



PEARSON IT  
CERTIFICATION

Save 10%  
on Exam  
Voucher

See Inside



Practice  
Tests



Flash  
Cards



Review  
Exercises



Study  
Planner

# Cert Guide

Advance your IT career with hands-on learning

# CompTIA® A+

Core 1 (220-1101)

Core 2 (220-1102)



RICK McDONALD

# **CompTIA® A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide**

Copyright © 2023 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: 978-0-13-767594-4

ISBN-10: 0-13-767594-1

Library of Congress Control Number: 2022941819

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.

# **Contents at a Glance**

## **Introduction**

### **Part I: Core 1**

**CHAPTER 1 Mobile Devices**

**CHAPTER 2 Networking**

**CHAPTER 3 Hardware**

**CHAPTER 4 Virtualization and Cloud Computing**

**CHAPTER 5 Hardware and Network Troubleshooting**

### **Part II: Core 2**

**CHAPTER 6 Operating Systems**

**CHAPTER 7 Security**

**CHAPTER 8 Software Troubleshooting**

**CHAPTER 9 Operational Procedures**

### **Part III: Final Preparation**

**CHAPTER 10 Final Preparation**

**APPENDIX A Answers to the “Do I Know This Already?”  
Quizzes and Review Questions**

**APPENDIX B *CompTIA A+ Core 1 (220-1101) and Core 2  
(220-1102) Cert Guide Exam Updates***

**Glossary**

**Index**

**Online Only Elements**

**APPENDIX C** Memory Tables

**APPENDIX D** Memory Tables Answer Key

**APPENDIX E** Study Planner

**Glossary**

# Table of Contents

## Introduction

### Part I: Core 1

#### Chapter 1 Mobile Devices

“Do I Know This Already?” Quiz

Foundation Topics

Installing and Configuring Laptop Hardware and Components

Laptop Access

Keyboard

Hard Drive Storage

HDD/SSD Migration

Memory

Mini PCIe

Wireless Card

USB Travel Routers and Wireless WAN Cards

Battery

Physical Privacy and Security Components

*Biometrics*

*Near-field Scanner Features*

## Display Components of Mobile Devices

Display Components

Screens

*LCD*

*OLED*

Wi-Fi Antenna Connector/Placement

Webcam

Microphone

Inverter

Touchscreen/Digitizer

## Setting Up and Configuring Accessories and Ports of Mobile Devices

Connection Methods: Wired

*Micro-USB/Mini-USB for Android and Windows*

*USB-C*

*Lightning for Apple iOS*

*Hotspot*

*Serial Interfaces*

*Proprietary Vendor-Specific Ports  
(Communication/Power)*

Connection Types: Wireless

*NFC*

*Bluetooth*

*Hotspot*

Accessories

*Headsets*

*Speakers*

*Touch Pens*

*Webcam*

*Trackpad/Drawing Pad*

*Docking Station*

*Port Replicator*

## Configuring Basic Mobile Device Network Connectivity and Application Support

*Wireless/Cellular Data Network Connectivity for Mobile Devices*

*Enabling and Disabling 2G/3G/4G(LTE)/5G*

*Enabling/Disabling Hotspots*

*Enabling/Disabling Tethering*

*GSM vs. CDMA*

*PRL Updates/Baseband Updates*

*Bluetooth*

*Steps to Configure a Bluetooth Headset on an Android-Based Device*

*Steps to Configure a Bluetooth Headset on an iOS Device*

*GPS and Cellular Location Services*

*Mobile Device Management (MDM)*

*Mobile Application Management (MAM)*

*Mobile Device Synchronization*

*Types of Data to Synchronize*

*Synchronization Methods*

## *Commercial Mail Synchronization*

Exam Preparation Tasks

Review All the Key Topics

Complete the Tables and Lists from Memory

Define Key Terms

## **Chapter 2 Networking**

“Do I Know This Already?” Quiz

Foundation Topics

TCP and UDP Ports, Protocols, and Their Purposes

FTP

SSH

Telnet

SMTP

DNS

DHCP

HTTP/HTTPS

POP3

NetBIOS/NetBT

IMAP

SNMP

LDAP

SMB/CIFS

RDP

TCP vs. UDP

Networking Hardware

- Router
- Switch
- Wireless Access Point
- Patch Panel
- Firewall
- Power over Ethernet
- Hub
- Modems: Cable and DSL
- Optical Network Terminal (ONT)
- Network Interface Card
- Software-Defined Networking

## Compare and Contrast Wireless Networking Protocols

- Frequencies
- MIMO*
- Channels
- Bluetooth
- Wi-Fi Standards
- Long-Range Fixed Wireless
- NFC
- RFID

## Services Provided by Networked Hosts

- DNS Server
- DHCP Server
- File Server
- Print Server

Mail Server  
Syslog Server  
Web Server  
Authentication, Authorization, and Accounting (AAA) Server  
Internet Appliances  
*Spam Gateways*  
*UTM*  
*IDS*  
*IPS*  
*Load Balancers*  
*Proxy Server*  
Legacy and Embedded Systems  
Internet of Things (IoT) Devices

Install and Configure a Basic Wired/Wireless SOHO Network

IP Addressing  
*IPv4*  
*Public and Private IP Addresses*  
*IPv6*  
*Viewing IP Address Information*  
*APIPA IP Addresses/Link Local Addresses*  
*Dynamic vs. Static IP Addresses*  
*DHCP*

IP Addressing  
NIC Configuration

## *NIC Configuration Steps*

End-User Device Configuration

Cable/DSL Modem

## Network Configuration Concepts

DNS

DHCP

VLAN

VPN

## Internet Connection Types, Network Types, and Their Features

### Internet Connection Types

*Cable*

*DSL*

*Fiber*

*Satellite*

*Cellular*

*Wireless Internet Service Provider*

### Network Types

*LAN*

*WAN*

*PAN*

*MAN*

*SAN*

*WLAN*

## Using Networking Tools

Cutting Tool

Cable Stripper  
Crimper  
Punchdown Tool  
Multimeter  
Toner Probe  
Cable Tester  
Loopback Plug  
Wi-Fi Analyzer  
Network Tap  
Exam Preparation Tasks  
Review All the Key Topics  
Complete the Tables and Lists from Memory  
Define Key Terms

