

EXAM CRAM

Save 10%
on Exam
Voucher

See Inside

CompTIA[®]

A+[®]

Core 1 (220-1001)

Core 2 (220-1002)

PEARSON IT
CERTIFICATION

DAVID L. PROWSE

FREE SAMPLE CHAPTER

SHARE WITH OTHERS



EXAM ✓ CRAM

**CompTIA® A+®
Core 1 (220-1001)
and
Core 2 (220-1002)**

David L. Prowse

CompTIA® A+® Core 1 (220-1001) and Core 2 (220-1002) Exam Cram

Copyright © 2020 by Pearson Education, Inc.

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ISBN-13: 978-0-7897-6057-9

ISBN-10: 0-7897-6057-6

Library of Congress Control Number: 2019944169

ScoutAutomatedPrintCode

Trademarks

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

Microsoft and/or its respective suppliers make no representations about the suitability of the information contained in the documents and related graphics published as part of the services for any purpose. All such documents and related graphics are provided, “as is” without warranty of any kind. Microsoft and/or its respective suppliers hereby disclaim all warranties and conditions with regard to this information, including all warranties and conditions of merchantability, whether express, implied or statutory, fitness for a particular purpose, title and non-infringement. In no event shall Microsoft and/or its respective suppliers be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of information available from the services.

The documents and related graphics contained herein could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Microsoft and/or its respective suppliers may make improvements and/or changes in the product(s) and/or the program(s) described herein at any time. Partial screenshots may be viewed in full within the software version specified.

Microsoft® and Windows® are registered trademarks of the Microsoft Corporation in the U.S.A. and other countries. Screenshots and icons reprinted with permission from the Microsoft Corporation. This book is not sponsored or endorsed by or affiliated with the Microsoft Corporation.

Warning and Disclaimer

This book is designed to provide information about the CompTIA A+ Core 1 (220-1001) and Core 2 (220-1002) exams for the CompTIA A+ certification. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

Editor-in-Chief

Mark L. Taub

Product Line Manager

Brett Bartow

Executive Editor

Paul Carlstroem

Development Editor

Christopher A.
Cleveland

Managing Editor

Sandra Schroeder

Senior Project Editor

Tonya Simpson

Copy Editor

Bill McManus

Indexer

Ken Johnson

Proofreader

Abigail Manheim

Technical Editor

Chris Crayton

Publishing Coordinator

Cindy Teeters

Cover Designer

Chuti Prasertsith

Compositor

codeMantra

Contents at a Glance

Part I: Introduction to Core 1 (220-1001)

Core 1 (220-1001) Domain 1.0: Mobile Devices

CHAPTER 1	Laptops, Part 1	7
CHAPTER 2	Laptops, Part 2	29
CHAPTER 3	Smartphones, Tablets, and Other Mobile Devices, Part 1	47
CHAPTER 4	Smartphones, Tablets, and Other Mobile Devices, Part 2	65

Core 1 (220-1001) Domain 2.0: Networking

CHAPTER 5	Ports, Protocols, and Network Devices	89
CHAPTER 6	SOHO Networks and Wireless Protocols	111
CHAPTER 7	Networked Hosts and Network Configuration	133
CHAPTER 8	Network Types and Networking Tools	151

Core 1 (220-1001) Domain 3.0: Hardware

CHAPTER 9	Cables and Connectors	169
CHAPTER 10	RAM and Storage	187
CHAPTER 11	Motherboards and Add-on Cards	215
CHAPTER 12	CPUs	233
CHAPTER 13	Peripherals and Power	249
CHAPTER 14	Custom PCs and Common Devices	271
CHAPTER 15	Printers and Multifunction Devices	287

Core 1 (220-1001) Domain 4.0: Virtualization and Cloud Computing

CHAPTER 16	Cloud Computing and Client-side Virtualization	311
------------	--	-----

Core 1 (220-1001) Domain 5.0: Hardware and Network Troubleshooting

CHAPTER 17	Computer Troubleshooting 101	329
CHAPTER 18	Troubleshooting Motherboards, CPUs, RAM, and Power	337
CHAPTER 19	Troubleshooting Hard Drives and RAID Arrays	353
CHAPTER 20	Troubleshooting Video Issues and Mobile Devices	365
CHAPTER 21	Troubleshooting Printers	381
CHAPTER 22	Troubleshooting Wired and Wireless Network Problems	393

A+ Core 1 (220-1001) Practice Exam	399
------------------------------------	-----

Part II: Introduction to Core 2 (220-1002)**Core 2 (220-1002) Domain 1.0: Operating Systems**

CHAPTER 23	Operating System Types and Windows Versions	449
CHAPTER 24	Operating System Installation	471
CHAPTER 25	Microsoft Command Line Tools	487
CHAPTER 26	Microsoft Operating System Features and Tools, Part 1	511
CHAPTER 27	Microsoft Operating System Features and Tools, Part 2	529
CHAPTER 28	Windows Control Panel Utilities	547
CHAPTER 29	Windows Networking and Application Installation	567
CHAPTER 30	Linux and macOS Tools	585

Core 2 (220-1002) Domain 2.0: Security

CHAPTER 31	Physical and Logical Security	603
CHAPTER 32	Wireless Security, Malware, and Social Engineering	623
CHAPTER 33	Windows Security Settings and Best Practices	645
CHAPTER 34	Mobile Device Security	669
CHAPTER 35	Data Destruction and SOHO Security	683

Core 2 (220-1002) Domain 3.0: Software Troubleshooting

CHAPTER 36	Troubleshooting Microsoft Windows	703
CHAPTER 37	Troubleshooting PC Security Issues and Malware Removal	723
CHAPTER 38	Troubleshooting Mobile Operating Systems	737

Core 2 (220-1002) Domain 4.0: Operational Procedures

CHAPTER 39	Documentation, Change Management, and Disaster Recovery	755
CHAPTER 40	Safety Procedures and Environmental Controls	779
CHAPTER 41	Incident Response, Communication, and Professionalism	797
CHAPTER 42	Basic Scripting and Remote Access Technologies	813

A+ Core 2 (220-1002) Practice Exam	837
------------------------------------	-----

CHAPTER 43	Getting Ready for the Exams, and Farewell	879
	Index	887

Table of Contents

Introduction	xxiii
------------------------	-------

Part I: Introduction to Core 1 (220-1001)

Core 1 (220-1001) Domain 1.0: Mobile Devices

CHAPTER 1:

Laptops, Part 1	7
1.1 – Given a scenario, install and configure laptop hardware and components	7
Keyboards	8
Touchpad	10
Hard Drives	11
Memory	13
Smart Card Readers	16
Optical Drives	16
Communications	16
Video	18
Power	19
Speaker	23
System Board and CPU	24
Fans	25
Cram Quiz	26

CHAPTER 2:

Laptops, Part 2	29
1.2 – Given a scenario, install components within the display of a laptop	29
Display Types	30
Inverter and Backlight	31
Digitizers and Touchscreens	32
Webcam and Microphone	33
Wi-Fi Antenna Connector and Placement	34
Cram Quiz	37
1.3 – Given a scenario, use appropriate laptop features	39
Special Function Keys	39
External Monitors	41
Docking Stations and Port Replicators	42
Rotating and Removable Screens	42

Securing Laptops with Cable Locks	43
Cram Quiz	44

CHAPTER 3:**Smartphones, Tablets, and Other Mobile Devices, Part 1 47**

1.4 – Compare and contrast characteristics of various types of other mobile devices	47
Tablets	48
Smartphones	49
Wearable Technology Devices	52
E-readers	52
GPS Devices	53
Cram Quiz	54
1.5 – Given a scenario, connect and configure accessories and ports of other mobile devices	56
Connection Types	56
Accessories	60
Cram Quiz	61

CHAPTER 4:**Smartphones, Tablets, and Other Mobile Devices, Part 2 65**

1.6 – Given a scenario, configure basic mobile device network connectivity and application support	65
Enabling Wireless Functions	66
USB Tethering	69
Bluetooth	69
E-mail Configuration	71
Cellular Radio Technologies	74
Cram Quiz	77
1.7 – Given a scenario, use methods to perform mobile device synchronization	79
Synchronization Methods	79
Types of Data to Synchronize and Authentication	83
Cram Quiz	84

Core 1 (220-1001) Domain 2.0: Networking**CHAPTER 5:****Ports, Protocols, and Network Devices 89**

2.1 – Compare and contrast TCP and UDP ports, protocols, and their purposes	89
TCP vs. UDP	90
Ports and Protocols	91
Cram Quiz	99

2.2 – Compare and contrast common networking hardware devices. . . .	101
Switches	101
Routers	102
Wireless Access Points	102
Firewalls	103
Network Interface Cards	103
Cloud-based Network Controllers	104
Repeaters	104
Hubs	104
Cable/DSL Modems	105
Bridges	105
Patch Panels	105
Power over Ethernet	106
Ethernet over Power	107
Cram Quiz	107
CHAPTER 6:	
SOHO Networks and Wireless Protocols	111
2.3 – Given a scenario, install and configure a basic wired/wireless SOHO network.	111
Router Setup and Wireless	112
Access Point Settings	115
NIC and End-user Device Configuration	116
IoT Device Configuration	118
Cable/DSL Modem Configuration	120
Firewall Settings and Additional Configurations	120
Configuring Wireless Encryption	123
Cram Quiz	124
2.4 – Compare and contrast wireless networking protocols.	126
802.11 Wireless	126
RFID	129
Zigbee and Z-Wave	129
Cram Quiz	131
CHAPTER 7:	
Networked Hosts and Network Configuration	133
2.5 – Summarize the properties and purposes of services provided by networked hosts	133
Server Roles	134
Internet Appliances	138
Embedded/Legacy Systems	139
Cram Quiz	140

2.6 – Explain common network configuration concepts	142
Configuring IPv4	142
Configuring IPv6	146
VLANs	147
VPNs	148
Cram Quiz	149

CHAPTER 8:**Network Types and Networking Tools 151**

2.7 – Compare and contrast Internet connection types, network types, and their features	151
Network Types	152
Internet Connection Types	154
Cram Quiz	158
2.8 – Given a scenario, use appropriate networking tools	160
Network Cabling Tools	160
Wi-Fi Analyzers	163
Cram Quiz	164

Core 1 (220-1001) Domain 3.0: Hardware**CHAPTER 9:****Cables and Connectors 169**

3.1 – Explain basic cable types, features, and their purposes	169
3.2 – Identify common connector types	170
Network Cables	170
Video Cables and Connectors	176
Multipurpose Cables and Connectors	178
Hard Drive Cables and Connectors	182
Adapters	182
Cram Quiz	183

CHAPTER 10:**RAM and Storage 187**

3.3 – Given a scenario, install RAM types	187
RAM Types	188
Installing RAM	191
RAM Technologies	194
Cram Quiz	196
3.4 – Given a scenario, select, install and configure storage devices	198
SATA	198
Magnetic Hard Drives	200

Solid-State Drives	201
RAID	202
Flash	204
Optical Drives	208
Cram Quiz	213
CHAPTER 11:	
Motherboards and Add-on Cards	215
3.5 – Given a scenario, install and configure motherboards, CPUs, and add-on cards	215
Motherboard Form Factors and Connectors	216
Expansion Cards	220
More Ports and Connectors.	226
BIOS/UEFI Settings	226
The POST	229
Cram Quiz	229
CHAPTER 12:	
CPUs	233
3.5 – Given a scenario, install and configure motherboards, CPUs, and add-on cards	233
CPU Features	233
CPU Compatibility	236
Power Consumption.	239
Cooling Mechanisms	239
Installing CPUs	242
Cram Quiz	245
CHAPTER 13:	
Peripherals and Power	249
3.6 – Explain the purposes and uses of various peripheral types.	249
Input Devices	250
Output Devices	256
Hybrid I/O Devices and Others	259
Cram Quiz	260
3.7 – Summarize power supply types and features	262
Planning Which Power Supply to Use	262
Installing the Power Supply.	266
Cram Quiz	268

CHAPTER 14:**Custom PCs and Common Devices 271**

- 3.8 – Given a scenario, select and configure appropriate components for a custom PC configuration to meet customer specifications or needs . . . 271
 - Graphic/CAD/CAM Design Workstation 272
 - Audio/Video Editing Workstation 272
 - Virtualization Workstation 273
 - Gaming PC 275
 - Network-Attached Storage Device 277
 - Thin Client 278
 - Standard Thick Client 280
 - Cram Quiz 280
- 3.9 – Given a scenario, install and configure common devices. 282
 - Desktop Devices and Settings 282
 - Laptop Configurations and Settings 283
 - Cram Quiz 286

CHAPTER 15:**Printers and Multifunction Devices 287**

- 3.10 – Given a scenario, configure SOHO multifunction devices/printers and settings. 287
 - Printer Configuration Settings 288
 - Local Versus Network Printers 291
 - Cram Quiz 292
- 3.11 – Given a scenario, install and maintain various print technologies. 294
 - Types of Printers 294
 - Virtual Printing 302
 - Printer Installation and Drivers 305
 - Cram Quiz 306

Core 1 (220-1001) Domain 4.0: Virtualization and Cloud Computing**CHAPTER 16:****Cloud Computing and Client-side Virtualization. 311**

- 4.1 – Compare and contrast cloud computing concepts 312
 - Common Cloud Models 312
 - Cloud Computing Concerns 314
 - Cram Quiz 316

4.2 – Given a scenario, set up and configure client-side virtualization . . .	318
Purpose of Virtual Machines	318
Hypervisors	319
Examples of Virtual Machine Software	320
Virtual Machine Requirements.	322
Cram Quiz	325

Core 1 (220-1001) Domain 5.0: Hardware and Network Troubleshooting

CHAPTER 17:

Computer Troubleshooting 101 329

5.1 – Given a scenario, use the best practice methodology to resolve problems.	329
Step 1: Identify the Problem	330
Step 2: Establish a Theory of Probable Cause (Question the Obvious).	332
Step 3: Test the Theory to Determine Cause.	333
Step 4: Establish a Plan of Action to Resolve the Problem and Implement the Solution	333
Step 5: Verify Full System Functionality and, If Applicable, Implement Preventive Measures.	333
Step 6: Document Findings, Actions, and Outcomes.	334
Cram Quiz	335

CHAPTER 18:

Troubleshooting Motherboards, CPUs, RAM, and Power 337

5.2 – Given a scenario, troubleshoot problems related to motherboards, RAM, CPUs, and power	337
Troubleshooting Motherboards	338
Troubleshooting CPUs.	340
Troubleshooting RAM	342
Troubleshooting Power Supply Issues.	344
Heating and Cooling	347
Cram Quiz	348

CHAPTER 19:

Troubleshooting Hard Drives and RAID Arrays 353

5.3 – Given a scenario, troubleshoot hard drives and RAID arrays.	353
Troubleshooting Hard Drives	354
Troubleshooting RAID Arrays.	359
Cram Quiz	361

**CHAPTER 20:
Troubleshooting Video Issues and Mobile Devices 365**

- 5.4 – Given a scenario, troubleshoot video, projector, and display issues 366
 - Video Troubleshooting 366
 - Cram Quiz 370
- 5.5 – Given a scenario, troubleshoot common mobile device issues while adhering to the appropriate procedures 372
 - Mobile Device Display Troubleshooting 372
 - Mobile Device Overheating 373
 - More Mobile Device Troubleshooting 375
 - Disassembling Processes for Proper Reassembly 376
 - Cram Quiz 378

**CHAPTER 21:
Troubleshooting Printers 381**

- 5.6 – Given a scenario, troubleshoot printers 381
 - Troubleshooting Printers 381
 - Print Jobs and the Print Spooler 385
 - Cram Quiz 389

**CHAPTER 22:
Troubleshooting Wired and Wireless Network Problems 393**

- 5.7 – Given a scenario, troubleshoot common wired and wireless network problems 393
 - Troubleshooting Common Symptoms 394
 - Cram Quiz 397

A+ Core 1 (220-1001) Practice Exam 399

- Exam Questions 400
- Answers at a Glance 418
- Answer Explanations 419

Part II: Introduction to Core 2 (220-1002)

Core 2 (220-1002) Domain 1.0: Operating Systems

**CHAPTER 23:
Operating System Types and Windows Versions 449**

- 1.1 – Compare and contrast common operating system types and their purposes 449
 - Workstation Operating Systems 450
 - 32-Bit Versus 64-Bit 451

Smartphone and Tablet Operating Systems	453
Vendor-Specific Limitations	457
Compatibility Concerns Between Operating Systems	458
Cram Quiz	459
1.2 – Compare and contrast features of Microsoft Windows versions. . .	461
Windows 7	461
Windows 8 and 8.1	462
Windows 10	464
Windows User Interfaces and Components	465
Cram Quiz	469
CHAPTER 24:	
Operating System Installation	471
1.3 – Summarize general OS installation considerations and upgrade methods	471
Boot Methods	472
Types of Installations	473
Partitioning	476
File System Types and Formatting	478
More OS Installation Considerations	481
Cram Quiz	485
CHAPTER 25:	
Microsoft Command Line Tools	487
1.4 – Given a scenario, use appropriate Microsoft command line tools. .	488
Command Prompt Basics	488
Navigating and Working with Directories and Files in the Command Prompt	490
Partitioning and File System-based Commands	493
Chkdsk and SFC	494
Networking Commands	496
Advanced Commands	504
Cram Quiz	507
CHAPTER 26:	
Microsoft Operating System Features and Tools, Part 1	511
1.5 – Given a scenario, use Microsoft operating system features and tools	511
Administrative Tools	511
System Configuration/MSConfig	523
Task Manager	524
Cram Quiz	526

CHAPTER 27:**Microsoft Operating System Features and Tools, Part 2 529**

1.5 – Given a scenario, use Microsoft operating system features and tools	529
Disk Management	529
System Utilities	535
Cram Quiz	544

CHAPTER 28:**Windows Control Panel Utilities 547**

1.6 – Given a scenario, use Microsoft Windows Control Panel utilities	547
Internet Options	548
Display	550
User Accounts	554
Folder Options	554
Performance (Virtual Memory)	556
Power Management	557
Credential Manager	558
Programs and Features	559
Program Compatibility	560
Devices and Printers	561
Sound	561
Troubleshooting	563
Sync Center	563
Cram Quiz	564

CHAPTER 29:**Windows Networking and Application Installation 567**

1.8 – Given a scenario, configure Microsoft Windows networking on a client/desktop	568
Workgroup, HomeGroup, and Domain	568
Sharing Resources and Making Network Connections	570
Establishing Networking Connections	574
Proxy Settings	576
Configuring an Alternate IP Address in Windows	577
Network Card Properties	578
1.7 – Summarize application installation and configuration concepts	580
Application Requirements	580
Method of Installation and Deployment	581
User Permissions	582

Security Considerations 582
Cram Quiz 583

CHAPTER 30:

Linux and macOS Tools 585
1.9 – Given a scenario, use features and tools of the macOS and
Linux client/desktop operating systems 585
 macOS 585
 Linux 590
 Cram Quiz 596

Core 2 (220-1002) Domain 2.0: Security

CHAPTER 31:

Physical and Logical Security 603
2.1 – Summarize the importance of physical security measures 604
 Physical Locks 604
 Entry Systems 604
 Biometrics 605
 Protecting Data Physically 606
 Cram Quiz 607
2.2 – Explain logical security concepts 608
 Authentication 608
 Principle of Least Privilege 609
 Active Directory 610
 Firewalls 615
 VPN 616
 Additional Security Considerations in Windows 617
 Cram Quiz 620

CHAPTER 32:

Wireless Security, Malware, and Social Engineering 623
2.3 – Compare and contrast wireless security protocols and
authentication methods 624
 Wireless and Encryption Protocols 624
 Cram Quiz 627
2.4 – Given a scenario, detect, remove, and prevent malware using
appropriate tools and methods 628
 Malicious Software Types 628
 Preventing Malicious Software 629
 Cram Quiz 635

- 2.5 – Compare and contrast social engineering, threats, and vulnerabilities 637
 - Phishing 637
 - Shoulder Surfing 638
 - Piggybacking/Tailgating 638
 - Dumpster Diving 639
 - Impersonation 639
 - Additional Attacks and Security Vulnerabilities 640
 - Cram Quiz 642

CHAPTER 33:

Windows Security Settings and Best Practices 645

- 2.6 – Compare and contrast the differences of basic Microsoft Windows OS security settings 645
 - Users and Groups 646
 - Permissions 648
 - File Security 652
 - Cram Quiz 656
- 2.7 – Given a scenario, implement security best practices to secure a workstation 659
 - Usernames and Passwords 659
 - Password Policies 660
 - Account Management 662
 - Disabling AutoPlay/Autorun 664
 - Cram Quiz 665

CHAPTER 34:

Mobile Device Security 669

- 2.8 – Given a scenario, implement methods for securing mobile devices 669
 - Screen Locks 670
 - Authenticator Applications 672
 - Theft and Loss of Mobile Devices 672
 - Compromised and Damaged Devices 673
 - Policies and Procedures 677
 - Cram Quiz 680

CHAPTER 35:

Data Destruction and SOHO Security 683

- 2.9 – Given a scenario, implement appropriate data destruction and disposal methods 683

Formatting Drives	684
Overwriting Drives	685
Clear	687
Purge	687
Destroy	688
Cram Quiz	689
2.10 – Given a scenario, configure security on SOHO wireless and wired networks	691
Changing Default Passwords	691
Wireless-Specific Security Settings	692
Enabling MAC Filtering	695
Assigning Static IP Addresses	695
Disabling Physical Ports and Physical Security	696
Content Filtering/Parental Controls	697
A Final Word on SOHO Routers	697
Cram Quiz	698

Core 2 (220-1002) Domain 3.0: Software Troubleshooting

**CHAPTER 36:
Troubleshooting Microsoft Windows 703**

3.1 – Given a scenario, troubleshoot Microsoft Windows OS problems	704
Windows Recovery	704
Boot Errors	710
Improper and Spontaneous Shutdowns	712
Stop Errors	713
Restoring Windows	715
Common Windows Symptoms and Solutions	716
Cram Quiz	719

**CHAPTER 37:
Troubleshooting PC Security Issues and Malware Removal 723**

3.3 – Given a scenario, use best practice procedures for malware removal	724
3.2 – Given a scenario, troubleshoot and resolve PC security issues	724
The CompTIA A+ Seven-Step Malware Removal Procedure	724
Malware Removal Scenario	725
Symptoms of Viruses	729
Symptoms of Spyware	730
Preventing and Troubleshooting Spam	730

