by putting a space between each set of four bits.**

The subnet mask is used to determine which portion of the IP address is the network ID. When the subnet mask is a 1, that portion of the IP address is the network ID. In the following example, notice that the 1s in the subnet mask match up to only the first 24 bits in the IP address:

- 192.168.1.5 = 1100 0000.1010 1000.0000 0001.---- ----
- 255.255.255.0 = 1111 1111.1111 1111.1111 1111.0000 0000

If you convert these bits back to decimal, you have 192.168.1. However, you always add trailing zeros for the network ID, so the network ID is 192.168.1.0.

The host ID is whatever is left over. Because the first three decimal numbers are used for the network ID, the last number (5) is the host ID.

- 192.168.1.5 = ---- ----.---- ----.---- ----.0000 0101
- 255.255.255.0 = 1111 1111.1111 1111.1111 1111.0000 0000

NOTE **When only 255 and 0 decimal numbers are used in the subnet mask, this can be simplified. When the subnet mask is a 255, that portion of the IP address is the network ID. When the subnet mask is a 0, that portion of the IP address is the host ID.**

EXAM TIP **The subnet mask is used to differentiate which portion of an IP address is the network ID and which portion of the IP address is the host ID. If the subnet mask bit is 1 (or the decimal number is 255), the corresponding portion of the IP address is the network ID. If the subnet mask is 0, the corresponding portion of the IP address is the host ID.**

MORE INFO **Chapter 21 of the CompTIA A+ Training Kit (Exam 220-801 and Exam 220-802), ISBN-10: 0735662681, goes into more depth about how the subnet mask is combined with the IP address to identify the network ID and the host ID portion.**

Gateway

The gateway (or default gateway) is an IP address on a router, and it provides a path out of the network. A router will have more than one network interface, and each is assigned an IP address.

True or false? If a client is assigned an incorrect default gateway address, it will not be able to communicate with any systems on the network.

Answer: *False.* The gateway provides a path to other networks through a router, but even if it is configured incorrectly, clients on the network will still be able to communicate with clients on the same subnet.

Figure 2-1 shows a diagram of a network with a router. All clients in Network 1 use a network ID of 192.168.1.0 and a default gateway of 192.168.1.1 (label 1). If clients in Network 1 need to communicate with clients in Network 2 or the Internet, they send the traffic to the default gateway and the router sends the traffic to the correct path.

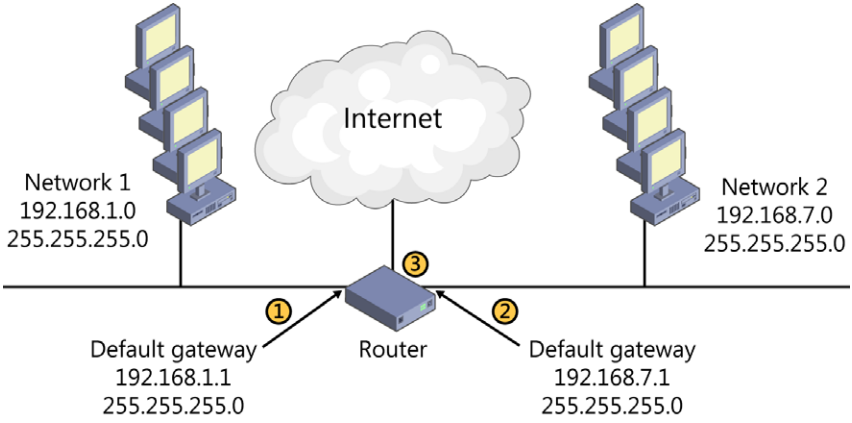


FIGURE 2-1 Router with two default gateways.

If the default gateway for any client on Network 1 is incorrect, this client will not be able to reach Network 2 or the Internet. However, it will still be able to communicate with other clients on Network 1.

In the diagram, you can see that the default gateway for Network 2 is 192.168.7.1 (label 2). All clients in Network 2 are assigned this address. Label 3 shows the interface card going to the Internet.

NOTE **While many people call the default gateway the router, that is not completely accurate. It is the IP address of a network interface on the router, but the router is much more than just a single default gateway. Routers have multiple interfaces providing gateways, or paths, to other networks.**

EXAM TIP **The gateway provides a path out of a network, and all clients in the same subnet are assigned the same default gateway. The gateway is commonly assigned the first number in the subnet (such as 192.168.1.1), but this isn't a requirement.**

Can you answer these questions?

You can find the answers to these questions at the end of this chapter.

1. What class is this IP address: 192.168.15.7?
2. What type of address is this: FC00::42A:0:0:7F5?
3. What type of address is this: 169.254.63.87?
4. What is the primary purpose of DNS?
5. What is the primary purpose of DHCP?

Objective 2.4: Explain common TCP and UDP ports, protocols, and their purpose

TCP and UDP are core protocols within the TCP/IP suite of protocols. They both use well-known port numbers to identify the type of traffic being sent to destination computers. Firewalls use these port numbers to allow or block traffic. Other protocols work within the TCP/IP suite for other purposes, and this objective expects you to know the primary purpose of some of these protocols. Also, you should know the primary differences between TCP and UDP.

Exam need to know...

- Ports
  For example: What ports are used for traffic in web browsers?
- Protocols
  For example: What is the difference between DHCP and DNS? What is SSH and SFTP?
- TCP vs. UDP
  For example: Which protocol (TCP or UDP) provides the best reliability?

Ports

TCP/IP packets include source IP addresses and ports, and destination IP addresses and ports. The IP address is used to get traffic from the source computer to the destination computer. When the packet reaches the destination, the destination computer uses the port to identify what to do with the traffic.

This is similar to how regular mail uses an address to get mail to a home. After it arrives, someone sorts the mail and determines who gets it. If it's addressed to you, you open and handle it. In this context, the mailing address is similar to the IP address, and the person the mail is addressed to is similar to the port.

For example, Hypertext Transfer Protocol (HTTP) uses port 80. When you use a web browser to browse the Internet, your computer sends a request to the web server using its IP address and a destination port of 80. When the web server receives it, it sees port 80 and sends the request to the service handling web requests.

If your web browser had a secure connection, it would use Hypertext Transfer Protocol Secure (HTTPS) and port 443. Instead of using a destination port 80, it uses a destination port of 443. Again, when the web server receives it, it recognizes port 443 and forwards the request to the web server.

True or false? Port 25 should be opened on a firewall to send email.

Answer: *True.* Port 25 is used by Simple Mail Transfer Protocol (SMTP) to send email.

Incoming email uses either port 110 with Post Office Protocol version 3 (POP3) or port 143 with Internet Message Access Protocol (IMAP).

True or false? Port 53 should be opened if a user wants to control a computer remotely with RDP.

Answer: *False*. Port 53 is used for DNS name resolution requests. Port 3389 should be opened when using the Remote Desktop Protocol (RDP).

EXAM TIP **There are several port numbers you should know for the exam. They are: FTP (20 and 21), Telnet (23), SMTP (25), POP3 (110), IMAP (143), DNS (53), HTTP (80), HTTPS (443), and RDP (3389).**

MORE INFO **If you want to get more details on how ports are used, you can check out the following blog: *http://blogs.getcertifiedgetahead.com/understanding-ports-security/*. It was written for the Security+ exam, but the same principles apply for the ports in A+ and Network+. Chapter 20 of the CompTIA A+ Training Kit (Exam 220-801 and Exam 220-802), ISBN-10: 0735662681, covers the ports and protocols in more depth.**

Protocols

Protocols provide the rules for transmitting traffic over a network. Most protocols are formally defined in Request For Comments (RFC) documents. For example, RFC 2131 defines how DHCP works, including the contents of packets sent back and forth between DHCP servers and DHCP clients.

True or false? SFTP is used to transfer large files in an encrypted format.

Answer: *True*. File Transfer Protocol (FTP) is used to transfer large files over a network, and Secure File Transfer Protocol (SFTP) uses Secure Shell (SSH) to encrypt the files.

You should know the primary purpose of the following protocols mentioned in this objective:

- **DHCP** Assigns an IP address and other TCP/IP configuration to clients.
- **DNS** Used to resolve user-friendly names of network resources (also called hosts or host names) to their IP addresses.
- **Lightweight Directory Access Protocol (LDAP)** Used to interact with services such as Active Directory Domain Services in Microsoft domains.
- **Simple Network Management Protocol (SNMP)** Used to communicate with and manage network devices such as switches and routers.
- **Server Message Block (SMB)** Used to transfer files over a network in a Microsoft network.
- **SSH** Used to encrypt some types of traffic such as SFTP.
- **SFTP** Used to transfer large files securely.

EXAM TIP **Know the basic purpose of the protocols in the list. All of these protocols have a lot more depth, but for the A+ exams, you need to be aware of only their primary purposes.**

TCP vs. UDP

Most IP traffic transmitted over an Ethernet network uses either Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). The characteristic differences determine which is the most suited for specific traffic, so you need to know the basic differences between them for the A+ exam.

True or false? TCP is known as a connectionless protocol, and UDP is known as a connection-oriented protocol.

Answer: *False.* The definitions are reversed. TCP is known as a connection-oriented protocol, and UDP is known as a connectionless protocol.

"Connection" in this context refers to how the protocols communicate. TCP exchanges three packets between two systems before sending data. These packets verify that the computers are able to connect. In contrast, UDP packets are just sent without checking to see whether the other system is operational.

Table 2-1 lists some of the common differences between TCP and UDP. TCP uses a three-way handshake to create a connection, but UDP does not. TCP provides guaranteed delivery by verifying that packets were received with receipt acknowledgements and resending them if necessary. In contrast, UDP makes a best effort to deliver the data but doesn't verify that it has been received. If a UDP packet isn't received, it's lost.

TABLE 2-1 TCP vs. UDP

TCP	UDP
Connection-oriented (uses three-way handshake before sending)	Connectionless (no handshake)
Guaranteed delivery	Best effort delivery
Receipt acknowledgements	No acknowledgments

NOTE **Table 2-1 highlights some of the best characteristics of TCP, so the benefits of UDP might not be apparent. UDP is very effective when transmitting audio and video where occasional data loss is acceptable. It has less overhead because it doesn't verify delivery of each packet, resulting in faster transmissions and bandwidth utilizations.**

You can think of TCP like a connection made with a phone call between two people. Imagine Bob wants to tell Susan that she was just announced as a winner of $1,000 on a local radio station but that she has to call in within ten minutes. The three-way handshake starts like this:

1. Bob calls Susan.
2. Susan answers the phone with "Hello."
3. Bob replies with "Hi, this is Bob" and then gives her the message.

If Susan doesn't hear or understand the message, she can ask Bob to repeat it. When the call is over, Bob knows that Susan did get the message.

UDP is similar to sending a text message. Bob might send messages to Susan all the time, so he could send a text message about Susan winning the prize and the need to call immediately. It will probably work, but any number of things might go wrong. There might be a problem with settings on Bob's system, Susan's system, or the network sending the traffic.

If the message is important and timely, the phone is the best option. If the message isn't important, a text message could be used.

Similarly, when you need guaranteed delivery of data over a network, TCP is used. If it's acceptable for some packets to be lost (such as when streaming audio or video), UDP is a good choice.

EXAM TIP **TCP creates a connection with a three-way handshake and provides guaranteed delivery. UDP is connection-less and uses a best-effort to deliver the data.**

Can you answer these questions?

You can find the answers to these questions at the end of this chapter.

1. What ports are used for email traffic?
2. What protocol is encrypted with SSH and is used to transfer large encrypted files?
3. When comparing TCP and UDP, which protocol provides guaranteed delivery of traffic?

Objective 2.5: Compare and contrast wireless networking standards and encryption types

Wireless networks are commonly used in home networks, small offices, and even large organizations. PC technicians are often asked to work on these networks and need to have a basic understanding of the various wireless standards that are available and their characteristics. Security is a primary consideration when configuring a wireless network, so you also need to know what encryption types are available, including which ones provide the best security.

Exam need to know...

- Standards
  For example: Which 802.11 standard is the fastest? Which 802.11 standard uses 5 GHz?
- Encryption types
  For example: What wireless encryption type is the least secure? Which wireless encryption type provides the best protection?

Standards

Wireless networks are known as 802.11 networks, and there are four primary standards you should know about. They are 802.11a, 802.11b, 802.11g, and 802.11n.

True or false? 802.11a networks broadcast on the 5-GHz frequency range.

Answer: *True*. 802.11a networks use only the 5-GHz frequency range. They have a maximum speed of 54 Mbps and have the shortest range when compared to the others.

The speed and range of wireless signals is affected by many variables. Physical obstructions such as walls and trees impede the signals. Also, other radio transmissions in the area can affect how far signals can travel. When wireless devices connect, they attempt to connect at the fastest possible speed of the standard without any errors. When devices are far from each other, they use a slower speed to eliminate errors.

True or false? 802.11g networks have the highest possible speed of each of the wireless standards.

Answer: *False*. 802.11n networks have the highest possible speed with throughputs of 150 Mbps, 300 Mbps, or 600 Mbps. 802.11g networks have a maximum throughput of 54 Mbps.

802.11n uses multiple input multiple output (MIMO) antennas, allowing it to transmit data on two different channels within the same frequency spectrum at the same time. The other standards use a single antenna. 802.11n is also backward compatible with 802.11g.

True or false? 802.11b networks have the lowest maximum speed of each of wireless the standards.

Answer: *True*. 802.11b networks have a maximum speed of 11 Mbps, which is the lowest throughput of all of the wireless standards.

Table 2-2 shows the characteristics of the four wireless standards.

TABLE 2-2 Wireless standards characteristics

STANDARD	FREQUENCY	MAXIMUM SPEED	RANGE
802.11a	5 GHz	54 Mbps	Shortest
802.11b	2.4 GHz	11 Mbps	Medium
802.11g	2.4 GHz	54 Mbps	Medium
802.11n	2.4 GHz and 5 GHz	Up to 600 Mbps	Longest

EXAM TIP **Know the key points listed in Table 2-2. One way to memorize facts like this is to simply draw the table from scratch once a day for several days. You probably won't remember everything at first, but after a few days or so, you'll know the information without looking to check your answers. This information is also needed if you plan on taking the Network+ exam.**

MORE INFO **The Microsoft article titled "Wireless Networking: Frequently Asked Questions" provides more details about wireless networks: *http://windows.microsoft.com/en-US/windows7/Wireless-networking-frequently-asked-questions*.**

Encryption types

Encryption types are used to provide security for wireless transmissions. The three wireless encryption types are Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and WPA2.

True or false? WPA is the least secure of the different encryption types.

Answer: *False*. WEP is the least secure of the different encryption types.

Attackers can easily discover the security key used for a WEP encrypted network. Because of this, WEP is not recommended for use.

WPA was created as an interim replacement for WEP. Later, WPA2 was standardized and is now recommended for use whenever possible. WEP, WPA, and WPA2 commonly use a passphrase or a pre-shared key. When joining a network, you need to know the name of the network, the type of security used, and the passphrase.

WPA and WPA2 both can use either Advanced Encryption Standard (AES) or Temporal Key Integrity Protocol (TKIP) to encrypt the data. AES is a widely used standard and recommended for use.

EXAM TIP **WEP is the least secure wireless encryption type, and WPA2 is the most secure wireless encryption type. WPA2 with AES provides strong security for wireless networks.**

MORE INFO **Check out the following article for steps used to set up a wireless router: *http://windows.microsoft.com/en-US/windows7/set-up-a-wireless-router*. You can also watch the following video, which shows how to view and connect to available wireless networks: *http://windows.microsoft.com/en-US/windows7/View-and-connect-to-available-wireless-networks*.**

Can you answer these questions?

You can find the answers to these questions at the end of this chapter.

1. Which 802.11 wireless standard uses the 5-GHz frequency range?
2. Which 802.11 wireless standard can transmit the most data at a time?
3. Which encryption type has been broken and should not be used?

Objective 2.6: Install, configure, and deploy a SOHO wireless/wired router using appropriate settings

It's very common for a small office home office (SOHO) to have a network with a wireless router used as the central networking device. Computers can connect to the wireless router to share resources on the network and for access to the Internet. Additionally, wireless routers commonly include wired connections and additional services for the network.

Exam need to know...

- MAC filtering
  For example: What is a MAC? What is the benefit of MAC filtering?
- Channels (1-11)
  For example: What is the default channel used for wireless? What channel(s) should you use instead for better performance?
- Port forwarding, port triggering
  For example: What is the difference between port forwarding and port triggering?
- Built-in networking services
  For example: What are the common services built into wireless routers? What should be enabled to automatically assign IP addresses?
- Wireless security
  For example: What is the SSID? What can be done to hide a wireless network from casual users?
- DMZ
  For example: What is a DMZ? What computers would be placed in a DMZ?

MAC filtering

Wired and wireless network interface cards (NICs) use media access control (MAC) addresses. MAC addresses are represented as six groups of two hexadecimal characters similar to this: 1A-2B-3C-4D-5E-6F. MAC addresses are burned into NICs and can be used to identify specific computers.

True or false? You can use MAC filtering on a wireless router to restrict access to only certain devices.

Answer: *True*. MAC filtering can be enabled on a wireless router by using only the MAC addresses of authorized devices.

You can also use MAC filtering with wired routers. The router will block access to the network to all systems except for ones with the specifically allowed MAC addresses.

EXAM TIP **MAC address filtering can be used to block access to a network based on the client's MAC address. It can be enabled on both wireless and wired routers. When enabled, it will block access to unidentified clients attempting to access the network.**

MORE INFO **The MAC address is also known as the physical address or the hardware address. You can view the MAC address of a system with the ipconfig /all command from the command prompt. In this command, it's listed as the physical address. Chapter 14 of the CompTIA A+ Training Kit (Exam 220-801 and Exam 220-802), ISBN-10: 0735662681, shows how to use the command prompt and the ipconfig /all command.**

Channels (1–11)

Wireless protocols are associated with specific frequency bands, such as 2.4 GHz or 5.0 GHz. However, each of these bands is divided into several channels. While a wireless router will automatically pick one of these channels, it is possible to manually select a specific channel.

True or false? If channel 6 has excessive interference, you should select channel 5 or 7 to improve performance.

Answer: *False.* Channel 6 is usually selected by default. However, channels 5, 6, and 7 all overlap with each other, so interference on channel 6 will also affect channels 5 and 7.

If channel 6 has excessive interference, it's recommended to select channel 1 or 11 instead. There isn't any overlap with the signals between these three channels.

Wireless networks in areas where multiple wireless networks are active frequently have performance problems due to interference from other networks. For example, an apartment complex might have several active wireless networks from different residents. You can eliminate interference with most networks by switching to channel 1 or 11.

EXAM TIP **Wireless networks include 11 channels. If channel 6 has interference, you can often get better performance by switching to channel 1 or 11.**

MORE INFO **Microsoft At Home has a good article titled "10 Tips to Help Improve Your Wireless Network." One of these tips is to change the wireless channel. You can view the article here: *http://www.microsoft.com/athome/setup/wirelesstips.aspx*.**

Port forwarding, port triggering

Many wireless routers and firewalls support port forwarding and port triggering. These are two methods used to allow specific types of traffic through a router or firewall.

True or false? Port forwarding opens a specific incoming port after traffic is sent out on a different port.

Answer: *False.* Port forwarding forwards all traffic from the Internet by using a specific port to a specific IP address.

Port forwarding can be used to provide access to a system within a private network from the Internet. For example, all traffic coming in port 80 can be forwarded to a web server on an internal network.

Port triggering uses one outgoing port as a trigger to open a specific incoming port. For example, an application might send traffic out on port 3456 and receive traffic in on port 5678. A port trigger on the router or firewall will automatically open incoming port 5678 only when traffic is sensed going out of port 3456.