## **Chapter 3 Hardware**

“Do I Know This Already?” Quiz

Foundation Topics

Basic Cable Types

Network Cables

*Ethernet*

*Fiber*

*Coaxial*

Video Cables

*VGA*

*HDMI*

*DisplayPort*

*DVI*

Peripheral Cables

*Thunderbolt*

*USB*

Peripheral Cables: Serial

Hard Drive Cables

*SATA Cables*

*IDE Cable*

*SCSI*

Adapters

*DVI to HDMI*

*USB to Ethernet*

*DVI-I to VGA*

Connector Types

Installing RAM Types

Virtual RAM

SODIMM Memory

DDR3 SDRAM

DDR4 SDRAM

DDR5 SDRAM: The Current Standard

Single Channel

Dual Channel

Triple Channel

Quad Channel

Parity vs. Nonparity

*Error Correction: ECC vs. non-ECC Memory*

Installing Memory

*Preparations for Installing DIMM Memory*

Installing Storage Devices

Optical Drives

*CD-ROM/CD-RW*

*DVD Recordable and Rewritable Standards*

*Blu-ray Disc (BD)*

*Drive Speed Ratings*

*Recording Files to Optical Discs*

Hard Drives

*Solid-State Drive (SSD)*

Magnetic Hard Disk Drives

*Speeds/Spin Rate*

*Form Factors*

Hybrid Drives

Flash Drives/Memory Cards

*Flash Card Reader*

Storage Device Configurations

*RAID Types*

*Creating a SATA RAID Array*

*Hot-Swappable Drives*

Installing Motherboards, CPUs, and Add-on Cards

Motherboard Form Factors

*ATX and mATX*

*ITX Family*

*Comparing ATX, microATX, and Mini-ITX Motherboards*

Motherboard Connector Types

*Peripheral Component Interconnect (PCI) Slots*

*PCIe (PCI Express) Slots*

*Power Connectors*

*SATA*

*eSATA*

*Headers*

*M.2*

Motherboard Compatibility

*Processor Compatibility*

*Central Processing Unit (CPU) Socket Types*

*Servers*

*Mobile*

Basic Input/Output System (BIOS)/Unified Extensible Firmware Interface (UEFI) Settings

*BIOS/UEFI Configuration*

*Accessing the BIOS/UEFI Setup Program*

*UEFI and Traditional BIOS*

*BIOS/UEFI Settings Overview*

*Boot Options: Settings and Boot Sequence*

*Firmware Updates*

*Security Features*

*Interface Configurations*

*CMOS Battery*

Encryption

*Trusted Platform Module (TPM)*

*Hardware Security Module (HSM)*

CPU Architecture

*x64/x86*

*Advanced RISC Machine (ARM)*

CPU Cores: Single Core and Multicore

Multithreading

Virtualization Support

CPU Speeds

Expansion Cards

*Installing Sound Cards*

*External USB Audio Sound Cards*

*Installing Video Cards*

*Integrated Graphics Processing Unit (GPU)*

*Video Capture Cards*

*Installing Network Cards*

Cooling Mechanisms

*Fans*

*Fanless/Passive Heat Sinks*

*Heat Sink*

*Phase-Change Material/Thermal Paste*

*Liquid-Based Cooling*

Power Supplies

Power Supply Ratings

Input 115V vs. 220V Multivoltage Power Supplies

20-Pin-to-24-Pin Motherboard Adapter

Output 3.3V vs. 5V vs. 12V

Redundant Power Supply

Modular Power Supply

## Multifunction Devices/Printers and Settings

Unboxing a Device/Setup Location Considerations

Appropriate Drivers for the Office Environment

Configuration Settings

Public/Shared Devices

*Integrated Ethernet Print/Multifunction Device Sharing*

*Wireless Device Sharing Options*

Using Public and Shared Devices

*Using Apps*

*Maintaining Data Privacy*

Network Scan Services

*Scanning to Email*

*Scanning to an SMB Folder*

*Cloud and Remote Printing*

*Automatic Document Feeder/Flatbed Scanner*

## Print Technologies

Laser Printers

*Toner Cartridges*

*Laser Imaging Process*

*Color Laser Printing Differences*

*Laser Media Types*

*Laser Maintenance*

Inkjet Printers

*Inkjet Components*

*Inkjet Printing Process*

*Inkjet Media Types*

*Inkjet Maintenance*

Thermal Printers

*Thermal Feed Assembly and Heating Element*

*Thermal Printer Ribbons*

*Thermal Print Process*

*Thermal Paper and Media*

*Thermal Maintenance*

Impact Printers

*Impact Components and Print Process*

*Impact Print Heads*

*Impact Printer Ribbons*

*Impact Printer Paper Types*

*Impact Printer Maintenance*

3D Printers

*Maintaining 3D Printers*

Exam Preparation Tasks

Review All the Key Topics

Complete the Tables and Lists from Memory

Define Key Terms

## **Chapter 4 Virtualization and Cloud Computing**

“Do I Know This Already?” Quiz

Foundation Topics

Common Cloud Models

IaaS

SaaS

PaaS

Public vs. Private vs. Hybrid vs. Community

Cloud Characteristics

*Shared Resources*

*Rapid Elasticity*

*High Availability*

*File Synchronization*

*On-Demand*

*Metered Utilization*

Desktop Virtualization

Client-Side Virtualization Overview

Host/Guest Virtualization

Purpose of Virtual Machines

Resource Requirements

Security Requirements

Exam Preparation Tasks

Review All the Key Topics

Define Key Terms

## **Chapter 5 Hardware and Network Troubleshooting**

“Do I Know This Already?” Quiz

Foundation Topics

Troubleshooting Methodology

Troubleshooting Motherboard, RAM, CPU, and Power Issues

POST Code Beeps

*POST Error Messages*

Proprietary Crash Screens (BSOD/Pinwheel)

*BSOD Errors*

*macOS Pinwheel*

Black Screen

No Power

Overheating

*Overloading*

*Fan Failure*

*Inadequate Airflow Outside the System*

*Inadequate Airflow Inside the System*

*Dirt and Dust*

*Installing/Replacing Case Fans*

No Power

Sluggish Performance

Overheating

Burning Smells

*Power Supply Tester*

*Step-by-Step Power Supply Troubleshooting*

Intermittent Shutdown

Application Crashes

*Log Entries and Error Messages*

Grinding Noise

Capacitor Swelling

Inaccurate System Date/Time

## Troubleshooting Storage Drives and RAID Arrays

Light-Emitting Diode (LED) Status Indicators

Read/Write Failure

Slow Performance

Grinding and Clicking Noises

Failure to Boot

Bootable Device Not Found

Data Loss/Corruption

RAID Failure

S.M.A.R.T. Failure

Extended Read/Write Times

Input/Output Operations per Second (IOPS)