Hijacked E-mail	731
More Symptoms of PC Security Issues and Potential Solutions	732
Cram Quiz	734

CHAPTER 38:**Troubleshooting Mobile Operating Systems 737**

3.4 – Given a scenario, troubleshoot mobile OS and application issues	737
3.5 – Given a scenario, troubleshoot mobile OS and application security issues	737
Wi-Fi Troubleshooting	738
Bluetooth Troubleshooting	740
Troubleshooting E-mail Connections	741
Troubleshooting and Stopping Applications	743
Initiating Resets	744
Additional Mobile Device Troubleshooting	746
Mobile Device Application and OS Troubleshooting	747
External Monitor Issues	748
Troubleshooting Mobile Device Security Issues	748
Cram Quiz	751

Core 2 (220-1002) Domain 4.0: Operational Procedures**CHAPTER 39:****Documentation, Change Management, and Disaster Recovery 755**

4.1 – Compare and contrast best practices associated with types of documentation	756
Network Topology Diagrams	756
Knowledge Bases/Articles	758
Incident Documentation	760
Compliance and Regulatory Policy	760
Acceptable Use Policy	761
Password Policy	762
Inventory Management	763
Cram Quiz	764
4.2 – Given a scenario, implement basic change management best practices	766
4.3 – Given a scenario, implement basic disaster prevention and recovery methods	769
Backup and Recovery	769
Cloud Storage vs. Local Storage Backups	773

Account Recovery Options 774
Cram Quiz 776

CHAPTER 40:
Safety Procedures and Environmental Controls 779

4.4 – Explain common safety procedures 779
 ESD Prevention and Equipment Grounding 780
 Electrical Safety 782
 Electrical Fire Safety 783
 Physical Safety 784
 Cram Quiz 786
4.5 – Explain environmental impacts and appropriate controls 788
 Temperature, Humidity, and Air 788
 MSDS and Disposal 789
 Power Devices 791
 Surge Protectors 792
 Uninterruptible Power Supplies 792
 Cram Quiz 794

CHAPTER 41:
Incident Response, Communication, and Professionalism 797

4.6 – Explain the processes for addressing prohibited
 content/activity, and privacy, licensing, and policy concepts 797
 Incident Response 798
 Licensing/DRM/EULA 801
 Regulated Data 803
 Cram Quiz 806
4.7 – Given a scenario, use proper communication techniques and
 professionalism. 808
 Communication Techniques and Professionalism 808
 Cram Quiz 811

CHAPTER 42:
Basic Scripting and Remote Access Technologies 813

4.8 – Identify the basics of scripting 813
 Basic Data Types 814
 Basic Script Constructs 815
 Environment Variables 817
 Comment Syntax 817
 Script File Types 818
 Cram Quiz 827

- 4.9 – Given a scenario, use remote access technologies 829
 - Remote Desktop 829
 - SSH 831
 - More Third-Party Tools 833
 - Cram Quiz 834

- A+ Core 2 (220-1002) Practice Exam 837**
 - Answers at a Glance 855
 - Answer Explanations 856

- CHAPTER 43:**
- Getting Ready for the Exams, and Farewell 879**
 - Getting Ready for the Exams 879
 - Tips for Taking the Real Exams 882
 - General Practices for Taking Exams 882
 - Smart Methods for Difficult Questions 884
 - Wrapping Up the Exam 885
 - Beyond the CompTIA A+ Certification 885

- Index 887**

About the Author

David L. Prowse is the author of more than a dozen computer training books and video products. He has worked in the computer field for 25 years and loves to share his experience through teaching and writing.

Acknowledgments

I'd like to give special recognition to Paul Carlstroem, Chris Cleveland, Chris Crayton, Tonya Simpson, and Bill McManus. Without you, this book wouldn't have made it to the presses. I'm serious here, writing a book is tough work, and this edition of the A+ Exam Cram was the toughest to date. Thank you.

Publishing a book takes a team of professional and talented people. My thanks to everyone else at Pearson for your expertise and help throughout this project.

About the Technical Reviewer

Chris Crayton (MCSE) is an author, technical consultant, and trainer. He has worked as a computer technology and networking instructor, information security director, network administrator, network engineer, and PC specialist. Chris has authored several print and online books on PC repair, CompTIA A+, CompTIA Security+, and Microsoft Windows. He has also served as technical editor and content contributor on numerous technical titles for several of the leading publishing companies. He holds numerous industry certifications, has been recognized with many professional teaching awards, and has served as a state-level SkillsUSA competition judge.

We Want to Hear from You!

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

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

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

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

Email: community@informit.com

Introduction

Welcome to the *CompTIA A+ Core 1 (220-1001) and Core 2 (220-1002) Exam Cram*. This book prepares you for the CompTIA A+ Core 1 (220-1001) and Core 2 (220-1002) certification exams. Imagine that you are at a testing center and have just been handed the passing scores for these exams. The goal of this book is to make that scenario a reality. My name is David L. Prowse, and I am happy to have the opportunity to serve you in this endeavor. Together, we can accomplish your goal to attain the CompTIA A+ certification.

Target Audience

The CompTIA A+ exams measure the necessary competencies for an entry-level IT professional with the equivalent knowledge of at least 12 months of hands-on experience in the lab or field.

This book is for persons who have experience working with desktop computers and mobile devices and want to cram for CompTIA A+ certification exams—*cram* being the key word. This book does not cover everything in the computing world; how could anyone do so in such a concise package? However, this guide is fairly thorough and should offer you a lot of insight...and a whole lot of test preparation.

If you do not feel that you have the required experience, have never attempted to troubleshoot a computer, or are new to the field, then I recommend the following:

- ▶ Attend a hands-on A+ class with a knowledgeable instructor.
- ▶ Consider purchasing the CompTIA A+ Core 1 (220-1001) and Core 2 (220-1002) (Video Training) (9780136526643), which goes into a bit more depth than this text and shows technology concepts from a hands-on perspective.

Essentially, I have written this book for three types of people: those who want a job in the IT field, those who want to keep their job in the IT field, and those who simply want a basic knowledge of computers and want to validate that knowledge. For those of you in the first group, the latest version of the CompTIA A+ certification can have a positive career impact, increasing the chances of securing a position in the IT world. It also acts as a stepping stone to more advanced certifications. For those in the second group, preparing for the exams serves to keep your skills sharp and your knowledge up to date, helping you to remain a well-sought-after technician. For those of you in the third group, the

knowledge within this book can be very beneficial to just about any organization you might work for—as long as that organization uses computers!

Regardless of your situation, one thing to keep in mind is that I write my books to teach you how to be a well-rounded computer technician. While the main goal for this book is to help you become A+ certified, I also want to share my experience with you so that you can grow as an individual.

A person might be tempted to purchase a study guide solely for the practice exams, but I recommend against studying from practice questions *only*. This book was designed from the ground up to build your knowledge in such a way that when you get to the practice exams, they can act as the final key to passing the real exams. The knowledge in the chapters is the cornerstone, whereas the practice exam questions are the battlements. Complete the entire book and you will have built yourself an impenetrable castle of knowledge.

About the CompTIA A+ Core 1 (220-1001) and Core 2 (220-1002) Exams

This book covers the CompTIA A+ 220-1001 and 220-1002 exams, also known as Core 1 and Core 2 respectively. There are quite a few changes and additions to these versions of the A+ exams compared to the previous versions, including the following:

- ▶ Increased content concerning the troubleshooting of computer hardware and software
- ▶ Addition of Windows 10 content
- ▶ Addition of Chrome OS content
- ▶ A large increase in operational procedures content
- ▶ Addition of basic scripting
- ▶ Addition of remote access technologies
- ▶ Increased virtualization concepts

This book covers all these changes and more within its covers. It does so in a concise way that allows you to memorize the facts quickly and efficiently.

For more information about how the A+ certification can help your career, or to download the latest official objectives, access CompTIA's web page at <https://certification.comptia.org/>.

About This Book

This book is organized into two parts comprising 43 chapters, each chapter pertaining to one or more particular objectives covered on the exams. The first part of the book—Chapters 1 through 22—applies to the Core 1 (220-1001) exam. The second part of the book—Chapters 23 through 42—applies to the Core 2 (220-1002) exam. At the beginning of each of those parts you will find a handy checklist you can use as you prepare for the exams. Chapter 43 discusses how to get ready for the real exams and gives some tips and techniques for passing the exams.

For this edition of the book I decided to organize the content based on the order of the official CompTIA objectives. Typically, you will find one to three objectives per chapter. The corresponding CompTIA objective or objectives are listed verbatim in the beginning of each chapter and in the subsequent major heading(s). By organizing the book this way, you can easily locate whatever objective you want to learn more about. In addition, you can use the index or the table of contents to quickly find the concept you are after. Some chapters (such as the troubleshooting chapters) are shorter than others; this is done by design so that you can better absorb the information.

Regardless of your experience level, I don't recommend skipping content. This book is designed to be read completely. The best way to study is to read the entire book. Then, go back and review the 220-1001 portion, and take the real CompTIA 220-1001 exam. Afterward, review the 220-1002 portion, and take that exam. The reason for this is because the two exams are inextricably linked. It's a good idea to get the whole picture first, and then break it down by the exam. While this might not be possible based on time constraints, I still must strongly recommend it as the best study method.

Note

I do *not* recommend taking both exams on the same day. Instead, space them apart by at least a week to give you time to prepare.

Chapter Format and Conventions

Every Exam Cram chapter follows a standard structure and contains graphical clues about important information. The structure of each chapter includes the following:

- ▶ **Opening topics list:** This defines the CompTIA A+ objective(s) to be covered in the chapter.

- ▶ **Topical coverage:** The heart of the chapter, this explains the topics from a hands-on and a theory-based standpoint. This includes in-depth descriptions, tables, and figures geared to build your knowledge so that you can pass the exams.
- ▶ **Cram Quiz questions:** At the end of each topic is a quiz. The quizzes, and ensuing explanations, are meant to help you gauge your knowledge of the subjects you have just studied. If the answers to the questions don't come readily to you, consider reviewing individual topics or the entire chapter. In addition to being in the chapters, you can find the Cram Quiz questions within the book's companion web page at www.pearsonitcertification.com. The questions are separated into their respective 220-1001 and 220-1002 categories for easier studying when you approach each exam.
- ▶ **Exam Alerts, Sidebars, and Notes:** These are interspersed throughout the book. Watch out for them!

ExamAlert

This is what an Exam Alert looks like. An alert stresses concepts, terms, hardware, software, or activities that are likely to relate to one or more questions on the exams.

Additional Elements

Beyond the chapters, there are a few more elements that I've thrown in for you. They include

- ▶ **Practice Exams:** These are located at the end of Part I and Part II. There is one for each CompTIA A+ exam. These practice exams (and additional exams) are available as part of the custom practice test engine at the companion web page also. They are designed to prepare you for the multiple-choice questions that you will find on the real CompTIA A+ exams.
- ▶ **Real-World Scenarios:** These are located on the companion web page as PDFs. They describe actual situations with questions that you must answer and potential solutions with supporting videos and simulations. These are designed to help prepare you for the performance-based questions within the real CompTIA A+ exams.
- ▶ **Cram Sheet:** The tear-out Cram Sheet is located in the beginning of the book. This is designed to jam some of the most important facts you need

to know for each exam into one small sheet, allowing for easy memorization. It is also in PDF format on the companion web page. If you have an e-book version, this might be located elsewhere in the e-book; run a search of the term “cram sheet” and you should be able to find it that way.

The Hands-On Approach

This book refers to two different computers as the following:

- ▶ **VM-House:** I built this rackmount server computer in September of 2018. It is a Xeon-based system that is designed to house all of my virtual machines and serve them to my workstations.
- ▶ **AV-Editor:** I built this desktop computer in July of 2015. It is an Intel Core i7 system and is designed to act as a powerful audio/video editing workstation. It has been my main workstation since then.

Note

The previous edition of this book included computers known as *Media PC* and *Tower PC*. Those were built in 2012 and 2009, respectively, and as such are based on older technologies. I have removed references to them from this edition of the book, but you can find information about them at my website: <https://dprocomputer.com>.

I built these systems using components that are good examples of what you will see in the field. These components are representative of the types of technologies that will be covered in the exams. I refer to the components throughout the book because I like to put things into context whenever possible. By referencing computers in actual scenarios presented in many of the chapters, I hope to infuse some real-world knowledge and to solidify the concepts you need to learn for the exams. This more hands-on approach can help you to visualize concepts better. I recommend that every computer technician build their own computer at some point (if you haven't already). This can help to reinforce the ideas and concepts expressed in the book.

You should also work with multiple operating systems while going through this book: namely Windows 10, Windows 8.1, and Windows 7. (Not to mention macOS, Linux, Android, iOS, and Chrome OS.) Or you might attempt to create a dual-boot on a single hard drive. Another option is to run one computer with one of the operating systems mentioned and virtual machines running the other operating systems. However, if at all possible, the best way to learn is to run individual computers. This will ensure that you discover as much as possible about the hardware and software of each computer system and how they interact with each other.

This book frequently refers to various support websites. Have a browser open all the time and be ready to perform more research as you read through the book.

Goals for This Book

I have three main goals in mind while preparing you for the CompTIA A+ exams.

My first goal is to help you understand A+ topics and concepts quickly and efficiently. To do this, I try to get right to the facts necessary for the exam. To drive these facts home, the book incorporates figures, tables, real-world scenarios, and simple, to-the-point explanations. Also, in the introductions for the Core 1 and Core 2 sections, you will find preparation checklists that give you orderly, step-by-step approaches to taking the exams. Be sure to complete all items on the checklists! For students of mine who truly complete every item, there is an extremely high passing rate. Finally, in Chapter 43, you will find some important test-taking tips that I've developed while sitting dozens of exams over the years.

My second goal for this book is to provide you with an abundance of *unique* questions to prepare you for the exams. Between the Cram Quizzes and the practice exams, that goal has been met, and I think it will benefit you greatly. Because CompTIA reserves the right to change test questions at any time, it is difficult to foresee exactly what you will be asked on the exams. However, to become a good technician, you must know the *concept*; you can't just memorize questions. Therefore, each question has an explanation and maps back to the chapter covered in the text. I've been using this method for more than a decade with my students (more than 3000 of them) and with great results.

Good luck in your certification endeavors. I hope you benefit from this book. Enjoy!

Sincerely,

David L. Prowse

Figure Credits

Figure 1-1 from David Prowse.
Figure 1-2 from David Prowse.
Figure 1-3 from David Prowse.
Figure 2-1 from David Prowse.
Figure 2-2 from David Prowse.
Figure 3-1a, Mini-USB Type B port, from David Prowse.
Figure 3-1b, Micro-USB Type B port, from David Prowse.
Figure 3-1c, USB-C port, from David Prowse.
Figure 3-1d, lightning connector, from David Prowse.
Figure 3-1e, USB-C connector, from David Prowse.
Figure 3-1f, Micro-USB Type B connector, from David Prowse.
Figure 3-1g, Mini-USB Type B connector, from David Prowse.
Figure 4-5 from David Prowse.
Figure 5-2, screenshot of RDP © Microsoft 2019.
Figure 6-3, screenshot of Wireless Properties © Microsoft 2019.
Figure 6-4 courtesy of Cisco Systems, Inc. Unauthorized use not permitted.
Figure 7-1, screenshot of Windows configuration © Microsoft 2019.
Figure 8-2a, wire stripper, from Pearson Education.
Figure 8-2b, punchdown tool, from Pearson Education.
Figure 8-2c, cable tester, from Pearson Education.
Figure 8-2d, RJ45 crimper, from Pearson Education.
Figure 8-2e, patch tester, from Pearson Education.
Figure 8-2f, tone generator, from Pearson Education.
Figure 8-2g, RJ45 lookback plug, from Pearson Education.
Figure 8-3, screenshot of Wi-Fi Analyzer © 2019 Adrian Granados.
Figure 9-1, wires organized for the 568B standard, from Pearson Education.
Figure 9-2a, RJ45 plugs, from Pearson Education.
Figure 9-2b, RJ11 plugs, from Pearson Education.
Figure 9-3a, ST connectors, from Pearson Education.
Figure 9-3b, SC connectors, from Pearson Education.
Figure 9-4a, DVI Typical video ports, from David Prowse.
Figure 9-4b, VGA, from David Prowse.
Figure 10-1 from Pearson Education.
Figure 10-2 from Pearson Education.
Figure 10-3 from Pearson Education.
Figure 10-4, screenshot of Task Manager © Microsoft 2019.
Figure 10-5 from Pearson Education.
Figure 10-6 from David Prowse.
Figure 10-9 from Pearson Education.
Figure 11-1 from Pearson Education.
Figure 11-2 from Pearson Education.
Figure 11-3 from Pearson Education.
Figure 11-4a from Pearson Education.
Figure 11-4b from Pearson Education.
Figure 11-5, screenshot of Boot Manager © Microsoft 2019.
Figure 12-1 from Pearson Education.
Figure 12-2 from Pearson Education.
Figure 13-1 from David Prowse.
Figure 13-2, screenshot of Task Manager © Microsoft 2019.
Figure 13-3 from David Prowse.
Figure 13-4a, 24-pin ATX CPU connectors, from David Prowse.
Figure 13-4b, EATX12V 8-pin CPU connectors, from David Prowse.
Figure 13-5a, SATA power connector, from David Prowse.
Figure 13-5b, Molex power connector, from David Prowse.
Figure 13-5c, PCIe power connector, from David Prowse.
Figure 13-6 from Pearson Education.
Figure 14-1, screenshot of VMware Workstation © 1998-2014 VMware, Inc.
Figure 14-2, screenshot of Task Manager © Microsoft 2019.
Figure 15-1, screenshot of configuring printing © Microsoft 2019.
Figure 16-1, screenshot of Windows Features © Microsoft 2019.
Figure 16-2, screenshot of Hyper-V Manager © Microsoft 2019.
Figure 16-3, screenshot of Virtual VM VirtualBox © Oracle.

Figure 17-1, screenshot of Event Viewer © Microsoft 2019.
Figure 18-1 from David Prowse.
Figure 19-1, screenshot of Intel RAID © Intel Corporation.
Figure 19-2, screenshot of Storage Manager © 2019 Google.
Figure 20-1 from David Prowse.
Figure 21-1, screenshot of Microsoft Windows © Microsoft 2019.
Figure 21-2, screenshot of Microsoft Windows © Microsoft 2019.
Figure 21-3, screenshot of Microsoft Windows © Microsoft 2019.
Figure 21-3-3, screenshot of Google Chrome © 2019 Google.
Figure 23-4, screenshot of Microsoft Windows © Microsoft 2019.
Figure 23-5, screenshot of Microsoft Windows © Microsoft 2019.
Figure 24-1, screenshot of Windows 10 boot drive © Microsoft 2019.
Figure 24-2, screenshot of Windows 10 boot drive © Microsoft 2019.
Figure 26-1, screenshot of Computer Management window © Microsoft 2019.
Figure 26-2, screenshot of MMC © Microsoft 2019.
Figure 26-3, screenshot of Device Manager © Microsoft 2019.
Figure 26-4, screenshot of Performance Monitor © Microsoft 2019.
Figure 26-5, screenshot of Mscconfig © Microsoft 2019.
Figure 26-6, screenshot of Windows Task Manager © Microsoft 2019.
Figure 26-7, screenshot of System Configuration utility © Microsoft 2019.
Figure 27-1, screenshot of Computer Management window © Microsoft 2019.
Figure 27-2, screenshot of NTFS folder © Microsoft 2019.
Figure 27-3, screenshot of System Properties dialog box © Microsoft 2019.
Figure 27-4, screenshot of Windows 10 DxDiag © Microsoft 2019.
Figure 27-5, screenshot of Registry Editor in Windows © Microsoft 2019.
Figure 28-1, screenshot of Internet Properties dialog box © Microsoft 2019.
Figure 28-2, screenshot of Folder Options dialog box © Microsoft 2019.
Figure 28-3, screenshot of Camtasia Studio © TechSmith.
Figure 28-4, screenshot of Sound dialog box © Microsoft 2019.
Figure 29-1, screenshot of Domain Changes dialog box © Microsoft 2019.
Figure 29-2, screenshot of Right-clicking © Microsoft 2019.
Figure 29-3, screenshot of Data Properties © Microsoft 2019.
Figure 29-4, screenshot of Map Network Drive window © Microsoft 2019.
Figure 29-5, screenshot of Add Printer window © Microsoft 2019.
Figure 29-6, screenshot of Set up a new connection © Microsoft 2019.
Figure 29-7, screenshot of LAN Settings dialog box © Microsoft 2019.
Figure 29-8, screenshot of IPv4 Properties dialog box © Microsoft 2019.
Figure 30-1, screenshot of Ubuntu © 2019 Canonical Ltd.
Figure 30-2, screenshot of Ubuntu © 2019 Canonical Ltd.
Figure 31-1, screenshot of Domain Controller in Active Directory © Microsoft 2019.
Figure 31-2, screenshot of Local Security Policy © Microsoft 2019.
Figure 31-3, screenshot of Firewall exceptions © Microsoft 2019.
Figure 32-1, screenshot of Manual Wireless Network Connection © Microsoft 2019.
Figure 32-2, screenshot of WPA2-Enterprise © Microsoft 2019.
Figure 33-1, screenshot of New User Window © Microsoft 2019.
Figure 33-2, screenshot of Group Membership © Microsoft 2019.
Figure 33-3, screenshot of Security tab © Microsoft 2019.
Figure 33-4, screenshot of Advanced Security Settings © Microsoft 2019.
Figure 33-5, screenshot of Windows Shares © Microsoft 2019.
Figure 33-6, screenshot of Local Security Policy © Microsoft 2019.
Figure 33-7, screenshot of Logon Hours Setting © Microsoft 2019.
Figure 36-1, screenshot of Windows 10 © Microsoft 2019.
Figure 36-2, screenshot of Windows 10 © Microsoft 2019.
Figure 36-3, screenshot of Startup and Recovery window © Microsoft 2019.
Figure 37-1, screenshot of System Properties © Microsoft 2019.
Figure 39-2, screenshot of Windows Backup screen © Microsoft 2019.
Figure 39-3, screenshot of Windows Backup screen © Microsoft 2019.
Figure 39-4, screenshot of Protecting a user account © Microsoft 2019.
Figure 42-1, screenshot of PowerShell ISE © Microsoft 2019.
Figure 42-2, screenshot of Remote Desktop Connection © Microsoft 2019.
Figure 42-3, screenshot of PuTTY © Simon Tatham.