EXAM TIP **Port forwarding sends traffic coming in from the Internet on a specific port to an internal system with a specific IP address. Port triggering opens a specific incoming port only after traffic is sent out on a specific port.**

MORE INFO **Port Forward (*http://portforward.com/*) includes many free resources that can be used to understand port forwarding and to configure port forwarding on many different routers.**

Built-in networking services

Hardware devices sold as wireless routers generally also include multiple services that are often enabled by default. This simplifies the setup of the internal network for users.

True or false? Wireless routers commonly include DHCP to assign IP addresses to internal devices.

Answer: *True*. Wireless routers include multiple services, including DHCP.

DHCP assigns a range of IP addresses to DHCP clients and also provides the IP address of the wireless router as each client's default gateway. If desired, you can disable DHCP and manually assign IP addresses to internal systems.

If DHCP has been disabled, DHCP clients will assign themselves an APIPA address starting with 169.254. However, you can manually assign IP addresses and other TCP/IP configuration information for all internal clients. It takes more time, but it is possible.

DHCP can be configured to assign IP addresses for a limited range in a network, and other IP addresses in the range can be manually assigned. For example, you can have DHCP assign IP addresses in the range of 192.168.1.100 through 192.168.1.254 with a subnet mask of 255.255.255.0. You can then manually assign other IP addresses from 192.168.1.1 through 192.168.1.99.

NOTE **It's common to manually assign IP addresses to servers and printers so that each always has the same IP address, even after being turned off and back on.**

It's also possible to have addresses assigned based on their MAC addresses. For example, you can have DHCP always assign the same IP address to a printer. When the printer requests an IP address, the request includes the printer's MAC address, and you can map this MAC address to a specific IP address in DHCP. This is known as a DHCP reservation.

Other services commonly included in a wireless router include the following:

- **Firewall** The firewall filters traffic in and out of a network. Traffic can be filtered based on IP addresses, MAC addresses, logical ports, and protocols. Most firewalls are configured to block all traffic except for traffic that is specifically allowed.
- **Network Address Translation (NAT)** NAT is a service that replaces private IP addresses used internally on a network with public IP addresses used on the Internet. The wireless router will have a single public IP address connected to the Internet, and all internal devices can share it when accessing the Internet.
- **Basic Quality of Service (QoS)** QoS is a group of a technologies used to control traffic on a network by assigning different priorities to specific types of traffic. For example, it can give streaming video a lower priority than other types of traffic.

EXAM TIP **DHCP is included as a service on most wireless routers. When enabled, it automatically assigns IP addresses to DHCP clients in a network. It can be disabled if desired, but IP addresses need to be manually assigned if DHCP is disabled.**

Wireless security

A primary step you need to take for wireless security is to select a secure encryption type such as WPA2, as described in Objective 2.4, "Explain common TCP and UDP ports, protocols, and their purpose," earlier in this chapter. A strong passphrase should be used, and the passphrase should be kept secret. In addition to using WPA2 with a strong passphrase, there are some additional steps you can take.

True or false? You can enable SSID broadcast to prevent users from connecting to a wireless network.

Answer: *False*. You can *disable* service set identifier (SSID) broadcasts to prevent users from easily seeing and connecting to a wireless network.

The SSID is the name of the network, and you need to know the SSID when connecting any device. When SSID broadcast is enabled, the network is visible to anyone in range of the network, making it easier for users to select the network. When SSID broadcast is disabled, users need to type in the name manually.

True or false? WPS allows users to configure security by pressing a button or entering a personal identification number (PIN).

Answer: *True*. Wi-Fi Protected Setup (WPS) is a feature on some wireless routers, designed to make security configuration almost as easy as pressing a button. Unfortunately, WPS is vulnerable to attacks and not recommended for use.

EXAM TIP **You can hide wireless networks from casual users by disabling SSID broadcast. When SSID broadcast is disabled, it is difficult for other users to see the network without using special tools.**

MORE INFO **Wireless topics are also mentioned on 220-802 objectives such as Objective 2.5 covered in Chapter 7, "Security," of this book. Chapter 23 of the CompTIA A+ Training Kit (Exam 220-801 and Exam 220-802), ISBN-10: 0735662681, covers wireless networks in more depth, including the differences between wireless access points and wireless routers, the different wireless security types, and how to configure wireless routers.**

DMZ

A demilitarized zone (DMZ) is a buffer network that provides a layer of protection for an internal network and a device that can be accessed from the Internet. DMZs are also known as screened subnets, perimeter networks, or buffer networks and are typically created with two firewalls. One firewall routes traffic between the Internet and the DMZ. The second firewall routes traffic between the internal network and the DMZ.

True or false? Internet-facing servers are placed in a DMZ to provide a level of protection.

Answer: *True*. Any server that can be accessed from the Internet has an added layer of protection when it is placed in a DMZ.

On home networks, users might place a gaming server in the DMZ to protect it while still making the server accessible to other users through the Internet. In larger networks, mail servers and web servers are commonly placed in a DMZ.

Without a DMZ, Internet-facing servers would need to be placed directly on the Internet with a public IP address or within an internal network. Note that you can place an Internet-facing server in one of the following three locations:

- **On the Internet** It has a public IP address and minimal protection. It is susceptible to a wide variety of attacks.
- **Internal network** If the system is successfully attacked, the attacker might be able to access other systems on the internal network. That is, this presents additional risks to internal systems.
- **DMZ** The Internet-facing server has a layer of protection against Internet attacks from the firewall between it and the Internet. The internal network has an additional layer of protection against a successful attack against the Internet-facing server.

EXAM TIP **Internet-facing servers are often placed in a DMZ for extra security. This includes gaming servers in home networks, and mail or web servers in corporate networks.**

MORE INFO **There are many different configurations for a DMZ. The Wikipedia article on DMZs includes good descriptions and diagrams of different DMZs. You can view it here: *http://en.wikipedia.org/wiki/DMZ_(computing)*.**

Can you answer these questions?

You can find the answers to these questions at the end of this chapter.

1. What type of address can you use to block network access for specific computers?
2. What channel(s) should you use if your wireless network has excessive interference on channel 6?
3. Where should you place a gaming server that needs to be accessible from the Internet but also needs protection?

Objective 2.7: Compare and contrast Internet connection types and features

This objective requires you to know about the different ways that users can connect to the Internet. You should know when the connection types are available or most appropriate. You should also have a basic understanding of the relative speeds of the different connections.

Exam need to know...

- Cable and fiber
  For example: What is the relationship of the speed of cable and fiber broadband connections compared to other connections?
- Phone lines
  For example: What types of connectors are used for phone lines?
- Satellite
  For example: When is satellite Internet access most appropriate?
- Cellular (mobile hotspot)
  For example: What is a MiFi device?
- WiMAX and line of sight wireless Internet service
  For example: Where is WiMAX used?

Cable and fiber

Years ago, all television broadcasts were sent over the air as radio frequency RF transmissions. Anyone that wanted to watch TV used an antenna on their TV or rooftop and had access to a limited number of channels. Telecommunications companies began running cables to as many houses as they could and then charging users to connect to the cable, so most homes now have cable TV. Cable TV provides a clearer picture and delivers more channels, so it quickly became popular.

In time, these telecommunications companies realized that in addition to sending television signals over the cable, they could also provide Internet access over the same cable. These companies expanded their services and became Internet Service Providers (ISPs).

True or false? Broadband cable Internet connections are significantly faster than any dial-up or ISDN access.

Answer: *True*. Broadband cable has been the fastest Internet connection available to home users for many years.

Cable television originally used copper coaxial cable, and many cable connections still use coaxial cable. However, some telecommunications companies have started to run fiber to neighborhoods and homes as a faster alternative. Fiber cable connections typically provide faster connections than traditional cable TV connections.

EXAM TIP **Fiber and cable Internet connections are often referred to as broadband connections. They provide significantly faster Internet connections than any type of connection using phone lines.**

MORE INFO **The Microsoft article titled "Set Up a Broadband (DSL or Cable) Connection" includes details and some diagrams showing how a single computer and a home network can be configured with a broadband Internet connection. You can view it here: *http://windows.microsoft.com/en-US/windows7/Set-up-a-broadband-DSL-or-cable-connection*.**

Phone lines

In the early days of the Internet, the only way people could connect to the Internet was through the plain old telephone service (POTS). Phone lines are still used to provide Internet access to many people living in rural areas that do not have cable or fiber connections available at their homes.

True or false? Computers with a modem and a POTS line can connect to the Internet.

Answer: *True*. A dial-up connection to the Internet needs only a computer with a modem and simple phone line.

A modem is a modulator/demodulator that converts the signals between the formats needed by the computer and by the transmission line. The modem can be built into the computer or added as an external device.

The following three different types of connections use phone lines:

- Dial-up connections use a simple POTS phone line and a traditional modem.
- Integrated Services Digital Networks (ISDNs) use digital signals and terminal adapters in place of modems. A benefit is that a user can talk on the phone at the same time that the phone line is being used for the Internet connection.
- Digital subscriber lines (DSLs) also use digital signals and are available in large metropolitan areas. Technically, they use a transceiver instead of a modem, but the transceiver is commonly called a DSL modem.

True or false? In an ADSL line, the upload speed is faster than the download speed.

Answer: *False.* An asymmetric DSL (ADSL) does have different speeds for uploads and downloads. However, the download speed is faster than the upload speed.

Most users need faster downloads than uploads. For example, when users are browsing the Internet, they typically send very small requests to view a webpage in upload requests. However, the webpage can include a significant amount of data, such as text, graphics, audio, and video that is downloaded to the users.

EXAM TIP **Common methods of Internet access that use a phone line are dial-up, ISDN, and DSL. Simple dial-up connections can use POTS lines. ISDN and DSL use digital signals. ADSL lines have faster download speeds than upload speeds. Because they connect through phone lines, they use twisted-pair cable and RJ-11 connectors.**

Satellite

Most rural areas do not have cable television, but they do have satellite television as an alternative. Users can subscribe with a satellite provider. They have satellite dishes that can receive television signals from an orbiting satellite. Additionally, many current satellite television systems can also transmit basic signals up to the satellite.

Just as telecommunications companies began using their cable and fiber connections for Internet access, many satellite providers began using their satellite connections for Internet access. Additionally, some companies specialize in only Internet access via satellite connections.

True or false? A major drawback with satellite signals is signal latency.

Answer: *True.* Signal latency refers to the amount of delay between when a user sends a request and receives a reply.

With broadband fiber and cable connections, users start to see a webpage download almost immediately when they send the request. In contrast, users with a satellite connection might see a significant delay between the time when they click a link and the webpage starts to load. This is because the signal must travel to the satellite in orbit, back down to Earth, back up to the satellite, and back to the user.

EXAM TIP **Satellite connections are used in rural areas and give users much faster connections than a dial-up connection. The primary drawback is the high degree of latency.**

MORE INFO **Satellite Internet services have historically received inconsistent reviews. They are sometimes great in one area but poor in another area. The following page includes reviews of some popular satellite Internet providers: *http://satellite-internet-review.toptenreviews.com/.***

Cellular (mobile hotspot)

Smartphones use cellular access both for telephone calls and for Internet access. When users subscribe to the service, they can surf the Internet and access email with their smartphones. This same service is available for mobile hotspots. A mobile hotspot connects to the cellular service and acts as a wireless router for multiple wireless devices.

True or false? Cellular Internet access is the best choice for a user who frequently travels.

Answer: *True.* Devices with cellular Internet access can access the Internet from almost anywhere.

Mobile hotspots are also known as MiFi devices. A MiFi device is a small battery-powered device that users can take with them just about anywhere. After turning it on, it automatically connects to the cellular service. Users can configure mobile devices with the MiFi SSID and passphrase and connect to the Internet through the MiFi device. A single MiFi device typically supports five or more wireless devices.

> ***EXAM TIP*** **Cellular hotspots are ideal for users who travel. They provide Internet access for users from anywhere cellular access is available.**

WiMAX and line of sight wireless Internet service

Worldwide Interoperability for Microwave Access (WiMAX) is another wireless standard. It can deliver high-speed wireless Internet access for large geographical areas, such as a metropolitan area network (MAN).

True or false? When connecting to WiMAX networks, WiMAX towers need a clear line of sight between each other.

Answer: *True.* WiMAX towers use microwave links between each other, and these require a clear line of sight between each other.

Internet service providers (ISPs) have a wired connection to a WiMAX tower. The WiMAX towers connect to each other wirelessly, and end users can connect to the closest tower wirelessly.

> ***EXAM TIP*** **WiMAX is used in metropolitan areas. When available, it provides fast wireless access over a large geographical area.**

Can you answer these questions?

You can find the answers to these questions at the end of this chapter.

1. Which wired Internet connection provides the highest speeds?
2. What type of Internet connections use phone lines?

3. What type of Internet connection is most appropriate for a traveling salesman?
4. What type of Internet connection is mobile and can be used to provide Internet access for multiple users?

Objective 2.8: Identify various types of networks

When people are talking about a network they are usually talking about a local area network in a single location. However, there are several other types of networks. As a PC technician, you don't necessarily need to be an expert in all the different types of networks, but you should understand the terminology used. Most local area networks are configured in a star topology, but there are other types, and you're expected to know what differentiates each type.

Exam need to know...

- LAN
  For example: What is a LAN?
- WAN
  For example: What is the primary characteristic of a WAN?
- PAN
  For example: Where is a PAN located?
- MAN
  For example: What is the difference between a MAN and a WAN?
- Topologies
  For example: What are the different topologies? Which topology provides the best fault tolerance?

LAN

A local area network (LAN) is a network in a single location. Devices connected to the LAN can access network resources such as servers and printers.

True or false? A LAN is the primary type of network used in a SOHO.

Answer: *True*. A SOHO network would be in a single location and is a LAN.

A LAN can include multiple networks (sometimes called subnets). For example, an organization could have one network for servers, one network for people in the Sales department, and another network for all other employees. Within each network, all of the devices are connected with switches. Within the organization, one or more routers connect the different networks and provide a path to the Internet.

EXAM TIP **A LAN is in a single location. It can include multiple networks within the location, but if all the networks are located together, it is called a LAN.**

WAN

A wide area network includes two or more LANs geographically separated. For example, a company might have a LAN in Virginia Beach and another LAN in New York. If they connect the two LANs, they are creating a WAN.

True or false? A WAN includes networks that can cover a large physical distance.

Answer: *True.* WANs can include networks in different cities, states, countries, or regions. The key is that they are geographically separated.

> ***EXAM TIP*** **A WAN includes networks that are geographically separated. They typically cover large physical distances.**

PAN

A personal area network (PAN) is a network of devices that are connected around a person. For example, a person might have a smartphone and a tablet device with wireless capabilities, and a mobile hotspot used to connect to a cellular network. After turning on the hotspot, they can use it to connect to the Internet with the smartphone and their tablet.

True or false? A PAN can include devices in a separate building within a single campus.

Answer: *False.* A PAN is centered around a single individual only. While the signals might travel farther than a few feet around a person, the PAN is still focused on the person.

> ***EXAM TIP*** **A PAN is centered around a person. It might include just a smartphone and a Bluetooth-enabled headset, or it might include more advanced devices, such as a mobile hotspot and a tablet.**

MAN

A metropolitan area network (MAN) is a group of networks in the same geographical location but spread across a wide area. For example, a university campus that has connected networks throughout several buildings is a MAN.

True or false? The MAN and WAN are essentially the same.

Answer: *False.* A WAN includes LANs that are separated by a large physical distance, but a MAN includes networks that are in the same general geographical location.

The difference between a LAN and a MAN is that a LAN is within a single building, while a MAN will span multiple buildings.

> ***EXAM TIP*** **A MAN includes multiple networks spread throughout two or more buildings in the same geographical location. WiMAX is used for some MANs.**

Topologies

Computers are organized within a network by using different network topologies. A *topology* refers to how the devices are logically connected, and the most common topology is the star topology.

True or false? A mesh topology provides redundancy for each network device.

Answer: *True.* A mesh topology includes multiple redundant connections for each device in the network. If any single connection fails, the device can tolerate the failure and continue to communicate with devices by using other connections.

True or false? A bus topology provides redundancy with a MAU.

Answer: *False.* A bus topology does not have any redundancy. If a single connection fails, the entire network fails. Token ring networks often use a multistation access unit (MAU) for redundancy. The four primary topologies are star, ring, mesh, and bus. Figure 2-2 shows diagrams of each, and they are defined as follows:

- In a star topology, devices connect to each other through a central network distribution device such as a hub or a switch.
- In a ring topology, devices are connected in a physical or logical ring. A logical token is passed to each device in turn, and devices can transmit only when they have the token. Some token rings use a central MAU to eliminate the possibility of a single device failing and breaking the ring.
- A mesh topology includes multiple connections. In a full mesh network, every single device has connections to every other device in the network.
- A bus network connects devices in a line. Each end of the bus must be terminated. If a terminator is removed, all devices stop communicating. Similarly, if the bus has a failed connection anywhere on the bus, it results in two separate segments that each have only a single terminator. That is, any break in the bus stops communication for all devices.

A hybrid network uses a combination of any two or more topologies.

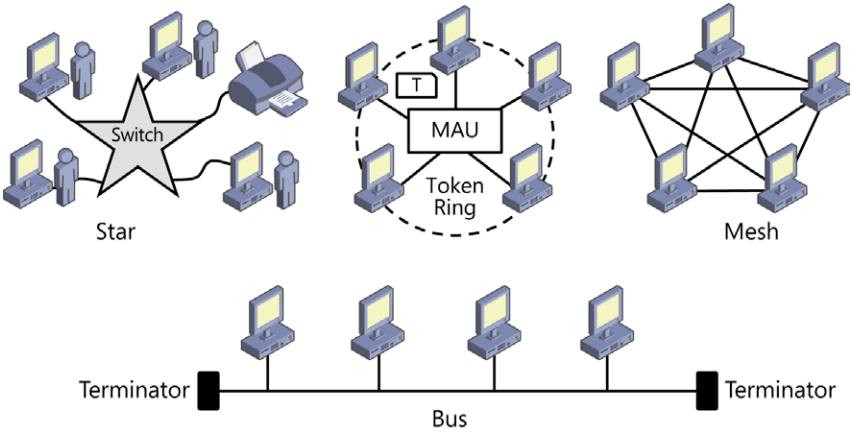


FIGURE 2-2 Topologies.

EXAM TIP **The bus topology has the worst reliability because any single failure can take down the entire network. A mesh topology has the best reliability due to the redundant connections, but it is the most expensive. Most networks use a star topology with twisted-pair cable between each device and a central switch or hub. The extra cable costs more money than a bus network, but if a single cable breaks, it affects only one system.**

MORE INFO **The Wikipedia article titled "Network Topology" provides a good overview and graphics of the different types of network topologies: *http://en.wikipedia.org/wiki/Network_topology*.**

Can you answer these questions?

You can find the answers to these questions at the end of this chapter.

1. What type of network is centered around an individual?
2. What type of network connects multiple networks located in separate geographical locations?
3. What network topology provides the most redundancy?

Objective 2.9: Compare and contrast network devices and their functions and features

Computers and printers within a network are connected to various network devices such as hubs, switches, routers, access points, bridges, and modems. This objective expects you to know the functions and features of each of these network devices.

Exam need to know...

- Hub
  For example: What is the difference between a hub and a switch?
- Switch
  For example: What are benefits of switches over hubs?
- Router
  For example: What additional protocols are often included on routers used in SOHOs?
- Access point
  For example: What is the difference between a WAP and a wireless router?
- Bridge
  For example: What is the difference between a bridge and a switch?
- Modem
  For example: What type of connector does an internal modem use?
- NAS
  For example: What is the primary purpose of a NAS?