Missing Drives in OS

## Troubleshooting Video, Projector, and Display Issues

Incorrect Data Source

Physical Cabling Issues

Burned-Out Bulb

Intermittent Projector Shutdown

Dead Pixels

Incorrect Color Display

Dim Image

Flashing Screen

Fuzzy or Distorted Image

Display Burn-in

*LCD Displays*

*Plasma Displays*

Audio Issues

## Mobile Device Troubleshooting

Poor Battery Health and Improper Charging

Swollen Battery

Broken Screen

Poor/No Connectivity

Liquid Damage

Overheating

Digitizer Issues

Nonresponsive Touchscreen

Physically Damaged Ports

Malware

Cursor Drift/Touch Calibration

## Printer Troubleshooting

Lines Down the Printed Pages

*Laser Printer*

*Inkjet Printer*

*Thermal Printers*

*Impact Printers*

Faded Prints

*Laser Printers*

*Inkjet Printers*

*Thermal Printers*

*Impact Printers*

Double/Echo Images on the Print

Toner Not Fusing to the Paper

Incorrect Paper Size

Paper Not Feeding

Paper Jams

*Paper Path Issues*

*Paper Loading, Paper Type, and Media Thickness Issues*

*Media Caught Inside the Printer*

Multipage Misfeed

Garbled Print

Vertical Lines on Page

Multiple Prints Pending in a Queue

*Releasing a Print Queue*

*Clearing Select Print Jobs or All Print Jobs in a Queue*

Speckling on Printed Pages

Incorrect Chroma Display

Grinding Noise

Finishing Issues

Incorrect Page Orientation

Print Logs

## Network Troubleshooting

No Connectivity

External Interference and Intermittent Wireless Connectivity

Slow Network Speeds

Limited Connectivity

Latency and Jitter

Poor Voice over Internet Protocol (VoIP) Quality

Port Flapping

## Exam Preparation Tasks

Review All the Key Topics

Complete the Tables and Lists from Memory

Define Key Terms

## **Part II: Core 2**

### **Chapter 6 Operating Systems**

“Do I Know This Already?” Quiz

Foundation Topics

Basic Features of Microsoft Windows Editions

Windows 10 Editions

Feature Differences

*Domain Access vs. Workgroup*

*Desktop Styles/User Interface*

*Remote Desktop Connection and Remote Assistance*

*Random Access Memory (RAM)*

*BitLocker*

*Group Policy Editor*

*Upgrade Paths*

## Microsoft Command-Line Tools

Starting a Command Prompt Session with Windows PowerShell

Commands Available with Standard Privileges vs. Administrative Privileges

Windows Command-Line Commands

*format*

*copy*

*xcopy*

*robocopy*

*diskpart*

*sfc*

*chkdsk*

*gpupdate*

*gpresult*

*pathping*

## Microsoft Windows 10 Operating System (OS) Features and Tools

*Task Manager*

*Microsoft Management Console (MMC) Snap-in*

*Event Viewer*

*Disk Management*

*Task Scheduler*

*Device Manager*

*Certificate Manager*  
*Local Users and Groups*  
*Performance Monitor*  
Additional Tools  
*System Information (msinfo32)*  
*Resource Monitor*  
*System Configuration Utility*  
*Disk Cleanup*  
*Disk Defragment/Optimize Drives*  
*Registry Editor*

## Windows 10 Control Panel Utilities

Starting Control Panel  
Internet Options  
User Accounts  
Device Manager  
Indexing Options  
Administrative Tools  
File Explorer Options  
Power Options  
*Hibernate*  
*Power Plans*  
*Sleep/Suspend*  
*Standby, Lid, and Fast Startup Options*  
*Universal Serial Bus (USB) Selective Suspend*  
Ease of Access