CHAPTER 3

Smartphones, Tablets, and Other Mobile Devices, Part 1

This chapter covers the following A+ 220-1001 exam objectives:

- ▶ **1.4** – Compare and contrast characteristics of various types of other mobile devices.
- ▶ **1.5** – Given a scenario, connect and configure accessories and ports of other mobile devices.

Welcome back! Now we'll think small; I'm talking about mobile devices such as tablets and smartphones. These are designed to be smaller than laptops, but with a limited loss of productivity in comparison to their larger brethren. For some work-related tasks—and for the general public—a laptop can be a bit unwieldy, and is a lot less “mobile” than a typical tablet or smartphone. That said, you will find that some organizations will opt to provide smaller devices for some of their users. What does this mean for you? It means that you need to know the different types of mobile devices available to users, but more importantly, you must be well-informed about those devices' connection types and accessories, and how to go about connecting and configuring them. So, think small, but remember the amazing power, and limitations, of these mobile devices. Onward!

1.4 – Compare and contrast characteristics of various types of other mobile devices

ExamAlert

Objective 1.4 focuses on the following concepts: tablets, smartphones, wearable technology devices (such as smart watches, fitness monitors, and VR/AR headsets), e-readers, and GPS.

This objective requires you to understand the differences between tablets, smartphones, e-readers, GPS devices, and wearable tech devices. You should be able to distinguish between one and another by looking at them, by analyzing the ports they use, and by being familiar with the uses for each type of device. Remember this: instead of thinking in terms of manufacturers, think in terms of technology types and uses. By this I mean don't worry too much about the popular brands of the day and instead think more in terms of what and how a device is supposed to perform for the user.

Tablets

A tablet computer, or simply “tablet,” is a thin, mobile device that is operated with a touchscreen and generally measures between 6 and 11 inches diagonally. It can be used for simple tasks such as reading books and browsing the Internet, but can also be used for more complex tasks such as word and spreadsheet processing, audio and video recording/editing, multimedia live streaming, photo editing, collaboration, and even programming. The more complex the task, the more powerful the tablet that is required.

A typical tablet as of the writing of this book might have hardware specifications similar to what you see in Table 3.1.

TABLE 3.1 **Typical Tablet Hardware Specifications**

Hardware Component	Description
1.85-GHz ARMv8 CPU	64-bit system on a chip (SoC) Example: A9 CPU + M9 motion coprocessor Note: This is as of early 2019. Also, there are more powerful models. This is just one mid-range example.
2-GB LPDDR4 RAM	Mobile DDR—similar DDR standard to what PCs use, but a much smaller form factor, and is included in the SoC
32- or 128-GB flash memory	Similar to solid-state flash memory in a USB flash drive Used for permanent storage
Multitouch touchscreen	Capacitive touchscreen that responds to one or more fingers and proprietary stylus devices
9.7-inch display (diagonal) LED-backlit widescreen multitouch display with in-plane switching (IPS) technology	Quad Extended Graphics Array (QXGA), 2048×1536 resolution 4:3 aspect ratio

Hardware Component	Description
Lithium-ion polymer battery (nonremovable)	Similar to lithium-ion batteries in laptops Can be made into any shape 8827 mAh (milliamp hours); 32.4 watt-hour; lasts for 10 hours on a full charge (typical usage)
High-definition cameras	Main camera: 8 megapixel, 1080p video recording Second camera: 1.2 megapixel, 720p video recording

ExamAlert

Be able to read and understand the typical specs of a mobile device.

As you can see from the table, the whole concept of this hardware configuration is based on portability and ease of use. Therefore, tablet computers are generally less powerful than desktop computers and laptops, but the hardware is matched to the type of applications the device will be used for.

The two main goals for tablets are to be highly portable and have powerful processing capabilities. One way this is accomplished is by using a system on a chip (SoC), which combines the CPU, RAM, storage, and more on one single substrate—essentially it is a system unto itself. The most common microarchitecture used for the SoC of a tablet is called ARM, which is a type of reduced instruction set computing (RISC). An ARM-based CPU uses fewer transistors than a CPU found in a PC or laptop, which makes it a great choice for portable systems that need lower power consumption while still maintaining a decent amount of processing power.

Apple iPads run iOS as their operating system and make use of the proprietary Lightning connector, or the USB-C connector, to charge and to transmit data. Similar tablets that are Android-based often use standardized USB-C, or Micro-USB, ports for charging and synchronization of data. iPads are well-known as some of the most powerful tablet computers on the market, and as such have been used heavily for media creation and editing. This type of work would not be possible on a lesser tablet. So, choose the right tool for the job, and choose wisely!

Smartphones

A smartphone is a type of mobile phone that has much more processing power and greater hardware capabilities than a basic feature phone. A basic feature phone is designed primarily to place voice calls and do texting, but

a smartphone is essentially a high-powered computer in the palm of your hand, allowing for desktop-like web browsing, high-definition playback of videos, and the downloading and usage of apps that can do just about anything you can think of. Smartphones also act as high-powered cameras, recording devices, music players, and personal assistants, among many other things. Remember, they are computers (though small), and as such, you are required to be able to troubleshoot and repair them.

A typical smartphone as of the writing of this book might have hardware specifications similar to what you see in Table 3.2.

TABLE 3.2 **Typical Smartphone Hardware Specifications**

Hardware Component	Description
2.45-GHz ARM CPU	Snapdragon 835 64-bit system SoC
4-GB LPDDR4 RAM	Mobile DDR version 4
32-, 64-, 128-, or 256-GB flash memory	Similar to solid-state drives' flash memory
Multitouch touchscreen	Capacitive touchscreen
Lithium-ion polymer battery (aka li-ion or li-po)	3300 mAh (nonremovable) Typically 20 to 25 hours (talktime)
6.0-inch display	Quad HD+ (QHD+), 2880×1440 resolution 18:9 aspect ratio
Dust and water proof	IP68 compliant

ExamAlert

Memorize the basic types of hardware used by a smartphone.

Those are just some of the specs of a typical smartphone. Here's an assignment for you: Go on the Internet and research the specs for *your* phone. Try to understand all of the terminology being used on the spec sheet. If you don't know a term, look it up and then try to relate that technology to your own device.

Just about all smartphones come with cellular access, be it 3G, 4G, LTE, 5G, and so on. This differs from tablets in that a tablet often will *not* come with cellular access, but it can be added with an upcharge.

IP Code

Some smartphones and other handheld computers are certified as being ingress protection (IP) compliant. Ingress protection means protection against dust and water, which are tested separately. There are a lot of different IP ratings, but let's use the IP68 example in the last row of Table 3.2. The first digit, 6, deals with dust and means that the device is dust tight and that no ingress of dust can occur. The second digit, 8, means that the device can be immersed in water up to and beyond 1 meter, generally for 30 minutes, though this can vary. The exact depth and length of time is up to the manufacturer, so IP68 could be slightly different from one smartphone to the next. You might also see IP67-compliant devices, which is very similar but means immersion only *up to* 1 meter for 30 minutes.

Other devices might be listed as IP65 compliant, which means they are dust tight and can protect from water jets for up to 3 minutes. The number associated with water protection is not cumulative, so if a device needs to be protected from water jets *and* immersion in water, it would, for example, have to be tested for IP65 *and* IP68 compliance. Many specialized handheld computers in the military (as well as in the medical, transportation, and surveying markets) meet both of these requirements, whereas consumer products might only meet IP68 or IP67 (depending on their age). What does this mean to the customer? Don't bring the device in the shower or spray it with a hose! It might survive, but it probably won't because it isn't tested for that type of abuse. You should also remember that some consumer smartphones do not meet any IP requirements and must be treated accordingly. In that case, if a device is damaged during use in a dusty environment or sprayed with or immersed in water, the warranty might become void. Familiarize yourself with the IP code. You can find it in various locations on the Internet, and you can get the authorized standard from the International Electrotechnical Commission (IEC).

ExamAlert

Understand what IP68 and similar IP ratings mean.

Note

Military usage often requires that devices are compliant with the MIL-STD-810 standard. This describes the lab testing of devices based on environmental conditions that are expected over the lifespan of the device. This standard is used commercially also.

Wearable Technology Devices

Moving outside of mobile devices, let's briefly discuss wearable technology. This concept has become quite the trend in recent years. One of the most common (as of the writing of this book) is the smartwatch. Initial product offerings required that a smartphone be nearby (with the watch connecting via Bluetooth), but newer versions are network-ready, meaning that you can use the smartwatch on Wi-Fi networks, and possibly cellular networks, increasing the usability (and range) of the device. Most of these allow a user to answer calls and communicate by e-mail and text. (If you like obscure references, you could say that Dick Tracy technology has finally arrived!)

Another common example of wearable technology is a fitness monitor, which is worn on the wrist or elsewhere and used by people who want to track their exercise routines and for physical rehabilitation purposes. They connect to compatible smartphones and tablets. However, most smartwatches also include fitness monitoring apps. Other wearable technology includes enhanced glasses (which can take photos and send them to your mobile device), specialized Bluetooth earpieces and headsets, and virtual/augmented reality headsets. Virtual reality (VR) headsets are used for gaming, watching movies, simulations, and so forth. Augmented reality (AR) headsets and glasses use holograms and other technology to overlay images on top of what a person actually sees (in the real world, that is—I know it's getting hard to tell what's real and what's not!).

The list keeps going when it comes to how you can add on to your mobile device. As a technician, you should understand that many of these wearable tech devices connect via Bluetooth (which might require a PIN code) and that Bluetooth has a limited range—usually 33 feet (10 meters). Some can work independently of the mobile device, but you would need to configure them to connect to Wi-Fi and/or cellular. You would do so by setting up a connection profile and/or by allowing automatic connections to “open,” which means using unsecured Wi-Fi networks. We discuss Bluetooth, Wi-Fi, and cellular in more depth later in the book, but for now, remember that wearable devices' wireless connections can fail and at times need to be troubleshoot like any other wireless device.

E-readers

By far the most common e-reader is the Amazon Kindle, but there are other brands as well. A true e-reader uses electronic paper technology—which is generally black and white—making longer-term reading easier on the eyes when

compared to reading on a tablet or a smartphone. However, e-readers are not great when it comes to surfing the Web, though some do have Internet access. For some people, the e-reader is the only way to go because of how easy it is on the eyes, and because it displays text well both in dark environments and in sunlight. Plus, battery life is far superior to tablets and smartphones. Most manufacturers of these devices also allow users to read their digital libraries by installing a reader app to their tablets or smartphones (or PCs) and synchronizing between the devices. E-readers are often charged via Micro-USB, and many can connect via Wi-Fi or with a cellular connection to facilitate the downloading of book files.

GPS Devices

If you have a smartphone, you probably use some kind of Global Positioning System (GPS) app, but there are also dedicated smart GPS systems for your car that can work independently, and possibly integrate with your smartphone and social media via Wi-Fi and Bluetooth. The beauty of these is that the bulk of the CPU in the device is dedicated to GPS. If you have ever run GPS on a smartphone while other apps are running—and you experience slow performance—then you can understand why a dedicated GPS system might be a valid option for delivery drivers, those in the transportation industry, or those who simply want more accurate and efficiently presented GPS data.

Many vehicles offer systems with touchscreens that can integrate with a person's smartphone. Basic versions are enabled via Bluetooth and can perform voice and text services. But in some cases, depending on the model and version of the vehicle, they will allow connectivity of CarPlay (Apple) and Android Auto. These are smartphone screen-mirroring programs that can display the GPS app for easier viewing. They can also control voice calls, text messaging, music playing, and more. Aftermarket head units are available as well. To utilize these systems, the vehicle must be compatible, the smartphone must have the correct app installed, and it is often connected in a wired fashion via USB. In this scenario, a technician should make sure that the vehicle's firmware and software are updated, that the smartphone's vehicle connectivity software and GPS software are updated, and that a *quality* cable is used.

The Internet of Things (IoT)

Collectively, tablets, smartphones, e-readers, and other mobile devices—not to mention their wearable counterparts—make up a portion of the “Internet of Things” (IoT). The IoT is the global network of physical objects which have embedded processors (of some sort) that can communicate with computers across the Internet. IoT devices also include household appliances such as smart refrigerators, digital thermostats, home automation devices, and so on. I’ve simplified the concept greatly, but for the purposes of this book, it should suffice. This is a buzz term that you will no doubt encounter more and more. But know that the IoT isn’t limited to just personal devices; it also includes devices used in the medical, manufacturing, and transportation industries, among others. Depending on the organization you work for, you will need to install, configure, secure, and troubleshoot a specific subset of IoT devices. Regardless, if you apply the methods and techniques in this book, you will be able to work with any device—in any market.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Which of the following is *not* a mobile device?
 - A. Tablet
 - B. Smartphone
 - C. Desktop PC
 - D. E-reader

2. Which type of memory do most mobile devices store long-term data to?
 - A. LPDDR4
 - B. SATA magnetic disk
 - C. SATA SSD
 - D. Solid-state flash memory

3. You have been tasked with connecting a wireless earpiece to a smartphone. Which technology would you most likely use?
 - A. Wi-Fi
 - B. NFC
 - C. 3.5 mm
 - D. Bluetooth

4. You have been tasked with setting up a device for a salesperson's vehicle. It should be able to display maps and give directions to the person while driving. Which of the following devices would perform these tasks? (Select the two best answers.)
- A. GPS
 - B. Smart camera
 - C. Smartphone
 - D. E-reader
 - E. VR headset

Cram Quiz Answers

1. **C.** The desktop PC is not a mobile device. It is a stationary computer that is meant to stay at a person's desk. Tablets, smartphones, and e-readers are all examples of mobile devices.
 2. **D.** Most mobile devices store their long-term data to solid-state flash memory. They do not use SATA as the method of connectivity. LPDDR4 is a common type of RAM used in mobile devices for short-term storage.
 3. **D.** When connecting an earpiece (those little cricket-looking devices) to a smartphone, you would most likely use Bluetooth—just remember that most of them have a 30-foot range (10 meters). Wi-Fi is less likely to be used; it is more likely to be used to connect the smartphone to the LAN and ultimately to the Internet. NFC (discussed in the next section) is used to transmit data between mobile devices in close proximity to each other. 3.5 mm refers to the audio port on a mobile device. It is quite possible that a user will utilize a wired headset, but the question focuses on wireless.
 4. **A and C.** A standalone GPS device or a smartphone (equipped with a GPS app) would do the job here. Both can display maps and give directions to a person while driving. The other devices are not designed to function in this manner.
-

1.5 – Given a scenario, connect and configure accessories and ports of other mobile devices

ExamAlert

Objective 1.5 focuses on the following concepts: wired connection types such as Micro-USB, Mini-USB, USB-C, and Lightning; wireless connectivity such as NFC, Bluetooth, and IR; and accessories such as memory cards, credit card readers, headsets, speakers, game pads, batteries, protective covers, and more.

Mobile device connectivity is imperative. For the exam, you need to know the physical ports used for charging and synchronizing, and for communicating with external devices. Then of course there are various wireless connectivity options available on today's mini-powerhouse computers. Let's not forget that people love to accessorize: headsets, speakers, add-on memory, the list is too long.... To simplify: be ready to provide support for a plethora of ports and gadgets!

Connection Types

Depending on what you need to accomplish with your mobile device, you might require a wired or a wireless connection. Let's discuss these now.

Wired Connections

Wired connections use physical ports. If you have ever plugged in a mobile device to charge it, then you have used a wired connection.

The most common wired connection is USB. USB has been around for a long time and has gone through several versions and port changes. USB is used by devices that run Android (among others). However, aside from USB-C, iOS-based devices from Apple use the proprietary Lightning connector or the older 30-pin dock connector (which is much wider). Figure 3.1 shows examples of the ports and connectors that you should know for the exam, including Mini-USB, Micro-USB, USB-C, and Lightning.

1.5 – Given a scenario, connect and configure accessories and ports of other mobile devices

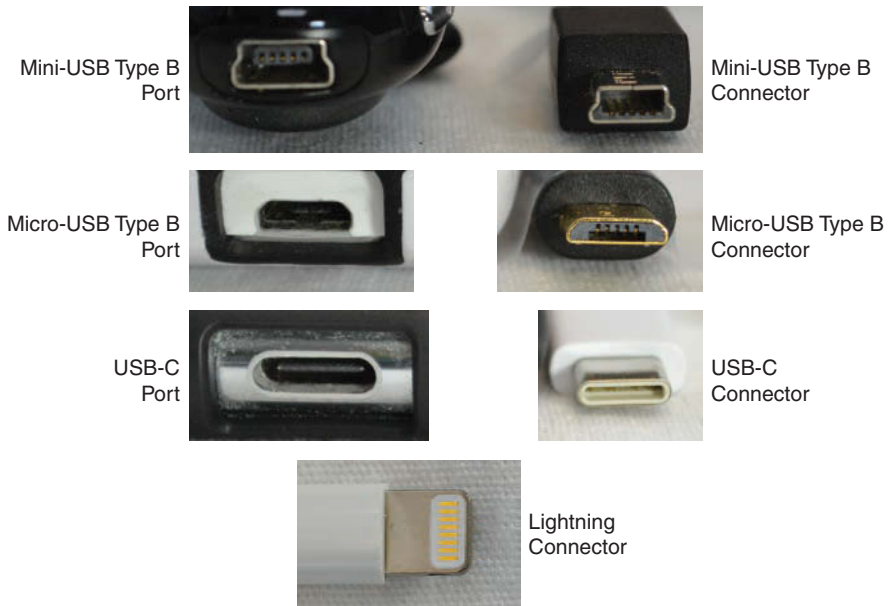


FIGURE 3.1 USB and Lightning ports and connectors

If you charge a device, almost all charging cables will use a standard Type A USB port on the other end, regardless of the connector type that is used to attach to the device. That allows connectivity to the majority of charging plugs and PCs and laptops in the world. However, there are tons of adapters out there, so be ready.

At the time of writing, USB-C has become common for many Android-based smartphones and some tablets. Most likely, USB-C (and other ports) will continue to gain acceptance compared to Micro-USB, which was used by Android devices almost exclusively for a decade. For example, after years and years, and several generations of devices to use Micro-USB, the Samsung S8 was the first of that series to use the USB-C port, and in 2019 the iPad Pro began using USB-C as well. On the other hand, Mini-USB is quite uncommon, but you might see it on older devices, especially accessories for smartphones.

ExamAlert

Know your mobile device ports and connectors. Remember that Android devices will generally use USB-C or Micro-USB, and iOS-based devices will use USB-C, Lightning, or the 30-pin dock connector.

Note

We'll cover more about ports and connectors in Chapter 9, "Cables and Connectors."

Another purpose of the wired port is to have the ability to tether the mobile device to a desktop or laptop computer (usually via the computer's USB port). This tethering can allow a desktop computer or laptop to share the mobile device's Internet connection. Tethering functionality can be very useful in areas where a smartphone has cellular access but the PC/laptop cannot connect to the Internet. Once the physical USB connection is made, the setting for this can be found in **Networking > Tethering > USB Tethering**, or something similar (you will usually find the Mobile Hotspot option there as well). Keep in mind that Wi-Fi capability on the smartphone will usually be disabled when USB tethering is enabled, and that the user must have hotspot service with their cellular provider for USB tethering to work. Also, depending on the operating system, the PC or laptop that is connected to the smartphone might need a driver installed to communicate with it via USB. Finally, the tethered connection might render current LAN connections on the PC inoperable.

Note

Older versions of smartphone operating systems allowed for the reverse, where a smartphone would use a PC's Internet connection—this is known as USB Internet and is still a possibility, though it is not commonly used.

Wireless Connections

Wireless technologies are what really make a smartphone attractive to users. It's a fact, most people would rather do without cables, so technologies such as Bluetooth, NFC, IR, and hotspots make a smartphone functional, and easier to use.

Given the inherent mobility of smartphones and tablets, most technologies regarding communications and control are wireless. If designed and configured properly, wireless connections offer ease of use, efficiency, and even great speed. We'll discuss Wi-Fi, cellular, GPS, and similar data-related wireless technologies later in the book. For now, let's focus on wireless connections used by mobile devices to communicate with accessories and other mobile devices.

1.5 – Given a scenario, connect and configure accessories and ports of other mobile devices

One of the most common technologies used is Bluetooth. This is a technology that allows users to incorporate wearable technology (such as headsets, earpieces, earbuds, and smartwatches) with their existing mobile devices. But the technology goes much farther; for example, it allows for the streaming of music to external speakers and an automobile's music system. However, Bluetooth is usually limited to about 33 feet (10 meters), which is the maximum transmission distance for Class 2 Bluetooth devices.

Another commonly used wireless technology is the mobile hotspot. When enabled on a properly equipped smartphone or tablet (with 4G or faster connection), it allows a user to connect desktops, laptops, and other mobile devices (wirelessly, of course) through the device running the hotspot, ultimately allowing access to the Internet. This can be a great way to connect your laptop or other computer if Wi-Fi goes down, often with speeds rivaling wired Internet access. But remember, there's usually a catch! Many providers charge for data usage (unless you have a corporate plan). Because of this, it is often used as a secondary connection or as a backup plan. In addition, the further the hotspot-enabled mobile device is from a cell tower, the lower the data transfer rate. So know the pros and cons of running a hotspot on your mobile device.

ExamAlert

Understand the difference between configuring USB tethering and creating a mobile hotspot.

Next, let's discuss near field communication (NFC). This allows smartphones to communicate with each other via radio frequency by touching the devices together or, in some cases, by simply having them in close proximity to each other. NFC uses the radio frequency 13.56 MHz and can transmit 100 to 400 kb/s. It doesn't sound like much—it transfers slower than Bluetooth for example—but it's usually plenty for sending and receiving contact information, MP3s, and even photos. Besides working in peer-to-peer mode (also known as ad hoc mode), a full NFC device can also act like a smart card performing payment transactions and reading NFC tags. If you are not sure whether your device supports NFC, check the settings in the mobile OS. Most smartphones incorporate NFC technology.

ExamAlert

NFC is used for close-proximity transactions, such as contactless payments.