- Firewall
  For example: What is created on a firewall to allow traffic through?
- VoIP phones
  For example: What type of calls can be made with VoIP phones?
- Internet appliance
  For example: What is the purpose of an Internet appliance?

Hub

A hub is a simple network device used to connect multiple devices together in a network. Ethernet hubs were once very common. They have multiple RJ-45 ports, which were connected to computers or other network devices via twisted-pair cable.

True or false? A hub sends unicast traffic that it receives to all other devices that are connected to the hub.

Answer: *True*. A hub transmits all data that it receives on one port to all other ports.

When looking at the features of various network devices, it's valuable to know the difference between unicast, broadcast, and multicast traffic, as follows:

- Unicast traffic is sent from one device and addressed to one other device. Even though unicast traffic is addressed to only one device, the hub still forwards unicast traffic to all other devices connected to the hub.
- Broadcast traffic is sent from one device to all other devices on a network. Broadcast traffic is not sent through a router.
- Multicast traffic is sent from one device to multiple other devices.

True or false? A hub has the most security when compared to a switch.

Answer: *False*. A hub has less security than a switch.

If sensitive data is sent to one port on the hub, it is automatically sent to all other ports. Any computer connected to the hub will receive this data and can intercept it with the right tools. In contrast, a switch forwards unicast traffic to only one port.

> ***NOTE*** **Both unicast and broadcast traffic sent to one port on a hub go to all physical ports on the hub.**

> ***EXAM TIP*** **A hub has no intelligence or selectivity. All data sent to one port of a hub goes to all other ports. It is less secure than a switch, and many organizations have replaced hubs with switches.**

Switch

A switch includes circuitry that allows it to be selective when sending data through the switch. It can identify which device is connected to each physical port, based on the media access control (MAC) address.

True or false? A switch sends unicast traffic to a single physical port.

Answer: *True*. A switch transmits data that it receives to specific ports. It analyzes packets to determine the destination MAC address and sends the packet to the port where that MAC address is being used.

Switches learn which devices are connected to which physical port by analyzing traffic that comes into the port. They build an internal table mapping the physical port number with the MAC address. They then send unicast traffic only to the specific port where the MAC address is used.

In contrast, a hub forwards traffic to all other ports on the hub. The selectivity of the switch provides better performance for devices connected to the switch. Additionally, the switch adds some security by not sending unicast traffic to all ports.

NOTE **Broadcast traffic sent through a switch goes to all physical ports on the switch. However, unicast traffic is sent to only a single port on the switch. The switch uses the MAC address to determine which port to use when sending unicast traffic.**

EXAM TIP **A switch sends unicast packets only to specific ports. This improves performance by segmenting the traffic and also improves security by restricting which ports receive traffic.**

Router

Routers are used to connect networks or subnets together. In general, the networking devices are connected together with a switch or a hub in a network, and multiple networks are connected together with a router. Routers evaluate the IP address of traffic and determine the best path to send it to get it to its destination. Each router in a path is also referred to as a hop.

True or false? A router is placed between an internal network and the Internet.

Answer: *True*. Routers connect networks, and in this case, the internal network is one network and the Internet is a huge network of networks.

Routers placed between the Internet and an internal network commonly uses network address translation (NAT). NAT translates private IP addresses used internally, within a network, to public IP addresses used on the Internet.

A company could have multiple routers, with some used to connect internal networks and another one used to connect to the Internet. The internal routers would not use NAT.

NOTE **Broadcast traffic sent to a router is not passed through the router. Unicast traffic is sent through the router port that provides the best path to the destination network. The router uses the IP address to determine the best path.**

EXAM TIP **Routers are used to connect networks together. Routers used in SOHOs often have additional capabilities, such as NAT and DHCP.**

MORE INFO **The Microsoft article "Start Here to Set Up a Home Network in Windows 7" includes details about six separate steps to set up a home network with Windows 7. It includes information about setting up a router, and it is available here: *http://windows.microsoft.com/en-US/windows7/start-here-to-set-up-a-home-network-in-windows-7*.**

Access point

A wireless access point (WAP) is sometimes referred to as simply an access point. It provides access for wireless clients to a network.

True or false? Wireless access points provide the same services as a wireless router.

Answer: *False*. A router provides more services than a mere access point.

A wireless access point and a wireless router are not the same things. Specifically, an access point provides connectivity only for wireless clients to other wireless clients and to a wired network. However, a wireless router includes multiple other components.

Figure 2-3 shows the components of a typical wireless router. It has RJ-45 connections for wired clients and wireless capabilities for wireless clients. These wired and wireless clients are connected to each other using the switch component of the wireless router. The wireless router has a wide area network (WAN) connection used to connect to the Internet, and all of the clients can go through this router for Internet access.

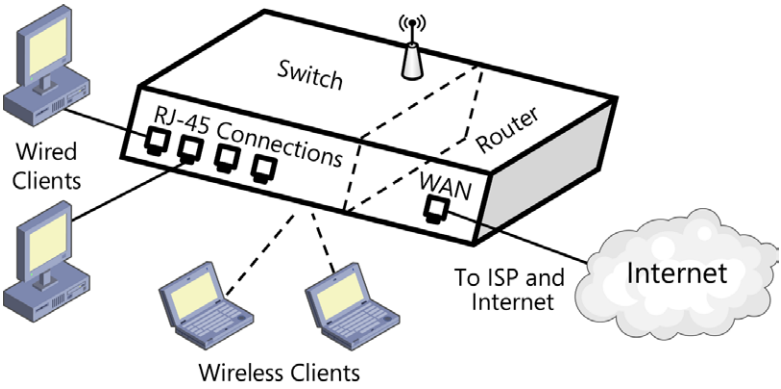


FIGURE 2-3 Wireless router.

NOTE **An access point might look similar to Figure 2-3, with the following differences. It would not have a router component or a WAN connection. Also, it would typically have only one RJ-45 connection to a wired network instead of multiple wired RJ-45 ports.**

EXAM TIP **Access points provide access to wired networks for wireless clients. Wireless routers include the capabilities of a wireless access point, with some additional services.**

Bridge

A bridge is similar to a switch but instead of connecting individual devices, it's used to connect groups of devices. For example, two groups of computers might be connected to each other with two separate hubs. You can then use a bridge to connect the two groups together via the bridge. Even though the two groups are connected, the bridge is selective about what data is forwarded between the two groups of devices.

True or false? Bridges are used instead of switches in most networks today.

Answer: *False.* Bridges are rarely used. When the functionality of a bridge is needed, switches are typically used instead.

Modem

Modems are used for Internet access connections for a computer via a phone line. They use RJ-11 connections to connect to the phone line. Many modems are internal to a computer, but external modems are also available. An external modem typically connects to a computer with a USB connection.

True or false? A modem converts digital signals to analog signals.

Answer: *True.* A modem converts digital signals coming from a computer to analog signals that can be transmitted on a phone line.

The analog signals are modulated by the modem before being placed onto the phone line. The modem is also able to demodulate received data to convert the analog data into digital data needed by the computer.

EXAM TIP **A modem modulates digital data from a computer, converting it to analog data for transmission. It also demodulates received analog data and converts it to digital data needed by the computer.**

NAS

Network attached storage (NAS) is a dedicated computer system used to provide disk storage on a network. A NAS device includes one or more disk drives, and storage sizes of 1 TB or greater are common. They have RJ-45 ports used to connect a twisted-pair cable to a switch or router on a network.

True or false? NAS devices do not have any security, so sensitive data should never be stored on the NAS.

Answer: *False.* NAS devices include an operating system that can be used to assign permissions and restrict access to folders.

Many NAS devices use Unix or Linux as the operating system and require very little configuration or management. They often include a web-based interface that you can use to create additional users, groups, and folders, and to assign permissions to the folders. In addition to using NAS devices to share data, many people use them to store backups.

EXAM TIP **A NAS device includes an operating system and provides disk storage for any device on the network. Access can be restricted by assigning permissions.**

Firewall

A firewall filters traffic in and out of a network or in and out of an individual computer. Firewalls are generally classified as either network-based or host-based. A network-based firewall is often used in conjunction with a router to filter traffic in and out of a network. A host-based firewall is additional software running on a computer for additional security protection.

True or false? Firewalls can block outgoing email by blocking traffic on port 25.

Answer: *True*. Firewalls can filter traffic based on ports. Port 25 is used for outgoing email, so if this port is not open on the firewall, it will block outgoing email.

Firewalls can also filter traffic based on IP addresses, network IDs, and protocols with simple packet filtering. Most firewalls also support more advanced filtering, allowing them to analyze traffic to determine whether the data should be allowed or blocked.

Most firewalls use an implicit deny philosophy with exceptions. That is, all traffic is blocked (denied) unless a rule or exception has been created to allow it. For example, if you wanted to allow outgoing email, the firewall needs to have a rule opening port 25 for outgoing traffic.

EXAM TIP **Firewalls can filter traffic based on IP addresses, ports, and protocols. Wireless routers include firewall capabilities allowing them to allow or block traffic.**

VoIP phones

A Voice over Internet Protocol (VoIP) phone is used to make telephone calls over an IP network. They resemble a regular phone, but instead of plugging into a telephone line with an RJ-11 connector, they plug into a network device like a switch or router with an RJ-45 connector.

True or false? VoIP phones can be used instead of traditional phones for long distance calls.

Answer: *True*. As long as you have Internet access, you can use the VoIP phone to make telephone calls.

EXAM TIP **You can mimic the capabilities of a VoIP phone with a headset and microphone connected to your computer. You'll need specialized software to make the connections, but this is often available when you subscribe to a service.**

MORE INFO **Skype is a popular service that people use to make long distance calls. People subscribe with a flat fee and can make phone calls by using their computer. You can read more about it here: *http://skype.com*.**

Internet appliance

Internet appliances are small devices used to access the Internet for web browsing or email access. Many of the features of an Internet appliance are included with mobile devices such as smartphones and tablets.

NOTE **The term *Internet appliance* is rarely used today. Also, there are very few Internet appliances available that are dedicated only to surfing the Internet or accessing email. However, many security appliances are common. For example, a network security appliance might include a firewall, along with malware and spam filters. Similarly, some SOHOs subscribe to Internet security services, such as an online spam filtering service. These services use Internet security appliances.**

Can you answer these questions?

You can find the answers to these questions at the end of this chapter.

1. What is a benefit of a switch over a hub?
2. What type of network device would include NAT?
3. What type of device is used to connect to a dial-up ISP?
4. What type of device blocks all traffic unless a rule is created to allow the traffic?

Objective 2.10: Given a scenario, use appropriate networking tools

Network technicians use several different tools to create cables, wire networks, and troubleshoot problems. This objective expects you to know about many of these tools, including the scenarios when these tools are appropriate to use.

Exam need to know...

- Crimper
  For example: What is the primary purpose of a crimper?
- Multimeter
  For example: What setting on a multimeter is used to check for cable breaks?
- Toner probe
  For example: What is the primary purpose of a toner probe?

- Cable tester
  For example: What information is provided by a cable tester?
- Loopback plug
  For example: What is tested with a loopback plug?
- Punchdown tool
  For example: Where is a punchdown tool used?

Crimper

Network technicians are often tasked with creating cables. The job is much easier when technicians have the correct tools, such as wire crimpers.

True or false? A crimper is used to secure an RJ-45 connector onto a twisted-pair cable.

Answer: *True*. Crimpers are used to secure connectors onto cables. The wires are placed into the connector in the proper location, and the crimper squeezes the connector onto the cable.

There are many specific types of crimpers, including those used to crimp RJ-45 cables onto twisted-pair cables. Other crimpers are available for other types of cables, and some can crimp multiple types of connectors. For example, crimpers are available to secure RJ-11 connectors to phone cables and to secure RJ-45 connectors onto network cables.

EXAM TIP **Crimpers are used to secure connectors onto cables, such as securing RJ-45 connectors to twisted-pair cables. In addition to knowing what a crimper is used for, you should also be able to identify a crimper in a group of different tools.**

MORE INFO **If you aren't familiar with the different hardware tools, check out *http://www.bing.com/images*. Enter search words, such as *crimper*. You can use the same technique to see pictures of any of the tools mentioned in this objective. Chapters 18 and 24 of the CompTIA A+ Training Kit (Exam 220-801 and Exam 220-802), ISBN-10: 0735662681, cover these tools in much more depth.**

Multimeter

Multimeters include two probes and are used to measure voltage, amperage, and resistance. These are commonly used to measure voltages from power supplies but have a different use with networks.

True or false? Multimeters are commonly used to measure amperage going through network cables.

Answer: *False*. Multimeters are rarely used to measure amperage (or current) through network cables.

Most multimeters include a continuity checker that can be used to verify that a cable doesn't have any breaks. This setting measures when a cable has zero resistance or is continuous from end to end. When you select the continuity check

function and touch both probes together, the multimeter beeps, indicating that there is a continuous connection. Similarly, when you touch both ends of a cable with each of the probes, it beeps if the cable is good. If you don't hear a beep, you know the cable has a break.

EXAM TIP **Multimeters may be used to measure voltage, amperage, and resistance. A continuity check function measures near-zero resistance and can be used to verify that a cable doesn't have a break.**

Toner probe

A toner probe includes two components. One component creates a tone, and the second component has a speaker to hear the tone.

True or false? A toner probe is used to verify that a NIC is operational.

Answer: *False.* A toner probe is used to trace network cables between two different locations.

For example, if you have 50 cables going from an office to a wiring closet, you sometimes need to identify both ends of the same cable. You can connect the component that creates the tone to one end of the wire in the office. Next, you go to the wiring closet and begin touching the speaker probe to different wires. When you hear the tone, you have found the wire.

EXAM TIP **Toner probes are used to trace cables between rooms in a building. One part of the toner probe creates a tone that is placed onto a wire. The other part has a speaker to play the tone when touched to the other end of the wire.**

Cable tester

Cable testers are used to verify that a cable is wired correctly and is operational. Many include LED displays to show exactly how the cable is wired. If the cable is wired incorrectly, the cable tester shows specifically which pins have the wrong wires.

True or false? A cable tester is used to trace cables going between two floors of a building.

Answer: *False.* The cable tester is used to test the operation of a cable but doesn't include the capabilities of a toner probe to trace cables.

Cable testers are often used with twisted-pair cables. They have RJ-45 ports where you connect the cable. The cable tester first verifies the wiring and then verifies that the cable meets operational characteristics. For example, a cable tester can verify that a CAT 6 cable can transmit data at a rate of 10 Gbps using a frequency of 250 MHz.

EXAM TIP **Cable testers are used to test the wiring and operational characteristics of a cable.**

Loopback plug

A loopback plug is a simple plug that loops transmit signals back into the receive signals. A simple loopback plug is an RJ-45 plug with send pins connected to the transmit pins.

True or false? A loopback plug is used to test the characteristics of a cable.

Answer: *False.* A loopback plug is used to check a NIC. Cable testers are used to check characteristics of a cable.

EXAM TIP **Loopback plugs are commonly used to check NICs. You can plug the loopback plug into the NIC and verify that signals can be sent and received with the plug.**

Punchdown tool

A punchdown tool is used to attach twisted-pair cables to wall jacks or punchdown blocks in wiring closets. The tool has a spring that punches down on a wire when pressed. The technician places the wire in the correct location on the wall jack or punchdown block and presses down with the punchdown tool. When the spring releases, it pushes the wire into the connector.

True or false? You must remove the jacket covering before securing a wire with a punchdown tool.

Answer: *False.* The jacket covering and insulation of a wire is removed when the punchdown tool forces the wire into place.

There are normally several individual segments between a computer in an office and a switch in a wiring closet, as follows:

- One cable runs from the computer to the wall jack. It has RJ-45 connectors on each end, and a crimper is used to secure the RJ-45 connectors onto the cable.
- Another cable runs between the wall jack and the wiring closet. This cable runs through walls, ceilings, and/or plenum spaces. It is connected to the wall jack on one end and to the back of a punchdown block on the other end. The punchdown tool secures the wire to the wall jack and the punchdown block.
- The last segment is a short patch cable that runs from the front of the punchdown block to a port on a hub or a switch. The devices are mounted in a bay close to each other. RJ-45 connectors are attached both ends of the patch cable with a crimper.

EXAM TIP **Punchdown tools are used to speed the process of connecting twisted-pair cables to wall jacks and punchdown blocks.**

Can you answer these questions?

You can find the answers to these questions at the end of this chapter.

1. What type of tool is used to connect RJ-45 connectors to twisted-pair cable?
2. What type of tool is used to trace wires between two rooms?
3. What computer component is a loopback plug commonly used to test?

Answers

This section contains the answers to the "Can you answer these questions?" sections in this chapter.

Objective 2.1: Identify types of network cables and connectors

1. Fiber cable uses LC, ST, and SC connectors.
2. RJ-11 connectors are used for phone lines, and RJ-45 connectors are used for networks. Both connectors use twisted-pair cable.
3. F-type screw-on connectors are used with coaxial cable.

Objective 2.2: Categorize characteristics of connectors and cabling

1. Fiber supports the longest cables without a repeater. SMF cable supports longer cable runs than MMF cable.
2. CAT 6 cable supports data transmissions up to 10 Gbps.
3. RG-6 cable supports both analog and digital transmissions.

Objective 2.3: Explain properties and characteristics of TCP/IP

1. The IP address 192.168.15.7 is a Class C address. The first number in the IP address 192.168.15.7 is 192, and addresses with the first number between 192 and 223 are Class C addresses.
2. The IP address FC00::42A:0:0:7F5 is an IPv6 address with leading zeros omitted and using zero compression.
3. Addresses starting with 169.254 are APIPA addresses, and they are assigned to DHCP clients when a DHCP server has not answered with an available IP address.
4. DNS provides a mapping for user friendly names (host names) to IP addresses. Clients send the name (such as bing.com) to the DNS server, and the DNS server responds with the IP address.
5. DHCP provides IP addresses and other TCP/IP configuration information to DHCP clients.

Objective 2.4: Explain common TCP and UDP ports, protocols, and their purpose

1. Email uses ports 25 (SMTP), 110 (POP3), and 143 (IMAP).
2. SFTP is encrypted with SSH, and it is used to transfer large encrypted files.
3. TCP uses a three-way handshake to establish a connection and provides guaranteed delivery.

Objective 2.5: Compare and contrast wireless networking standards and encryption types

1. Both 802.11a and 802.11n use the 5-GHz frequency range.
2. 802.11n can transmit up to 150 Mbps, 300 Mbps, or 600 Mbps at a time by using multiple antennas. In comparison, 802.11g has a maximum of 54 Mbps.
3. WEP has been broken and should not be used.

Objective 2.6: Install, configure, and deploy a SOHO wireless/wired router using appropriate settings

1. You use MAC addresses with MAC address filtering to block network access to specific computers.
2. Channels 1 and 11 are good alternative channels if channel 6 has excessive interference from other wireless networks.
3. Internet-facing servers (including gaming servers) should be placed in a DMZ to provide an extra layer of protection.

Objective 2.7: Compare and contrast Internet connection types and features

1. Fiber and cable broadband connections provide the highest speeds when compared with other wired connections.
2. Dial-up, DSL, and ISDN connections use phone lines.
3. Cellular Internet connections are appropriate for people who frequently travel.
4. Mobile hotspots (also called MiFi) connections are mobile and can be used to provide Internet access for multiple users.

Objective 2.8: Identify various types of networks

1. A network centered on an individual is a PAN.
2. A WAN connects two or more networks located in separate geographical locations.
3. A mesh topology provides the most redundancy.