## Windows Settings

Time and Language

Update and Security

Personalization

Apps

Privacy

System

Devices

Network and Internet

Gaming

Accounts

## Microsoft Windows Networking Features on a Client/Desktop

Workgroup vs. Domain Setup

*Workgroup Networking*

*Creating a Workgroup*

*Domain Setup*

*Network Shares*

*Administrative Shares*

*Sharing a Folder*

*Mapped Drives*

Printer Sharing vs. Network Printer Mapping

Local OS Firewall Settings

Client Network Configuration

*Internet Protocol (IP) Addressing Scheme*

*Subnet Mask*

*Domain Name System (DNS) Settings*

*Gateway*

*Static vs. Dynamic*

Establish Networking Connections

*VPN Connections*

*Wireless Connections*

*Wired Connections*

*WWAN (Cellular) Connections*

Proxy Settings

Public Network vs. Private Network

File Explorer Navigation: Network Paths

Metered Connections and Limitations

Installation and Configuration Concepts

System Requirements for Applications

*32-Bit vs. 64-Bit File Systems*

*FAT32*

*exFAT (FAT64)*

*32-Bit vs. 64-Bit Dependent Application Requirements*

*Dedicated Graphics Card vs. Integrated Graphics Card*

*Video Random Access Memory (VRAM) Requirements*

*RAM Requirements*

*Central Processing Unit (CPU) Requirements*

*External Hardware Tokens*

*Storage Requirements*

OS Requirements for Applications

*Application-to-OS Compatibility*

*32-Bit vs 64-Bit OS*

Distribution Methods

*Physical Media vs. Downloadable*

Other Considerations for New Applications

Understanding Common OS Types

Workstation OSs

*Windows*

*Apple Macintosh OS*

*Linux*

*Chrome OS*

Cellphone/Tablet Operating Systems

*Android*

*iOS*

Various File System Types

Vendor Life-Cycle Limitations

*End of Life (EOL)*

*Update Limitations*

Vendor-Specific Limitations/Compatibility Concerns  
Between OSs

OS Installations and Upgrades in a Diverse OS  
Environment

Boot Methods

Types of Installations

*Unattended Installation*

*Types of Installations*

*Upgrades*

*Clean Install*

*Repair Installation*

*Remote Network Installation*

*Image Deployment*

*Recovery Partition*

*Refresh/Restore*

*Other Considerations/Third-Party Drivers*

*Partitioning Methods*

*Partitioning Overview*

*MBR vs. GPT Partition Types*

*Disk Preparation Using MBR*

*Partitioning Using GPT*

*Dynamic and Basic Disks*

*Creating Partitions During Windows Installation*

*Formatting*

*Upgrade Considerations*

*Backup Files and User Preferences*

*Application and Driver Support/Backward Compatibility*

*Hardware and Application Prerequisites and Compatibility*

*Feature Updates*

*Update Life Cycle*

Common Features and Tools of the macOS/Desktop OS

*Installation and Uninstallation of Applications*

*File Types*

*App Store*

*Uninstallation Process*

Apple ID and Corporate Restrictions

Best Practices

*Backups*

*Antivirus/Anti-malware Updates*

*Updates/Patches*

System Preferences

Features

Disk Utility

FileVault

Terminal

Force Quit

Common Features and Tools of the Linux Client/Desktop OS

Common Linux Commands

*ls*

*grep*

*cd*

*shutdown*

*pwd*

*mv*

*cp*

*rm*

*chmod*

*chown*

*su/sudo*

*apt-get*

*YUM (Yellowdog Updater, Modified)*

*ip*

*df (Disk Free)*

*ps*

*man*

*top*

*find*

*DIG (Domain Information Groper)*

*cat*

*nano*

Best Practices

*Scheduled Backups*

*Antivirus*

*Updates and Patches*

Tools

*shell/terminal*

*Samba*

Exam Preparation Tasks

Review All the Key Topics

Complete the Tables and Lists from Memory

Define Key Terms

## **Chapter 7 Security**

“Do I Know This Already?” Quiz

Foundation Topics

Security Measures

Physical Security

*Access Control Vestibule*

*Badge Reader*

*Video Surveillance*

*Alarm Systems*

*Motion Sensors*

*Guards*

*Door Locks*

*Equipment Locks*

*Bollards*

*Fences*

Physical Security for Staff

*Key Fobs*

*Smart Card*

*Keys*

*Biometrics*

*Lighting*

*Magnetometers*

Privacy Screen

Logical Security Concepts

*Principle of Least Privilege*

*Access Control Lists*

*Multifactor Authentication*

*Email*

*Hard Tokens*

*Soft Tokens*

*Short Message Service*

*Voice Call*

*Authentication Application*

Mobile Device Management

Active Directory

Wireless Security Protocols and Authentication

Protocols and Encryption

Authentication

*Single-Factor*

*Multifactor*

*RADIUS*

*TACACS+*

*Kerberos*

Malware Removal and Prevention

Malware

*Trojan*

*Rootkit*

*Virus*

*Spyware*

*Ransomware*

*Keylogger*

*Boot Sector Virus*

*Cryptominers*

Tools and Methods

*Antivirus/Anti-malware*

*Recovery Mode*

*User Education*

*Anti-Phishing Training*

*OS Reinstallation*

## Social Engineering Threats and Vulnerabilities

*Social Engineering*

*Phishing*

*Vishing*

*Whaling*

*Impersonation*

*Shoulder Surfing*

*Tailgating*

*Dumpster Diving*

*Evil Twin*

*Threats*

*DDoS*

*DoS*

*Zero-Day*

*Spoofing*

*On-Path Attack*

*Brute Force*

*Dictionary Attacks*

*Insider Threat*

*Structured Query Language (SQL) Injection*

*Cross-Site Scripting (XSS)*

*Vulnerabilities*

*Noncompliant Systems*

*Unpatched Systems*

*Unprotected Systems*

*EOL OSs*

*Bring Your Own Device (BYOD)*

## Microsoft Windows OS Security Settings

*Defender Antivirus*

*Firewall*

*Activate/Deactivate*

*Port Security*

*Application Security*

*Access Control*

*Users and Groups*

*NTFS vs. Share Permissions*

*Run as Administrator vs. Standard User*

*User Account Control*

*Login OS Options*

*BitLocker*

*BitLocker To Go*

*EFS*

## Security Best Practices to Secure a Workstation

Data-at-Rest Encryption  
Password Best Practices  
*Setting Strong Passwords*  
*Password Expiration*  
*Screensaver Required Password*  
*BIOS/UEFI Passwords*  
*Requiring Passwords*  
End-User Best Practices  
*Use Screensaver Locks*  
*Log Off When Not in Use*  
*Secure/Protect Critical Hardware*  
*Secure Personally Identifiable Information (PII)*  
Account Management  
*Restricting User Permissions*  
*Login Time Restrictions*  
*Disabling Guest Account*  
*Failed Attempts Lockout*  
Changing Default Usernames and Passwords  
Disabling Autorun/AutoPlay  
Securing Mobile Devices  
Screen Locks  
Remote Wipes  
Locator Applications  
Remote Backup Applications  
Failed Login Attempts Restrictions

Antivirus/Anti-malware

Patches and OS Updates

Biometric Authentication

Full-Device Encryption

Firewalls

Policies and Procedures

*BYOD vs. Corporate-Owned Devices*

*Profile Security Requirements*

*Internet of Things*

Data Destruction and Disposal

Physical Destruction Methods

Recycling or Repurposing Best Practices

Outsourcing Concepts

Configuring Security on SOHO Networks

Home Router Settings

*Change Default Passwords*

*IP Filtering*

*Firmware Updates*

*Content Filtering*

*Physical Placement/Secure Locations*

*Dynamic Host Configuration Protocol (DHCP)*

*Reservations*

*Static WAN IP*

*Universal Plug and Play*

*Screened Subnet*

Wireless-Specific Security

*Changing the Service Set Identifier (SSID)*

*Encryption Settings*

*Disabling SSID Broadcast*

*Disabling Guest Access*

*Changing Channels*

Firewall Settings

Port Forwarding/Mapping

Disabling Ports

Configuring Browser and Relevant Security Settings

Browser Download and Installation

*Hashing*

*Untrusted Sources*

Extensions and Plug-ins

Password Managers

Secure Connection/Sites—Valid Certificates

*Transport Layer Security (TLS)*

*Hypertext Transfer Protocol Secure (HTTPS)*

Settings

*Pop-up Blocker*

*Clearing Browsing Data*

*Clearing the Cache*

*Private Browsing Mode*

*Sign-in/Browser Data Synchronization*

*Ad Blockers*

Exam Preparation Tasks

Review All the Key Topics

Define Key Terms

## **Chapter 8 Software Troubleshooting**

“Do I Know This Already?” Quiz

Foundation Topics

Troubleshooting Common Windows OS Problems

Common Symptoms

*BSOD*

*Sluggish Performance*

*Boot Problems*

*Frequent Shutdowns*

*Services Not Starting*

*Application Crashes*

*Low Memory Warnings*

*USB Controller*

*System Instability*

*No OS Found*

*Slow Profile Load*

*Time Drift*

Common Troubleshooting Steps

*Rebuild Windows Profiles*

Troubleshooting Common PC Security Issues

Common Symptoms

Browser-Related Symptoms

Best Practice Procedures for Malware Removal

Troubleshoot Common Mobile OS and Application Issues  
Troubleshoot Common Mobile OS and Application Security Issues

    Security Concerns

*Android Package (APK) Source*

*Developer Mode*

*Root Access/Jailbreak*

*Bootleg/Malicious Application Spoofing*

    Common Symptoms

*Slow Data Speeds*

*Leaked Personal Files/Data*

*Data Transmission Over Limit*

*Tools*

*Factory Reset/Clean Install*

Exam Preparation Tasks

    Review All the Key Topics

    Complete the Tables and Lists from Memory

    Define Key Terms

## **Chapter 9 Operational Procedures**

“Do I Know This Already?” Quiz

Foundation Topics

Best Practices and Documentation

    Ticketing Systems

*User Information*

*Device Information*

*Description of Problems*

*Categories*

*Severity*

*Escalation Levels*

*Clear, Concise, Written Communication*

Asset Management

Types of Documents

*Acceptable Use Policy (AUP)*

*Network Topology Diagrams*

*Regulatory and Compliance Policy*

Knowledge Base and Articles

Change Management

Documented Business Processes and Practices

*Rollback Plan*

*Sandbox Testing*

*Responsible Staff Member*

Change Management

*Request Forms*

*Purpose of the Change*

*Scope the Change*

*Date and Time of the Change*

*Affected Systems/Impact*

*Risk Analysis*

Change Board Approvals

*End User Acceptance*

Workstation Backup and Recovery Methods

Backup and Recovery  
Backup Testing  
Account Recovery Options  
*System Image*  
*File-Level Backup*  
*Critical Applications*  
Backup Rotation Schemes  
*Onsite vs. Offsite Backups*  
*Grandfather-Father-Son (GFS) Backup Rotational Scheme*  
*3-2-1 Backup Rotational Rule*