Another wireless technology used by some smartphones and tablets is infrared (IR). Though it is not included on many flagship smartphones as of 2017, some mobile devices come with an IR blaster that can take control of televisions and some other devices (given they have the proper app installed). Infrared works on a different (and higher) frequency range than Wi-Fi, Bluetooth, and cellular connections, so it does not interfere with those technologies when it is used. Because so many appliances and electronics are “smart” enabled, the IR blaster becomes less important on today’s smartphones.

Accessories

Well, a person has to accessorize, right? It almost seems a requirement with today’s mobile devices. Probably the number one thing that people do to augment their device is to protect it. That means using protective covers or cases, plastic or glass-based screen protectors, waterproofing, car mounts, and so on.

Then there’s add-on storage. You can never have enough memory, right? Adding long-term storage is usually accomplished with the addition of a microSD card, for example 32, 64, or 128 GB. It is common for people who shoot a lot of videos (or a whole lot of photos) to need more memory than the mobile device comes with when purchased. Some devices allow for add-on storage via a slide-out tray on the side of the device. Others don’t allow upgrades. Older devices that can have the back cover removed can be upgraded internally.

Next on the list are audio accessories. The 3.5 mm audio jack (*if you have one*) allows a user to connect headsets, earbuds, or small speakers. Or you can connect a 3.5 mm to 3.5 mm cable from your phone to the auxiliary port of your car radio or your all-in-one music device—though Bluetooth is usually the easier option. When it comes to music, you can connect a mobile device to anything (given the right cable or adapter): stereos or TVs, and you can even use the device when performing live. The possibilities are endless. And today’s mobile device audio ports can be programmed in such a way as to accept special credit-card readers and a host of other devices. Appliance repair persons and other maintenance workers that need to be paid onsite will often make use of this technology, though that can also be accomplished in a wireless fashion.

Getting a bit more advanced, you will also see devices such as game pads that can connect to the Micro-USB port using On-The-Go (OTG) USB technology. However, most game pads will connect wirelessly, either via Bluetooth or through Wi-Fi.

1.5 – Given a scenario, connect and configure accessories and ports of other mobile devices

Most of today's devices cannot be opened by the consumer without voiding the warranty. So, replacing a battery is not as easy as it once was. To do this, a heat gun and proper shims are required. However, if not done correctly, it can defeat the IP rating. That's why manufacturers require that battery replacements be done by an authorized repair center. More important when it comes to accessories are battery chargers. Smartphones and tablets can be charged with their included AC chargers, or possibly with wireless chargers, where the unit is laid down directly on the charger. A user might also opt to use a power brick which stores a charge for a long time. Keep in mind that these "bricks" (also known as battery packs or battery charges) take a long time to charge up themselves.

We could go on for days about the accessories available for mobile devices, but that should be enough for the exams. Remember, protecting the mobile device and memory capacity are crucial. The rest of the things we discussed enable a user to increase functionality, or just plain make it more fun, but these things are usually not essential to the device performing its job. Plus, in a bring your own device (BYOD) or choose your own device (CYOD) environment, the users will often be quite limited when it comes to accessorizing. This is to prevent compatibility issues, which lead to lower productivity, and to avoid security vulnerabilities.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Which type of charging connector would you find on an iPad?
 - A. Micro-USB
 - B. Lightning
 - C. Thunderbolt
 - D. IP68
2. You are required to add long-term storage to a smartphone. Which type would you most likely add?
 - A. DDR4
 - B. microSD
 - C. LPDDR4
 - D. SSD
 - E. SIM

3. The organization you work for allows employees to work from their own mobile devices in a BYOD manner. You have been tasked with setting up the devices so that they can “beam” information back and forth between each other. What is this known as?
- A. Mobile hotspot
 - B. IoT
 - C. CYOD
 - D. IR
 - E. NFC
4. Which of the following can be useful in areas where a smartphone has cellular access but the PC (or laptop) cannot connect to the Internet?
- A. Proprietary vendor-specific connector
 - B. Accessories
 - C. IP codes
 - D. Tethering

Cram Quiz Answers

220-1001 Answers

1. **B.** The Lightning connector is one of Apple's proprietary charging and synchronization connectors used by iPads and iPhones, although Apple also uses USB-C. Micro-USB is used by older Android-based mobile devices—while USB-C is more common on newer devices. Thunderbolt is a high-speed hardware interface used in desktop computers, which we will discuss more in Chapter 9. IP68 deals with ingress protection from dust and water jets.
2. **B.** You would most likely add a microSD card (if the smartphone has a slot available for add-on or upgrading). This is the most common method for adding long-term storage. DDR4 is a type of RAM; it is not used for adding long-term memory storage. Some smartphones will use LPDDR4 as their main memory, but this is part of the SoC, and not accessible to the typical user. An SSD is a solid-state drive, which generally means a hard drive that is installed to a PC or laptop, connected either as SATA or M.2. These are too large for smartphones and tablets. A SIM is a subscriber identity module, usually represented as a small card (mini-SIM) used in smartphones that securely stores authentication information about the user and device, such as the international mobile subscriber identity (IMSI), which we will discuss more in the following chapter.
3. **E.** “Beaming” the information back and forth can be accomplished in a couple of ways, primarily by using near field communication (NFC). This can only be done if the devices are in close proximity to each other. NFC is commonly used for contactless payment systems. Another potential option would be Apple's AirDrop, but this relies on Bluetooth (for finding devices) and Wi-Fi (for transmitting data), and of course relies on using Apple-based devices. A mobile hotspot enables a

1.5 – Given a scenario, connect and configure accessories and ports of other mobile devices

smartphone or tablet to act as an Internet gateway for other mobile devices and computers. IoT stands for the Internet of Things. In the question, it said employees can use their mobile devices in a BYOD manner, but CYOD is a bit different. This means that employees can *choose* a device to use for work purposes (most likely whichever type they are more familiar with). Whether or not the employees can use those for personal purposes is usually defined by company policy. IR stands for infrared, which is less commonly found on smartphones as of 2017.

4. **D.** Tethering can allow a desktop computer or laptop to share the mobile device's Internet connection. Tethering functionality can be very useful in areas where a smartphone has cellular access but the PC/laptop cannot connect to the Internet. Mobile device accessories such as headsets, speakers, game pads, extra battery packs, and protective covers are useful, but they are not used to connect to the Internet. IP codes are used to classify and rate the degree of protection against dust and water (for example, IP68). A perfect example of a proprietary, vendor-specific connector is the Apple Lightning connector that can only be used on iOS devices.
-

Chapter 3 is in the books, so to speak. Excellent work, keep going!

This page intentionally left blank

Index

Numbers

- 3-way handshakes, 90
- 3D printers, 301–302, 385
- 30-second trick, 22
- 32-bit CPU architectures, 451–453
- 64-bit CPU architectures, 451–453
- 120-V AC electrical lines, 107
- 568A wiring standard, 171–173
- 568B wiring standard, 171–173
- 802.11 wireless standards, 126–128
- 802.1X, 626

A

- Access Denied error messages (printing), 384
- accessories (mobile devices), 60–61
- ACK packets, 90
- ACL (Access Control Lists), 616
- active-matrix screens, 19–23
- AD (Active Directory), 610–611, 614
 - domains, 610, 612–614
 - group policies, 613–614
 - home folder, 613
 - logon scripts, 612–613
 - LDAP, 96–98
 - OU, 611–612
 - roaming profiles, 612
 - user profiles, 612–613
- adapters, 178, 182–183
- additive manufacturing. *See* 3D printers
- add-on storage/memory, 60
- ADF (Automatic Document Feeder) scanners, 253
- ADK (Assessment and Deployment Kit), 474
- administrative shares, 571–572, 653–654
- Administrative Tools (Windows), 511–512
 - Component Services, 521–522
 - Computer Management, 512–513

Administrative Tools (Windows)

- Device Manager, 514–516
- Event Viewer, 519–521
- Local Security Policy, 516
- Local Users and Groups, 516
- MMC, 513–514
- ODBC, 522
- Performance Monitor, 516–518
- Print Management, 518
- Services console, 518
- Task Scheduler, 518
- Windows Defender Firewall with Advanced Security, 519
- Windows Memory Diagnostics, 518–519

administrators

- administrator accounts, 554, 646, 662
- command help files, 490
- elevated mode (Command Prompt), 489
- PowerShell ISE, 490

ADSL (Asymmetrical Digital Subscriber Lines), 155–156**Advanced Boot Options, 707–709****Advanced tab (Internet Options), 549****AES (Advanced Encryption Standard), 123–124, 624–625****AFP (Apple Filing Protocol), 97–98****AHCI (Advanced Host Configuration Interface), 360****air flow/treatment, 347–348, 355, 788–789****airplane mode, 67–68, 74–75****alternate IP addresses, 577–578****Amazon Kindle, 52–53****AMD (Advanced Micro Devices) 236–238****Android Auto, 82–83****Android OS (Operating System), 454–455**

- applications, creating, 455
- Bluetooth, pairing/linking devices, 69–71
- email configuration, 72–73
- email connections, 741–742
- force stopping, 743
- KB (Knowledge Bases)/articles, 759
- mobile hotspots, 68–69
- rooting, 675
- screen locks, 670
- tablets, 49, 56–57
- wireless connections, 66–67, 68–71

antennas (Wi-Fi)

- external adapters, 36
- IEEE 802.11 standards, 36
- laptops, 34–36
- M.2 cards, 34–36
- MAC addresses, 36
- Mini PCIe cards, 34–36
- security, 693–694

antimalware, 356, 674–675**antistatic devices, 339, 780****antivirus software, mobile devices, 674****AP (Access Points)**

- MAC filtering, 695
- security, 693–694
- SOHO AP settings, 115–116
- WAP, 67, 102–103, 115–116

APIPA (Automatic Private IP Addressing), 144, 396–397**Apple CarPlay, 82–83****Apple devices. See iPads; iPhones****Application logs, 520****application windows (Windows Desktop), 468****applications**

- Android apps, 455
- AUP, 631
- authenticator applications, 672
- closing, 250
- cloud computing, 314–315
- crashes, 717
- finding (macOS), 586
- force stopping, 743–744
- installing, 580–582
- iOS apps, creating, 455
- locator/tracker applications, 672–673
- OS installation, 484
- side-by-side applications, 469
- stopping, 743–744
- tracker/locator applications, 672–673
- troubleshooting, 717, 743–744, 747
- virtual application streaming, 314–315
- Windows computers 717

APU (Accelerated Processing Units), 236**AR (Augmented Reality) headsets/glasses, 52, 258****ARM, tablets, 49**

ARP (Address Resolution Protocol), 499–500

arrays. See RAID arrays

artifacts (video), 368–369

aspect ratio (displays), 551

asset tags, 763

assistants (virtual), 467

ATX (Advanced Technology Extended), 216–218, 263–264

audio

accessories (mobile devices), 60

audio/video workstations, 272–273

microphones, 34, 253

MIDI devices, 254

mobile devices, 60

modifying devices, 562

ports, 226

Sound (Windows Control Panel), 561–562

speakers, 258, 376, 562

audit success events (Event Viewer), 520–521

AUP (Acceptable Use Policies), 631, 761–762

authentication, 624

802.1X, 626

AES, 624–625

authenticator applications, 672

COA, 763

logical security, 608–609

MFA, 608–609, 670

mobile device synchronization, 83–84

multifactor authentication, 639

RADIUS, 625–626

servers, 136

SSO authentication, 83, 648, 664

TKIP, 624

two-step authentication, 672

WEP, 624

WPA, 624

WPA2, 624–626

WPA2-Enterprise, 625–626

WPA2-Personal, 625

automobiles

Android Auto, 82–83

Apple CarPlay, 82–83

mobile device synchronization, 82–83

AutoPlay, disabling, 664–665

AutoRun, disabling, 664–665

B

backed-up print queues, 384

backlights (laptop displays), 31–32

backups, 332, 769

cloud storage backups, 80, 773–774

Files History (Windows 10/8), 770–771

full backups, 771

incremental backups, 771

local storage backups, 773–774

LTO backups, 770

mobile devices, 80, 673

RAID arrays, 361

security, 634

System Image Backups, 770–771

testing, 772–773

Time Machine (macOS), 589

user accounts, 774–775

Windows Registry, 542–543

Windows Server Backup, 771–772

badge readers, 604–605

bandwidth

PCIe expansion buses, 219–220

speed, 118

Thunderbolt cables, 181

unshielded twisted-pair cables, 170–171

USB cables, 178–179

barcode scanners, 254

barcodes, inventory management, 763

BASE, 114

baseband updates, 75

Bash, 817, 821–823

basic drives, 477

batch files (bat), 820

batteries, 19–23

CMOS batteries, 227

environmental controls, 790

mobile devices, 61

overheating, 373–375

recycling/disposal, 790

smartphones, 50

batteries

- tablets, 49

- troubleshooting, 373–375

BD-R (Blu-ray Disc Recordable), 212**BD-RE (Blu-ray Disc Recordable Erasable), 212****Berg connectors, 266****BGA (Ball Grid Arrays), 24–25****BIOS (Basic Input/Output Systems), 8**

- boot orders, 227–228

- CMOS batteries, 227

- flashing the BIOS, 227

- hard drives, 356

- motherboards, 226–229, 338

- passwords, 228

- POST, 229

- RAM, 194, 343

- security, 228

- video, 367

- virtualization, 229

BitLocker encryption, 655–656**blacklists, 731****blackouts (electrical safety), 791–792****blank pages (troubleshooting), 382****Blu-rays, 211–212****Bluetooth, 17, 59**

- automobile synchronization, 83

- classes of, 255

- devices, 255–256

- pairing/linking devices, 69–71

- troubleshooting, 740–741

- wearable technology devices, 52

BNC connectors, 175**Boot Camp (macOS), 588****boot orders, BIOS, 227–228****bootups, 472–473**

- Advanced Boot Options, 707–709

- Boot Camp (macOS), 588

- bootrec command, 710–711

- dual-booting, 588

- internal drive installations, 473

- Linux, 595–596

- local installations, 472

- MBR, 477–478

- multiboots, 475–476

- network boot (PXE) OS installations, 472

- RAM, 343

- Windows Boot Manager (bootmgr), 710, 711–712

- Windows computers, 716–717

botnets, 629, 640**BRI ISDN (Basic Rate ISDN), 155****bridged networking, 323****bridges, 105****brightness (displays), 372–373****brownouts (electrical safety), 792****browsers, redirecting, 733****brute-force attacks, 641****BSOD (Blue Screen of Death), 338–339, 344, 358, 367–368, 713–715, 717****bus speeds (motherboards), 234****BYOD (Bring Your Own Device) environments, 677–678****C****cable cutters, 160****cable locks, 43****cable modems, 105, 120****cable strippers, 161****cable testers, 161****cables**

- 568A wiring standard, 171–173

- 568B wiring standard, 171–173

- adapters, 182–183

- BNC connectors, 175

- coaxial cables, 170, 174–175

- crossover cables, 173

- DisplayPort cables, 177

- DVI cables, 177

- DVI-A cables, 177

- DVI-D cables, 177

- DVI-I cables, 177

- EMI, 173

- fiber optic cables, 157, 170, 175–176

- HDMI cables, 177

- IDE cables, 182

- Internet connections, 156

- LC connectors, 175

- Lightning cables, 180

- managing, 785

- patch cables, 161

- plenum-rated cables, 173–174
- RJ11 plugs, 172–173
- RJ45 plugs, 172–173
- SATA cables, 182
- SC connectors, 175–176
- SCSI cables, 182
- Serial ATA cables, 182
- serial cables, 181–182
- shielded twisted-pair cables, 174
- signal attenuation, 173
- single-mode fiber optic cables, 175
- ST connectors, 175–176
- straight-through cables, 173
- SVGA cables, 177
- Thunderbolt cables, 180–181
- twisted-pair cables, 170
- unshielded twisted-pair cables, 114, 170–174
- USB cables, 178–179
- VGA cables, 177
- video cables, 177–178, 182
- cabling tools, 160–163**
- cache memory, CPU, 236**
- CAD (Computer-Aided Design) workstations, 272**
- CAL (Client-Access Licenses), 763**
- CAM (Computer-Aided Manufacturing) workstations, 272**
- cameras**
 - tablets, 49
 - webcams, 34, 253
- capacity requirements, power supplies, 264–265**
- CarPlay (Apple), 82–83**
- cars/trucks**
 - Android Auto, 82–83
 - Apple CarPlay, 82–83
 - mobile device synchronization, 82–83
- case connectors, 226**
- CCFL, laptop displays, 31–32**
- CD (Compact Discs), data storage, 209–210**
- CD-ROM Mode 1/Mode 2, 479–480**
- CDFS (Compact Disc File Systems), 479–480**
- cell phones. See smartphones**
- cellular connections, 66, 74**
 - airplane mode, 74–75
 - baseband updates, 75
 - GSM, 74–75
 - IMEI, 76
 - IMSI, 76
 - IMT-Advanced requirements, 74
 - ITU IMT-2020 standard, 74
 - PRL updates, 75
 - VPN, 76
- cellular networks, 17–18, 50**
- centralized computing, 279**
- certificates**
 - COA, 763
 - invalid certificate issues/trusted root CA, 733
 - invalid email certificates, 733
 - security, 619–620, 632–633
- certification exam preparation, 879–880, 882**
 - cheat sheets, 881
 - passing the exam, 885–886
 - questions, 880–881, 884–885
 - reviewing answers, 885
 - taking the exam, 882–884
 - tips/tricks for taking, 882–884
- CF (CompactFlash), 208**
- chains of custody (incident response), 800–801**
- change management, 766–768**
 - backout plans, 767
 - business process documentation, 767
 - change boards, 767
 - documentation, 767
 - end-user acceptance, 767
 - purpose of the change, 767
 - risk analysis, 767
 - scope the change, 767
- channel bonding, 802.11 wireless standards, 128**
- cheat sheets (exam preparation), 881**
- chemicals (environmental controls), 789–790**
- chip readers, 254**
- chipsets, 220, 237**

Chrome OS, 456**Chromebook 13, 457****Chromebook 3400, 457****CIA triad, 646****CIDR (Classless Inter-Domain Routing), 145****CIFS (Common Internet File System) protocol, 97****classful IP addresses, 145****classless IP addresses, 145****clean OS installations, 473****cleaning, mobile devices, 375****cleanup (disk), 354****clearing hard drives, 687****CLI (Command-Line Interfaces)**

- command help files, 490

- Command Prompt, 488–492, 535

- Linux, 591–595

- PowerShell, 489

- PowerShell ISE, 490

clock speeds

- CPU, 234

- maximum clock rates, 234

- motherboard bus speeds, 234

closed-source (commercial) software, 455, 802**closing applications, 250****cloud computing, 316**

- applications, 314–315

- backups, 80

- benefits of, 312

- community clouds, 314

- DaaS, 313

- DBaaS, 313

- defined, 311–312

- on-demand services, 316

- example of, 312

- hybrid clouds, 314

- IaaS, 313

- iCloud, 589

- measured services, 315

- metered services, 315

- mobile device synchronization, 79–80

- NaaS, 313

- network controllers, 104

- PaaS, 313

- printing, 292

- private clouds, 314

- public clouds, 314

- rapid elasticity, 316

- resource pooling, 316

- SaaS, 312–313

- SOHO multifunction devices/printers, 292

- storage backups, 773–774

CMOS batteries, 227**COA (Certificates of Authenticity), 763****coaxial cables, 170, 174–175****collating print jobs, 289****color**

- calibration (video), 368–369

- depth of, resolution (displays), 552–553

- errors (printing), 384

command line, 496

- ARP, 499–500

- chkdsk command, 494–495

- command help files, 490

- Command Prompt, 488–492, 535

- convert command, 494

- defrag command, 493

- diskpart command, 493

- DISM, 504–506

- gresult command, 506–507

- gpupdate command, 506–507

- ipconfig command, 496–497

- Linux, 591–595

- nbtstat command, 502

- net command, 503–504

- netstat command, 501

- nslookup command, 502

- ping command, 497–499

- PowerShell, 489

- PowerShell ISE, 490

- SFC, 495

- shutdown command, 506

- taskkill command, 504

- tasklist command, 504

- tracert command, 500–501

Command Prompt, 450

- dd command, 686

- directories, 490–492

- diskpart command, 686
- edit command, 535
- elevated mode, 489
- format command, 685
- mapping drives, 573
- net use command, 573
- opening, 488–489
- command_block, 816**
- comments (scripting), syntax, 817–818**
- commercial (closed-source) software, 455, 802**
- communication techniques/professionalism, 808–811**
- community clouds, 314**
- compatibility**
 - CPU, 236–238
 - OS, 458–459, 484
 - power supplies, 263–264
 - printers, 305
 - Program Compatibility (Windows Control Panel), 560–561
 - RAM, 188, 196, 342
- compliance/regulatory policies, 760–761**
- component failures (motherboards), 339**
- Component Services (Windows), 521–522**
- compromised/damaged mobile devices, 673**
 - antimalware, 674–675
 - antivirus software, 674–675
 - backups, 673
 - BYOD environments, 677–678
 - COPE environments, 677–678
 - CYOD environments, 678
 - full device encryption, 676–677
 - MDM, 675, 678–679
 - updating, 674
- connection-oriented sessions. See TCP**
- connectionless sessions. See UDP**
- Connections tab (Internet Options), 549**
- containment (incident response), 800**
- content filtering, SOHO networks, 697**
- Content tab (Internet Options), 549**
- continuity testers, 161**
- Control Panel (Windows), 548**
 - Credential Manager, 558–559
 - Devices and Printers, 561
 - Display, 550–552
 - Folder Options, 554–555
 - Internet Options, 548–549
 - Power Management, 557–558
 - Program Compatibility, 560–561
 - Programs and Features, 559
 - Sound, 561–562
 - Sync Center, 563–564
 - Troubleshooting, 563
 - User Accounts, 554
 - Virtual Memory (Performance), 556–557
- cooling systems**
 - CPU, 239–242
 - fans, 25, 241
 - heat sinks, CPU, 239–241
 - liquid cooling systems, CPU, 241–242
 - thermal compound, CPU, 240–241
- COPE (Corporate-Owned Personally Enabled) environments, 677–678**
- copying files/folders, 651–652**
- corrupted/missing files, 357–358**
- Cortana (Windows 10), 467**
- CPU (Central Processing Units), 233**
 - 32-bit CPU architectures, 451–453
 - 64-bit CPU architectures, 451–453
 - APU and, 236
 - ARM-based CPU, 49
 - cache memory, 236
 - chipsets, 237
 - clock speeds, 234
 - compatibility, 236–238
 - connectors, 266
 - cooling systems, 239–242, 340
 - GPU and, 236
 - heat sinks, 239–241, 341
 - HT, 235
 - installing, 242–245, 340–341
 - laptops, 24–25
 - liquid cooling systems, 241–242
 - multicore CPU, 235, 239
 - overclocking, 235, 239
 - PCH, 237
 - power consumption, 239
 - smartphones, 50
 - sockets, 237–238, 243–244
 - tablets, 48–49