Objective 2.9: Compare and contrast network devices and their functions and features

1. Switches provide performance improvements because each device connected to the switch uses a separate segment, resulting in less traffic for each segment. Also, switches provide some security because traffic is not sent to all devices connected to the switch.
2. Routers used to connect to the Internet commonly include NAT to translate public and private IP addresses. In many cases, the router also includes firewall capabilities.
3. Modems are used for dial-up Internet connections.
4. Firewalls block all traffic unless an exception or rule is created to allow the traffic.

Objective 2.10: Given a scenario, use appropriate networking tools

1. Crimpers are used to connect RJ-45 connectors to twisted-pair cable.
2. A toner probe is an effective tool used to trace cables.
3. Loopback plugs are commonly used to test NICs.

CHAPTER 4

Printers

The Printers domain covers approximately 11 percent of the A+ 220-801 exam. A PC technician will be expected to perform regular maintenance on printers and needs to be aware of common printers used in different organizations and how to install and maintain them. The corporate world uses laser printers extensively, so it's extremely important for PC technicians to have an in-depth understanding of laser printers. Because of this, you can expect the exam to have more questions related to laser printers than other types. However, the objectives also mention inkjet, thermal, and impact printers, so you'll need to understand the differences between these printers.

This chapter covers the following objectives:

- Objective 4.1: Explain the differences between the various printer types and summarize the associated imaging process
- Objective 4.2: Given a scenario, install, and configure printers
- Objective 4.3: Given a scenario, perform printer maintenance

Objective 4.1: Explain the differences between the various printer types and summarize the associated imaging process

For this objective, you need to understand each of the four basic printer types (laser, inkjet, thermal, and impact) and their differences. Laser printers have the most complex imaging process, but if you understand this process, you'll be better prepared to troubleshoot common laser printer problems. Inkjet printers are used within homes and small offices and provide superb printouts. They are often used in place of laser printers by home users and some small businesses. Thermal printers and impact printers are less common than laser printers and inkjet printers, but they do have specific abilities that make them useful in certain situations.

Exam need to know...

- Laser
  For example What is the purpose of a fuser assembly? What occurs during the cleaning process?

- Inkjet
  For example: When should an inkjet printer be calibrated? What is needed to print two-sided copies with an inkjet printer?
- Thermal
  For example: Where are thermal printers used? What are the components in a thermal printer?
- Impact
  For example: What is the primary usage of impact printers? How is carbon paper used with an impact printer?

Laser

Laser printers provide high-quality output at a relatively low cost per printed page. They are commonly used in corporate environments, and their reasonable cost makes them economical for many small businesses too.

True or false? Laser printers can print two-sided output as long as they have a transfer belt.

Answer: *False.* A duplexing assembly (not a transfer belt) is required to print two-sided output on a laser printer. Many inkjet printers also use duplexing assemblies to print two-sided paper.

A transfer belt is used on some high-end color laser printers. Colors are applied to the transfer belt and then to the paper. This step is repeated for different colors.

> ***EXAM TIP*** **Duplexing assemblies are needed for two-sided printing. They are typically mounted on the back of a laser or inkjet paper. After one side is printed, the paper is routed to the duplexing assembly, which turns the paper over and reroutes it through the printer a second time. Without a duplexing assembly, dual-sided printing must be done manually.**

True or false? The primary purpose of the fuser assembly is to melt toner onto a piece of paper.

Answer: *True.* The fuser assembly generates heat, which melts the plastic particles in the toner and fuses them onto the paper.

Other components of a laser printer include the following:

- A raster image processor (RIP) accepts data to be printed and converts it to a raster image. The raster image is a group of dots organized as characters, words, and graphic images.
- An imaging drum is a round rotating cylinder covered with a photosensitive surface. Images are written onto the drum by shining a focused light from the laser onto the drum. Laser printers have a drum.
- A primary charge roller (or in some cases a corona wire) applies between -500 and -1,000 VDC to the imaging drum. This charge neutralizes the photosensitive surface of the drum and prepares it to receive an image.

- A highly focused laser shines light onto the imaging drum through one or more mirrors. The laser writes the raster image created by the RIP onto the drum by removing the negative charge wherever the light from the laser hits it.
- The toner is charged with a high negative charge and applied to the drum. Because of the electrical charge, the toner is only attracted to the drum where the laser wrote the image.
- Pickup rollers applied to the top of the paper are used to pick up paper from the paper tray and begin feeding it through the printer.
- Separator pads spin in the opposite direction from under the paper and push extra paper back. These pads help prevent more than one piece of paper from being sent through the printer at a time.
- The transfer roller charges the paper with a high voltage. As the drum turns and the paper is moved through the printer, the charged paper attracts the toner away from the drum. The result is that the toner is transferred from the drum onto the paper.
- A static eliminator or electrostatic discharger removes the charge from the paper as it passes the drum. This helps prevent the paper from sticking to the drum.
- A fuser assembly melts the toner onto the paper with a combination of friction and heat.
- An erase lamp shines light onto the drum to neutralize the voltage on the entire drum. This removes the previous image from the drum.
- Similar to a windshield wiper, a scraper removes residual or excess toner from the drum.

EXAM TIP **When preparing for the CompTIA A+ 220-801 exam, ensure that you know what the common components are within a laser printer and their purposes. For example, you should know that the fuser assembly melts the toner onto the page, so if the toner smudges or wipes off the printed page, it's because of a faulty fuser assembly.**

MORE INFO **Laser printers are the primary printers used in many businesses, and the A+ exams focus heavily on it over the other printers. Ensure that you can identify all of its components and understand the laser printing process. For additional information, Chapter 7 of the CompTIA A+ Training Kit (Exam 220-801 and Exam 220-802), ISBN-10: 0735662681, provides more detailed information about printers. In addition to explaining the components, it covers many of the basics of printing including terminology, paper types, and many common tools. It also includes pictures of different printer components.**

True or false? The order of the imaging process in a laser printer is processing, charging, exposing, developing, transferring, and fusing.

Answer: *True*. This is the proper order of the laser printer imaging process.

Figure 4-1 shows the seven steps of the laser imaging process. Each of the steps occurs as the imaging drum turns.

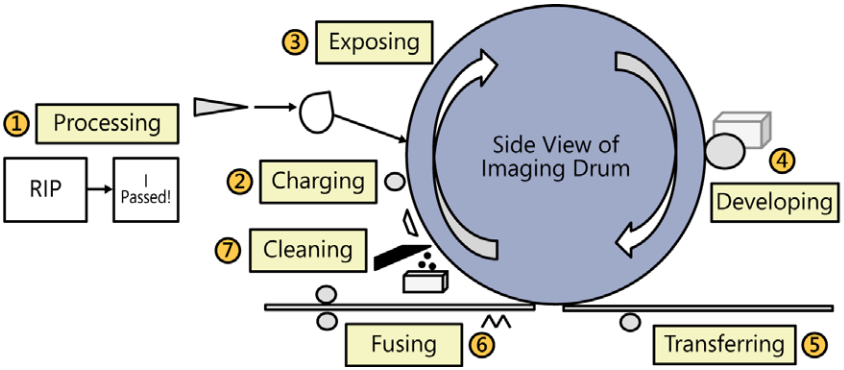


FIGURE 4-1 Laser imaging process.

NOTE **You might see documentation that indicates that cleaning occurs first, and other documentation that indicates it occurs last. As long as remnants of the last job are cleaned at the end of a print job, the drum doesn't need to be cleaned again, so it could be argued that this happens last. However, cleaning the drum first ensures that it's ready to accept a new image. Regardless, CompTIA lists all the other processes in the correct order and lists cleaning as the last step in the imaging process. Some people might like to debate it, but when taking the exam, remember that CompTIA lists cleaning last.**

The first two steps in the laser imaging process are processing and charging, which consist of the following operations:

- **Processing** The image is converted to a raster image by the RIP and stored in the printer's memory.
- **Charging** The imaging drum is charged with a high negative voltage (between -500 and -1,000 VDC) with a primary charge roller. In older laser printers, a corona wire applied the high negative voltage instead of a primary charge roller.

Figure 4-2 shows these two stages.

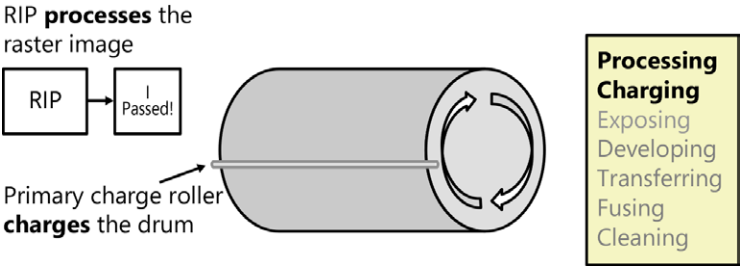


FIGURE 4-2 Processing and charging stage in the laser imaging process.

True or false? The laser writes the image onto the imaging drum during the developing stage.

Answer: *False.* The image is written onto the drum during the exposing stage, not the developing stage.

The next two steps in the laser imaging process are exposing and developing, consisting of the following operations:

- **Exposing** During this stage, the laser writes the raster image onto the drum as shown in Figure 4-3.
- **Developing** The toner is applied to the drum during the developing stage, as shown in Figure 4-4.

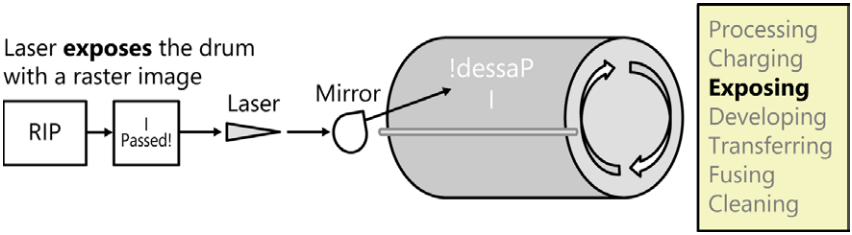


FIGURE 4-3 The exposing stage in the laser imaging process.

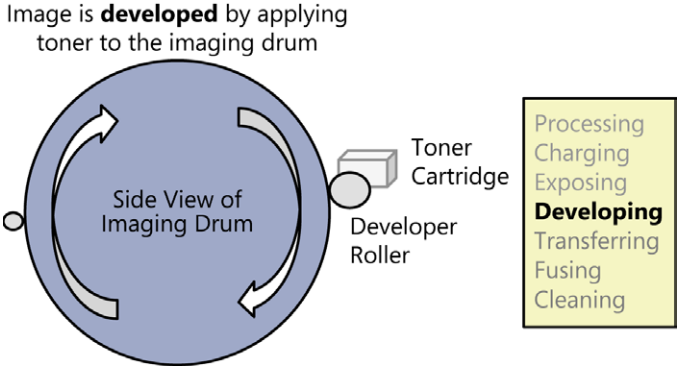


FIGURE 4-4 The exposing stage in the laser imaging process.

True or false? The toner is applied to the paper in the transferring stage of the laser imaging process.

Answer: *True.* During the transferring stage, toner is transferred from the imaging drum to the paper.

After the toner is transferred to the paper, it is melted onto the paper during the fusing stage. During the transferring stage, pickup rollers and separator pads pick up a single sheet of paper and start moving it through the printer. A transfer roller (or a transfer corona) applies a charge to the paper as it passes. The charged paper attracts the toner and the toner is transferred from the imaging drum to the paper.

At this point, the only thing holding the toner in place on the page is electrostatic charge. As the paper passes the drum, an electrostatic discharger removes the charge from the paper to prevent it from sticking to the drum, as shown in Figure 4-5. At this point, only gravity and friction hold the toner in place on the page.

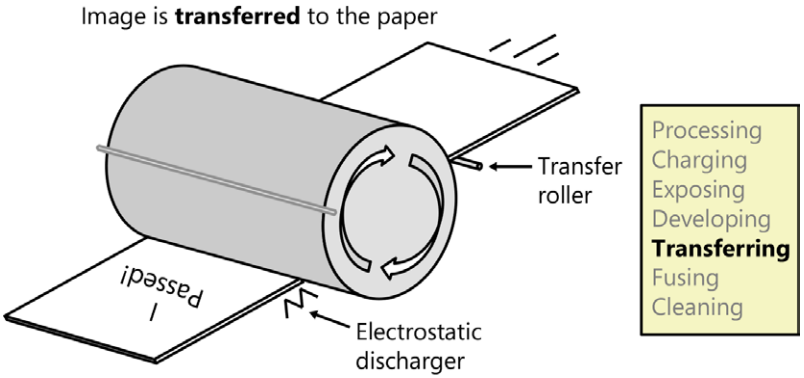


FIGURE 4-5 The transferring stage in the laser imaging process.

True or false? If toner falls off the printed pages, the most likely cause is a faulty fuser assembly.

Answer: *True*. The fuser assembly melts the toner, so if the toner is not sticking to the paper, the most likely cause is a faulty fuser assembly.

Figure 4-6 shows the fusing stage of the laser imaging process. The fusing assembly provides both friction and heat to the paper as it passes through, melting the toner onto the paper.

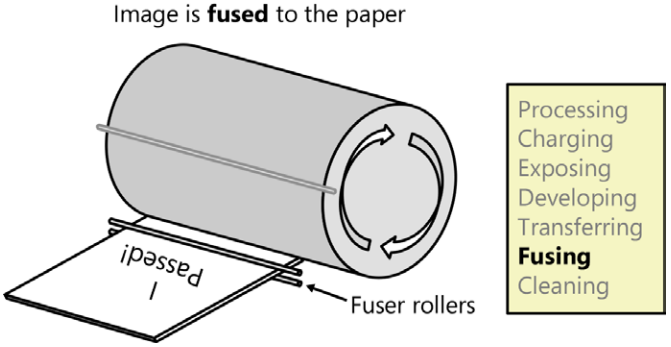


FIGURE 4-6 The fusing stage in the laser imaging process.

EXAM TIP **The fuser assembly gets as hot as 356 degrees Fahrenheit (180 degrees centigrade), which presents two concerns. First, if you open a laser printer, be careful when working around the fuser assembly because it can cause serious burns. Second, the fuser will melt regular transparency paper if a user tries to print on it. This can actually ruin the laser printer. Special transparency is available that will not melt and can be used with laser printers.**

True or false? If print jobs show a ghost image of a previous printed page, the erase lamp or scraper might be the problem.

Answer: *True*. The erase lamp and scraper work together to remove remnants of the previous print job during the cleaning phase of the imaging process.

Figure 4-7 shows the cleaning process. A plastic or hard rubber scraper removes excess or residual toner. If the toner is not being removed, the scraper might need to be replaced. The lamp shines over the entire photosensitive surface of the drum, exposing it all and neutralizing the electrical charge. In contrast, the laser has a focused beam to expose only parts of the drum.

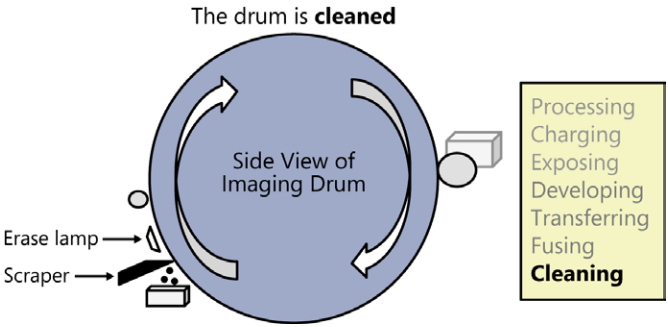


FIGURE 4-7 The cleaning stage in the laser imaging process.

EXAM TIP **When preparing for the 220-801 exam, ensure that you know the seven stages of the laser imaging process, including their proper order. Understanding these stages will also help you when you take the 220-802 exam, when you are faced with printer troubleshooting questions.**

MORE INFO **Lexmark has posted a video on how laser printers work that you can access here: *http://www.youtube.com/watch?v=PHxXmjxcAIo*.**

Inkjet

Inkjet printers are popular with home users and small businesses. They provide excellent quality printouts and are relatively inexpensive to purchase. The biggest drawback is that the cost of the ink is exceptionally high, resulting in a high cost per printed page.

True or false? Inkjets use small pins to hammer the ink onto the page.

Answer: *False*. Impact printers (not inkjet printers) use small pins to hammer ink onto a page from a ribbon.

Inkjet printers have one or more print heads that move from side to side on a carriage and belt assembly. In some printers, each ink cartridge includes a disposable print head. In other printers, the ink is separate and is fed to a fixed print head when needed. Disposable print heads will last as long as the ink but aren't built to last for a long time. In contrast, fixed print heads are meant to last much longer.

Paper is fed though an inkjet printer with a roller and feeder assembly similar to how paper is fed through a laser printer. A pickup roller works with one or more separator pads to ensure that only one piece of paper is picked up at a time. Many inkjet printers include a duplexing assembly used to print on both sides. When used, the rollers feed the paper through the printer to print on one side. The paper is then routed to the duplexing assembly where it is turned over and then rerouted through the printer to print on the back.

Inkjet printers use one of the following two methods to print:

- **Thermal printing** This is also known as bubble jet printing. Small heaters within the print head heat the ink, creating small ink bubbles. These bubbles are then ejected onto the paper.
- **Piezoelectric printing** In this method, a crystal oscillator vibrates, causing the ink to break up into small droplets. These small droplets are given an electrical charge as they leave the print head, causing them to either stick to the paper or fall off. Ink that falls off is recaptured.

EXAM TIP **In thermal inkjet (or bubble jet) printing, only the ink that is needed is sent through the print head. In piezoelectric printing, a steady stream of ink is sent through the print head, and unused ink is recaptured to be used again. Because of this, thermal inkjet printers are more prone to clogging up if they aren't used very often.**

MORE INFO **Jeff Tyson wrote an informative article, entitled "How Inkjet Printers work," available at *http://computer.howstuffworks.com/inkjet-printer3.htm*. Page 3 of the article compares heat and vibration methods.**

True or false? Printouts with colors that aren't aligned on an inkjet printer indicate that the printer should be calibrated.

Answer: *True*. Inkjet printers commonly have calibration programs that can be used to align the print heads when colors are misaligned. A calibration program performs electronic adjustments to improve the print quality.

Inkjet printers include one or more test pages that you can print to check the quality of the printouts. These usually include specific patterns, with notes on what to do if the printout isn't perfect.

EXAM TIP **Calibrate an inkjet printer if the printout is degraded or not clear. Calibration often resolves many issues, but if it doesn't, the next step is to clean the print head(s). Many inkjet printers have separate print heads for different colors, and if the printer is not printing a specific color, clean that print head. This is normally done with a utility program provided by the printer manufacturer.**

Thermal

Thermal printers are frequently used to create receipts at point of sale (POS) locations. After the sale is completed, the printer creates the receipt.

True or false? The print head in a thermal printer includes a heating element used to heat the paper.

Answer: *True*. Thermal printers use a special type of paper that responds to heat. The print head heats the paper to create the printout.

The paper on thermal printers is typically wound around a spindle. The spindle is attached to a sprocket type of feed assembly, and as the printer prints, the sprocket turns, feeding the paper through the printer.

NOTE **Thermal printers and are not the same as thermal inkjet printers. Thermal inkjet printers heat the ink before it is sent to the paper, while thermal printers heat only specially treated paper.**

EXAM TIP **Thermal printers are primarily used at point of sale locations to create receipts. This includes at gasoline pumps that provide receipts, grocery stores, or anywhere else where a receipt can be printed. They generally don't require much maintenance, and the paper can be replaced by a non-technical user.**

Impact

Impact printers include pins within the print head. These pins strike an ink ribbon, and the ink ribbon leaves a dot on the paper.

True or false? Impact printers are also known as dot matrix printers.

Answer: *True*. Impact printers use pins to print dots within a matrix, and by printing different dots, they can print characters and images.

Figure 4-8 shows how a 9-pin print head can be used to print the capital *B* by printing specific dots in a dot matrix. Near letter-quality impact printers have print heads with 24 or 48 pins. The extra pins fill in the holes between the dots, providing a higher-quality printout.