Explain Common Safety Procedures  
Equipment Grounding/Proper Power Handling  
Proper Component Handling and Storage  
*Antistatic Bags*  
*ESD Straps*  
*ESD Mats*  
*Self-Grounding*  
Compliance with Local Government Regulations  
Personal Safety  
*Disconnect Power First*  
*Remove Jewelry*  
*Lifting Techniques*  
*Weight Limitations*  
*Electrical Fire Safety*  
*Cable Management*

*Safety Goggles*

*Air Filter Mask*

## Environmental Impacts and Appropriate Controls

*Material Safety Data Sheet (MSDS)*

*Toxic Waste Handling/Disposal*

*Recycling Batteries*

*Toner*

*Cellphones and Tablets*

Temperature and Humidity Level Awareness and Proper Ventilation

*Proper Ventilation*

*Compressed Air and Vacuum Systems*

Power Surges, Under-voltage Events, and Power Failures

*Surge Suppressors*

*Battery Backup Units*

## Addressing Prohibited Content/Activity and Privacy, Licensing, and Policy Concepts

*Incident Response*

*First Response*

*Documentation*

*Chain of Custody*

Licensing/Digital Rights Management (DRM)/End-User License Agreement (EULA)

*DRM*

*EULA*

Understanding Open Source and Commercial Licenses

Personal vs. Enterprise Licenses

Valid Licenses and Non-expired Licenses

Regulated Data

Communication Techniques and Professionalism

Professional Appearance and Attire

Use Proper Language and Avoid Jargon, Acronyms, and Slang When Applicable

Maintain a Positive Attitude/Project Confidence

Actively Listen, Take Notes, and Avoid Interrupting the Customer

Be Culturally Sensitive

Be on Time

Avoid Distractions

Dealing with Difficult Customers or Situations

Set and Meet Expectations/Timeline and Communicate Status with the Customer

Dealing Appropriately with Customers' Confidential and Private Materials

Scripting Basics

Script File Types

Use Cases for Scripting

Other Scripting Considerations

Remote Access Technologies

Methods/Tools

RDP

VPN

Virtual Network Computing

SSH

Remote Monitoring and Management

Microsoft Remote Assistance

Third-Party Tools

*Screen-Sharing and Videoconferencing Software*

*File Transfer Software*

*Desktop Management Software*

Security Considerations of Each Access Method

Exam Preparation Tasks

Review All the Key Topics

Complete the Tables and Lists from Memory

Define Key Terms

## **Part III: Final Preparation**

### **Chapter 10 Final Preparation**

Exam Information

Core 1 (220-1101) Exam Domains and Objectives

Core 2 (220-1102) Exam Domains and Objectives

Getting Ready

Tools for Final Preparation

Pearson Cert Practice Test Engine and Questions on the Website

*Accessing the Pearson Test Prep Software Online*

*Accessing the Pearson Test Prep Software Offline*

[Customizing Your Exams](#)

[Updating Your Exams](#)

[\*Premium Edition\*](#)

[Memory Tables](#)

[Chapter-Ending Review Tools](#)

[Suggested Plan for Final Review/Study](#)

[Summary](#)

[Appendix A Answers to the “Do I Know This Already?” Quizzes and Review Questions](#)

[Appendix B \*CompTIA A+ Core 1 \(220-1101\) and Core 2 \(220-1102\) Cert Guide\* Exam Updates](#)

[Glossary](#)

[Index](#)

## **Online Only Elements**

[Appendix C Memory Tables](#)

[Appendix D Memory Tables Answer Key](#)

[Appendix E Study Planner](#)

[Glossary](#)

# Introduction

CompTIA A+ certification is widely recognized as the first certification you should receive in an information technology (IT) career. Whether you are planning to specialize in PC or mobile device hardware, operating systems management, security, or network management, the CompTIA A+ certification exams measure the baseline skills you need to master to begin your journey toward greater responsibilities and achievements in IT.

CompTIA A+ certification is based on a vendor-neutral exam that measures your knowledge of industry-standard technology.

## Goals and Methods

The primary goal of this book is a simple one: to help you prepare to pass the CompTIA A+ certification Core 1 (220-1101) and Core 2 (220-1102) exams.

Because CompTIA A+ certification exams now stress problem-solving capabilities and reasoning more than memorization of terms and facts, our goal is to help you master and understand the required objectives for each exam.

To aid you in mastering and understanding the A+ certification objectives, this book uses the following methods:

- The beginning of each chapter defines the topics to be covered in the chapter and also lists the corresponding CompTIA A+ objective numbers.

- The body of the chapter explains the topics from hands-on and theory-based standpoints. Each chapter includes in-depth descriptions, tables, and figures that are geared toward building your knowledge so that you can pass the exam. The chapters are divided into several topics.
- The key topics indicate important figures, tables, and lists of information that you should know for the exam. They are interspersed throughout the chapter and are listed in table format at the end of the chapter.
- You can find memory tables online in [Appendix C, “Memory Tables,”](#) and [Appendix D, “Memory Tables Answer Key.”](#) Use them to help you memorize important information.
- Key terms without definitions are listed at the end of each chapter. Write down the definition of each term and check your work against the Key Terms in the glossary.

## How the Book Is Organized

Each chapter in this book maps one-to-one with the domains of the A+ Core 1 (220-1101) and Core 2 (220-1102) exam domains:

<b>Chapter</b>	<b>Core 1 (220-1101) Domain Covered</b>	<b>Percentage of Exam</b>
<a href="#">Chapter 1</a>	1.0 Mobile Devices	15%
<a href="#">Chapter 2</a>	2.0 Networking	20%
<a href="#">Chapter 3</a>	3.0 Hardware	25%
<a href="#">Chapter 4</a>	4.0 Virtualization and Cloud Computing	11%

<b>Chapter</b>	<b>Core 1 (220-1101) Domain Covered</b>	<b>Percentage of Exam</b>
Chapter 5	5.0 Hardware and Network Troubleshooting	29%
<b>Chapter</b>	<b>Core 2 (220-1102) Domain Covered</b>	
Chapter 6	1.0 Operating Systems	31%
Chapter 7	2.0 Security	25%
Chapter 8	3.0 Software Troubleshooting	22%
Chapter 9	4.0 Operational Procedures	22%

Chapter 10, “Final Preparation,” provides you with tools for last-minute preparation and some tips for preparing yourself mentally and confidently to take the exams. Be sure to visit CompTIA’s web page at <https://certification.comptia.org> to ensure that you have the latest information for the CompTIA A+ exams.