CPU (Central Processing Units)

- TDP ratings, 239
- testing installations, 244–245
- thermal compound, 240–241
- troubleshooting, 340–342
- voltage, 239
- x64, 452
- x86, 452

cracking passwords, 641–642

creased paper, 382

Credential Manager (Windows Control Panel), 558–559

crossover cables, 173

CRT (Cathode Ray Tube) monitors, 366–367, 783

cryptanalysis attacks, 641

custody (incident response), chains of, 800–801

custom PC

- audio/video workstations, 272–273
- CAD workstations, 272
- CAM workstations, 272
- editing workstations (audio/video), 272–273
- gaming PC, 275–276
- graphic workstations, 272
- NAS servers, 277–278
- thick clients (standard), 280, 282–283
- thin clients, 278–279, 282–283
- virtualization workstations, 273–275
- VMM, 273–275
- VMware workstations, 274

CYOD (Choose Your Own Device) environments, 678

D

DaaS (Data as a Service), 313

daisy wheel printers, 300

damaged/compromised mobile devices, 673

- antimalware, 674–675
- antivirus software, 674–675
- backups, 673
- BYOD environments, 677–678
- COPE environments, 677–678
- CYOD environments, 678
- full device encryption, 676–677

- MDM, 675, 678–679

- updating, 674

Dashboard (macOS), 587

data

- access, Windows networks, 570–573
- authentication, mobile devices, 83–84
- destruction/disposal, 684–689
- physical security, 606
- privacy, 292
- regulations, 803–805
- sharing, Windows networks, 570–573
- throughput, 118
- transfer rates
 - 802.11 wireless standards, 127
 - PCIe expansion buses, 219–220
 - SATA drives, 200
 - Thunderbolt cables, 181
 - unshielded twisted-pair cables, 170–171
 - USB cables, 178–179

data packets, latency, 497

Data Sources (ODBC), 522

date/time settings, 482

DBaaS (Database as a Service), 313

DDoS (Distributed Denial-of-Service) attacks, 640–641

DDR (Double Data Rate) memory, 11–12

DDR2 RAM, 188

DDR3 RAM, 189

DDR4 RAM, 189–190

dead/stuck pixels (video), 368

defragmenting hard drives, 354–355, 493, 534–535

degaussing hard drives, 687–688

desktops, 188

- configuring, 282–283
- Linux desktop distributions, 591–592
- logins, 283
- macOS, 586
- mobile devices
 - synchronizing, 80–81
 - tethering, 58
- passwords, 283
- security, 283
- Windows GUI, 465–468

- destroying**
 - data, 684
 - hard drives, 684–689
- detection/analysis (incident response), 799–800**
- Device Manager (Windows), 252, 254–255, 514–516**
- Devices and Printers (Windows Control Panel), 561**
- DHCP (Dynamic Host Configuration Protocol), 94–95, 98, 136, 143**
- dialog boxes (Windows Desktop), 468**
- dial-up modems, 105, 154–155**
- dictionary attacks, 641**
- digitizers, 32–33**
- dim displays, 372–373**
- DIMM (Dual-Inline Memory Modules), 188**
- directories, 490–492**
- DirectX, 368, 540**
- disaster prevention/recovery, 769**
- disconnecting USB devices, 255**
- disk cleanup, 354**
- Disk Management, 493, 529–530**
 - Disk Defragmenter, 534–535
 - drives, 531–533
 - hard drives, initializing, 530
 - Import Foreign Disks, 531–532
 - logical drives, 530
 - Optimize Drives, 534–535
 - partitioning, 482–483, 530–531
 - Storage Spaces, 533. *See also* RAID
 - volumes (letter assignments), 530–531
- Disk Utility (macOS), 589**
- DISM (Deployment Image Servicing and Management), 504–506**
- Display (Windows Control Panel), 550–551**
 - aspect ratio, 551
 - color depth, 552–553
 - HD 1080i mode, 550
 - HD 1080p mode, 550
 - HD Ready mode, 550
 - list of resolutions, 550
 - modifying, 551
 - refresh rates, 553
 - troubleshooting, 551–552
 - UHD 4K mode, 550
 - VGA mode, 550
 - video cards, 551–552
 - video scaling, 552
 - WSXGA+ mode, 550
 - WUXGA mode, 550
 - WXGA mode, 550
- DisplayPort cables, 177**
- DisplayPort connectors, Thunderbolt cables, 181**
- displays**
 - artifacts (video), 368–369
 - brightness, 372–373
 - BSOD, 338–339, 713–715, 717
 - calibration, 368–369
 - CRT monitors, 366–367, 783
 - digitizers, 32–33
 - dim displays, 372–373
 - dual displays, 41
 - external displays, 41–42, 747–748
 - filters, 369
 - Fn key, 41–42
 - KVM switches, 259
 - laptops
 - backlights, 31–32
 - CCFL, 31–32
 - external monitors, 41–42
 - inverters, 31–32
 - LCD, 30–31
 - LED, 30, 32
 - OLED, 30–32
 - removable screens, 42–43
 - rotating screens, 42–43
 - troubleshooting, 372–373
 - LCD, 256, 782–783
 - LED displays, 48, 257
 - OLED displays, 257
 - printer displays, 383
 - projectors, 257
 - QLED, 257
 - refresh rates, 553
 - removable screens, 42–43
 - resolution, 550–551
 - aspect ratio, 551
 - color depth, 552–553

displays

- HD 1080i mode, 550
- HD 1080p mode, 550
- HD Ready mode, 550
- list of resolutions, 550
- modifying, 551
- refresh rates, 553
- troubleshooting, 551–552
- UHD 4K mode, 550
- VGA mode, 550
- video cards, 551–552
- video scaling, 552
- WSXGA+ mode, 550
- WUXGA mode, 550
- WXGA mode, 550

- rotating screens, 42–43

- Screen Sharing (macOS), 587–588

- smartphones, 50, 372–373

- tablets, 48, 372–373

- touchscreens, 32–33, 259, 376

- gestures (macOS), 587

- laptop configuration, 284

- removing, 33

- smartphones, 50

- tablets, 48

- troubleshooting, 368–369, 376

- video cards, 551–552

- video scaling, 552

DLP (Data Loss Prevention), 617–618**DMZ (Demilitarized Zones), SOHO router firewalls, 121****DNS (Domain Name Systems), 96, 98**

- DNS servers, 136–137, 144–145

- erasing caches, 497

- ipconfig/flushdns command, 497

- nslookup command, 502

Dock (macOS), 586**docking stations, laptops, 42****documentation, 756, 764**

- AUP, 761–762

- business processes, 767

- CAL, 763

- change management, 767

- COA, 763

- compliance policies, 760–761

- DRP, 769

- EULA, 763

- findings/actions/outcomes, 334

- incident documentation, 760

- incident response, 799

- inventory management, 763

- KB/articles, 758–759

- MSDS, 789–790

- network topology diagrams, 756–758

- password policies, 762–763

- regulatory policies, 761

- reviewing (troubleshooting), 331–332

- saving documents, 250

- software licenses, 763

- VM, 763

domains

- defined, 610

- group policies, 613–614

- logon scripts, 612–613

- OS installation, 482

- Windows, 568–569

DORA (Discovery Offering Request Acknowledgement) process, 95**dot matrix printers, 300****DRAM (Dynamic Random Access Memory), 187–188****drivers**

- keyboard installations, 251

- OS installation, 482

- printer drivers, 305, 383

- third-party drivers, 481

- video drivers, 367–368

drives

- basic drives, 477

- dynamic drives, 477

- “foreign” status, 531–532

- hard, 16

- Import Foreign Disks (Disk Management), 531–532

- letter assignments, 477, 532–533

- logical drives, 476–477, 530

- mapping, 572–573

- mounting, 532–533

- optical, 16

- Optimize Drives, 534–535

- volumes (letter assignments), 477

DRM (Digital Rights Management), 802
DRP (Disaster Recovery Plans), 769
DSL (Digital Subscriber Line) modems, 105, 120, 155–156
 dual displays, 41
 dual-booting, 588
 dual-channel RAM (Random Access Memory), 194
 dual-rail PSU (Power Supply Units), 264
 dump files, 714–715
 dumpster diving, 639
 duplexing (printing), 289, 382
 dust. *See* IP (Ingress Protection)
DVD (Digital Versatile Discs), 210–211
DVD-ROM, 472
DVI (Digital Visual Interface) cables, 177
DVI-A (Digital Visual Interface-A) cables, 177
DVI-D (Digital Visual Interface-D) cables, 177
DVI-I (Digital Visual Interface-I) cables, 177
DxDiag (DirectX Diagnostic Tool), 540
 dynamic drives, 477
 dynamic IPv4 addressing, 143

E

e-readers, 52–53
EATX12V power ports, 263–264
ECC (Error Correction Codes), 196
 editing workstations (audio/video), 272–273
 ejecting USB devices, 255
 elasticity (rapid), cloud computing, 316
electrical safety, 782–783, 791
 blackouts, 791–792
 brownouts, 792
 CRT monitors, 783
 ESD prevention/grounding, 780–782
 fire safety, 783–784
 grounding, 780–782
 laser printers, 783
 LCD, 782–783
 power supplies, 782–783, 792–794
 sags, 791
 surge protectors, 783, 792
 surges, 791–792
 UPS, 783, 792–794
elevated mode (Command Prompt), 489
email, 93
 Android devices, 72–73
 encryption, 741–742
 hijacking, 731–732
 IMAP, 73, 93, 98
 invalid email certificates, 733
 mail servers, 135
 mobile device configuration, 71–74
 POP3, 72–73, 93, 98
 port configuration, 72–73
 S/MIME, 74
 SMTP, 73, 92–93, 98
 SSL, 72–73
 TLS, 72–73
 troubleshooting, 72, 741–742
embedded systems, 139–140
EMI (Electromagnetic Interference), 173–175
emulation versus virtualization, 319
encryption, 624
 802.1X, 626
 AES, 123–124, 624–625
 BitLocker, 655–656
 email, 741–742
 file systems, 654–655
 full device encryption, mobile devices, 676–677
 RADIUS, 625–626
 SD cards, 676
 SOHO routers, 123–124
 TKIP, 123, 624
 WEP, 123–124, 624
 WPA, 123, 624
 WPA2, 123–124, 624–626
 WPA2–Enterprise, 625–626
 WPA2–Personal, 625
end-of-life/end-of-support dates (OS/software), 457–458
endpoint management servers, 139
entry control rosters, 604–605
entry systems (security), 604–605
environment variables, 817

environmental controls

environmental controls, 788

- air treatment, 788–789
- batteries, 790
- chemicals, 789–790
- humidity measurements, 788
- ink/toner cartridges, 790
- MSDS, 789–790
- power supplies, 790
- recycling/disposal, 790
- temperature measurements, 788
- toner/ink cartridges, 790

eradication (incident response), 800**erasing DNS caches, 497****ergonomics, 785–786****error codes, printers, 383****error detection/correction, 196****error events (Windows), 520****error messages, troubleshooting**

- Access Denied error messages (printing), 384
- IP conflict error messages, 396
- kernel panic errors, 596
- low memory error messages (printers), 383
- No OS found messages, 717
- out of memory error messages (printers), 383

eSATA (external SATA), 225–226**ESD (Electrostatic Discharge), 10, 24–25**

- motherboards, 338–339
- preventing, 780–782
- RAM, 342–343

Ethernet

- Ethernet over Power, 107
- PoE, 106
- RJ45 ports, 225
- switches, 102
- USB to Ethernet adapters, 183

EULA (End-User Licensing Agreements), 763, 801–802**Event Viewer, 519–520**

- Application logs, 520
- audit success events, 520–521
- error events, 520
- information events, 520
- Security logs, 520

shutdowns, 712

System logs, 520

warning events, 520

exam preparation, 879–880, 882

- cheat sheets, 881
- passing the exam, 885–886
- questions, 880–881, 884–885
- reviewing answers, 885
- taking the exam, 882–884
- tips/tricks for taking, 882–884

exFAT (FAT64), 478–479**expansion buses, 218–220****expansion cards, 220–225****extended partitions, 476–477****extenders/repeaters, 104****extending volumes, 531****external host communications, 94**

FTP, 94, 98

SSH, 94, 98

Telnet, 94, 98

external monitors, 41–42, 747–748**external Wi-Fi adapters/antennas, 36****external/flash drives, 472****F****faded prints (printing), 383****failed print jobs, 384****fans**

- CPU, 241, 340
- laptops, 25
- power supplies, 346

FAT, 478–479**FAT32, 478–479, 494****FAT64 (exFAT), 478–479****FDM (Fused Deposition Modeling), 301****fiber optic cables, 157, 170, 175–176****File Explorer, 535–536****file servers, 134****file systems**

- encryption, 654–655
- Linux file systems, 592
- OS installation, 478–481
- security, encryption, 654–655

files

- administrative shares, 653–654
- command help files, 490
- copying, 651–652
- dump files, 714–715
- finding, 586
- hidden files, viewing, 555, 652–653
- .ISO files, 472
- log files, reviewing, 331
- missing files at startup, 357
- moving, 651–652
- offline files, managing, 563–564
- ownership, 651
- permissions, 648–651
- print to file (virtual printing), 302–303
- security, 652–653
- SFC, 495
- XPS files, 303–304

Files History (Windows 10/8), 770–771**filters**

- content filtering, SOHO networks, 697
- MAC filtering, 695
- monitors, 369
- phishing filters, 632–633
- screen filters, 638
- spam filters, 731

Finder (macOS), 586**fire safety (electrical), 783–784****firewalls, 103, 615**

- ACL, 616
- exceptions, 615–616
- network firewalls, 138
- SOHO routers, 120–123
- troubleshooting, 616
- UTM, 138
- Windows Defender Firewall with Advanced Security, 519, 616

firmware

- 3D printers, 302
- RAM installations, 194

first response (incident response), 798–799**fitness monitors, 52****fixed (line-of-sight) wireless Internet service, 158****flash drives, 204**

CF, 208

NAND-based flash memory, 205–206

OS installation, 472

SD cards, 206–208

USB flash drives, 205–206

flash memory, 48, 50**flashing the BIOS, 227****flatbed scanners, 253****floating-point numbers, 814****flood attacks, 105****Folder Options (Windows Control Panel), 554–555****folders**

- %systemroot% folders, 495
- administrative shares, 653–654
- copying, 651–652
- home folder (AD), 613
- moving, 651–652
- ownership, 651
- permissions, 648–651
- security, 652–653

for loops, 815–816**Force Quit (macOS), 589****force stopping applications, 743–744****“foreign” status, drives, 531–532****fox and hound tools, 161****FreeBSD, 595****frequency ranges, 802.11 wireless standards, 127–128****frozen/locked up mobile devices, 375–376****FRU (Field Replaceable Units), 782****FTP (File Transfer Protocol), 94, 98****FTTB (Fiber to the Building/Business) Internet connections, 157****FTTC (Fiber to the Cabinet) Internet connections, 157****FTTD (Fiber to the Desktop) Internet connections, 157****FTTdp (Fiber to the Distribution Point) Internet connections, 157****FTTH (Fiber to the Home) Internet connections, 157****FTTN (Fiber to the Neighborhood) Internet connections, 157****FTTP (Fiber to the Premises) Internet connections, 156–157**

full backups

full backups, 771**full device encryption, mobile devices, 676–677****full duplex network adapters, 118, 579****full formatting, 479****fuses, 346****G****gamepads, 60, 253****gaming PC, 275–276****garbage printouts, 383****garbled characters (printing), 383****gateway addresses, 144****GDPR (General Data Protection Regulation), 804–805****gestures (macOS), 587****ghosted images (printing), 383****glasses (AR), 52, 258****Google**

Chrome OS, 456

Chromebook 13, 457

Chromebook 3400, 457

GPS (Global Positioning System) devices, 53**GPT (GUID Partition Tables), 477–478, 592****GPU (Graphics Processing Units), 18, 236****graphic workstations, 272****grounding (electrical safety), 780–782****group policies, 613–614****GSM (Global System for Mobile Communication), 74–75****guest accounts, 554, 646, 662****GUI (Graphical User Interfaces), 465–469, 585–586, 590–592****H****half duplex network adapters, 579****hard drives, 8–13, 198**

air flow, 355

antimalware scans, 356

BIOS recognition, 356

CF, 208

clearing, 687

convert command, 494

data destruction/disposal, 684–689

defragmenting, 354–355, 493

degaussing, 687–688

drive space, 355

flash drives, 204–208

formatting, 493, 684–685

HDD, 200–201

high-performance drives, 355

IDE cables, 182

initializing, 530

NAND-based flash memory, 205–206

overwriting, 685–686

physical destruction of, 688–689

purging, 687–688

RAID, 202–204

SATA, 182, 198–200, 358,

SCSI cables, 182

SD cards, 206–208

secondary drives, 356

S.M.A.R.T. data, 357–358

SSD, 201–202

troubleshooting, 354–358

USB flash drives, 205–206

VM connections, 324

volumes (letter assignments), 494

hard resets, 22, 745–746**HD 1080i mode (displays), 550****HD 1080p mode (displays), 550****HD Ready mode (displays), 550****HDD (Hard Disk Drives), 200–201****HDMI (High-Definition Multimedia Interface) cables, 177****headless motherboards, 259****headsets (AR/VR), 52, 258****heat sinks, 239–241, 341****hibernate mode (Power Management), 558****hidden files, viewing, 555, 652–653****high-level formatting, 684****high-performance hard drives, 355****hijacking**

email, 731–732

sessions, 632–633

hives (Windows Registry), 541–542**home folder (AD), 613****HomeGroup, 568, 572**

host availability tests, 497
 host-only networking, 323
 hotspots (mobile), 59, 68–69
 HT (Hyper-Threading), 235
 HTTP (Hypertext Transfer Protocol), 91, 98
 HTTPS (Hypertext Transfer Protocol Secure), 91–92, 98
 hubs, 104–105, 237
 humidity measurements (environmental controls), 788
 hybrid clouds, 314
 hybrid I/O devices, 259
 hypervisors, 319–322

I

IaaS (Infrastructure as a Service), 313
 IANA (Internet Assigned Numbers Authority) port list, 99
 icons (Windows Desktop), 467
 ID (Identification), security, 604–605, 639
 IDE (Integrated Drive Electronics) cables, 182
 IDS (Intrusion Detection Systems), 138–139
 IEEE 802.11 standards, 36, 126–128
 image OS deployments, 474
 IMAP (Internet Message Access Protocol), 73, 93, 98
 IMEI (International Mobile Equipment Identity), 76
 impact printers, 300, 385
 IMPI (Intelligent Platform Management Interface), 259
 Import Foreign Disks (Disk Management), 531–532
 improper/spontaneous shutdowns, 712–713
 IMSI (International Mobile Subscriber Identity), 76
 IMT-Advanced requirements, 74
 incident documentation, 760, 799
 incident response, 798–801
 incremental backups, 771
 indicators, NIC, 116–117
 information events (Event Viewer), 520–521
 information security, 646–656, 662–665
 inheritance (permissions), 650–651
 initializing hard drives, 530
 inkjet printers, 298–299, 383, 385
 ink/toner cartridges, 790
 integers, 814
 integrated audio ports, 226
 integrated GPU, 236
 internal clock speeds, CPU, 234
 internal drives, 473
 Internet Options (Windows Control Panel), 548–549
 Internet-based (remote) resources, 394
 invalid certificate issues/trusted root CA, 733
 invalid email certificates, 733
 inventory management documentation, 763
 inverters, 31–32
 iOS, 455

- applications, 455
- force stopping, 744
- jailbreaking, 674–675
- KB (Knowledge Bases)/articles, 759
- resetting, 744–746

IoT (Internet of Things), 54, 118–120
 IP (Ingress Protection) and smartphones, 50–51
 IP addresses

- alternate IP addresses, 577–578
- APIPA, 396–397
- ARP, 499–500
- DHCP, 94–95, 98
- DNS, 96, 98
- IP conflict error messages, 396
- ipconfig command, 497
- IPv4 addressing, 142–146
- IPv6 addressing, 146–147
- link-local addresses, 396–397
- loopback addresses, 498
- static IP addressing, 695–696
- troubleshooting, 396–397

IP subnetting, 148
 iPads, 49, 56–57, 455
 iPhones, 455
 IPS (In-Plane Switching), 256