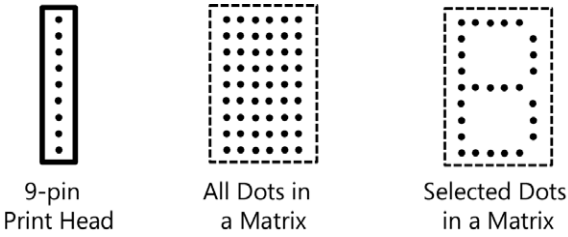


FIGURE 4-8 A dot matrix from an impact printer.

True or false? Businesses that need multiple copies of printouts commonly use impact printers.

Answer: *True*. Impact printers are ideal for printing multipart forms using carbon or carbonless paper to create multiple copies at a time.

Many businesses use multipart forms that have carbon paper between each copy. When the print head strikes the top paper, the force is felt through each page and presses the carbon paper onto the other copies.

> ***EXAM TIP*** **Impact printers were the primary type of printers used for a long time. However, at this time, their use is limited. The most common usage is within businesses that require multipart forms separated with carbon paper. Only impact printers will print multipart forms with carbon paper. Some businesses have switched over to laser printers and just print multiple copies individually, but impact printers are still being used in some businesses.**

True or false? It's common to use a tractor feed mechanism to feed paper through an impact printer.

Answer: *True*. Impact printers often use continuous feed paper with holes along the sides. The tractor feed mechanism has sprockets that fit into these holes to pull the paper through.

Impact paper used in impact printers can be continuous feed paper or individual sheets. When continuous feed paper is used, the paper is fed through the printer with the tractor feed mechanism. Single sheets of impact paper are fed through with friction from the platen, similar to how paper was fed through old typewriters. For best print quality, continuous feed paper and a tractor feed mechanism are used to ensure the paper is fed through at a consistent rate. Continuous feed paper is available with carbon paper to print multipart forms, or multiple copies at the same time.

Can you answer these questions?

You can find the answers to these questions at the end of this chapter.

1. What voltages are inside a laser printer that aren't in other printers?
2. Name two safety concerns related to laser printers.
3. What are two common types of inkjet printing?

4. Where are thermal printers used?
5. What can be easily printed by impact printers but not by laser printers?

Objective 4.2: Given a scenario, install, and configure printers

A common task with printers is to install and configure them. This objective expects you to know common methods used to connect printers to a computer or a network. Additionally, you should understand how printers are shared across a network and how to connect to a shared printer.

Exam need to know...

- Use appropriate printer drivers for a given operating system
  For example: When should you install a printer driver? What steps are required to install a USB printer?
- Print device sharing
  For example: What wired methods are used for printer connections? What wireless methods are supported for printer connections?
- Printer sharing
  For example: What comes after the "\\" in a Universal Naming Convention (UNC) name? What comes after the "\" in a UNC name?

Use appropriate printer drivers for a given operating system

All hardware devices require specific drivers so that the operating system can communicate with them. A software driver is one or more files that give the operating system the details it needs to send and receive information to and from the device.

True or false? When installing a USB printer, you should always install the print driver after inserting the USB cable.

Answer: *False.* When installing any device, you should follow the directions provided by the manufacturer, and manufacturers often indicate that the print driver should be installed before inserting the cable.

As a general guideline, it's usually best to install the provided driver before installing a device. Manufacturers include the drivers on a CD with directions for how to install the drivers and in what order.

When the device is installed, the operating system uses plug and play technology to automatically install the driver it identifies as the best choice. In many cases, this works fine even if the driver wasn't installed first. However, in some cases, the device won't work correctly or won't support all the features. It requires additional troubleshooting steps to uninstall the device, install the recommended drivers, and then reinstall the device.

EXAM TIP **When installing a USB printer in a PC that is running Windows, install appropriate drivers first if recommended to do so by the manufacturer. When this is done, you can simply plug the printer into the USB port, and Windows will manage the remaining steps.**

True or false? You should install 64-bit print drivers on an x86-based system.

Answer: *False*. You should install 32-bit print drivers on x86-based systems and 64-bit drivers on x64 based systems.

Print drivers are specific to the operating system, such as Windows XP or Windows 7. Additionally, different print drivers are used for 32-bit and 64-bit Windows versions.

MORE INFO **The following link includes two short videos on how you can check for a new print driver in Windows 7 or manually install a print driver: *http://windows.microsoft.com/en-us/windows7/Find-and-install-printer-drivers*.**

Print device sharing

It's common to share a printer among several users. There are multiple ways this can be done, depending on how the printer is connected.

True or false? A single printer with an Ethernet connection can be shared in a wired network.

Answer: *True*. If the printer has an Ethernet connection, it can be added to the network, and all users within the network can use it.

It's also possible to share a printer that is connected directly to a computer. For example, a printer connected to a computer with a USB or parallel connection can be shared on that computer, and other users in the network can print to it.

EXAM TIP **A network printer using an Ethernet or wireless connection should be assigned a static Internet Protocol (IP) address, either manually or by reserving a specific IP address for it via Dynamic Host Configuration Protocol (DHCP). If not, it might receive a different IP address after it is turned off and back on, such as after a power failure. When it receives a different IP address, users might no longer be able to print to it until their systems are reconfigured with its new IP address or until the printer is reconfigured with its original IP address.**

True or false? A printer can be connected directly to a computer by using a USB port as long as the printer has a USB connection.

Answer: *True*. USB connections are very common with printers.

The printer typically has a USB Type B port, and a USB cable goes from the printer to a common USB Type A port on a computer. Methods used to connect a printer directly to a computer include the following:

- **USB** This is the most common direct connection method used with printers today.
- **Parallel** This is an older method used before USB became popular. The cable connects to a DB-25 connection on the computer and to a Centronics or other type of parallel connection on the printer. Parallel ports are designated as LPT1 through LPT4.
- **Serial** A serial cable connects from the printer to a DB-9 or DB-25 connection on the computer. This is not common at all for current printers. Serial ports are designated as COM1 through COM4.

EXAM TIP **Printers can be connected directly to a computer by using USB, parallel, or serial connections. USB connections are the most popular and the easiest to install. On Windows 7, you can often just plug in the printer and it will be available. Serial and parallel printers require additional steps to install.**

True or false? Wireless printers can be shared by multiple computers within a wireless network.

Answer: *True*. Wireless printers are becoming very popular and most often use one of the 802.11x protocols (802.11a, 802.11b, 802.11g, or 802.11n).

A wireless printer connects to a wireless network just like any other wireless device. When connected, it is available to all other users on the network.

EXAM TIP **Wireless printers are configured to connect to a wireless access point (WAP) or wireless router. You need to have the service set identifier (SSID) and password or passphrase used by the wireless network. Also, the printer should be assigned a specific IP address, just as a wired network printer should use a specific IP address.**

MORE INFO **Chapter 2 "Networking" of this book covers all of the 802.11x protocols in the context of Objective 2.5. This includes the speeds, distances, and frequencies used by these protocols, and the encryption types used to secure wireless networks. Chapter 2 also covers other networking topics, such as how IP addresses are assigned. By default, a network printer will typically be configured to receive an IP address using DHCP. However, it's recommended to statically assign an IP address to the printer or to configure DHCP to always assign the same IP address to the printer based on the printer's media access control (MAC) address.**

True or false? Printers using infrared have a shorter wireless range than printers using 802.11g.

Answer: *True*. Infrared wireless ranges are very short, with a maximum distance of 5 meters (about 16 feet). Wireless printers using 802.11g have a range of about 38 meters (about 125 feet).

Some wireless printers can use Bluetooth or infrared technologies in the following scenarios:

- **Bluetooth** Printers that support Bluetooth connections typically use Class 2 Bluetooth, allowing the printer to be as far as 10 meters (33 feet) away.

- **Infrared (IR)** If the printer has a clear line of sight from the computer, an IR connection can be used. This is the same type of IR used in TV remote controls. The drawback is that the connection is lost if the line of sight is broken. That is, if anything is placed between the computer and the printer, the printer will no longer print.

Printer sharing

After connecting a printer to a computer, it's possible to share it with other network users. A computer sharing a printer is referred to as a print server, although it could be running Windows XP, Windows 7, or some other desktop operating system. That is, a print server isn't necessarily running a server operating system.

Sharing a printer is similar in concept to sharing a folder on a computer. After a folder is shared, users with permissions can access the folder. Similarly, after sharing a printer, users with permissions can print to the printer.

True or false? Network printers are accessible by using a Universal Naming Convention (UNC) path similar to \\ShareName\ServerName.

Answer: *False*. Network printers are accessible by using a UNC path, but the UNC path has the format of \\ServerName\ShareName. The server name must be placed first in the UNC name, or the connection will fail.

For example, if you have a computer named Win7, sharing a printer named ClrLaser, other users can connect to it with the UNC path of \\Win7\ClrLaser. If users try to connect with \\ClrLaser\Win7, their systems will look for a computer named ClrLaser and the connections will fail.

> ***EXAM TIP*** **Printers can be connected directly to computers by using USB, parallel, or serial connections. When the printer is connected, it can be shared and other users can connect to it by using a UNC path name.**

True or false? Printers can be shared from Devices and Printers in Windows 7.

Answer: *True*. This is accessible from the Start menu, and the Printers And Faxes section includes all of the printers installed on the computer.

You can share a printer in Windows 7 with the following steps:

1. Right-click the printer icon in Devices And Printers, and select Printer Properties.
2. Click the Sharing tab.
3. Select the Share This Printer check box. Optionally, change the name of the shared printer in the Share Name text box.

By default, the Everyone group can print to a printer when it is shared. You can modify this by using the Security tab of the Printer Properties dialog box.

If you are unable to share a printer, verify that print sharing is enabled on the computer. On Windows 7–based systems, this is accessed on the Networking tab of the network interface card's properties page and is called File And Printer Sharing For Microsoft Networks.

NOTE **You can share a printer from Printers And Faxes in Windows XP. This is accessible from the Control Panel after changing the view to list the items individually. You can also find it in the Printers And Other Hardware category within the Control Panel.**

MORE INFO **The following video shows how to share a printer on Windows 7: *http://windows.microsoft.com/en-US/windows7/help/videos/sharing-a-printer*.**

True or false? You can add drivers for multiple operating systems when sharing a printer from a Windows-based system.

Answer: *True*. When sharing a printer, an Additional Drivers button is available on the Sharing tab. You can click this to add drivers for different operating systems.

When users connect to a shared printer by using the UNC path, the correct driver is automatically downloaded from the print server if it is available. If you need to update the driver, you need to update it only on the print server. The updated driver is automatically downloaded to clients the next time they connect.

True or false? Print jobs sent to a printer via a print server will not print if the print server loses network connectivity.

Answer: *True*. If the print server is not accessible on the network, users will not be able to send print jobs to it.

EXAM TIP **A print server is any computer used to share printers. If a shared printer is powered on but users cannot print to it, verify that the print server is powered on and has network connectivity. Print drivers for multiple operating systems can be added to the print server and will automatically be downloaded to clients when they connect.**

MORE INFO **The following two videos show how you can change printing options or change the default printer on Windows 7: *http://windows.microsoft.com/en-US/windows7/change-your-default-printer* and *http://windows.microsoft.com/en-US/windows7/help/videos/printing-options*.**

Can you answer these questions?

You can find the answers to these questions at the end of this chapter.

1. What is the most common method used to connect a printer directly to a computer?
2. What is a primary concern with networked printers to ensure that users can continue to access them even after the printer is turned off and back on?
3. What information do network users need for connecting to a shared network printer?

Objective 4.3: Given a scenario, perform printer maintenance

PC technicians are expected to perform basic maintenance on printers in the workplace. Laser printers require more maintenance than other printers, but they are also used more often. CompTIA doesn't include inkjet printers in this objective because there is very little maintenance required. You might need to replace inkjet cartridges, replace print heads, or run calibration programs on an inkjet printer, but those tasks are covered in Objective 4.1, "Explain the differences between the various printer types and summarize the associated imaging process."

Exam need to know...

- Laser
  For example: What determines when a maintenance kit should be applied to a laser printer? What is typically included in a laser printer maintenance kit?
- Thermal
  For example: How can the thermal head be cleaned? What should you use to clean a thermal printer?
- Impact
  For example: What are common maintenance tasks required with an impact printer? What can help prevent damage to the pins on a print head?

Laser

Many components within a laser printer will wear out and should be replaced periodically. Maintenance kits include key components that should be replaced and typically include the following items:

- Pickup rollers and separator pads
- Transfer rollers
- Fuser assemblies
- Toner

True or false? When a laser printer displays a message such as "Service Required," a maintenance kit should be applied to the printer.

Answer: *True*. "Service Required" or "Perform Printer Maintenance" are two common error messages indicating that a maintenance kit should be applied.

Laser printers often count how many pages have been printed and display maintenance messages when specific counts are reached. At other times, the laser printer might develop problems that can be resolved by applying a maintenance kit.

> ***EXAM TIP*** **Laser printers track the count of printed pages and notify users when printer maintenance is required. These error messages sometimes alarm users, but they are normal. The manual for the printer provides clear directions about what to do.**

True or false? If toner spills, it's best to vacuum it up with a regular vacuum cleaner.

Answer: *False.* If toner spills, it's best to consult the Material Safety Data Sheet (MSDS) to identify the best method of cleaning it. If a regular vacuum cleaner is used, the toner will pass through the vacuum cleaner and go back out into the air.

Vacuums with high-efficiency particulate arresting (HEPA) filters can be used to vacuum toner. The HEPA filter will capture the toner particles. If a vacuum cleaner with a HEPA filter isn't available, you can often clean the spill by dabbing with a paper or cloth towel soaked with cold water. Warm water or the heat of friction generated by scrubbing can melt the resin and can make the spilled toner more difficult, if not impossible, to remove.

EXAM TIP **Replacing toner in a laser printer is a task that many users can do themselves. The directions are generally clear and easy to follow. Some common problems that occur are that users don't shake the new toner cartridge prior to installing it or they forget to remove the cover before installing it. If the toner cartridge isn't shaken to redistribute the toner, it can all settle during shipping or storage to one end of the drum, and the other end might produce pale or blank output. When the toner cover is not removed, the printouts are blank.**

True or false? If two or more pieces of paper are regularly being pulled into the laser printer, replacing the separator roller will likely solve the problem.

Answer: *True.* The pickup and separator rollers work together to pick up a single piece of paper, and if the separator roller is worn, the printer will often pick up more than one sheet of paper. Replacing the roller solves the problem.

Using the wrong type of paper or damp paper can cause the same problem. When paper is stored or used in areas with high humidity, it can absorb the water and start jamming within the printer. The solution is to use the correct paper and/or store it in an area with an acceptable level of humidity.

EXAM TIP **Clean or replace pickup rollers and separator pads if a printer is picking up more than one sheet of paper from a tray and you've verified that the paper is not the problem.**

EXAM TIP **Color laser printers have calibration programs similar to inkjet calibration programs. If the printout isn't clear or the colors are misaligned, calibrate the printer by using the manufacturer-supplied calibration program, just as you would do for an inkjet printer.**

Thermal

Thermal printers don't require a lot of attention or maintenance, but they can still benefit from some basic care. One of the primary concerns is a buildup of paper dust within the printer, which should be periodically removed.

True or false? An electrostatic discharge (ESD)–safe vacuum cleaner should be used when cleaning a thermal printer.

Answer: *True*. An ESD-safe vacuum cleaner helps prevent ESD damage to the printer while it is being cleaned.

Paper used in thermal printers is typically on a single continuous roll with the last part of the roll marked with a different color on one side. When the user sees the printouts with the different color paper, they know the printer is almost out of paper. For most thermal printers, replacing this paper is as simple as replacing a roll of paper towels. You simply open the printer, remove the empty roll of paper, and install the new roll of paper.

When removing dust from the printer, the heating element on the print head should also be cleaned. The heating element on the print head can be cleaned with isopropyl alcohol and a lint-free cloth or cotton swab.

> ***EXAM TIP*** **If thermal printers are not periodically cleaned, the print dust within the printer can shorten the life of the thermal print head. Cleaning it consists of cleaning the heating element on the print head and removing the print dust.**

Impact

Impact printers have a lot of activity as paper is pulled through the printer and the print head pins hammer onto the ink ribbon to the paper. Because of this, it's highly recommended to regularly clean these with an ESD-safe vacuum to remove the paper dust. Alternatively, you can take the printer outside and use compressed air to blow the dust out.

True or false? The ink cartridge should be refilled when the printout on an impact printer is faded.

Answer: *False*. Impact printers use ink ribbons not ink cartridges. The ink ribbon should be replaced when the printout is faded.

It's sometimes possible to re-ink the ribbon to get more use out of it. However, this can be done only a limited number of times because, eventually, the repeated impacts to the print head will tear through the ribbon.

> ***EXAM TIP*** **The ink ribbon on an impact printer is held in place by two spindles. One spindle pulls the ribbon to it, and the other spindle releases the ribbon. When it gets to the end, the process is reversed so that the ribbon is pulled by the other spindle. This allows the ribbon to be continuously reused. However, if the printout is faded, the ribbon should be replaced.**

True or false? Paper jams in impact printers can be caused by tractor feed problems.

Answer: *True*. Impact printers commonly use continuous feed paper, and problems with the tractor feed mechanism are the most common source of paper jams.

True or false? Keeping an impact printer clean can help prevent problems with the print head.

Answer: *True*. Impact printers generate a lot of paper dust, and this can cause pins in the print head to jam.

A jammed pin might rip the paper if it's jammed in the out position. If it's jammed in the in or out position, it will impact the print quality.

In addition to keeping the inside of the printer clean, the platen should be periodically cleaned also. The platen is the round cylinder that turns with the paper. The print head pins hammer through the ribbon and paper onto the platen. Over time, the platen can have multiple indentations, but you can renew the platen by rubbing it with isopropyl alcohol.

EXAM TIP **Keeping an impact printer clean is the primary maintenance required, besides replacing the paper and replacing the ink ribbon. The print heads are durable and normally last a long time if the printer is kept clean. If a pin jams, you'll need to replace the print head.**

Can you answer these questions?

You can find the answers to these questions at the end of this chapter.

1. What is included in a laser printer maintenance kit?
2. What is the primary maintenance required for a thermal printer?
3. When would a print head on an impact printer need to be replaced?

Answers

This section contains the answers to the "Can you answer these questions?" sections in this chapter.

Objective 4.1: Explain the differences between the various printer types and summarize the associated imaging process

1. A laser printer has a high-voltage power supply, providing between -500 and -1,000 VDC. This voltage is used by the primary charge roller (or in older laser printers, a corona wire) to charge the imaging drum.
2. The two primary safety concerns related to laser printers are the high-voltage power supplies and the high-temperature fuser assemblies. The high-voltage power supply can deliver lethal electric shocks, and the fuser assembly can cause burns.
3. The two types of inkjet printing are thermal (or bubble jet) printing and piezoelectric printing. Thermal inkjets heat the ink, creating small bubbles that are sent out the heads. Piezoelectric printing uses a crystal to create small droplets, and these droplets are charged so that they stick to the paper or drop off.

4. Thermal printers are commonly used at point of sale locations to create receipts.
5. Impact printers are used to print multipart forms that have carbon paper within them. The impact of the pins on the head prints on each form. In contrast, a laser printer cannot print multipart forms, but it can print multiple individual copies.

Objective 4.2: Given a scenario, install, and configure printers

1. USB connections are the most common method used to connect printers directly to a computer. They are also the easiest, especially on Windows 7. If the driver is installed, the printer is automatically added when the USB connection is plugged in.
2. A primary concern with networked printers is ensuring that they are assigned the same IP address each time they are turned off and back on. This can be done by manually assigning an IP address or by configuring DHCP to assign the same IP address to the printer based on the printer's MAC address.
3. Users need to know the UNC path to a shared printer in order to connect to it. This is in the format of \\ServerName\ShareName, where the server name is the name of the computer sharing the printer and the ShareName is the share name of the printer.