## Book Features

To help you customize your study time using this book, the core chapters have several helpful features:

- **1:1 correlation with exam domains:** The chapters are presented to match the A+ 220-1101 and 220-1102 exam domains and objectives.
- **Foundation Topics:** These are the core sections of each chapter. They explain the concepts for the topics in each chapter.

- **Exam Preparation Tasks:** After the “Foundation Topics” section of each chapter, the “Exam Preparation Tasks” section lists a series of study activities that you should do at the end of the chapter.
- **Review All Key Topics:** The Key Topic icon appears next to the most important items in the “Foundation Topics” section of the chapter. The Review All Key Topics activity lists the key topics from the chapter, along with their page numbers. Although the contents of the entire chapter could be on the exam, you should definitely know all the information highlighted with Key Topic icons.
- **Define Key Terms:** This section lists the most important terms from the chapter. To ensure that you know the terms, write a short definition of each and compare your answer to the glossary at the end of the book.
- **Review Questions:** Confirm that you understand the content that you just covered by answering these questions and reading the answer explanations.
- **Web-based practice exam:** The companion website includes the Pearson Cert Prep Practice Test engine, which enables you to answer practice exam questions. Use it to prepare with a sample exam and to pinpoint areas where you need more study.

## What's New?

You'll find plenty that's new and improved in this edition, including the following content:

- More material on troubleshooting mobile devices
- Focus on Windows 10
- New discussion of Chrome OS

- New discussion of macOS
- A large increase in operational procedures content
- Basic scripting material
- New discussion of remote access technologies
- Increased emphasis on virtualization concepts
- Increased coverage of 3D printing
- New discussion of cloud computing concepts
- Reorganized text to minimize duplicated coverage among objectives
- New coverage of Linux and OS X features and troubleshooting
- New coverage of MacBook features, such as Thunderbolt 2
- Updated processor coverage
- Updated material on BIOS dialogs, including more UEFI/BIOS examples
- USB 3.1 and USB-Type C information
- mSATA and M.2 SSDs material
- Improved photos and illustrations
- Enhanced procedures for laptop teardown and subassembly replacement
- Updated memory coverage (DDR4 DIMMs and UniDIMMs)
- Updated coverage of mobile devices, including teardown tips
- Enhanced discussion of desktop and laptop upgrades, including Thunderbolt and the miniPCIe card
- Updated material on port replicators, docking stations, and video cable adapters
- Updated information on power supply and cooling systems

- Improved coverage of network hardware and cabling
- Enhanced coverage of device troubleshooting, teardown, and upgrades
- New material on dealing with prohibited content and activities
- Enhanced coverage of Windows features
- Enhanced discussion of Windows upgrade paths and methods
- New coverage of Windows 10 features
- Coverage of ESD protection issues
- Enhanced instruction on Windows OS troubleshooting
- Enhanced Control Panel discussion
- Enhanced coverage of iOS and Android devices
- Enhanced coverage of security issues (physical, digital, wireless network, wired network, workgroup, and homegroup folders)
- New material on network and cloud computing concepts
- Enhanced discussion of security issues
- New coverage of Linux and macOS X troubleshooting

For more information about how the A+ certification can help your career, or to download the latest official objectives, access CompTIA's A+ web page at

<https://certification.comptia.org/certifications/a>.

In this book, we cover the major objectives but also combine some of them, when necessary, to make a topic easier to understand. To make sure you can relate the book's contents to the CompTIA A+ certification objectives, each chapter contains cross-references to the appropriate objectives, as needed.

## Who Should Read This Book?

The CompTIA A+ exams measure the necessary competencies for an entry-level IT professional with knowledge equivalent to what is learned in 6 to 12 months of hands-on experience in a lab or in the field. This book is written for people who have that amount of experience working with desktop PCs, laptops, and mobile devices. Average readers have attempted in the past to replace a hardware component within a PC or mobile device; they should also understand how to navigate through Windows and access the Internet, as well as have (or be willing to learn) a basic knowledge of macOS and Linux features.

Readers range from people who are attempting to attain a position in the IT field, to people who want to keep their skills sharp or perhaps retain their job as a result of a company policy mandating that they take the new exams.

This book is also aimed at readers who want to acquire additional certifications beyond the A+ certification (Network+, Security+, and so on). The book is designed to provide an easy transition to future certification studies.

## **Strategies for Exam Preparation**

Strategies for exam preparation vary, depending on your existing skills and knowledge and the equipment you have available. Of course, the ideal exam preparation consists of building a PC from scratch and installing and configuring the operating systems covered.

The next best step you can take is to read through the chapters in this book, jotting down notes about key concepts or configurations in a dedicated notepad. Each chapter contains a quiz that you can use to test your knowledge of the chapter's topics. This quiz is located near the end of the chapter.

After you have read through the book, take a look at the current exam objectives for the CompTIA A+ certification exams, listed at

<https://certification.comptia.org/certifications/a>. If you still want to study any areas shown in the certification exam outline, find those sections in the book and review them.

When you feel confident in your skills, attempt the practice exams included on the companion website with this book. As you work through the practice exams, note the areas where you lack confidence and review those concepts or configurations in the book. After you have reviewed the areas, work through the practice exams a second time and rate your skills. Keep in mind that the more you work through the practice exams, the more familiar the questions will become.

After you have worked through the practice exams and feel confident with your skills, schedule the real CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) exams through Pearson VUE ([www.vue.com](http://www.vue.com)). To keep the information from evaporating out of your mind, you typically want to take the exam within a week of when you consider yourself ready.

## Companion Website

Register this book to get access to the Pearson IT Certification test engine and other study materials, plus additional bonus content. Check this site regularly for new and updated postings written by the author that provide further insight into the more troublesome topics on the exam. Be sure to check the box indicating that you want to hear from us about updates and exclusive discounts on future editions of this book or related products.

To access this companion website, follow these steps:

**Step 1.** Go to [www.pearsonitcertification.com/register](http://www.pearsonitcertification.com/register) and log in or create a new account.

**Step 2.** Enter the ISBN for this book: **9780137675944**.

**Step 3.** Answer the challenge question as proof of purchase.

**Step 4.** Click the **Access Bonus Content** link in the Registered Products section of your account page to be taken to the page where your downloadable content is available.

Note that many of our companion content files are very large, especially image and video files.

If you cannot locate the files for this title by following these steps, visit [www.pearsonITcertification.com/contact](http://www.pearsonITcertification.com/contact) and select the **Site Problems/Comments** option. Our customer service representatives will assist you.