IPS (Intrusion Prevention Systems), 138–139

IR (Infrared) wireless connections, 60

ISDN (Integrated Services Digital Networks), 155

.ISO files, 472

iterations, 815

ITU IMT-2020 standard, 74

J

jailbreaking, 674–675

JavaScript, 817, 823–824

K

KB (Knowledge Bases)/articles, 758–759

Kernel Memory Dumps, 714–715

kernel panic errors, 596

keyboards

\ backslash key, 252

Alt+F4, 250

backspace key, 252

Ctrl+S, 250

Ctrl+Shift+Esc, 250

Device Manager (Windows 10), 252

displaying, 252

driver installations, 251

F1–12 keys, 39–41

Fn key, 39–42

KVM switches, 259

laptops, 8–10

layouts, 250–251

mechanical keyboards, 251

membrane keyboards, 251

Num Lock key, 40–41

PS/2 connectors, 251

shortcuts, 250

special function keys, 39–41

wired keyboards, 251

wireless keyboards, 251

Keychain (macOS), 588

keyloggers, 629

Kindle (Amazon), 52–53

KVM (Keyboard-Video-Mouse) switches, 259, 366–367

L

LAN (Local Area Networks), 16–17, 152

bridges, 105

routers, 102

SOHO routers, 113–114

star topologies, 152

switches, 102

VLAN, 147–148

laptops

accessories, 60–61

add-on storage/memory, 60

airplane mode, 67–68, 74–75

antimalware, 674–675

antivirus software, 674–675

applications, 743–744, 747

audio accessories, 60

authenticator applications, 672

backups, 80, 673

batteries, 61, 373–375

biometric security, 670

Bluetooth devices, 69–71

BYOD environments, 677–678

cellular connections, 74–76

cleaning, 375

cloud-based backups, 80

compromised/damaged laptops, 673–679

configuring, 283–285

COPE environments, 677–678

CPU, 24–25

CYOD environments, 678

displays

backlights, 31, 32

CCFL, 31–32

digitizers, 32–33

dual displays, 41

external monitors, 41–42

inverters, 31–32

LCD, 30–31

LED, 30, 32

OLED, 30–32

removable screens, 42–43

rotating screens, 42–43

touchscreens, 32–33

- disposal/recycling, 790–791
- docking stations, 42
- email configuration, 71–74
- external monitors, 41–42
- F1–12 keys, 39–41
- fans, 25
- Fn key, 39–42
- full device encryption, 676–677
- game pads, 60
- hard drives, 8–13
- keyboards, 8–10
- locator/tracker applications, 672–673
- lockouts, 671
- loss of, 672–673
- M.2 cards, 34–36
- MDM, 618, 670–671, 675, 678–679, 742
- memory, 13–16
- mice, 283–284
- microphones, 34
- Mini PCIe cards, 34–36
- mobile devices, tethering to desktop computers, 58
- mobile hotspots, 68–69
- monitors (external), 747–748
- networking, 16–18
- Num Lock key, 40–41
- optical drives, 16
- OS, 747
- pairing/linking devices, 69–71
- port replicators, 42
- power, 19–23
- RAM, 188
- recycling/disposal, 790–791
- repair kits, 33
- resetting, 744–746
- screen locks, 670–671
- screen mirroring, 747–748
- security, 669
 - antimalware, 674–675
 - antivirus software, 674–675
 - authenticator applications, 672
 - backups, 673
 - biometric security, 670
 - BYOD environments, 677–678
 - cable locks, 43
 - compromised/damaged mobile devices, 673–677
 - COPE environments, 677–678
 - CYOD environments, 678
 - full device encryption, 676–677
 - locator/tracker applications, 672–673
 - lockouts, 671
 - MDM, 670–671, 675, 678–679
 - screen locks, 670–671
 - security profiles, 679
 - theft/loss, 672–673
 - troubleshooting, 748–750
 - two-step authentication, 672
 - updating, 674
 - visible passwords, 671
- smart card readers, 16
- speakers, 23
- special function keys, 39–41
- synchronization, 79–84
- system board, 24–25
- tethering to desktop computers, 58
- theft of, 672–673
- touchpads, 10–11
- touchscreens, 284
- troubleshooting, 372
 - applications, 743–744, 747
 - Bluetooth, 740–741
 - cleaning, 375
 - disassembly processes, 376–377
 - displays, 372–373
 - email, 741–742
 - frozen/locked up laptops, 375–376
 - monitors (external), 747–748
 - OS, 747
 - overheating, 373–375
 - screen mirroring, 747–748
 - Wi-Fi, 738–740
- two-step authentication, 672
- updating, 674
- USB tethering, 69
- video subsystem, 18–19
- webcams, 33–34
- Wi-Fi antennas, 34–36
- wireless connections, 66–71, 74–76

laser printers

laser printers, 294–298, 385, 783

laser sintering, 3D printers, 301

latency, 201, 497

LC connectors, 175

LCD (Liquid Crystal Displays), 256

electrical safety, 782–783

IPS, 256

laptops, 30–32

TN technology, 256

LDAP (Lightweight Directory Access Protocol), 96–98

LED (Light-Emitting Diode) displays, 30, 32, 48, 257

legacy systems, 140

LGA (Land Grid Array) sockets, 237–238, 243–244

licenses (software), 763, 801–802

lifespans of OS/software, 457–458

Lightning cables, 180

Lightning connectors, 49, 56–57

line-of-sight (fixed) wireless Internet service, 158

link-local addresses, 144, 396–397

Linux

apt-get command, 593, 595–596

Bash, 817, 821–823

cd command, 593

chmod command, 593

chown command, 593

command line, 591–595

cp command, 593

dd command, 593

desktop distributions, 591–592

df-T command, 480

fdisk -l command, 480–481

file systems, 480–481, 592

GPT, 592

grep command, 593

GUI, 590

ifconfig command, 593–594

ip a command, 593

iwconfig command, 593

Kali, VM, 322

kernel panic errors, 596

kill command, 593

ls command, 593

man prefix (Linux commands), 595

mv command, 593

OS installation, file systems, 480–481

parted/dev/sda print command, 480–481

partitioning schemes, 592

passwd command, 593

ps command, 593

pwd command, 593

rm command, 593

shutdown command, 593

start commands, 595–596

su command, 593

sudo command, 593, 595–596

swap partitions, 481

Terminal, opening, 480

troubleshooting, 595–596

Ubuntu, VM, 320–321

vi command, 593

workstations, 451

liquid cooling systems, 241–242

local printers, 291

Local Security Policy (Windows), 516

local storage backups, 773–774

Local Users and Groups (Windows), 516

locator/tracker applications, 672–673

lockouts, mobile devices, 671

locks

cable locks, 43

physical, 604

screen locks, 670–671

log files, reviewing (troubleshooting), 331

logical drives, 476–477, 530

logical security, 608

AD, 610–614

authentication, 608–609

certificates, 619–620

DLP, 617–618

firewalls, 615–616

MDM, 618

MFA, 608–609

principle of least privilege, 609–610

trusted/untrusted software sources, 618–619

UAC, 609–610

VPN, 616–617

logins, desktop devices, 283
 logon hours, user accounts, 662–663
 logon scripts, 612–613
 lookup tables, 641
 loopback addresses, 145, 146, 498
 loopback plugs, 162
 loopbacks, crossover cables, 173
 loops, 815–816
 low memory error messages (printers), 383
 low RF signals, 396
 low-level formatting, 684–685
 LTO (Linear Tape-Open) backups, 770

M

M.2 cards, 34–36
MAC addresses, 36, 499–500
MAC filtering, 121–122, 695
macOS, 585–586
 application installation, 581
 Boot Camp, 588
 Dashboard, 587
 desktop, 586
 df-t command, 481
 Disk Utility, 589
 diskutil list command, 481
 Dock, 586
 file systems, 481
 Finder, 586
 Force Quit, 589
 gestures, 587
 GPT, 592
 GUI, 585–586
 iCloud, 589
 KB/articles, 759
 Keychain, 588
 ls -lh/private/var/vm/swapfile*
 command, 481
 maintenance, 589–590
 managing, 588–589
 Mission Control, 587
 partitioning, 481
 remote discs, 589
 Screen Sharing, 587–588
 spinning pinwheels, 589
 SPOD, 589
 Spotlight tool, 586
 Terminal, 480, 588–589
 Time Machine, 589
 updating, 590
 workstations, 450
magnetic hard drives. See HDD
magnetic readers, 254
mail servers, 135
malware, 628
 antimalware, 674–675
 best practices, 642
 botnets, 629, 640
 keyloggers, 629
 ransomware, 629
 removal procedure, 724–729
 rootkits, 628, 633–634
 spreading, 629
 spyware, 628, 632–633, 730
 Trojan horses, 628–632
 types of, 628–629
 viruses, 628–632, 729–730
 worms, 628–632
MAN (Metropolitan Area Networks), 153
man prefix (Linux commands), 595
Man-In-The-Middle attacks (MITM attacks), 640
managed/unmanaged switches, 102, 147
mantraps, 605
mapping drives, 572–573
mats (antistatic), 339
mATX (microATX) motherboards, 217–218
maximum clock rates, CPU, 234
MBR (Master Boot Records), 477–478
MDM (Mobile Device Management), 618, 671, 675, 678–679, 742
measured services, cloud computing, 315
mechanical keyboards, 251
membrane keyboards, 251
memory
 add-on storage/memory, 60
 cache memory, CPU, 236
 CF, 208
 compatibility, 188
 DDR2 RAM, 188

memory

- DDR3 RAM, 189
- DDR4 RAM, 189–190
- desktop RAM, 188
- DIMM, 188
- DRAM, 187–188
- flash memory, 48, 50
- installation, 13–16
- Kernel Memory Dumps, 714–715
- laptop RAM, 188
- low memory error messages (printers), 383
- NAND-based flash memory, 205–206
- optical drives, 208–212
- out of memory error messages (printers), 383
- RAM
 - BIOS updates, 194
 - compatibility, 188, 196
 - DDR2 RAM, 188
 - DDR3 RAM, 189
 - DDR4 RAM, 189–190
 - desktop RAM, 188
 - DIMM, 188
 - DRAM, 187–188
 - dual-channel RAM, 194
 - ECC, 196
 - firmware updates, 194
 - installation, 191–194
 - laptop RAM, 188
 - parity/nonparity, 196
 - quadruple-channel RAM, 194–196
 - single-channel RAM, 194
 - smartphones, 50
 - SODIMM, 188
 - swap partitions, 481
 - tablets, 48
 - testing, 344
 - testing installations, 192–193
 - troubleshooting, 342–344
 - UEFI updates, 194
 - underclocking, 194
- SODIMM, 188
- testing, 344
- video cards, 551–552
- Virtual Memory (Performance), 556–557
- Windows Memory Diagnostics, 518–519

- metered services, cloud computing, 315**
- MFA (Multifactor Authentication), 608–609, 670**
- mice, 252**
 - Device Manager (Windows 10), 252
 - displaying, 252
 - KVM switches, 259
 - laptop configuration, 283–284
 - sensitivity, 252
- microATX (mATX) motherboards, 217–218**
- microphones, 34, 253**
- Microsoft Knowledge Base, 758**
- Microsoft Support, 758–759**
- Microsoft TechNet, 759**
- Micro-USB ports, 49, 56–57**
- MIDI (Musical Instrument Digital Interface) devices, 254**
- MIL-STD-810 standard, 51**
- MIMO (Multiple-Input Multiple-Output) technology, 127**
- Mini PCIe cards, 34–36**
- Mini-ITX motherboards, 217–218**
- mirroring screens, 747–748**
- missing/corrupted files, 357–358**
- Mission Control (macOS), 587**
- MITM (Man-In-The-Middle) attacks, 640**
- MMC (Microsoft Management Console), 513–514**
- mobile devices. See laptops; smartphones; wearable technology devices**
- mobile hotspots, 59, 68–69**
- modems**
 - cable modems, 105, 120
 - dial-up modems, 105, 154–155
 - DSL modems, 105, 120, 155–156
- Molex power connectors, 265**
- monitors**
 - artifacting (video), 368–369
 - BSOD, 338–339, 713–715, 717
 - calibration, 368–369
 - CRT monitors, 366–367, 783
 - dual displays, 41
 - external monitors, 41–42, 747–748
 - filters, 369
 - fitness monitors, 52

- LCD, 256, 782–783
- LED displays, 257
- OLED displays, 257
- projectors, 257
- QLED, 257
- refresh rates, 553
- resolution, 550–551
 - aspect ratio, 551
 - color depth, 552–553
 - HD 1080i mode, 550
 - HD 1080p mode, 550
 - HD Ready mode, 550
 - list of resolutions, 550
 - modifying, 551
 - refresh rates, 553
 - troubleshooting, 551–552
 - UHD 4K mode, 550
 - VGA mode, 550
 - video cards, 551–552
 - video scaling, 552
 - WSXGA+ mode, 550
 - WUXGA mode, 550
 - WXGA mode, 550
- Screen Sharing (macOS), 587–588
- touchscreens, 284, 587
- troubleshooting, 368–369
- video cards, 551–552
- video scaling, 552
- motherboards, 216**
 - ATX motherboards, 216–218
 - audio ports, 226
 - BIOS, 226–229
 - bus speeds, 234
 - case connectors, 226
 - chipsets, 220
 - CMOS batteries, 227
 - CPU installations, 243
 - EATX12V power ports, 263–264
 - eSATA, 225–226
 - expansion buses, 218–220
 - expansion cards, 220–225
 - headless motherboards, 259
 - IMPI, 259
 - microATX (mATX) motherboards, 217–218
 - Mini-ITX motherboards, 217–218
 - NIC, 225
 - overclocking, 235
 - POST, 229
 - RAM, 195–196
 - riser boards, 226
 - RJ45 ports, 225
 - SATA connectors, 226
 - sockets, 237–238, 243–244
 - sound cards, 223–225
 - troubleshooting, 229, 338–340
 - UEFI, 226–228, 338
 - USB cards, 225
 - USB ports, 226
 - video cards, 221–223
- motion sensors, 254**
- mounting drives, 532–533**
- moving files/folders, 651–652**
- MSConfig (System Configuration tool), 523–524, 712**
- MSDS (Material Safety Data Sheets), 789–790**
- MSinfo32 (System Information), 537**
- MSTSC (Remote Desktop Connection), 539**
- MT (Megatransfers), 188**
- MU-MIMO technology, 127**
- multiboots, 475–476**
- multicore CPU, 235, 239**
- multifactor authentication, 639**
- multimeters, 162**
- multipath propagation, 127**
- multiple pages are fed at once, 383**
- multiple-choice questions (exam preparation), 880**
- multipurpose cables**
 - IDE cables, 182
 - Lightning cables, 180
 - SATA cables, 182
 - SCSI cables, 182
 - serial cables, RS-232 data transmission standard, 181–182
 - Thunderbolt cables, 180–181
 - USB cables, 178–179
- music, MIDI devices, 254**

N

NaaS (Network as a Service), 313

NAND-based flash memory, 205–206

NAS (Network-Attached Storage) servers, 134, 277–278

NAT (Network Address Translation), 120–121, 323

NetBIOS, 98, 502

NetBT, 98

network adapters, 118, 579

network boot (PXE) OS installations, 472

network cards, 578–580

networked hosts

- embedded systems, 139–140
- Internet appliances, 138–139
- legacy systems, 140
- server roles, 133–137

networks, 16–18

- botnets, 640
- bridges, 105
- brute-force attacks, 641
- cabling tools, 160–163
- cloud-based network controllers, 104
- connectivity, 394–396
- cryptanalysis attacks, 641
- DDoS attacks, 640–641
- dictionary attacks, 641
- extenders/repeaters, 104
- firewalls, 103, 138
- hubs, 104–105
- IPv4 addressing, 142–146
- IPv6 addressing, 146–147
- ISDN, 155
- LAN, 152
- laptops, 16–18
- MAN, 153
- MITM attacks, 640
- NIC, 103
- PAN, 153
- password cracking, 641–642
- patch panels, 105–106
- printers, 290–292
- PSTN, 155
- repeaters/extenders, 104
- routers, 102–103

security, 640–642

SOHO networks, 691

- antennas, 693–694

- AP, 693–694

- content filtering, 697

- MAC filtering, 695

- multifunction devices/printers, 290–292

- parental controls, 697

- passwords, 691–692

- physical ports, 696–697

- physical security, 696–697

- radio power levels, 693–694

- SSID, 692–693

- static IP addressing, 695–696

- WPS, 694

spoofing attacks, 640

switches, 101–102, 105

topology diagrams, 756–758

troubleshooting, 394–397

VLAN, 147–148

VM, 323–324

VPN, 148, 616–617

WAN, 153

WAP, 102–103

Windows

- administrative shares, 571–572

- alternate IP addresses, 577–578

- data access, 570–573

- data sharing, 570–573

- domains, 568–569

- establishing connections, 574–576

- full duplex network adapters, 579

- half duplex network adapters, 579

- HomeGroup, 568, 572

- mapping drives, 572–573

- network cards, 578–580

- printer sharing, 573–574

- proxy server settings, 576–577

- workgroups, 568–570

WMN, 153

zero-day attacks, 640

zombies, 640

new user accounts, 647–648

NFC (Near Field Communication), 59, 254

NFS (Network File Systems), 480
NIC (Network Internet Cards), 103,
 116–118, 225
NMI (Non-Maskable Interrupts), 344
NMS (Network Management System),
 97, 98
no networking option, VM, 323
No OS found messages, 717
non-parity/parity, RAM (Random Access
Memory), 196
Notepad, 493, 535
Notification Area (Windows Desktop),
 467–468
NTFS (NT File System), 478, 494, 649–650

O

ODBC (Data Sources), 522
offline files, managing, 563–564
OLED displays, 30–32, 257
on-demand services, cloud computing, 316
open source software, 455, 802
optical drives, 16, 208–212, 472
Optimize Drives, 534–535
orientation (page), 289–290
OS (Operating Systems), 49, 450, 451. See
also iOS; Linux; macOS, Windows
 32-bit CPU architectures, 451–453
 64-bit CPU architectures, 451–453
 Android, 454–455, 675, 743
 bootup process, 472–473, 475–476
 closed-source software, 455
 compatibility, 458–459
 end-of-life/end-of-support dates, 457–458
 FreeBSD, 595
 installing
 application compatibility, 484
 basic drives, 477
 bootup process, 472–473
 CDFS, 479–480
 clean installs, 473
 compatibility, 484
 date/time settings, 482
 domains, 482
 driver installations, 482
 dynamic drives, 477
 exFAT (FAT64), 478–479
 extended partitions, 476–477
 FAT, 478–479
 FAT32, 478–479
 file systems, 478–479
 formatting, 478–479
 GPT, 477–478
 hardware compatibility, 484
 image deployments, 474
 language settings, 482
 Linux file systems, 480–481
 logical drives, 476–477
 macOS file system, 481
 MBR, 477–478
 multiboots, 475–476
 NFS, 480
 NTFS, 478
 partitioning, 476–478, 482–484
 prerequisites, 484
 primary partitions, 476–477
 recovery discs/partitions, 475, 484
 Refresh your PC, 475
 regional settings, 482
 remote network installations, 474–475
 Reset your PC, 475
 software installations, 482
 third-party drivers, 481
 time/date settings, 482
 unattended installations, 474
 upgrade installations, 473
 upgrade paths, 484
 Windows file system, 478–479
 Windows updates, 482
 workgroups, 482
 iPads, 49
 lifespans, 457–458
 mobile devices, 453–455, 738–751
 open source software, 455
 OS X. *See* macOS
 “parked” states, 354
 partitioning, 476–478, 482–484
 PRI, 75
 smartphones, 453–455
 tablets, 453–455
 updating, PRI, 75

OS (Operating Systems)

- vendor-specific limitations, 457–458
- workstations, 450–451, 659–665
- x64, 452
- x86, 452

OU (Organizational Units), 611–612**out of memory error messages (printers), 383****overclocking, 235, 239****overheating, 347–348, 368, 373–375, 382****overwriting hard drives, 685–686****ownership, files/folders, 651****P****PaaS (Platform as a Service), 313****packets (data), latency, 497****page orientation (printing), 289–290****page printers, 294–298****PAN (Personal Area Networks), 17, 153****paper/printers**

- blank pages, 382
- creased paper, 382
- jams, 382
- multiple pages are fed at once, 383
- paper not feeding, 383
- streaks/smearing on page, 383
- vertical lines on page, 383

paper clips, 210**parental controls, SOHO networks, 697****“parked” states, OS, 354****partitioning, 476**

- Disk Management, 482–483, 530–531
- diskpart command, 493
- diskpart utility, 482–483
- letter assignments (volumes), 477
- Linux partitions, 480–481, 592
- macOS partitions, 481
- OS installation, 475–478, 482–484
- swap partitions, 481
- volumes, 477, 531–532

passwords

- BIOS, 228
- brute-force attacks, 641
- cracking, 641–642
- cryptanalysis attacks, 641

- desktop devices, 283
- dictionary attacks, 641
- Keychain (macOS), 588
- policies, 762–763
- precomputation attacks, 641
- SOHO networks, 691–692
- SOHO routers, 113
- spam prevention, 731
- synchronization, 84
- user accounts, 647
- visible passwords, disabling, 671
- workstations, 659–661

patch cables, 161**patch management, 537****patch panels, 105–106****patch testers, 162****Path variable, 817****payments, tap pay devices, 254****PCH (Platform Control Hubs), 237****PCI (Peripheral Component Interconnect) buses, 220****PCI-DSS (Payment Card Industry Data Security Standards), 804****PCIe (PCI Express)**

- expansion buses, 218–220
- power connectors, 265–266
- Thunderbolt cables, 181
- video cards, 221–223

PDF files, 304**performance**

- Performance Monitor (Windows), 516–518
- performance-based questions (exam preparation), 880
- Virtual Memory, 556–557
- Windows computers, 716

permissions

- files/folders, 648–651
- inheritance, 650–651
- lockouts, 663–664
- NTFS permissions, 649–650
- printers, 291
- propagation, 650–651
- share permissions, 649
- SOHO multifunction devices/printers, 291

- user accounts, 662
- user permissions, applications, 582
- PGA (Pin Grid Arrays), 24–25, 238, 244**
- PHI (Protected Health Information), 803–804**
- phishing, 637–638**
- phishing filters, 632–633**
- phones See smartphones**
- physical destruction of hard drives, 688–689**
- physical ports, disabling, 696–697**
- physical safety, 784**
 - cable management, 785
 - ergonomics, 785–786
 - heavy objects, lifting, 785
 - hot components, 785
 - tools/equipment, 785
- physical security, 604**
 - badge readers, 604–605
 - biometric security, 605–606
 - data, 606
 - entry control rosters, 604–605
 - entry systems, 604–605
 - hardware-based tokens, 605
 - key fobs, 604–605
 - locks, 604
 - mantraps, 605
 - smart cards, 605
 - SOHO networks, 696–697
 - workplace safety, 785
- piezoelectric inkjets (inkjet printers), 298**
- piggybacking/tailgating, 638–639**
- PII (Personally Identifiable Information), 803–804**
- pinwheels (spinning), macOS, 589**
- PIV (Personal Identity Verification), 16**
- In-Plane Switching (IPS), LCD, 256**
- PLC (Power-Line Communication), 107**
- plenum-rated cables, 173–174**
- PNAC (Port-based Network Access Control), 626**
- PoE (Power over Ethernet), 106**
- pointing sticks, 11**
- POP3 (Post Office Protocol Version 3), 72–73, 93, 98**
- port forwarding, 121**
- port replicators, 42**
- ports**
 - audio ports, 226
 - EATX12V power ports, 263–264
 - email configuration, 72–73
 - IANA list, 99
 - KVM switches, 259
 - Lightning ports, 180
 - Micro-USB ports, 49, 56–57
 - physical ports, disabling, 696–697
 - PNAC, 626
 - RJ45 ports, 225
 - security, PNAC, 626
 - USB ports, 226
 - USB-C ports, 49, 56–57
 - video ports, 176–178
- POST (Power-On Self-Tests), 229, 339**
- post-incident activity (incident response), 800**
- POTS (Plain Old Telephone Service), 155**
- power connectors, 265–266**
- Power Management (Windows Control Panel), 557–558**
- power supplies, 262**
 - ATX, 217, 263–264
 - capacity requirements, 264–265
 - compatibility, 263–264
 - EATX12V power ports, 263–264
 - electrical safety, 782–783, 792–794
 - FRU, 782
 - installing, 266–268
 - PSU, 262, 264, 266
 - rails, 264
 - recycling/disposal, 790
 - testing, 345
 - troubleshooting, 344–347
 - types of, 263–264
 - UPS, 783, 792–794
 - wattage, 264–265
- Power User accounts, 646**
- PowerShell, 489–490**
 - comment syntax, 817–818
 - constructs, 815–816
 - environment variables, 817