Objective 4.3: Given a scenario, perform printer maintenance

1. A laser printer maintenance kit typically includes one or more pickup rollers, a separator pad, a transfer roller, a fuser assembly, and toner. Toner can be replaced at other times.
2. The primary maintenance required for a thermal printer is to periodically clean out the paper dust and the print head. An ESD-safe vacuum cleaner can be used to remove the dust, and isopropyl alcohol with a lint-free cloth can be used to clean the print head.
3. An impact printer print head needs to be replaced if one or more of the pins jam.

Index

Symbols

$ (dollar sign) character, 235
4/8-pin connector, 45, 50
-4 switch, 201
6-pin alpha connector, 45
-6 switch, 201
7B stop error, 306
9-pin beta connector, 45
20-pin connector, 50
24-pin connector, 50
64-bit support, Windows 7, 186
802.11a/b/g/n networks, 94, 95
- (dash) character, 201
/ (forward slash) character, 201
/? switch, 201
µATX (micro-ATX), 12

A

AC (alternating current) power, 18, 126, 129
Accelerated Graphics Port (AGP), 14
accelerometers, 283
access denied error, 347
access points
    overview, 112–113
    placement of, 273–274
Account Lockout Duration setting, 206
Account Lockout Policy, 206
Account Lockout Threshold setting, 206
Additional Drivers button, Sharing tab, 153
Add/Remove Programs applet, 219
Admin$ folder, 235
administration tools
    Administrative Tools (Contol Panel), 187, 206–207
    command line tools, 214–215
    Disk Management tool, 210–212
    migrating data and settings, 213–214
    msconfig command, 208–209
    required knowledge, 205–206
    Task Manager tool, 209–210
administrative access via rootkit, 255
Administrator account, 234
ADSL (asymmetric DSL), 104
Advanced Encryption Standard (AES), 96, 271
Advanced Micro Devices (AMD), 8, 15, 40, 183
Advanced tab, System Properties applet, 217
Advanced Technology Extended (ATX), 12
Aero feature, 186, 188
AES (Advanced Encryption Standard), 96, 271
AGP (Accelerated Graphics Port), 14, 20
airborne particles, 167–168
air cans, 349
airplane mode, 285
/all switch, 98, 200
alternating current (AC) power, 18, 126, 129
alternative IP address, 228
AMD (Advanced Micro Devices), 8, 15, 40, 183
analog vs. digital display devices, 60–61
Android vs. iOS, 282–283
antiglare filters for displays, 61
antivirus software for mobile devices, 291
APIPA (Automatic Private IP Addressing), 85–86, 228
Application log, 327
Applications tab, Task Manager tool, 210
-a switch, 201
asymmetric DSL (ADSL), 104
ATX (Advanced Technology Extended), 12
audio editing workstation, configurations for, 53
Automatic Private IP Addressing (APIPA), 228
autorun feature, disabling, 264–265

B

backlight in laptop display, 130–131
Backup and Restore feature, Windows 7, 186
ball grid array (BGA), 15
Basic Input/Output System (BIOS). *See* BIOS (Basic Input/Output System)
BCD (boot configuration data), 324
BD (Blu-Ray disc), 34
Berg connector, 39, 50

BGA (ball grid array), 15
biometric authentication device, 249
BIOS (Basic Input/Output System)
  built-in diagnostics for, 9–10
  component information, 5–6
  configurations, 6–9
  installing firmware upgrades, 4
  monitoring, 10–11
  overview, 3–4
  in PXE systems, 192
  required knowledge, 4, 11
BitLocker Drive Encryption feature, 186, 188
blackouts, 166–167
Black TRS, 72
Blue Screen of Death (BSOD), 306
Bluetooth, 151, 286–287
Blu-Ray disc (BD), 34
BNC connectors, 63
bootcfg command, 324
boot configuration data (BCD), 324
Boot.ini file, 325
boot methods, 192
bootrec command, 204, 324, 325
Boot tab, msconfig tool, 209
bridges, 113
brightness of displays, 60
broadcast traffic, 110
brownouts, 166–167
Brown TRS, 72
BSOD (Blue Screen of Death), 306
bubble jet printing, 146
bus speeds for motherboards, 20
bus topology, 108

C

cable Internet, 102–103
cable lock for laptops, 135–136
cables
  coaxial, 79–80, 82
  device cable types, 67
  display cable types, 64–65
  fiber, 78, 80–81
  overview, 62, 80
  required knowledge, 62, 67–68, 78, 80
  twisted-pair, 78–79, 81–82
cable select (CS), 310
cable tester, 117
CAD/CAM design workstation, configurations for, 52–53
capacity of storage devices, 39–40
Caps Lock key, 133, 340
cathode ray tube (CRT), 58, 317
CCFL (cold cathode fluorescent lamp), 58, 129, 341
cd command, 203
CDFS (Compact Disc File System), 195
CD-ROM (compact disc read only memory), 34
cellular data network
  cards for, 32
  Internet connections via, 105
  overview, 285–286
central processing unit (CPU), 3, 15, 126, 304
CF (CompactFlash), 37
chain of custody, 177
Change permission, 236
channels (wireless), 98
charging stage, 142, 345
chassis ground, 161–162
Check Disk tool, 196, 232
chipsets for motherboards, 16–17
chkdsk command, 196, 202, 231, 232, 313
Class A/B/C/D fires, 163
cleaning stage, 145, 345
client-side DNS (Domain Name System), 87
clock multiplier (Clk Mult), 24
closed-ended questions, 300–301
cmd command, 214
/cmdcons switch, 204
CMOS (complementary metal oxide semiconductor) battery, 8, 307
CNR (Communications and Networking Riser), 14
coaxial cables, 65, 79–80, 82
cold cathode fluorescent lamp (CCFL), 58, 129, 341
combo drives, 34–35
command line tools
  file system, 202–204
  for networks, 200–202
  for OS administration, 214–215
  overview, 200
  recovery console, 204–205
  required knowledge, 200
Command Prompt tool, 214
communication
  avoiding distractions, 172
  being culturally sensitive, 172
  dealing appropriately with confidential materials, 174
  dealing with difficult customers or situations, 172–173

listening to customer, 171–172
maintaining positive attitude, 170–171
meeting expectations, 173–174
overview, 170
using proper language, 170–171
required knowledge, 170, 175
Communications and Networking Riser (CNR), 14
Compact Disc File System (CDFS), 195
compact disc read only memory (CD-ROM), 34
CompactFlash (CF), 37
compatibility
Compatibility Mode feature, 187
of RAM, 24–25
complementary metal oxide semiconductor (CMOS) battery, 8, 307
component cables, 64
composite cables, 64
Computer Management tool, 207
confidential materials, 174
connections
for mobile devices
Bluetooth, 286–287
cellular data network, 285–286
overview, 285
required knowledge, 285
interfaces
overview, 43
physical connections, 44–47
required knowledge, 44, 49
for storage devices, 35–36
wireless device connections, 48
connectors
display connector types, 62–63
hardware devices, 65–66
overview, 62
for power supply, 49–50
required knowledge, 62, 67–68
Control Panel utilities (Windows)
common utilities, 215–216
overview, 215
required knowledge, 215
unique to Windows 7, 220–221
unique to Windows Vista, 220–221
unique to Windows XP, 219
cookies, 257
copy command, 204
CPU (central processing unit), 3, 15, 126, 304
creased paper error, 346
crimper tool, 116
CRT (cathode ray tube), 58, 317
CS (cable select), 310
cultures, sensitivity to, 172
customers
dealing with difficult, 172–173
listening and not interrupting, 171–172
custom hardware configurations
audio/video editing workstation, 53
gaming PC, 54
graphic/CAD/CAM design workstation, 52–53
home server PC, 56
home theater PC, 55
overview, 52
required knowledge, 52, 57
standard thick client, 55
thin client, 56
virtualization workstation, 54

D

dash (-) character, 201
data destruction
hard drive sanitation methods, 267–268
low-level format vs. standard format, 266–267
overview, 265
physical destruction, 268
required knowledge, 265–266
data preservation, 176
date, setting, 197–198
DB-15 connectors, 63
DC (direct current) power, 18, 126, 129
DDR/2/3 (Double Data Rate/2/3) RAM, 14–15, 21–25
dead pixels, 316
default gateway, 89
defrag command, 231, 232, 330
degaussing, 268
del command, 204
deny all philosophy, 225
developing stage, 143, 345
Device Manager tool, 207
device preservation, 176
devices, network
access points, 112–113
bridges, 113
firewalls, 114
hubs, 110
Internet appliance, 115
modems, 113

NAS, 113–114
overview, 109
required knowledge, 109–110
routers, 111–112
switches, 110–111
VoIP phones, 114–115
DHCP (Dynamic Host Configuration Protocol), 87–88, 150, 200, 274, 319
diagnostics in BIOS, 9–10
differential backups, 231
Digital Linear Tapes (DLTs), 39
digital subscriber line (DSL), 31, 79, 103
digital versatile disc (DVD), 34
digital video recorder (DVR), 55, 79
Digital Visual Interface (DVI). *See* DVI (Digital Visual Interface)
digital vs. analog display devices, 60–61
DIMMS (dual in-line memory modules), 14
direct current (DC) power, 18, 126, 129
direct memory interface (DMI), 16
DirectX Diagnostic Tool, 214
disabling features
autorun, 264–265
Guest account, 263–264
ports, 277–278
SSID broadcast, 270–271
Disk Defragmenter tool, 231
Disk Management tool, 210–212
diskpart command, 203
Display applet, 217
display devices
analog vs. digital, 60–61
brightness/lumens, 60
cable types, 64–65
connector types, 62–63
laptop components
backlight, 130–131
inverter, 130
overview, 128
required knowledge, 128, 131
types of, 128–129
Wi-Fi antenna connector, 129–130
multiple displays, 61
overview, 57
privacy/antiglare filters, 61
refresh rates, 59
required knowledge, 57, 62
resolution, 59
resolution, native, 60
types of, 58
/displaydns switch, 200
DisplayPort connector, 63
distances for wireless connections, 48
distractions, avoiding, 172
DLLs (dynamic link libraries), 331
DLTs (Digital Linear Tapes), 39
DMI (direct memory interface), 16
DMZ (demilitarized zone), 101
DNS (Domain Name System), 87, 200
docking station vs. port replicator, 134–135
documenting troubleshooting results, 304
dollar sign ($) character, 235
Domain Name System (DNS), 87, 200
domain setup vs. workgroup setup, 197, 223
dotted decimal notation, 88
Double Data Rate/2/3 (DDR/2/3) RAM, 14–15, 21–25
DP (double pumping) of RAM, 25
drivers
installing, 198–199
installing third-party, 196
for printers, 150
DRVs (digital video recorders), 79
DSL (digital subscriber line), 31, 79, 103
dual in-line memory modules (DIMMs), 14
dumpster diving attacks, 268
duplexing assembly, 140
duplex mode, 229
dust buildup, 305
DVD (digital versatile disc), 34
DVI (Digital Visual Interface)
DVI-A (analog) connectors, 63
DVI-D (digital) connectors, 63
DVI-I (integrated) connectors, 63
overview, 47, 129, 315
DVR (digital video recorder), 55
dxdiag command, 214
Dynamic Host Configuration Protocol (DHCP), 86, 150, 200, 274, 319
dynamic link libraries (DLLs), 331
dynamic vs. static addresses, 87

E

Earth ground, 161–162
Ease of Access Center applet, 68
Easy Transfer feature, 188
ECC (error correction code), 22
EFS (Encrypting File System), 186
EIDE cables, 67
electromagnetic interference (EMI), 80, 274

electrostatic discharge (ESD)
causes for, 30, 31, 156
mats, 160–161
overview, 159
straps, 160
EMI (electromagnetic interference), 80, 274
emulators, 242
Encrypting File System (EFS), 186
encryption for wireless networks, 96, 271–272
Enforce Password History setting, 261
environmental controls
airborne particles, 167–168
blackouts, 166–167
brownouts, 166–167
complying with government regulations, 169
component handling and protection, 168–169
humidity, 166
MSDS documentation, 165–166
overview, 165
power surges, 166–167
required knowledge, 165, 169
temperature, 166
ventilation, 166
erase command, 204
error codes, 348
error correction code (ECC), 22
eSATA (external SATA), 30, 65, 67
ESD (electrostatic discharge)
causes for, 30, 31, 156
mats, 160–161
overview, 159
straps, 160
Ethernet
cables, 65, 67
connections, 150
Event Viewer feature, 187
EVGA (Extended VGA), 59
expansion cards
modem cards, 31
network cards, 29
options for laptops, 124–125
overview, 26
required knowledge, 26, 33
riser cards, 33
serial and parallel cards, 29
slots for motherboards, 13–14
sound cards, 27
storage cards, 30
TV tuner cards, 32
USB and FireWire cards, 30
video capture cards, 32–33
video cards, 27–28
wireless/cellular cards, 32
expectations, setting and meeting, 173–174
explorer command, 214
exposing stage, 143, 345
ExpressCard/34, 124
ExpressCard/54, 124
Express setting, Windows Update, 198
extended display option, 133
Extended GA (XGA), 59
Extended VGA (EVGA), 59
external enclosures, 313
external SATA (eSATA), 30

F

factory recovery partition, 199
faded print error, 346
Failed indicator, Disk Management tool, 212
failed login attempts restrictions, 290–291
fans, 19
FAST (File and Settings Transfer) wizard, 213
FAT (File Allocation Table), 194
fdisk command, 203, 314
fiber cables
Internet connections via, 102–103
overview, 78, 80–81
field serviceable parts, 292
File Allocation Table (FAT), 194
File and Settings Transfer (FAST) wizard, 213
file & printer sharing, 152, 222–223
file recovery software, 314
file system types, 195–196
File Transfer Protocol (FTP), 92
fingerprint readers, 249
fire tetrahedron, 163
firewalls
filters for, 100
overview, 114
settings for, 225
Firewire
cards, 30
connectors, 66
firmware upgrades, 4, 230
/fixboot switch, 204, 324, 325
/fixmbr switch, 204, 324, 325
flash drives, 37

floppy drives
cables for, 67
overview, 39
/flushdns switch, 200
Fn key, 132, 137, 339
Folder Options applet, 216
fonts folder, 238
Foreign indicator, Disk Management tool, 212
format command, 203, 313
formatting drives
overview, 195–196
standard vs. low-level format, 266–267
forwarding ports, 98–99
forward slash (/) character, 201
FQDN (fully qualified domain name), 87
frequencies for wireless connections, 48
front panel connectors, 19
FTP (File Transfer Protocol), 92
full backups, 231
Full Control permission, 235, 236
full image backups, 232
fully qualified domain name (FQDN), 87
function keys, 132–134
fuser assembly, 141, 144
fusing stage, 144, 345

G

Gadgets feature, 188
gaming PCs, 54
gateway, 89–90
General tab, msconfig tool, 209
global positioning system (GPS). *See* GPS (global positioning system)
government regulations, 164, 169
gpedit.msc command, 214
GPS (global positioning system)
on mobile devices, 284
overview, 281
GPU (graphics processing unit), 27, 42, 53, 317
graphical user interface (GUI), 203
graphic design workstation, configurations for, 52–53
graphics processing unit (GPU), 27, 42, 53, 317
grounding
equipment grounding, 161–162
self-grounding, 161
Group Policy Editor tool, 214
groups, security for, 233–234
Guest account, 234, 263–264
GUI (graphical user interface), 203
gyroscopes, 283

H

hard drives
overview, 36
sanitation of, 267–268
sharing, 223–224
standard format vs. low-level format, 266–267
troubleshooting
common symptoms, 310–312
overview, 310
required knowledge, 310
tools for, 313–314
hardware
BIOS settings
using built-in diagnostics, 9–10
component information, 5–6
configurations, 6–9
installing firmware upgrades, 4
monitoring, 10–11
overview, 3–4
required knowledge, 4, 11
cables and connectors
device cable types, 67
device connectors and pin arrangements, 65–66
display cable types, 64–65
display connector types, 62–63
overview, 62
required knowledge, 62, 67–68
connection interfaces
overview, 43
physical connections, 44–47
required knowledge, 44, 49
speeds, distances, and frequencies, 48
CPUs
characteristics, 42
cooling, 43
overview, 40
required knowledge, 40, 43
socket types, 40–41
custom configurations
audio/video editing workstation, 53
gaming PC, 54
graphic/CAD/CAM design workstation, 52–53

home server PC, 56
home theater PC, 55
overview, 52
required knowledge, 52, 57
standard thick client, 55
thin client, 56
virtualization workstation, 54
display devices
analog vs. digital, 60–61
brightness/lumens, 60
multiple displays, 61
native resolution, 60
overview, 57
privacy/antiglare filters, 61
refresh rates, 59
required knowledge, 57, 62
resolution, 59
types of, 58
expansion cards
modem cards, 31
network cards, 29
overview, 26
required knowledge, 26, 33
riser cards, 33
serial and parallel cards, 29
sound cards, 27
storage cards, 30
TV tuner cards, 32
USB and FireWire cards, 30
video capture cards, 32–33
video cards, 27–28
wireless/cellular cards, 32
laptops
component replacement, 125–127
expansion options, 124–125
overview, 123
required knowledge, 123, 127–128
motherboard components
bus speeds, 20
chipsets, 16–17
CPU sockets, 15
expansion slots, 13–14
fan connectors, 19
front panel connectors, 19
jumpers, 18
overview, 11
power connections, 18
RAM slots, 14–15
required knowledge, 11–12, 20–21
sizes, 12–13
peripheral devices
input devices, 68–71
multimedia devices, 71
output devices, 72
overview, 68
required knowledge, 68, 73
power supply
connector types, 49–50
dual voltage options, 51
overview, 49
required knowledge, 49, 51
specifications for, 50–51
RAM
compatibility and speed, 24–25
overview, 21
required knowledge, 21, 26
types of, 21–23
storage devices
combo drives, 34–35
connection types, 35–36
floppy drive, 39
hard drives, 36
media capacity, 39–40
optical drives, 34
overview, 33
RAID types, 37–39
required knowledge, 34, 40
solid state/flash drives, 37
tape drive, 39
troubleshooting
common symptoms, 304–307
overview, 304
required knowledge, 304
tools for, 308–309
HAV (hardware assisted virtualization), 241
HDMI (High-Definition Multimedia Interface)
780 resolution, 59
1080 resolution, 59
cables for, 64
configuring monitors for, 315
on laptops, 129
Type C connectors, 47, 63
Healthy indicator, Disk Management tool, 212
help switch (/?), 201
HEPA (high-efficiency particulate arresting) filters, 155
hexadecimal characters, 84
High-Definition Multimedia Interface (HDMI). *See* HDMI (High-Definition Multimedia Interface)

high-efficiency particulate arresting (HEPA) filters, 155
homegroup, 187, 188, 222–223
Home network, 227–228
home theater PCs, configurations for, 55
host name, 87
HTTP (Hypertext Transfer Protocol), 91, 277
HTTPS (Hypertext Transfer Protocol Secure), 91
hubs, 110
humidity, 166
Hypertext Transfer Protocol (HTTP), 91, 277
Hypertext Transfer Protocol Secure (HTTPS), 91
hypervisors, 242