## Pearson Test Prep Practice Test Software

As noted previously, this book comes complete with the Pearson Test Prep practice test software, including four full exams (two for Core 1 and two for Core 2). These practice tests are available to you either online or as an offline Windows application. To access the practice exams that were developed with this book, see the instructions in the card inserted in the sleeve in the back of the book. This card includes a unique access code that enables you to activate your exams in the Pearson Test Prep software.

## Accessing the Pearson Test Prep Software Online

The online version of this software can be used on any device with a browser and connectivity to the Internet, including desktop machines, tablets, and smartphones. To start using your practice exams online, simply follow these steps:

**Step 1.** Go to [www.PearsonTestPrep.com](http://www.PearsonTestPrep.com).

**Step 2.** Select **Pearson IT Certification** as your product group.

**Step 3.** Enter your account email and password. If you don't have an account on PearsonITCertification.com or

CiscoPress.com, you need to establish one by going to PearsonITCertification.com/join.

**Step 4.** In the **My Products** tab, click the **Activate New Product** button.

**Step 5.** To activate your product, enter the access code printed on the insert card in the back of your book. The product is now listed in your My Products page.

**Step 6.** Click the **Exams** button to launch the exam settings screen and start your exam.

## **Accessing the Pearson Test Prep Software Offline**

If you want to study offline, you can download and install the Windows version of the Pearson Test Prep software. You can use the download link for this software on the book's companion website, or you can just enter this link in your browser:

[www.pearsonitcertification.com/content/downloads/pcpt/engine.zip](http://www.pearsonitcertification.com/content/downloads/pcpt/engine.zip)

To access the book's companion website and the software, simply follow these steps:

**Step 1.** Register your book by going to PearsonITCertification.com/register and entering the ISBN: **9780137675944**.

**Step 2.** Answer the challenge question.

**Step 3.** Go to your account page and click the **Registered Products** tab.

**Step 4.** Click the **Access Bonus Content** link under the product listing.

**Step 5.** Click the **Install Pearson Test Prep Desktop Version** link under the Practice Exams section of the page to

download the software.

**Step 6.** When the software finishes downloading, unzip all the files on your computer.

**Step 7.** Double-click the application file to start the installation, and follow the onscreen instructions to complete the registration.

**Step 8.** When the installation is complete, launch the application and click the **Activate Exam** button on the My Products tab.

**Step 9.** Click the **Activate a Product** button in the Activate Product Wizard.

**Step 10.** Enter the unique access code found on the card in the sleeve in the back of your book, and click the **Activate** button.

**Step 11.** Click **Next**, and then click **Finish** to download the exam data to your application.

**Step 12.** Start using the practice exams by selecting the product and clicking the **Open Exam** button to open the exam settings screen.

Note that the offline and online versions sync together, so saved exams and grade results recorded on one version are available to you on the other as well.

## Customizing Your Exams

When you are on the exam settings screen, you can choose to take exams in one of three modes:

- **Study mode:** Enables you to fully customize your exams and review answers as you are taking the exam. This is typically the mode you use first to assess your knowledge and identify information gaps.

- **Practice Exam mode:** Locks certain customization options because it presents a realistic exam experience. Use this mode when you are preparing to test your exam readiness.
- **Flash Card mode:** Strips out the answers and presents you with only the question stem. This mode is great for late-stage preparation, when you really want to challenge yourself to provide answers without the benefit of seeing multiple-choice options. This mode does not provide the detailed score reports that the other two modes do, so do not use it if you are trying to identify knowledge gaps.

In addition to choosing among these three modes, you can select the source of your questions. You can choose to take exams that cover all the chapters, or you can narrow your selection to just a single chapter or the chapters that make up specific parts in the book. By default, all chapters are selected. If you want to narrow your focus to individual chapters, simply deselect all the chapters and then, in the Objectives area, select only those you want to focus on.

You can make several other customizations to your exam from the exam settings screen, including the time of the exam, the number of questions served up, whether to randomize questions and answers, whether to show the number of correct answers for multiple-answer questions, and whether to serve up only specific types of questions. You can also create custom test banks by selecting only questions that you have marked or questions on which you have added notes.

## Updating Your Exams

If you are using the online version of the Pearson Test Prep software, you should always have access to the latest version of the software and the exam data. If you are using the Windows desktop version, every time you connect to the Internet and launch the software, it checks for any updates to your exam data and

automatically downloads any changes made since the last time you used the software.

When you activate your exam, sometimes the exam data does not fully download. If figures or exhibits are missing, you might need to manually update your exams. To update a particular exam that you have already activated and downloaded, simply click the Tools tab and click the Update Products button. Again, this is an issue only with the desktop Windows application.

If you want to check for updates to the Windows desktop version of the Pearson Test Prep exam engine software, simply click the Tools tab and click the Update Application button to ensure that you have the most up-to-date version of the software.

# Figure Credits

Cover: Guardia/Shutterstock

Chapter Opener: Charlie Edwards/Getty Images

[Figures 1-16, 1-19, 2-13a](#): Samsung Group

[Figures 1-17, 1-18, 1-20, 2-7, 2-13b, 3-43, 3-88, 3-89, 5-3, 6-40](#) through [6-43, 6-49](#) through [6-60, 9-4, 9-5](#): Apple Inc

[Figures 2-3, 2-10, 3-24, 3-38, 3-42, 3-58, 3-65](#) through [3-67, 3-95, 4-3, 4-5, 5-1, 5-2, 5-10, 5-17, 5-20](#) through [5-22, 6-1](#) through [6-38, 6-44, 6-46](#) through [6-48, 7-3](#) through [7-12, 7-15, 7-16, 8-1](#) through [8-6, 9-3, 9-12](#): Microsoft Corporation

[Figure 2-4](#): OlegD/Shutterstock

[Figure 2-8](#): Linux Kernel Organization, Inc

[Figure 2-9](#): Cisco Systems, Inc

[Figure 2-11](#): Ookla, LLC

[Figures 2-19, 2-20, 3-40, 3-41](#): Intel Corporation

[Figures 3-39, 3-55](#) through [3-57, 3-59](#) through [3-62, 3-68, 3-69, 5-5, 6-45](#): American Megatrends International LLC

[Figure 3-63](#): BIOSTAR Group

[Figure 3-75](#): Techpowerup

[Figures 3-93](#) through [3-94a-b, 5-18](#): Epson America, Inc

[Figure 3-101](#): wklzzz/123RF

[Figure 4-1](#): Zern Liew/Shutterstock

[Figures 4-2, 7-17](#): Google LLC

[Figure 4-4](#): Oracle

[Figure 5-19](#): Canon U.S.A., Inc

[Figure 6-39](#): Robert Koczera/123RF

[Figure 6-41](#): Linux Mint

[Figures 6-61](#) through [6-63](#): Red Hat, Inc

[Figures 6-64](#) through [6-66](#): Canonical Ltd

[Figures 7-13, 7-14](#): Linksys Holdings, Inc

[Figure 10-1](#): CompTIA, Inc

# **Part I: Core 1**

# Chapter 1

## Mobile Devices

**This chapter covers the four A+ 220-1101 exam objectives related to knowledge of mobile devices. These objectives may comprise 15 percent of the exam questions:**

- **Core 1 (220-1101): Objective 1.1:** Given a scenario, install and configure laptop hardware and components.
- **Core 1 (220-1101): Objective 1.2:** Compare and contrast the display components of mobile devices.
- **Core 1 (220-1101): Objective 1.3:** Given a scenario, set up and configure accessories and ports of mobile devices.
- **Core 1 (220-1101): Objective 1.4:** Given a scenario, configure basic mobile device network connectivity and application support.