PowerShell

IF-THEN statements, 815

loops, 816

Path variable, 817

psl files, 818–821

VBScript, 825–827

precomputation attacks, 641

preparation (incident response), 799

PRI (Product Release Instructions), 75

PRI ISDN (Primary Rate ISDN), 155

primary partitions, 476–477

Print Management (Windows), 518

print servers, 135

print to image (virtual printing), 304

printers, 294

3D printers, 301–302, 385

calibrating, 305–306

cloud-based printing, 292

compatibility, 305

configuring, 288–290

connectivity, 305, 384

daisy wheel printers, 300

data privacy, 292

Devices and Printers (Windows Control Panel), 561

displays, 383

dot matrix printers, 300

drivers, 305, 383

duplexing printers, print paths, 382

impact printers, 300, 385

inkjet printers, 298–299, 383, 385

installing, 305–306, 384

laser printers, 294–298, 383, 385, 783

local printers, 291

maintenance, 384–385

managing, 385–386

networking, 290–292

no image on printer display, 383

overheating, 382

page printers, 294–298

permissions, 291

preferences, 290

quality of printing (resolution), 290

resolution, 290

RIP, 384

sharing, 290–292, 573–574

spooling, 386–388

testing installations, 306

thermal printers, 299–300, 385

troubleshooting, 381–382, 385, 717

Access Denied error messages, 384

backed-up print queues, 384

color errors, 384

connectivity, 384

creased paper, 382

drivers, 383

drums, 383

error codes, 383

faded prints, 383

failed print jobs (multiple), 384

garbage printouts, 383

garbled characters, 383

ghosted images, 383

inkjet printers, 383

installation, 384

laser printers, 383

low memory error messages, 383

multiple pages are fed at once, 383

no image on printer display, 383

out of memory error messages, 383

overheating, 382

paper jams, 382

paper not feeding, 383

printing blank pages, 382

streaks/smearing on page, 383

toner, 382–383

transfer corona wires, 382–383

vertical lines on page, 383

virtual printing, 302–304

Windows computers, 717

Windows Print Spooler, 386–388

privacy

confidential/private material (communication techniques/professionalism), 810–811

data privacy, printers, 292

Privacy tab (Internet Options), 549

WEP (Wireless Equivalent Privacy), 624

private clouds, 314

PRL (Preferred Roaming List) updates, 75

probe kits, 161

processors, 24–25

professionalism/communication techniques, 808–811

Program Compatibility (Windows Control Panel), 560–561

Programs and Features (Windows Control Panel), 559

Programs tab (Internet Options), 549

projectors (video), 257

propagation (permissions), 650–651

proxy servers, 135–136, 576–577, 632–633

PS/2 (Personal System/2) connectors, 251

psl files, 818–821

PSTN (Public Switched Telephone Networks), 155

PSU (Power Supply Units), 262, 264, 266, 345

public clouds, 314

punchdown tools, 161

purging hard drives, 687–688

PXE (Preboot Execution Environment), 472

Python, 825

Q

QLED, 257

QoS (Quality of Service), SOHO router firewalls, 122–123

QR scanners, 254

quadruple-channel RAM, 194–196

quality of printing (resolution), 290, 297

queues (print), backed-up, 384

quick death (power supplies), 346

quick formatting, 479

Quick Launch (Windows Desktop), 467

quitting, Force Quit (macOS), 589

R

radio power levels, security, 693–694

RADIUS (Remote Authentication Dial-In User Service), 625–626

RAID (Redundant Array of Independent Disks), 202–204

RAID arrays, 359–361. See also Storage Spaces

rails, 264

rainbow tables, 641

RAM (Random Access Memory)

compatibility, 188, 196

DDR2 RAM, 188

DDR3 RAM, 189

DDR4 RAM, 189–190

desktop RAM, 188

DIMM, 188

DRAM, 187–188

dual-channel RAM, 194

ECC, 196

installation, 191–194

laptop RAM, 188

parity/nonparity, 196

quadruple-channel RAM, 194–196

single-channel RAM, 194

smartphones, 50

SODIMM, 188

swap partitions, 481

tablets, 48

testing, 344

testing installations, 192–193

troubleshooting, 342–344

underclocking, 194

ransomware, 629, 733

rapid elasticity, cloud computing, 316

RDP (Remote Desktop Protocol), 96–98

recovery

backups and, 769–775

disaster prevention and, 769

incident response, 800

recovery discs/partitions, 475, 484

recycling/disposal

batteries, 790

ink/toner cartridges, 790

mobile devices, 790–791

redirecting browsers, 733

refresh rates, 367, 553

Refresh your PC, 475

regional settings, 482

Registry Editor, 541

regulated data, 803–805

regulatory/compliance policies, 761

remote access, 827–833

Remote Assistance, 829

remote connectivity, 543

remote control of computers by unknown entities

remote control of computers by unknown entities, 733

Remote Desktop Connection (MSTSC), 539

remote discs, 589

remote network OS installations, 474–475

repair kits, 33

repeaters/extenders, 104

replacing batteries in mobile devices, 61

Reset your PC, 475

resolution

displays, 550–553

printing, 290, 297

video, 367

resource pooling, 316

restore points, 728

reverse proxies, 136

RF signals, 396

RFID (Radio Frequency Identification), 129

RG-6 coaxial cables, 174–175

RG-6/U coaxial cables, 175

RG-6/UQ coaxial cables, 175

RG-58 coaxial cables, 175

RG-59 coaxial cables, 174

RIP (Raster Image Processing), 384

riser boards, 226

RJ11 plugs, 172–173

RJ45 crimpers, 161

RJ45 plugs, 172–173

RJ45 ports, 225

roaming profiles, 612

rooting Android devices, 675

rootkits, 628, 633–634

rosters (entry control), 604–605

rotating screens, 42–43

rotational speeds, HDD, 201

routers, 102–103, 112, 115, 691, 697

accessing, 112–113

antennas, 693–694

AP, 693–694

content filtering, 697

default settings, 112

firewalls, 120–123

LAN connections, 113–114

MAC filtering, 695

parental controls, 697

passwords, 113, 691–692

physical ports, 696–697

physical security, 696–697

placement, 124

plug-and-play, 112

radio power levels, 693–694

security, 112–113

SSID, 692–693

static IP addressing, 695–696

WAN connections, 113–114

wireless encryption, 123–124

WPS, 694

RS-232 data transmission standard, 181–182

S

S/MIME (Secure/Multipurpose Internet Mail Extensions), 74

SaaS (Software as a Service), 312–313

Safe mode, 712, 745

safety

antistatic mats, 339

antistatic wrist straps, 339

electrical safety, 780–784, 791–794

fire safety (electrical), 783–784

physical safety, 784–786

procedures, 779–780

workplace safety, 785

sags (electrical safety), 791

SATA (Serial ATA)

cables, 182

connectors, 226

controllers, 339

hard drives, 11–12, 198–200

magnetic disk drives, 358

power connectors, 265

saving documents, 250

SC connectors, 175–176

scaling video, 552

scanners, 253, 254

Screen Sharing (macOS), 587–588

screens, 18–19

filters, 638

locks, 670–671

- mirroring, 747–748
- removable screens, 42–43
- rotating screens, 42–43
- screwdrivers, 33**
- scripting, 813, 827**
 - batch files (bat), 820
 - command_block, 816
 - comment syntax, 817–818
 - Condition command, 816
 - constructs, 815–816
 - data types, 814
 - environment variables, 817
 - floating-point numbers, 814
 - IF statements, 815
 - IF-THEN statements, 815
 - Init command, 816
 - integers, 814
 - iterations, 815
 - js files, 823–824
 - for loops, 815–816
 - loops, 815–816
 - Path variable, 817
 - psl files, 818–821
 - py files, 825
 - Repeat command, 816
 - sh files, 821–823
 - strings, 814
 - vbs files, 825–827
 - while loops, 816
- SCSI (Small Computer System Interface) cables, 182**
- SD (Secure Digital) cards, 206–208, 676**
- SDSL (Symmetrical Digital Subscriber Lines), 156**
- Search tool (Windows), 488**
- searches (macOS), 586**
- secondary drives, 356**
- secondary IP addresses, 145**
- security, 603**
 - 802.1X, 626
 - AD, 610–614
 - administrative shares, 653–654
 - AES, 624–625
 - antimalware, 674–675
 - antivirus software, 674–675
 - AP, 693–694
 - applications, 582
 - AUP, 631
 - authentication, 608–609, 624–626, 639, 648, 664, 670, 672
 - AutoPlay, disabling, 664–665
 - AutoRun, disabling, 664–665
 - backups, 634
 - badge readers, 604–605
 - best practices, 642
 - biometric security, 605–606, 670
 - BIOS, 228
 - BitLocker, 655–656
 - botnets, 629, 640
 - browsers, 733
 - brute-force attacks, 641
 - cable locks, 43
 - certificates, 619–620, 632–633
 - CIA triad, 646
 - compromised/damaged mobile devices, 673–679
 - cryptanalysis attacks, 641
 - data destruction/disposal, 684–689
 - DDoS attacks, 640–641
 - desktop devices, 283
 - dictionary attacks, 641
 - DLP, 617–618
 - dumpster diving, 639
 - email, 731–733, 741–742
 - encryption, 123–124, 624–626, 676–677, 741–742
 - entry control rosters, 604–605
 - entry systems, 604–605
 - file systems, 654–655
 - files/folders, 648–654
 - firewalls, 103, 519, 615–616
 - full device encryption, 676–677
 - hard drives, 684–689
 - hardware-based tokens, 605
 - hijacking
 - email, 731–732
 - sessions, 632–633
 - impersonation, 639
 - information security, 646–656, 664–665
 - Internet appliances, 138–139
 - invalid certificate issues/trusted root CA, 733
 - jailbreaking, 674–675

- Keychain (macOS), 588
- keyloggers, 629
- laptops, 34, 43, 669–677
- Local Security Policy (Windows), 516
- locator/tracker applications, 672–673
- lockouts, 663–664
- locks (physical), 604
- logical security, 608–620
- logon hours, 662–663
- malware, 628–634, 640, 642, 724–730
- mantraps, 605
- MDM, 618, 675, 678–679
- MFA, 608–609, 670
- microphones, 34
- MITM attacks, 640
- mobile devices, 669–677
- multifactor authentication, 639
- parental controls, SOHO networks, 697
 - passwords, 84, 113, 283, 588, 641–642, 647, 659–661, 671, 691–692, 731, 762–763
- PC, 724–733
- PCI-DSS, 804
- permissions, 648–652, 662
- phishing, 637–638
- phishing filters, 632–633
- physical security, 604–606, 696–697
- piggybacking/tailgating, 638–639
- ports, 626, 696–697
- precomputation attacks, 641
- principle of least privilege, 609–610
- printers, 292
- proxy servers, 632–633
- radio power levels, 693–694
- RADIUS, 625–626
- ransomware, 629, 733
- redirecting browsers, 733
- remote control of computers by unknown entities, 733
- restoring systems, 634
- rooting, 675
- rootkits, 628, 633–634
- routers, 691
 - antennas, 693–694
 - AP, 693–694
 - content filtering, 697
 - MAC filtering, 695
 - parental controls, 697
 - passwords, 691–692
 - physical ports, 696–697
 - physical security, 696–697
 - radio power levels, 693–694
 - SOHO routers, 112–113, 691–697
 - SSID, 692–693
 - static IP addressing, 695–696
 - WPS, 694
- SD cards, 676
- Security logs, 520
- security profiles, 679
- Security tab (Internet Options), 549
- session hijacking, 632–633
- shoulder surfing, 638
- Sleep mode, user accounts, 664
- smart cards, 605
- smartphones, 669–677
- social engineering, 637–639
- software, trusted/untrusted, 618–619
- SOHO networks, 691
 - antennas, 693–694
 - AP, 693–694
 - content filtering, 697
 - MAC filtering, 695
 - multifunction devices/printers, 292
 - parental controls, 697
 - passwords, 691–692
 - physical ports, 696–697
 - physical security, 696–697
 - radio power levels, 693–694
 - routers, 112–113, 691–697
 - SSID, 692–693
 - static IP addressing, 695–696
 - WPS, 694
- spam, 730–731
- spoofing attacks, 640
- spyware, 628, 632–633, 730
- SSO authentication, 648, 664
- system restores, 634
- tablets, 669–677
- tailgating/piggybacking, 638–639
- threat models, 677
- TKIP, 624

- tracker/locator applications, 672–673
- Trojan horses, 628–632
- trusted root CA/invalid certificate issues, 733
- trusted/untrusted software sources, 618–619
- UAC, 609–610
- user accounts, 646–648, 656, 662–664
- virtualization, 323–324
- viruses, 628–632, 713, 729–730
- VM, 323–324
- VPN, 616–617
- webcams, 34
- WEP, 624
- Wi-Fi antennas, 693–694
- Windows Defender Firewall with Advanced Security, 519, 616
- wired connections, 691–692
- wireless connections, 691–697
- wireless security, 624–626
- workstations, 659–664
- worms, 628, 629–632
- WPA, 624
- WPA2, 624–626
- WPA2-Enterprise, 625–626
- WPA2-Personal, 625
- WPS, disabling, 694
- zero-day attacks, 640
- zombies, 640
- self-grounding, 780**
- sensitivity, mice, 252**
- serial cables, 181–182**
- servers, 133–134**
 - authentication servers, 136
 - DHCP servers, 136, 143
 - DNS servers, 136–137, 144–145
 - endpoint management servers, 139
 - file servers, 134
 - mail servers, 135
 - NAS servers, 134, 277–278
 - print servers, 135
 - proxy servers, 135–136, 576–577, 632–633
 - syslog servers, 137
 - virtualization servers, 324
 - web servers, 134–135
- Services console (Windows), 518**
- session hijacking, 632–633**
- SFC (System File Checker), 495**
- sh files, 821–823**
- share permissions, 649**
- shares (administrative), 653–654**
- sharing**
 - data, Windows networks, 570–573
 - printers, 290–292, 573–574
 - Screen Sharing (macOS), 587–588
 - SOHO multifunction devices/printers, 290–292
- shielded twisted-pair cables, 174**
- shoulder surfing, 638**
- shrinking volumes, 531**
- shutdowns, 712–713**
- side-by-side applications, Windows GUI, 469**
- signal attenuation, 173**
- signal boosters, 178**
- signature pads, 254**
- simple storage spaces, 533**
- single-channel RAM, 194**
- single-mode fiber optic cables, 175**
- Sleep mode, 557–558, 664**
- slow death (power supplies), 347**
- slow transfer speeds (networks), 395–396**
- SLP (Service Location Protocol), 98**
- smart card readers, 16, 254**
- smart cards, security, 605**
- S.M.A.R.T. data, 357–358, 360–361**
- smartphones, 49–50**
 - accessories, 60–61
 - add-on storage/memory, 60
 - airplane mode, 67–68, 74–75
 - antimalware, 674–675
 - antivirus software, 674–675
 - applications, 743–744, 747
 - audio accessories, 60
 - authenticator applications, 672
 - backups, 80, 673
 - batteries, 50, 61, 373–375
 - biometric security, 670
 - Bluetooth devices, 69–71

smartphones

BYOD environments, 677–678
 cellular connections, 74–75, 76
 cellular networks, 50
 cleaning, 375
 compromised/damaged mobile devices, 673–679
 COPE environments, 677–678
 CPU, 50
 CYOD environments, 678
 digitizers, 32–33
 displays, 50
 disposal/recycling, 790–791
 email configuration, 71–74
 flash memory, 50
 full device encryption, 676–677
 hardware specifications, 50
 IP, 50–51
 locator/tracker applications, 672–673
 lockouts, 671
 loss of, 672–673
 MDM, 618, 670–671, 675, 678–679, 742
 MIL-STD-810 standard, 51
 mobile hotspots, 68–69
 monitors (external), 747–748
 OS, 453–455, 747
 pairing/linking devices, 69–71
 RAM, 50
 recycling/disposal, 790–791
 repair kits, 33
 resetting, 744–746
 screen locks, 670–671
 screen mirroring, 747–748
 security, 669–679, 748–750
 synchronization, 79–84
 theft of, 672–673
 touchscreens, 32–33, 50
 troubleshooting, 372–377, 738–745, 747–748
 two-step authentication, 672
 updating, 674
 USB tethering, 69
 wireless connections, 66–71, 74–76

smartwatches, 52

SMB (Server Message Block) protocol, 97, 98

smearing/streaks on page (printers), 383

smells (burning), 348

smoke, 348

SMTP (Simple Mail Transfer Protocol), 73, 92–93, 98

Snap technology, 469

SNMP (Simple Network Management Protocol), 97–98

SNMPTRAP, 98

SoC (System on a Chip), tablets, 49

social engineering, 637–639

 sockets, 237–238, 243–244

SODIMM (Small Outline Dual Inline Memory Modules), 13–16, 188

soft resets, 744

software

 antivirus software, 674–675

 AUP, 631

 closed-source software, 455

 end-of-life/end-of-support dates, 457–458

 licenses, 763, 801–802

 lifespans, 457–458

 open source software, 455

 OS installation, 482

 security, 618–619

 trusted/untrusted software sources, 618–619

 vendor-specific limitations, 457–458

SOHO networks

 AP settings, 115–116

 cable modem configurations, 120

 DSL modem configurations, 120

 end-user device configuration, 117–118

 IoT device configuration, 118–120

 multifunction devices/printers, 288–292

 NIC, 116–118

 routers, 103, 112–115, 120–124, 697

 security, 691–697

solid-state drive (SSD), formatting, 493

sound

 modifying devices, 562

 Sound (Windows Control Panel), 561–562

 sound cards, 223–225

 speakers, 23, 258, 376, 562

spam, preventing/troubleshooting, 730–731

speed

- clock speeds, 234
- defined, 118
- laser printers, 297
- PCIe expansion buses, 219–220
- Thunderbolt cables, 181
- unshielded twisted-pair cables, 170–171
- USB cables, 178–179

spinning pinwheels (macOS), 589**splitters, video cables, 178****splitting volumes, 531****SPOD (Spinning Pinwheels of Death), 589****spontaneous/improper shutdowns, 712–713****spoofing attacks, 640****spooling (printers), 386–388****Spotlight tool (macOS), 586****spyware, 628, 632–633, 730****SSD (Solid-State Drives), 11–12, 201–202, 493****SSH (Secure Shell), 94, 98, 831–833****SSID (Service Set Identifiers), 67, 692–693****SSL (Secure Sockets Layer), email configuration, 72–73****SSO (Single Sign-On) authentication, 83, 648, 664****ST connectors, 175–176****standard thick clients, 280, 282–283****Standard User accounts, 554, 646, 656****standby mode (Power Management), 557–558****star topologies, 102, 152****Start menu (Windows Desktop), 467****Start screen (Windows 8/8.1), 466****Startup Settings, 707–709****static IP addressing, 695–696**

- static IPv4 addressing, 143, 145
- static IPv6 addressing, 147

stop errors (BSOD), 713–715, 717**stopping applications, 743–744****storage**

- add-on storage/memory, 60
- CF, 208
- cloud storage backups, 773–774
- flash drives, 204–208
- hard drives, 198–201, 204–208

HDD, 200–201**local storage backups, 773–774****NAND-based flash memory, 205–206****NAS servers, 134, 277–278****optical drives, 208–212****parity, 533****RAID, 202–204. *See also* Storage Spaces****RAM****BIOS updates, 194****compatibility, 188, 196****DDR2 RAM, 188****DDR3 RAM, 189****DDR4 RAM, 189–190****desktop RAM, 188****DIMM, 188****DRAM, 187–188****dual-channel RAM, 194****ECC, 196****firmware updates, 194****installation, 191–194****laptop RAM, 188****parity/nonparity, 196****quadruple-channel RAM, 194–196****single-channel RAM, 194****SODIMM, 188****testing installations, 192–193****UEFI updates, 194****SATA drives, 198–200****SD cards, 206–208****simple storage spaces, 533****SSD, 201–202****Storage Spaces, 533. *See also* RAID****three-way mirror storage spaces, 533****two-way mirror storage spaces, 533****USB flash drives, 205–206****straight-through cables, 173****streaks/smearing on page (printers), 383****streaming virtual applications, 314–315****strings, 814****stuck/dead pixels (video), 368****styluses, 32–33****subnet masks, 144, 145****surge protectors, 783, 792****surges (electrical safety), 791, 792****SVGA cables, 177**

swap partitions

swap partitions, 481

switches, 101

- Ethernet standard, 102
- flood attacks, 105
- KVM switches, 259
- LAN, 102
- managed/unmanaged switches, 102, 147
- ping command, 498–499
- star topologies, 102
- unmanaged/managed switches, 102, 147
- virtual switches, 324

SYN packets, 90

SYN-ACK packets, 90

Sync Center (Windows Control Panel), 563–564

synchronization

- applications in cloud computing, 315
- mobile devices, 79–84
- passwords, 84

syslog servers, 137

system board, laptops, 24–25

System Configuration tool (MSConfig), 523–524

System Image Backups, 770–771

System Information (MSinfo32), 255, 537

System logs, 520

System Restore, 538–539, 634, 726–728

System Utilities, 534–535

- DxDiag, 540
- File Explorer, 535–536
- Notepad, 535
- patch management, 537
- Remote Desktop Connection (MSTSC), 539
- System Information (MSinfo32), 537
- System Restore, 538–539
- Windows Explorer, 535–536
- Windows Registry, 541–543
- Windows Update, 536–537