I

ICH (I/O controller hub), 16
IC (integrated circuit) chips, 14, 294
IDE (Integrated Drive Electronics), 35, 46, 67, 310
IEEE 1394 cables, 67
IMAP (Internet Message Access Protocol), 91, 287
impact printers
    maintenance for, 156–157
    overview, 147–148
implicit deny, 225
incremental backups, 231
Infrared (IR), 48, 152
inkjet printers, 145–146
input devices, 68–71
installing OSes
    boot methods, 192
    drivers, 198–199
    drivers, third-party, 196
    factory recovery partition, 199
    file system types, 195–196
    formatting drives, 195–196
    installation types, 192–194
    partitions for, 192–194
    required knowledge, 191
    updates, 198–199
integrated circuit (IC) chips, 14, 294
Integrated Drive Electronics (IDE), 35, 46, 310
Integrated Services Digital Networks (ISDNs), 103
Internet appliance, 115
Internet connections
    cable and fiber, 102–103
    cellular, 105
    overview, 102
    phone lines, 103–104
    satellite, 104
    WiMAX, 105
Internet Message Access Protocol (IMAP), 91, 287
Internet Options applet, 215
Internet Protocol (IP) address, 150
Internet Service Providers (ISPs), 102, 105
inverter in laptop display, 130
I/O controller hub (ICH), 16
iOS vs. Android, 282–283
ipconfig command, 200, 272, 322
IP (Internet Protocol) address
    alternative IP address in Windows, 228
    class for, 83–84
    for network printers, 150
    IPv4 vs. IPv6, 84–85
IPv4 vs. IPv6, 84–85
IR (Infrared), 48, 152
ISDNs (Integrated Services Digital Networks), 103
ISPs (Internet Service Providers), 102, 105

J

Join a domain feature, Windows 7, 186
Join homegroup feature, Windows 7, 186
jumpers for motherboards, 18

K

Keyboard applet, 68
keyboard video mouse (KVM), 69, 76
key fobs, 249
kill command, 203
KVM (keyboard video mouse), 69, 76

L

land grid array (LGA) sockets, 15, 41
language
    using appropriate, 170–171
    setting, 197–198
LAN (local area network), 29, 106
laptops
    display components
        backlight, 130–131

inverter, 130
overview, 128
required knowledge, 128, 131
types of, 128–129
Wi-Fi antenna connector, 129–130
features of
docking station vs. port replicator, 134–135
overview, 131
physical laptop lock and cable lock, 135–136
required knowledge, 132, 136
special function keys, 132–134
hardware for
component replacement, 125–127
expansion options, 124–125
overview, 123
required knowledge, 123, 127–128
overview, 123
vs. tablets
no field serviceable parts, 292
overview, 292
required knowledge, 292
solid state drive, 294
touch interface, 293–294
typically not upgradable, 293
troubleshooting
common symptoms, 339–342
disassembling process, 343–344
overview, 339
required knowledge, 339
laser printers
maintenance for, 154–155
overview, 139–145
LCD (liquid crystal display), 58, 75, 317, 340
LC (Lucent Connector), 78
LDAP (Lightweight Directory Access Protocol), 92, 226
LED (light emitting diode), 19, 58, 126, 301
LGA (land grid array) sockets, 15, 41
Light blue TRS, 72
light emitting diode (LED), 19, 58, 126, 301
Lightweight Directory Access Protocol (LDAP), 92, 226
Lime green TRS, 72
Linear Tape-Open (LTO), 39
line of sight wireless Internet service. *See* WiMAX (Worldwide Interoperability for Microwave Access)
link aggregation, 29
liquid crystal display (LCD), 58, 75, 317, 340
lmhost file, 334
load letter error, 346
loadstate tool, 213
local area network (LAN), 29
Local Security Policy tool, 206, 214
Location Services setting, 284
locator applications on mobile devices, 289–290
loopback plug, 118
low-level format vs. standard format, 266–267
low memory errors, 347
LTO (Linear Tape-Open), 39
lumens, 60

M

MAC (media access control) address
defined, 110
filtering, 97–98, 272–273, 276, 319
for printers, 151
viewing, 200
maintenance
for OSes
best practices, 230–231
overview, 229
required knowledge, 229
tools for, 231–232
for printers
impact, 156–157
laser, 154–156
overview, 154
required knowledge, 154, 157
thermal, 155–156
make directory (md) command, 203
malware, 254–255
MAN (metropolitan area network), 105, 107
man traps, 248
master boot record (MBR), 324
Material Safety Data Sheet (MSDS), 155, 165, 348
mATX (micro-ATX), 12
MAU (multistation access unit), 108
Maximum Password Age setting, 261
MBR (master boot record), 324
MCH (memory controller hub), 16
md command, 203
media access control (MAC) address. *See* MAC (media access control) address
memory controller hub (MCH), 16
memory effect, 342

mesh topology, 108
metropolitan area network (MAN), 105, 107
Micro-A connector, 45
micro-ATX (mATX), 12
Micro-B connector, 45
Microsoft Management Console tool, 214
Microsoft Operating Systems
overview, 182
upgrade options for, 189–190
Windows 7 features, 187–188
Windows 7 versions, 185–186
Windows upgrade OS advisor, 189–190
Windows Vista versions, 183–184
MiFi devices, 105
migrating data and settings, 213–214
MIMO (multiple input multiple output) antennas, 95
Mini-A connector, 45
Mini-B connector, 45
Mini connector, 50
Mini-DIN 6-pin connectors, 63
Mini HDMI connectors, 63
Mini-ITX, 13
mini-Molex connector, 39, 50
Minimum Password Age setting, 262
Minimum Password Length setting, 262
mirrored display option, 133
Missing indicator, Disk Management tool, 213
MMC command, 214
MMC (MultiMediaCard) memory, 37
MMF (multi-mode fiber), 81
mobile devices
email configuration on, 287–288
network connectivity
Bluetooth, 286–287
cellular data network, 285–286
overview, 285
required knowledge, 285
operating systems for
Android vs. iOS, 282–283
GPS (global positioning system) on, 284
overview, 281
required knowledge, 281–282
screen orientation, 283–284
updating, 291
overview, 281
security for
antivirus software, 291
failed login attempts restrictions, 290–291
locator applications, 289–290
OS updates, 291
passcode locks, 289
remote backup applications, 290
remote wipes, 289
required knowledge, 288–289
synchronizing
methods for, 296–297
overview, 295
required knowledge, 295
software requirements, 296
types of data for, 295–296
tablets vs. laptops
no field serviceable parts, 292
overview, 292
required knowledge, 292
solid state drive, 294
touch interface, 293–294
typically not upgradable, 293
modems, 31, 113
Modify permission, 235
Molex connector, 50
monitoring BIOS, 10–11
motherboard components
bus speeds, 20
chipsets, 16–17
CPU sockets, 15
expansion slots, 13–14
fan connectors, 19
front panel connectors, 19
jumpers, 18
overview, 11
power connections, 18
RAM slots, 14–15
required knowledge, 11–12, 20–21
sizes, 12–13
Mouse applet, 68
msconfig command, 208–209, 214, 330
MSDS (Material Safety Data Sheet), 155, 165–166, 348
msinfo32 command, 214
mstsc command, 214, 227
multicast traffic, 110
MultiMediaCard (MMC) memory, 37
multimedia devices, 71
multimeter, 116–117
multi-mode (MMF) fiber, 81
multiple display devices, 61
multiple input multiple output (MIMO) antennas, 95
multistation access unit (MAU), 108

N

Nano-ITX, 13
NAS (Network Attached Storage), 35, 113–114
National Television System Committee (NTSC), 32
native resolution, 60
NAT (Network Address Translation), 100, 111
nbtstat command, 202, 323
netstat command, 202, 323
Net Use command, 224
Network Address Translation (NAT), 100, 111
Network Attached Storage (NAS), 35, 113–114
Networking tab, Task Manager tool, 210
network interface card (NIC). *See* NIC (network interface card)
networks
  cables
    coaxial, 79–80, 82
    fiber, 78, 80–81
    overview, 80
    required knowledge, 78, 80
    twisted-pair, 78–79, 81–82
  command line tools for, 200–202
  devices
    access points, 112–113
    bridges, 113
    firewalls, 114
    hubs, 110
    Internet appliance, 115
    modems, 113
    NAS, 113–114
    overview, 109
    required knowledge, 109–110
    routers, 111–112
    switches, 110–111
    VoIP phones, 114–115
  Internet connections
    cable and fiber, 102–103
    cellular, 105
    overview, 102
    phone lines, 103–104
    satellite, 104
    WiMAX, 105
  ports, 91–92
  protocols, 92
  SOHO routers
    built-in networking services, 99–100
    MAC filtering, 97–98
    overview, 97
    port forwarding, 98–99
    port triggering, 98–99
    required knowledge, 97
    wireless channels, 98
    wireless security, 100–101
TCP/IP
  APIPA, 85–86
  client-side DNS, 87
  DHCP, 87–88
  gateway, 89–90
  IP classes, 83–84
  IPv4 vs. IPv6, 84–85
  overview, 83
  public vs. private addresses, 85–86
  required knowledge, 83
  static vs. dynamic addresses, 87
  subnet mask, 88–89
TCP vs. UDP, 93–94
tools
  cable tester, 117
  crimper, 116
  loopback plug, 118
  multimeter, 116–117
  overview, 115
  punchdown tool, 118
  required knowledge, 115–116
  toner probe, 117
troubleshooting
  common symptoms, 318–320
  overview, 318
  required knowledge, 318
  tools for, 321–323
types of
  LAN, 106
  MAN, 107
  overview, 106
  PAN, 107
  required knowledge, 106
  topologies, 108–109
  WAN, 107
virtual machine requirements, 241–242
for Windows clients
  alternative IP address, 228
  connections for, 224
  file & printer sharing, 222–223
  firewall settings, 225
  homegroup, 222–223
  Home vs. Work vs. Public network settings, 227–228
  network card properties, 228–229

overview, 221–222
proxy settings, 226
remote desktop connections, 226–227
required knowledge, 221–222
sharing drives, 223–224
workgroup vs. domain setup, 223
wireless networking
encryption types, 96
overview, 94
required knowledge, 94
standards, 94–96
New Technology File System (NTFS), 194, 235–238, 251
NIC (network interface card)
boot options, 6
MAC address for, 272
on motherboard, 14
overview, 29
properties for, 228–229
in PXE system, 192
for servers, 56
north bridge, 16
notepad command, 214
nslookup command, 202
NTFS (New Technology File System), 194, 235–238, 251
NTSC (National Television System Committee), 32
Num Lock key, 133, 340

O

Offline Files feature, Windows 7, 186, 238
Offline indicator, Disk Management tool, 213
OLED (Organic Light Emitting Diode), 58, 128
Online indicator, Disk Management tool, 213
open-ended questions, 300–301
operating systems (OSes). *See* OSes (operating systems)
operational procedures
communication and professionalism
avoiding distractions, 172
being culturally sensitive, 172
dealing appropriately with confidential materials, 174
dealing with difficult customers or situations, 172–173
listening to customer, 171–172
maintaining positive attitude, 171
meeting expectations, 173–174
overview, 170
using proper language, 170–171
required knowledge, 170, 175
environmental controls
airborne particles, 167–168
blackouts, 166–167
brownouts, 166–167
complying with government regulations, 169
component handling and protection, 168–169
humidity, 166
MSDS documentation, 165–166
overview, 165
power surges, 166–167
required knowledge, 165, 169
temperature, 166
ventilation, 166
overview, 159
prohibited content/activity
and security policies, 176–177
chain of custody, 177
first response, 175–176
overview, 175
required knowledge, 175, 177
safety procedures
complying with government regulations, 164
equipment grounding, 161–162
ESD mats, 160–161
ESD strap, 160
overview, 159
personal safety, 162–164
required knowledge, 160, 164
self-grounding, 161
optical drives, 34
Orange TRS, 72
Organic Light Emitting Diode (OLED), 58, 128
OSes (operating systems)
administration tools
Administrative Tools (Contol Panel), 206–207
command line tools, 214–215
Disk Management tool, 210–212
migrating data and settings, 213–214
msconfig command, 208–209
required knowledge, 205–206
Task Manager tool, 209–210

command line tools
for file system, 202–204
for networks, 200–202
overview, 199
recovery console, 204–205
required knowledge, 200
configuring
language settings, 197–198
required knowledge, 191
time & date, 197–198
time/date/region settings, 197–198
workgroup vs. domain setup, 197
Control Panel utilities in Windows
common utilities, 215–216
overview, 215
required knowledge, 215
unique to Windows 7, 220–221
unique to Windows Vista, 220–221
unique to Windows XP, 219
installing
boot methods, 192
drivers, 198–199
drivers, third-party, 196
factory recovery partition, 199
file system types, 195–196
formatting drives, 195–196
installation types, 192–194
partitions for, 194–195
required knowledge, 191
updates, 198–199
maintenance procedures
best practices, 230–231
overview, 229
required knowledge, 229
tools for, 231–232
Microsoft Operating Systems
overview, 182
upgrade options for, 189–190
Windows 7 Enterprise, 185–186
Windows 7 feature comparison, 187–188
Windows 7 Home Premium, 185–186
Windows 7 Professional, 185–186
Windows 7 Starter, 185–186
Windows 7 Ultimate, 185–186
Windows upgrade OS advisor, 189–190
Windows Vista Business, 183–184
Windows Vista Enterprise, 183–184
Windows Vista Home Basic, 183–184
Windows Vista Home Premium, 183–184
Windows Vista Ultimate, 183–184
Windows XP Home, 182–183
Windows XP Media Center, 182–183
Windows XP Professional, 182–183
for mobile devices
Android vs. iOS, 282–283
GPS on, 284
overview, 281
required knowledge, 281–282
screen orientation, 283–284
updating, 291
overview, 181
security for
NTFS vs. share permissions, 235–238
overview, 233
required knowledge, 233
shared files and folders, 234–235
system files and folders, 238–239
user and groups, 233–234
user authentication, 239
troubleshooting
common symptoms, 323–326
overview, 323
required knowledge, 323
tools for, 326–331
virtualization of
hypervisor and emulator requirements, 242
overview, 239
purpose of, 240–241
required knowledge, 239–240
resource and network requirements, 241–242
security for, 242–243
Windows networking
alternative IP address, 228
connections for, 224
file & printer sharing, 222–223
firewall settings, 225
homegroup, 222
Home vs. Work vs. Public network settings, 227–228
network card properties, 228–229
overview, 221
proxy settings, 226
remote desktop connections, 226–227
required knowledge, 221–222
sharing drives, 223–224
workgroup vs. domain setup, 223
output devices, 72

P

PAL (Phase Alternating Line), 32
PAN (personal area network), 48, 107, 286
paper jams, 347
Parallel ATA (PATA) drives. *See* PATA (Parallel ATA) drives
parallel connections
    cables for, 67
    cards for, 29
    connectors for, 46, 66
    for printers, 151
partitions, 194–195
passcode locks for mobile devices, 289
passwords
    changing default, 270
    creating strong, 260–261
    requiring, 261–262
    requiring for screensaver, 264
PATA (Parallel ATA) drives
    connectors for, 65
    multiple on same IDE channel, 310
    overview, 35
    speed of, 294
patch management, 230
PCIe (Peripheral Component Interconnect Express), 50, 125, 315
PCI (Peripheral Component Interconnect), 20
PCI-X (Peripheral Component Interconnect-Extended), 13, 20
PCMCIA (Personal Computer Memory Card International Association), 124
PDF (Portable Document Format), 256
Performance Monitor tool, 207
Performance tab, Task Manager tool, 210
Perform Printer Maintenance error message, 154
Peripheral Component Interconnect Express (PCIe), 50, 125, 315
Peripheral Component Interconnect-Extended (PCI-X), 13, 20
Peripheral Component Interconnect (PCI), 20
peripheral devices
    input devices, 68–71
    multimedia devices, 71
    output devices, 72
    overview, 68
    required knowledge, 68, 73
permissions, 262–263
personal area network (PAN), 48, 107, 286
Personal Computer Memory Card International Association (PCMCIA), 124
personal identification number (PIN), 100, 286
personal safety, 162–164
PGA (pin grid array), 15
Phase Alternating Line (PAL), 32
phishing, 255–256
phone lines, Internet via, 103–104
physical connections, 44–47
physical destruction, 268
physical security
    for SOHO wireless network, 278
    overview, 248–250
Pico-ITX, 13
PID (process ID), 210
piezoelectric printing, 146, 157
pin arrangements, 65–66
ping command, 201, 322
pin grid array (PGA), 15
Pink TRS, 72
PIN (personal identification number), 100, 286
plain old telephone service (POTS), 31, 79, 103
plan of action for troubleshooting, 303
PoE (Power over Ethernet), 228
point of sale (POS), 147
polyvinyl chloride (PVC), 82
POP3 (Post Office Protocol v3), 91, 287
Portable Document Format (PDF), 256
port replicator vs. docking station, 134–135
ports
    disabling, 277–278
    forwarding, 98–99
    overview, 91–92
    triggering, 98–99
positive attitude, 170–171
POS (point of sale), 147
Post Office Protocol v3 (POP3), 91, 287
POST (power-on self-test)
    built-in decoders for, 309
    errors from, 305
    overview, 9, 305
    POST card, 309
POTS (plain old telephone service), 31, 79, 103
power-on self-test (POST). *See* POST (power-on self-test)
Power Options applet, 218, 341
Power over Ethernet (PoE), 228

Power Schemes, Windows XP, 218
power supply tester, 308
power supply unit (PSU)
  connections on motherboards for, 18
  connector types, 49–50
  dual voltage options, 51
  overview, 49
  required knowledge, 49, 51
  specifications for, 50–51
  troubleshooting, 306
power surges, 166–167
Power Users account/group, 233, 234
preboot execution environment (PXE), 192
primary display only option, 133
principle of least privilege, 252–253
Print$ folder, 235
printers
  installing and configuring
    drivers, 149–150
    overview, 149
    printer sharing, 150–153
    required knowledge, 149, 153
  maintenance for
    impact, 156–157
    laser, 154–155
    overview, 154
    required knowledge, 154
    thermal, 155–156
  overview, 139
  sharing, 152
  troubleshooting
    common symptoms, 344–348
    overview, 344
    required knowledge, 344
    tools for, 348–349
  types of
    impact, 147–148
    inkjet, 145–146
    laser, 139–145
    overview, 139
    required knowledge, 139–140, 148–149
    thermal, 147
Print Spooler service, 347, 349
privacy filters, 61, 257
private addresses vs. public addresses, 85–86
probable cause, troubleshooting, 301–302
Processes tab, Task Manager tool, 210
process ID (PID), 210
processing stage, 142, 345
professionalism
  avoiding distractions, 172
  being culturally sensitive, 172
  dealing appropriately with confidential materials, 174
  dealing with difficult customers or situations, 172–173
  listening to customer, 171–172
  maintaining positive attitude, 170–171
  meeting expectations, 173–174
  overview, 170
  using proper language, 170–171
  required knowledge, 170, 175
Program Compatibility tool, 187
Program files location, 238
Programs And Features applet, 220
prohibited content/activity
  and security policies, 176–177
  chain of custody, 177
  first response, 175–176
  overview, 175
  required knowledge, 175, 177
protocols, 92
proxy settings, 226
PS/2 connectors, 66
PSU (power supply unit). *See* power supply unit (PSU)
public addresses vs. private addresses, 85–86
Public network, 227–228
pulse-width modulation (PWM), 19
punchdown tool, 118
punctuality, 173–174
PVC (polyvinyl chloride), 82
PWM (pulse-width modulation), 19
PXE (preboot execution environment), 192

Q

QoS (Quality of Service), 100

R

radio frequency identification (RFID), 248
radio frequency interference (RFI), 80, 274
radio power levels, 274
RAID-0 (striped array) configuration, 211, 312
RAID-1 (mirror) configuration, 211, 312
RAID-5 (striping with parity) configuration, 38, 312

RAID-10 (a stripe of mirrors) configuration, 38, 312
RAID (redundant array of independent disks)
controllers for, 30
drivers for, 196
overview, 37–39
troubleshooting, 310
RAM (random-access memory)
in BIOS, 5
compatibility and speed, 24–25
overview, 21
required knowledge, 21, 26
slots for, 14–15
troubleshooting, 304–305
types of, 21–23
raster image processor (RIP), 140, 345
RCA connectors, 63
rd command, 203
RDC (Remote Desktop Connection), 214, 226
RDP (Remote Desktop Protocol), 92, 226
Read & Execute permission, 235
Read permission, 235, 236
ReadyBoost feature, 188
/rebuildbcd switch, 324, 325
/rebuild switch, 324
recordable erasable (RE), 35
recordable (R), 34
Recovery Console tool, 204–205, 324
redundant array of independent disks (RAID). *See* RAID (redundant array of independent disks)
refresh rates for display devices, 59
regedit command, 331
Region and Language applet, 197
regsvr32 command, 331
/release switch, 200
Remote Assistance feature, 226
remote backup applications, 290
remote desktop connections, 214, 226–227
Remote Desktop Protocol (RDP), 92, 226
remote wipe for mobile device, 289
remove directory (rd) command, 203
/renew switch, 200
replacements for laptop components, 125–127
Request for Comments (RFC), 86, 92
RE (recordable erasable), 35
Reset Account Lockout Counter After setting, 206
resolution for display devices, 59
resources needed for virtual machines, 241–242
revolutions per minute (RPM), 311
rewritable (RW), 35
RFC (Request for Comments), 86, 92
RFID (radio frequency identification), 248
RFI (radio frequency interference), 80, 274
RG-6 cable, 82
RGB cables, 65
ring topology, 108
RIP (raster image processor), 140, 345
riser cards, 33
RJ-11 connectors, 66, 318
RJ-45 connectors, 63, 66, 319, 321
robocopy command, 204
root access, 255
Root drive, 238
rootkits, 255
Rotation Lock, iPad, 283
routers
built-in networking services, 99–100
DMZ, 101
MAC filtering, 97–98
overview, 111–112
port forwarding, 98–99
port triggering, 98–99
required knowledge, 97
wireless channels, 98
wireless security, 100–101
RPM (revolutions per minute), 311
R (recordable), 34
RSA tokens, 249
/r switch, 196, 202
run line utilities. *See* command line tools
RW (rewritable), 35

S

safe mode, 328
safety procedures
complying with government regulations, 164
equipment grounding, 161–162
ESD mats, 160–161
ESD strap, 160
overview, 159
personal safety, 162–164
required knowledge, 160, 164
self-grounding, 161
sag, 167. *See also* brownouts
SAM (security accounts manager), 197

sanitation of hard drives, 267–268
SATA (Serial ATA) interface. *See also* serial interface
  cables for, 67
  connectors for, 50, 65
  drive performance, 36, 294
  expansion cards for, 30
  solid state drives, 125
satellite, Internet via, 104
/scanfile switch, 327
/scannow switch, 327
scanstate tool, 213
screen orientation, mobile devices, 283–284
screensaver passwords, 264
SCSI (Small Computer System Interface), 30, 65, 196
SC (Square connector), 78
SDRAM (Synchronous Dynamic RAM), 14, 21
SD (Secure Digital), 37
secondary display only option, 133
secpol command, 214
Secure Digital (SD), 37
Secure File Transfer Protocol (SFTP), 92
Secure Shell (SSH), 92
Secure Simple Pairing (SSP), 286
security
  best practices
    changing default user names, 263
    disabling autorun, 264–265
    disabling Guest account, 263–264
    overview, 259
    required knowledge, 259–260
    requiring passwords, 261–262
    restricting user permissions, 262–263
    screensaver required password, 264
    strong passwords, 260–261
  data destruction
    hard drive sanitation methods, 267–268
    low-level format vs. standard format, 266–267
    overview, 265
    physical destruction, 268
    required knowledge, 265–266
  digital security, 250–251
  for mobile devices
    antivirus software, 291
    failed login attempts restrictions, 290–291
    locator applications, 289–290
    OS updates, 291
    overview, 288
    passcode locks, 289
    remote backup applications, 290
    remote wipes, 289
    required knowledge, 288–289
  for OSes
    NTFS vs. share permissions, 235–238
    overview, 233
    required knowledge, 233
    shared files and folders, 234–235
    system files and folders, 238–239
    user and groups, 233–234
    user authentication, 239
  physical security, 248–250
  principle of least privilege, 252–253
  and prohibited content, 176–177
  for SOHO wired network
    common security steps, 276–277
    disabling ports, 277–278
    overview, 276
    physical security, 278
    required knowledge, 276
  for SOHO wireless network
    access point placement, 273–274
    assigning static IP addresses, 274–275
    changing default user names and passwords, 270
    changing SSID and disabling SSID broadcast, 270–271
    filtering MAC addresses, 272–273
    overview, 100–101, 269
    radio power levels, 274
    required knowledge, 269
    using encryption, 271–272
  threats to
    malware, 254–255
    overview, 253–259
    phishing, 255–256
    required knowledge, 253–254
    rootkits, 255
    shoulder surfing, 256–257
    social engineering, 254
    spyware, 257–258
    viruses, 258–259
  troubleshooting
    common symptoms, 332–334, 344
    overview, 332
    removing malware, 337–338
    required knowledge, 332
    tools for, 335–336
  user education, 251–252
  for virtual machines, 242–243

security accounts manager (SAM), 197
security identifier (SID), 193
Security log, 327
Security tab, Printer Properties dialog box, 152
self-grounding, 161
Serial ATA (SATA) interface. *See* SATA (Serial ATA) interface
serial interface
  cables for, 67
  cards for, 29
  connectors for, 46, 66
  for printers, 151
Server Message Block (SMB), 92
server PCs, 56
Service Required error message, 154, 348
Services applet, 214, 327
service set identifier (SSID). *See* SSID (service set identifier)
Services.msc command, 214
Services tab
  msconfig tool, 209
  Task Manager tool, 210
Services tool, 207
sfc command, 203, 327
SFTP (Secure File Transfer Protocol), 92
Shadow Copy feature, 188
sharing
  drives on Windows, 223–224
  files and folders securely, 234–235
  printers, 150–153
  share permissions vs. NTFS permissions, 235–238
Sharing tab, Printer Properties dialog box, 152
shielded twisted-pair (STP), 81
shoulder surfing, 256–257
Shrink tool, 211
shutdown command, 204
Shut Down The System setting, 263
SID (security identifier), 193
signal ground, 161–162
signature definition files, 250
Simple Mail Transfer Protocol (SMTP), 91, 287
Simple Network Management Protocol (SNMP), 92
single-mode fiber (SMF), 81
sizes of motherboards, 12–13
Small Computer System Interface (SCSI), 30, 65, 196
small office/home office (SOHO) networks. *See* SOHO (small office/home office) networks
small outline dual inline memory modules (SODIMMs), 14, 124–125, 293
SMB (Server Message Block), 92
SMF (single-mode fiber), 81
SMTP (Simple Mail Transfer Protocol), 91, 287
SNMP (Simple Network Management Protocol), 92
social engineering, 254
Socket 940 socket, 41
Socket AM2 socket, 41
Socket AM2+ socket, 41
Socket AM3 socket, 41
Socket AM3+ socket, 41
Socket B, 41
Socket F, 41
Socket FM1 socket, 41
Socket H, 41
Socket H2, 41
Socket R, 41
Socket T, 41
SODIMMs (small outline dual inline memory modules), 14, 124–125, 293
soft power, 163
software for synchronizing mobile devices, 296
SOHO (small office home office) networks
  overview, 77, 106
  routers for
    built-in networking services, 99–100
    DMZ, 101
    MAC filtering, 97–98
    overview, 97
    port forwarding, 98–99
    port triggering, 98–99
    required knowledge, 97
    wireless channels, 98
    wireless security, 100–101
  security for
    access point placement, 273–274
    assigning static IP addresses, 274–275
    changing default user names and passwords, 270
    changing SSID and disabling SSID broadcast, 270–271
    common security steps, 276–277
    disabling ports, 277–278

filtering MAC addresses, 272–273
overview, 269, 276
physical security, 278
radio power levels, 274
required knowledge, 269, 276
using encryption, 271–272
workgroup vs. domain setup, 197
solid state drives (SSDs), 37, 74, 125, 136, 293, 294
Sony/Philips Digital Interconnect Format (S/PDIF), 47, 72, 76
sound cards, 27
south bridge, 16
S/PDIF (Sony/Philips Digital Interconnect Format), 47, 72, 76
speed
of RAM, 24–25
for wireless connections, 48
spyware, 257–258
Square connector (SC), 78
SRAM (Static RAM), 42
SSDs (solid state drives), 37, 74, 125, 136, 293
SSH (Secure Shell), 92
SSID (service set identifier)
changing default, 270–271
connecting when hidden, 320
disabling broadcast of, 270–271
overview, 100
and wireless printers, 151
SSP (Secure Simple Pairing), 286
standard format vs. low-level format, 266–267
standards for wireless networks, 94–96
Standard Type A connector, 45
Standard Type B connector, 45
standard user account, 234
Startup Repair tool, 329
static addresses
for wireless network security, 274–275
vs. dynamic addresses, 87
static buildup, 166
Static RAM (SRAM), 42
Sticky Keys, 69
storage devices
cards for, 30
combo drives, 34–35
connection types, 35–36
floppy drive, 39
hard drives, 36
media capacity, 39–40
optical drives, 34
overview, 33
RAID types, 37–39
required knowledge, 34, 40
solid state/flash drives, 37
tape drive, 39
Store Passwords Using Reversible Encryption setting, 262
STP (shielded twisted-pair), 81
Straight tip (ST), 78
streaks, 346
strong passwords, 260–261
ST (Straight tip), 78
stuck pixels, 316
subnet mask, 88–89
Super XGA (SXGA), 59
SVGA (Super VGA), 59
S-video cables, 64
switches, 110–111
SXGA (Super XGA), 59
synchronizing mobile devices
methods for, 296–297
overview, 295
required knowledge, 295
software requirements, 296
types of data for, 295–296
Synchronous Dynamic RAM (SDRAM), 14, 21
Sysprep tool, 193
System applet, 217
System Configuration tool, 214
System File Checker (sfc) command, 203, 327
system files and folders, 238–239
System Information tool, 214
System log, 327
System Properties applet, 217
System Recovery Options menu, 330
System Restore feature, 187, 232, 337

T

tablets
no field serviceable parts, 292
overview, 292
required knowledge, 292
solid state drive, 294
touch interface, 293–294
typically not upgradable, 293
tape drives, 39
taskkill command, 203
tasklist command, 203
Task Manager tool, 209–210
Task Scheduler tool, 207

TCP/IP (Transmission Control Protocol/Internet Protocol)
APIPA, 85–86
client-side DNS, 87
DHCP, 87–88
gateway, 89–90
IP classes, 83–84
IPv4 vs. IPv6, 84–85
overview, 83
public vs. private addresses, 85–86
required knowledge, 83
static vs. dynamic addresses, 87
subnet mask, 88–89
TCP (Transmission Control Protocol) vs. UDP, 93–94
telephone cables, 67
temperature, 166
Temporal Key Integrity Protocol (TKIP), 96, 271
Temporary files location, 238
testing, 302–303
theory of troubleshooting
documenting, 304
establishing plan of action, 303
establishing probable cause, 301–302
identifying problem, 300–301
overview, 300
required knowledge, 300
testing, 302–303
verifying full system functionality, 303
thermal printers
maintenance for, 155–156
overview, 147
thick clients, 56
thin clients, 56
third-party drivers, 196
threats to security
malware, 254–255
overview, 253–259
phishing, 255–256
required knowledge, 253–254
rootkits, 255
shoulder surfing, 256–257
social engineering, 254
spyware, 257–258
viruses, 258–259
time, setting, 197–198
tip ring sleeve (TRS), 19, 47, 66, 72
TKIP (Temporal Key Integrity Protocol), 96, 271
tlist command, 203
toner probe, 117, 321, 322
tools
administration tools
Administrative Tools (Contol Panel), 206–207
command line tools, 214–215
Disk Management tool, 210–212
migrating data and settings, 213–214
msconfig command, 208–209
required knowledge, 205–206
Task Manager tool, 209–210
cable tester, 117
command line tools
for file system, 202–204
for networks, 200–202
for OS administration, 214–215
overview, 200
recovery console, 204–205
required knowledge, 200
crimper, 116
loopback plug, 118
multimeter, 116–117
for OS maintenance, 231–232
overview, 115
punchdown tool, 118
required knowledge, 115–116
toner probe, 117
for troubleshooting
hard drives, 313–314
hardware, 308–309
networks, 321–323
OSes, 326–331
printers, 348–349
security issues, 335–336
Tools tab, msconfig tool, 209
topologies, network, 108–109
touch interface of tablets, 293–294
TPM (Trusted Platform Module), 9
tracert command, 202, 323
transfer corona, 143
transferring stage, 345
transfer roller, 143
triggering ports, 98–99
Trojan, 258
troubleshooting
hard drives
common symptoms, 310–312
overview, 310
required knowledge, 310
tools for, 313–314

hardware
common symptoms, 304–307
overview, 304
required knowledge, 304
tools for, 308–309
laptops
common symptoms, 339–342
disassembling process, 343–344
overview, 339
required knowledge, 339
networks
common symptoms, 318–320
overview, 318
required knowledge, 318
tools for, 321–323
OSes
common symptoms, 323–326
overview, 323
required knowledge, 323
tools for, 326–331
printers
common symptoms, 344–348
overview, 344
required knowledge, 344
tools for, 348–349
security issues
common symptoms, 332–334
overview, 332
removing malware, 337–338
required knowledge, 332
tools for, 335–336
theory of
documenting, 304
establishing plan of action, 303
establishing probable cause, 301–302
identifying problem, 300–301
overview, 300
required knowledge, 300
testing, 302–303
verifying full system functionality, 303
video & displays
common symptoms, 315–317
overview, 314
required knowledge, 314
TRS (tip ring sleeve), 19, 47, 66, 72
Trusted Platform Module (TPM), 9
-t switch, 201
turnstiles, 248
TV tuner cards, 32
twisted-pair cables, 78–79, 81–82

U

UDP (User Datagram Protocol) vs. TCP, 93–94
Ultra XGA (UXGA), 59
unattended installations, 194
UNC (Universal Naming Convention), 149, 152, 223
unicast traffic, 110
uninterruptible power supply (UPS), 4, 167
Universal Naming Convention (UNC), 149, 152, 223
Universal Serial Bus (USB). *See* USB (Universal Serial Bus)
Unreadable indicator, Disk Management tool, 213
unshielded twisted-pair (UTP), 81
upgrades
to BIOS, 4
installing updates, 198–199
migrating data and settings, 213–214
tablets vs. laptops, 293
between Windows Operating Systems, 189–190
UPS (uninterruptible power supply), 4, 167
USB (Universal Serial Bus)
boot options, 6
cables for, 67
connectors for, 45
expansion cards for, 30
for printers, 151
solid state drives and, 125
User Account Control feature, 188, 234
user authentication, 239
user education, 251–252
user names, changing default, 263, 270
User Rights Assignment node, 207, 263
users and groups, 207, 233–234
Users tab, Task Manager tool, 210
USMT (User State Migration tool), 189, 213
UTP (unshielded twisted-pair), 81
UXGA (Ultra XGA), 59

V

VAC (volts alternating current), 167
ventilation, 166
/verifyfile switch, 327
/verifyonly switch, 327

vertical lines error, 347
VGA (Video Graphics Array), 46, 59, 129, 315
video capture cards, 32–33
video cards, 27–28
video displays, troubleshooting
common symptoms, 315–317
overview, 314
required knowledge, 314
video editing workstation, configuration for, 54
Video Graphics Array (VGA), 46, 59, 129, 315
Virtual Box, Oracle, 241
virtualization
hardware configuration for, 54
hypervisor and emulator requirements, 242
overview, 239–240
purpose of, 240–241
required knowledge, 239–240
resource and network requirements, 241–242
security for, 242–243
virtual private network (VPN), 224
viruses, 226, 258–259
VMs (virtual machines). *See* virtualization
VoIP (Voice over Internet Protocol), 114–115
voltage for power supply, 51
volts alternating current (VAC), 167
VPN (virtual private network), 224

W

Wake-on-LAN (WoL), 229
WAN (wide area network)
overview, 107, 112
WAP (wireless access point), 112, 151, 274, 319
WEP (Wired Equivalent Privacy), 96, 271
wide area network (WAN), 107, 112
Wide UXGA (WUXGA), 59
Wi-Fi Protected Access (WPA), 96, 271
Wi-Fi Protected Access version 2 (WPA2), 271, 319
Wi-Fi Protected Setup (WPS), 100
WiMAX (Worldwide Interoperability for Microwave Access), 105
Windows 7
Control Panel utilities in, 215–217
feature comparison for, 187–188
versions, 185–186
Windows Advanced Boot Options menu, 328
Windows Advanced Options menu, 328
Windows Advanced Options page, 328
Windows Defender feature, 187
Windows Explorer tool, 214
Windows files location, 238
Windows Firewall, 187, 207
Windows Libraries feature, 188
Windows networking
alternative IP address, 228
connections for, 224
file & printer sharing, 222–223
firewall settings, 225
homegroup, 222–223
Home vs. Work vs. Public network settings, 227–228
network card properties, 228–229
overview, 221–222
proxy settings, 226
remote desktop connections, 226–227
required knowledge, 221–222
sharing drives, 223–224
workgroup vs. domain setup, 223
Windows Recovery Environment, 330
Windows Update Express setting, 198
Windows upgrade OS advisor, 189–190
Windows Vista
Control Panel utilities in, 215–217
versions, 183–184
Windows XP
Control Panel utilities in, 215–217
versions, 182–183
Windows XP Mode feature, 186, 188
Windows XP Presentation Power Scheme, 218
winnt32.exe command, 204
Wired Equivalent Privacy (WEP), 96, 271
wireless access point (WAP), 112, 151, 274, 319
Wireless locator tool, 323
wireless networking
channels for, 98
connection types, 48
encryption types, 96
overview, 94
required knowledge, 94
standards for, 94–96
Wi-Fi antenna in laptops, 129–130
wireless cards, 32
wireless wide area networks (WWANs), 224

WoL (Wake-on-LAN), 229
workgroup vs. domain setup, 197
Work network, 227–228
worm (security threat), 258
WORM (write once read many), 34
WPA (Wi-Fi Protected Access), 96, 271
WPA2 (Wi-Fi Protected Access version 2), 96, 271, 319
WPS (Wi-Fi Protected Setup), 100
write once read many (WORM), 34
Write permission, 235
WUXGA (Wide UXGA), 59
WWANs (wireless wide area networks), 224

X

xcopy command, 204
XGA (Extended GA), 59

Z

zero-fill utility, 267, 336
ZIF (zero insertion force) socket, 15

About the author

DARRIL GIBSON, A+, Network+, Security+, CASP, SSCP, CISSP, MCT, CTT+, MCSE, MCITP is founder and CEO of Security, Consulting, and Training, LLC. Darril has written or co-written more than 25 books, including several on security and security certifications. He regularly posts articles on *http://blogs.GetCertifiedGetAhead.com* and can be reached at *darril@GetCertifiedGetAhead.com*.

What do you think of this book?

We want to hear from you!

To participate in a brief online survey, please visit:

microsoft.com/learning/booksurvey

Tell us how well this book meets your needs—what works effectively, and what we can do better. Your feedback will help us continually improve our books and learning resources for you.

Thank you in advance for your input!

Microsoft Press