System Window, testing RAM installations, 192

T

tables

- lookup tables, 641
- rainbow tables, 641

tablets, 48

- accessories, 60–61
- add-on storage/memory, 60
- airplane mode, 67–68, 74–75
- Android tablets, 49, 56–57
- antimalware, 674–675
- antivirus software, 674–675
- applications, 743–744, 747
- ARM, 49
- audio accessories, 60
- authenticator applications, 672
- backups, 80, 673
- batteries, 49, 61, 373–375
- biometric security, 670
- Bluetooth devices, 69–71
- BYOD environments, 677–678
- cameras, 49
- cellular connections, 74–76
- cleaning, 375
- cloud-based backups, 80
- compromised/damaged mobile devices, 673–679
- COPE environments, 677–678
- CPU, 48–49
- CYOD environments, 678
- digitizers, 32–33
- disposal/recycling, 790–791
- email configuration, 71–74
- flash memory, 48
- full device encryption, 676–677
- goals for, 49
- hardware specifications, 48–49
- iPads, 49, 56–57
- locator/tracker applications, 672–673
- lockouts, 671
- loss of, 672–673
- MDM, 618, 670–671, 675, 678–679, 742
- MIL-STD-810 standard, 51
- mobile hotspots, 68–69
- monitors (external), 747–748
- OS, 49, 453–455, 747
- pairing/linking devices, 69–71
- RAM, 48
- recycling/disposal, 790–791
- repair kits, 33
- resetting, 744–746

- screen locks, 670–671
- screen mirroring, 747–748
- security, 669–679, 748–750
- SoC, 49
- synchronization, 79–84
- theft of, 672–673
- touchscreens, 32–33, 48
- troubleshooting, 371–377, 738–741, 743–744, 747–748
- two-step authentication, 672
- updating, 674
- USB tethering, 69
- wireless connections, 66–71, 74–76
- writing tablets, 253
- tailgating/piggybacking, 638–639**
- tap pay devices, 254**
- Task Manager, 192–193, 250, 524–526**
- Task Scheduler (Windows), 518**
- taskbar (Windows Desktop), 467**
- TCP (Transmission Control Protocol), 90–91**
- TCP/IP (Transmission Control Protocol/Internet Protocol), 145–146, 498, 502**
- TDP (Thermal Design Power) ratings, CPU, 239**
- TechNet (Microsoft), 759**
- Telnet, 94, 98, 833**
- temperature measurements (environmental controls), 788**
- Terminal (Linux/macOS), opening, 480–480, 588–589**
- testing**
 - backups, 772–773
 - CPU installations, 244–245
 - host availability, 497
 - memory, 344
 - power supplies, 345
 - printer installations, 306
 - RAM, 192–193, 344
 - TCP/IP installations, 498
 - video cards, 222–223
- tethering mobile devices, 58, 69**
- thermal compound, 240–241**
- thermal inkjets (inkjet printers), 298**
- thermal printers, 299–300, 385**
- thick clients (standard), 280, 282–283**
- thin clients, 278–279, 282–283**
- third-party drivers, 481**
- threat models (security), 677**
- three-way mirror storage spaces, 533**
- throughput (data), 118**
- Thunderbolt cables, 180–181**
- Time Machine (macOS), 589**
- time/date settings, 482**
- TKIP (Temporal Key Integrity Protocol), 123, 624**
- TLS (Transport Layer Security), 72–73**
- TN (Twisted Nematic) technology, 256**
- tokens (hardware-based), security, 605**
- tone generators, 161**
- toner/ink cartridges, 296–297, 382–383, 790**
- topologies**
 - network topology diagrams, 756–758
 - star topologies, 102, 152
- touchpads, 10–11, 253**
- touchscreens, 32–33, 50, 259, 284, 376, 587**
- tracker/locator applications, 672–673**
- TrackPoint, 11**
- transfer corona wires (printers), 382–383**
- transfer speeds (networks), 395–396**
- Trojan horses, 628–632**
- troubleshooting, 329, 348. See also configuration**
 - air flow, 347–348
 - APIPA, 396–397
 - applications, 717, 743–744, 747
 - artifacting (video), 368–369
 - backlights, 32
 - backups, 332
 - batteries, 373–375
 - Bluetooth, 740–741
 - bootups, 716, 717
 - brightness (displays), 372–373
 - BSOD, 338–339, 344, 367–368, 713–715, 717
 - burning smells, 348
 - connectivity, Windows computers, 717
 - corrupted/missing files, 357–358
 - CPU, 340–342
 - CRT monitors, 366–367
 - dim displays, 372–373
 - DirectX, 368

troubleshooting

- disassembly processes, mobile devices, 376–377
- displays, 31–32, 41–42, 368–369, 376, 747–748
- email, 72, 741–742
- external monitors, 41–42, 747–748
- firewalls, 616
- hard drives, 354–358
- improper/spontaneous shutdowns, 712–713
- Internet-based (remote) resources, 394
- inverters, 31–32
- IP addresses, 396–397
- kernel panic errors, 596
- keyboards, 8–10
- KVM switches, 366–367
- laptops, 31–32, 372–377, 738–744, 747–750
- link-local addresses, 396–397
- Linux, 595–596
- local network resources, 394
- methodology of, 330–334
- missing files at startup, 357
- missing/corrupted files, 357–358
- mobile devices, 375–377, 738–744, 747–750
- monitors, 368–369, 747–748
- motherboards, 229, 338–340
- networks, 394–397
- No OS found messages, 717
- overheating, 347–348, 373–375
- performance, Windows computers, 716
- power supplies, 344–347
- printers, 381–385, 717
- RAID arrays, 359–361
- RAM, 342–344
- remote (Internet-based) resources, 394
- resolution (displays), 551–552
- restoring systems, 538–539
- RF signals, 396
- SATA, 339, 358
- screen mirroring, 747–748
- security, 748–750
- shutdown command, 712–713
- smartphones, 371–377, 738–741, 743–744, 747–750
- smoke, 348

- spam, 730–731
- speakers, 376
- spontaneous/improper shutdowns, 712–713
- spyware, 632–633
- stop errors (BSOD), 713–715, 717
- System Restore, 538–539
- tablets, 372–377, 738–744, 747–750
- touchpads, 10–11
- touchscreens, 376
- Troubleshooting (Windows Control Panel), 563
- upgrades, power drains, 347
- user profiles, 718–719
- video, 366–370
- video cards, 368–369
- Wi-Fi, 738–740
- Windows, 704–719
- Windows Boot Manager (bootmgr), 710–712
- wireless connections, 738–740

trucks/cars

- Android Auto, 82–83
- Apple CarPlay, 82–83
- mobile device synchronization, 82–83

truncated IPv6 addresses, 147**trusted root CA/invalid certificate issues, 733****trusted/untrusted software sources, 618–619****twisted-pair cables, 170**

- cabling tools, 163
- shielded twisted-pair cables, 174
- unshielded twisted-pair cables, 114, 170–174

two-step authentication, 672**two-way mirror storage spaces, 533****U****UAC (User Account Control), 609–610****Ubuntu, 320–321, 591–592****UDP (User Datagram Protocol), 90–91****UEFI (Unified Extensible Firmware Interfaces), 8, 194, 226–229, 338, 367****UHD 4K mode (displays), 550**

unattended OS installations, 474
underclocking, RAM installations, 194
unmanaged/managed switches, 102, 147
unshielded twisted-pair cables, 114, 170–174
untrusted/trusted software sources, 618–619

updating

3D printers, 302
 baseband updates, 75
 BIOS updates, 194
 firmware, 194
 gpupdate command, 506–507
 macOS, 590
 mobile devices, 674
 PRI, 75
 PRL updates, 75
 scheduling scans/run updates, 728
 UEFI, 194
 Windows updates, 482, 536–537

upgrades

OS installation, 473, 484
 power drains, 347
 troubleshooting, 347
 upgrade paths, 484

UPnP (Universal Plug and Play), SOHO router firewalls, 121

UPS (Uninterruptible Power Supplies), 783, 792–794

USB (Universal Serial Bus)

cables, 178–179
 cards, 225
 connectivity, 254–255
 connectors, 179
 Ethernet adapters, 183
 flash drives, 205–206, 472
 ports, 226
 tethering, 69

USB-C connectors, 49, 56–57, 181

USB-C ports, Android tablets, 49, 56–57

user accounts

administrator accounts, 646, 662
 backups, 774–775
 groups, 646–648
 guest accounts, 646, 662
 lockouts, 663–664

logon hours, 662–663
 new user accounts, 647–648
 OU, 611–612
 passwords, 647
 permissions, 662
 Power User accounts, 646
 recovery, 774–775
 roaming profiles, 612
 security, 646–648, 656, 664
 Sleep mode, 664
 SSO authentication, 648, 664
 Standard User accounts, 646, 656
 UAC, 609–610
 user profiles, 612–613, 718–719

User Accounts (Windows Control Panel)

Administrator accounts, 554
 Guest accounts, 554
 modifying, 554
 Standard User accounts, 554

user interfaces, Windows GUI, 465–469

user permissions, applications, 582

usernames, workstations, 659–661

UTM (Unified Threat Management), 138

V

varistors, surge protectors, 792

VBScript, 825–827

vendor-specific OS/software) limitations, 457–458

vertical lines on page (printers), 383

vertical refresh rates (displays), 553

VGA (Video Graphics Array) cables, 177

VGA mode (displays), 550

video

artifacts, 368–369
 audio/video workstations, 272–273
 calibration, 368–369
 dead/stuck pixels, 368
 DirectX, 368
 KVM switches, 259
 projectors, 257
 refresh rates, 367
 resolution, 367
 scaling, 552

video

- stuck/dead pixels, 368
- troubleshooting, 366–370

video cables, 177–178, 182**video card connectors, 176–178**

- video cards, 18, 221–223, 275–276, 368–369, 551–552

video ports, 176–178**video subsystems, 18–19****View tab (Folder Options), 555****virtual applications, streaming, 314–315****virtual assistants, 467****virtual drives, 324****Virtual Memory (Performance), 556–557****virtual printing, 302–304****virtual switches, 324****VirtualBox, 321–322****virtualization, 322**

- BIOS, 229
- bridged networking, 323
- defined, 311, 318
- emulation versus, 319
- hard drive connections, 324
- host-only networking, 323
- hypervisors, 319–322
- NAT, 323
- no networking option, 323
- purpose of, 318
- security, 323–324
- servers, 324
- virtual drives, 324
- virtual switches, 324
- VirtualBox, 321–322
- VM, 318, 320–324
- workstations, 273–275, 321

viruses, 279, 628–632, 674–675, 713, 729–730**visible passwords, disabling, 671****VLAN (Virtual LAN), 147–148****VM (Virtual Machines)**

- documentation, 763
- emulation versus, 319
- hard drive connections, 324
- host-only networking, 323
- Hyper-V, 320–321
- managing, 763

NAT, 323

networking connections, 324

no networking option, 323

purpose of, 318

requirements, 322–324

security, 323–324

Ubuntu VM, 320–321

virtual drives, 324

virtual switches, 324

VirtualBox, 321–322

virtualization servers, 324

VMware workstations, 321

Windows 10 VM, 322–323

VMM (Virtual Machine Managers), 273–275**VMware workstations, 274, 321****VNC (Virtual Network Computing), 833****voltage**

- ATX motherboards, 217
- CPU, 239

volumes (letter assignments), 477

- convert command, 494
- Disk Management, 530–531
- partitions versus, 531–532

VPN (Virtual Private Networks), 76, 148, 616–617**VR (Virtual Reality) headsets, 52, 258****W****WAN (Wide Area Networks), 102, 113–114, 153****WAP (Wireless Access Points), 67, 102–103, 115–116****warning events (Event Viewer), 520****waterproofing. See IP (Ingress Protection)****wattage, power supplies, 264–265****wearable technology devices**

- accessories, 60–61
- airplane mode, 67–68, 74–75
- AR headsets/glasses, 52
- audio accessories, 60
- backups, cloud, 80
- batteries, replacing, 61
- Bluetooth, 52, 69–71
- cellular connections, 74–76
- email configuration, 71–74

- fitness monitors, 52
- MIL-STD-810 standard, 51
- smartwatches, 52
- synchronization, 79–84
- VR headsets, 52
- wireless connections, 66–71, 74–76
- web servers, 134–135**
- webcams, 33–34, 253**
- WEP (Wireless Equivalent Privacy), 123–124, 624**
- Western Digital, 759**
- while loops, 816**
- whitelists, 731**
- Wi-Fi**
 - 802.11 wireless standards, 126–128
 - airplane mode, 67–68
 - establishing connections, 66–67
 - mobile hotspots, 69
 - RFID, 129
 - troubleshooting, 738–740
 - WPA-2, 67
 - WPS, disabling, 694
 - Z-Wave, 129–130
 - Zigbee, 129–130
- Wi-Fi analyzers, 128, 163–164**
- Wi-Fi antennas, 34–36, 693–694**
- WiMAX (Worldwide Interoperability for Microwave Access), 158**
- Windows 7**
 - Command Prompt, elevated mode, 488–489
 - Computer Management, 512–513
 - displays, color depth, 553
 - editions of, 461–462
 - end-of-life/end-of-support dates, 457
 - mapping drives, 572
 - PowerShell, 489
 - restoring, 715
 - Search tool, 488
 - upgrade paths, 484
 - User Accounts (Windows Control Panel), 554
- Windows 8**
 - Command Prompt, elevated mode, 488–489
 - Computer Management, 512–513
 - displays, color depth, 553
 - editions of, 462–463
 - File Explorer, 535–536
 - Files History, 770–771
 - mapping drives, 572
 - Search tool, 488
 - Start screen, 466
 - User Accounts (Windows Control Panel), 554
 - Windows RE, 704–705
- Windows 8.1**
 - ADK, 474
 - Command Prompt, elevated mode, 488–489
 - Computer Management, 512–513
 - displays, color depth, 553
 - editions of, 462–463
 - end-of-life/end-of-support dates, 457
 - File Explorer, 535–536
 - Files History, 770–771
 - mapping drives, 572
 - Refresh your PC, 475
 - Reset your PC, 475
 - Search tool, opening, 488
 - Start screen, 466
 - upgrade paths, 484
 - User Accounts (Windows Control Panel), 554
 - Windows RE, 704–705
- Windows 10, 461**
 - ADK, 474
 - Command Prompt, elevated mode, 488–489
 - Computer Management, 512–513
 - Cortana, 467
 - Desktop, 465–466
 - Device Manager, 252
 - Display, 550
 - displays, color depth, 553
 - DxDiag, 540
 - editions of, 464–465
 - end-of-life/end-of-support dates, 457
 - File Explorer, 535–536
 - Files History, 770–771
 - mapping drives, 572
 - PowerShell, 489

Windows 10

- Reset your PC, 475
- Search tool, opening, 488
- Startup Settings, 708–709
- upgrade paths, 484
- User Accounts (Windows Control Panel), 554
- Windows RE, 704–707

Windows 10 VM, 322–323**Windows Boot Manager (bootmgr), 710–712****Windows computers**

- %systemroot% folders, 495
- AD, 610–614
- ADK, 474
- administrative shares, 653–654
- Advanced Boot Options, 707–709
- application installation, 581–582
- Application logs, 520
- applications, 717
- AutoPlay, disabling, 664–665
- AutoRun, disabling, 664–665
- BitLocker, 655–656
- bootrec command, 710–711
- bootups, 716–717
- BSOD, 713–715, 717
- certificates (security), 619–620
- chkdsk command, 494–495
- command help files, 490
- Command Prompt, 450, 488–492, 573, 685–686
- connectivity, 717
- convert command, 494
- defrag command, 493
- Disk Defragmenter, 493
- Disk Management, 482, 483
- diskpart command, 493
- diskpart utility, 482–483
- DLP, 617–618
- domains, 568–569, 610, 612–614
- Explorer, viewing hidden files, 555
- file systems, encryption, 654–655
- Files History, 770–771
- files/folders, 648–654
- firewalls, 615–616
- GUI, 465–469
- HomeGroup, 568, 572

MDM, 618

networking

- administrative shares, 571–572
- alternate IP addresses, 577–578
- data access, 570–573
- data sharing, 570–573
- domains, 568–569
- establishing connections, 574–576
- full duplex network adapters, 579
- half duplex network adapters, 579
- HomeGroup, 568, 572
- ipconfig command, 496–497
- mapping drives, 572–573
- network cards, 578–580
- ping command, 497–499
- printer sharing, 573–574
- proxy server settings, 576–577
- workgroups, 568–570

No OS found messages, 717

Notepad, 493

OS

- Administrative Tools, 511–522
- Component Services, 521–522
- Computer Management, 512–513
- Control Panel, 548–564
- Device Manager, 514–516
- Disk Defragmenter, 534–535
- Disk Management, 529–535
- DxDiag, 540
- editions of, 461
- Event Viewer, 519–521
- File Explorer, 535–536
- Local Security Policy, 516
- Local Users and Groups, 516
- minimum requirements, 4530
- MMC, 513–514
- mounting drives, 532–533
- MSConfig (System Configuration tool), 523–524
- Notepad, 535
- ODBC (Data Sources), 522
- Optimize Drives, 534–535
- patch management, 537
- Performance Monitor, 516–518
- Print Management, 518

- Remote Desktop Connection (MSTSC), 539
 - Services console, 518
 - Storage Spaces, 533–534
 - System Information (MSInfo32), 537
 - System Restore, 538–539
 - System Utilities, 535–543
 - Task Manager, 524–526
 - Task Scheduler, 518
 - versions of, 461
 - Windows Defender Firewall with Advanced Security, 519
 - Windows Explorer, 535–536
 - Windows Memory Diagnostics, 518–519
 - Windows Registry, 541–543
 - Windows Update, 536–537
 - workstations, 450
 - performance, 716
 - PowerShell, 489–490, 815–821, 825–827
 - printers, 717
 - Refresh your PC, 475
 - Remote Desktop, 827–831
 - Reset your PC, 475
 - restoring, 715
 - Search tool, 488
 - Security logs, 520
 - SFC, 495
 - Startup Settings, 707–709
 - stop errors (BSOD), 713–715, 717
 - System logs, 520
 - System Restore, 726–728
 - System Window, testing RAM installations, 192
 - Task Manager, testing RAM installations, 192–193
 - troubleshooting, 707–709, 716, 719
 - applications, 717
 - bootrec command, 710–711
 - bootups, 716–717
 - connectivity, 717
 - device issues, 718
 - No OS found messages, 717
 - performance, 716
 - printers, 717
 - restoring Windows, 715
 - services fail to start, 718
 - shutdowns, 712–713
 - Startup Settings, 707–709
 - user profiles, 718–719
 - Windows Boot Manager (bootmgr), 710–712
 - Windows RE (Recovery Environment), 704–707
 - trusted/untrusted software sources, logical security, 618–619
 - updates, 482
 - user accounts, 646
 - administrator accounts, 646, 662
 - groups, 646–648
 - guest accounts, 646, 662
 - lockouts, 663–664
 - logon hours, 662–663
 - new user accounts, 647–648
 - passwords, 647
 - permissions, 662
 - Power User accounts, 646
 - Sleep mode, 664
 - SSO authentication, 648, 664
 - Standard User accounts, 646, 656
 - VPN, 616–617
 - Windows Boot Manager (bootmgr), 710–712
 - Windows RE (Recovery Environment), 704–707, 713
 - workgroups, 568–570
 - workstations, 450, 659–665
- Windows Control Panel, 548**
- Credential Manager, 558–559
 - Devices and Printers, 561
 - Display, 550–552
 - Folder Options, 554–555
 - Internet Options, 548–549
 - Power Management, 557–558
 - Program Compatibility, 560–561
 - Programs and Features, 559
 - Sound, 561–562
 - Sync Center, 563–564
 - Troubleshooting, 563
 - User Accounts, 554
 - Virtual Memory (Performance), 556–557
- Windows Credential Manager (Windows Control Panel), 558–559**

Windows Defender Firewall with Advanced Security, 519, 616

Windows Explorer, 535–536

Windows file system, 478–479

Windows Memory Diagnostics, 518–519

Windows Print Spooler, 386–388

Windows RE (Recovery Environment), 704–707, 713

Windows Registry, 541–543

Windows Server Backup, 771–772

Windows Update, 536–537

wired connections

mobile devices, 56–58

security, 691–692

wired keyboards, 251

wireless connections

Bluetooth devices, 69–71

cellular connections, 66, 74–76

mobile devices, 58–60, 66–69

mobile hotspots, 69

pairing/linking devices, 69–71

security, 691–697

troubleshooting, 738–740

USB tethering, 69

wireless encryption, 123–124

wireless keyboards, 251

wireless networking, 16–17

802.11 wireless standards, 126–128

RFID, 129

Z-Wave, 129–130

Zigbee, 129–130

wireless security, 624–626

WLAN (Wireless Local Area Networks), 16–17

WMN (Wireless Mesh Networks), 153

workgroups, 482, 568–570

workplace safety, 785

workstations

account management, 662–664

audio/video workstations, 272–273

CAD workstations, 272

CAM workstations, 272

editing workstations (audio/video), 272–273

gaming PC, 275–276

graphic workstations, 272

OS, 450–451

passwords, 659–661

security, 659–664

usernames, 659–660

virtualization workstations, 273–275

VMM, 273–275

VMware workstations, 274, 321

worms, 628–632

WPA (Wi-Fi Protected Access), 123, 624

WPA2 (Wi-Fi Protected Access Version 2), 67, 123–124, 624–626

WPA2-Enterprise, 625–626

WPA2-Personal, 625

WPS (Wi-Fi Protected Access), disabling, 694

wrist straps (antistatic), 339

writing tablets, 253

WSXGA+ mode (displays), 550

WUXGA mode (displays), 550

WWAN (Wireless Wide Area Networks), 17–18

WXGA mode (displays), 550

X

x64, 452

x86, 452

Xeon, virtualization servers, 324

XPS files, 303–304

Y – Z

Z-Wave, 129–130

zero-day attacks, 640

ZIF (Zero Insertion Force) sockets, 238, 244

Zigbee, 129–130

zombies, 640