The mobile device category includes laptops, tablets, and smartphones. Because of the variety of operating systems, form factors, port types, and capabilities, supporting these devices is a bigger challenge than ever.

### “Do I Know This Already?” Quiz

The “Do I Know This Already?” quiz allows you to assess whether you need to read the entire chapter. [Table 1-1](#) lists both the major headings in this chapter and the “Do I Know This Already?” quiz questions covering the material in those headings so that you can assess your knowledge of these specific areas. The answers to the

“Do I Know This Already?” quiz appear in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes and Review Questions.”

**Table 1-1** “Do I Know This Already?” Section-to-Question Mapping

Foundation Topics Section	Questions
Installing and Configuring Laptop Hardware and Components	1–2
Display Components of Mobile Devices	3
Setting Up and Configuring Accessories and Ports of Mobile Devices	4–5
Configuring Basic Mobile Device Network Connectivity and Application Support	6–10

## CAUTION

The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for the purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

- 1.** You are researching options for adding a hard drive to your laptop. You want speed, but price is a consideration. Which of these is the middle-of-the-road option for speed and price?
  - a.** HDD
  - b.** SSD
  - c.** SSHD
  - d.** OLED

- 2.** Which of these are generally accessed through the bottom of a laptop? (Choose all that apply.)
- a. Battery
  - b. Wireless adapter
  - c. SODIMM RAM
  - d. SSHD
- 3.** Which screen type would you choose for maximum brightness and efficiency?
- a. LCD with IPS
  - b. OLED
  - c. LCD with TN
  - d. LED
- 4.** Which of the following is not featured on a common docking station?
- a. SSD
  - b. Power connection
  - c. USB ports
  - d. Display output port
- 5.** Which device is most like a docking station?
- a. Inverter
  - b. GPS
  - c. Port replicator
  - d. External HDD
- 6.** Which term describes using a phone and USB cable to provide secure Internet access to a laptop in an airport lounge?
- a. Biometrics
  - b. USB Type-C
  - c. Tethering

- d. Two-factor authentication
7. You are using your iPhone to pay for your groceries. Your receipt is sent to your email. Which technology is used in this payment transaction?
- a. ActiveSync
  - b. HTTPS
  - c. NFC
  - d. Hotspot
8. Which transmissions **cannot** be enabled in airplane mode?  
(Choose two.)
- a. Bluetooth
  - b. GPS
  - c. Cellular
  - d. Wi-Fi
9. Which of the following is **not** considered to be a method to avoid exceeding data limits on a phone?
- a. Disabling mobile data
  - b. Setting syncs to Wi-Fi only
  - c. Not streaming music and videos
  - d. Disconnecting from Wi-Fi
10. Which of the following are required for cloud-based synchronization on a mobile device? (Choose two.)
- a. Bluetooth 4.0
  - b. App or web service installed
  - c. Web access
  - d. Data caps

## Foundation Topics

# Installing and Configuring Laptop Hardware and Components

220-1101  
Exam

**220-1101: Objective 1.1:** Given a scenario, install and configure laptop hardware and components.

Because the display, keyboard, and network hardware are integrated into a laptop, the laptop uses specialized or proprietary components for the hard drive, optical drive, system board, memory, CPU, and other components. Replacing these devices involves far different procedures than on a desktop computer.

The following are some of the general differences:

- **Component sources:** Replacement components such as display, keyboard, wireless network card, and system board are available only from the original equipment manufacturer (OEM). These are known as *OEM parts*. Other components, such as optical drives and hard drives, memory, and the CPU, can be purchased from third-party sources but differ greatly from their desktop counterparts.
- **Power sources:** A laptop is powered by an internal battery and an AC adapter that also charges the battery. As with other laptop components, the original vendor is the most typical source for replacements, although some third-party vendors sell “universal” replacement AC adapters that work.
- **Components unique to laptops:** Laptops include several components that are typically not included on desktop computers, including an antenna in the display that is connected to a mini-PCIe card to provide wireless networking, a keyboard

with an integrated touchpad or pointing stick, a touchscreen or non-touchscreen display, and integrated speakers.

These differences, along with the extensive use of plastics and the use of tiny screws, make servicing a laptop a major challenge, even for those who are experienced with servicing a desktop computer.

## Laptop Access

When disassembling a laptop to upgrade internal hardware or to replace a defective component, several **best practices** should be followed to make the reassembly process as easy as possible:

- **Refer to manufacturer documentation:** Documentation helps properly identify screw types, screw lengths, number of screws (some laptops have more than 100), cable and component locations, and other information needed. Most vendors offer this information online, but some manufacturers insist on doing the repairs themselves and do not provide documentation for access to these components.
- **Use appropriate hand tools for case disassembly and component removal:** Using recommended tool types and sizes helps prevent problems such as damaging screw heads by using a screwdriver that is too large. Repair documentation typically lists the recommended tools for each procedure. Proceed with caution! If part of the laptop is broken, a replacement will have to be ordered.
- **Document and label cable and screw locations:** Laptops typically use a mixture of screw lengths and sometimes screw types, and it is important to keep them separate and put them back in the original holes. Swapping screws could damage components. Taking photos at different stages of disassembly can be valuable during the reassembly process.
- **Organize parts:** Consider using a multiple-compartment parts tray with a lid (available at hardware stores) for parts

sorting and storage. A magnetic dish also helps prevent loss of parts.

## Note

The Laptop Repair 101 website ([www.laptoprepair101.com](http://www.laptoprepair101.com)) provides many useful resources, including links to major vendors' laptop service manuals, illustrated step-by-step procedures for the removal of many components, and links to parts sources.

If you need to replace the battery, mass storage (hard disk, SSD, SSHD, or optical drive), SODIMM RAM, or wireless adapter on a typical laptop, you need to access these components from the bottom of the laptop. [Figure 1-1](#) shows the underside of a typical laptop and its access panels. [Figure 1-2](#) shows the same laptop after the access panels have been removed for component upgrades or replacements.



1. Access panel for hard disk or SSHD and wireless card
2. Optical drive ejector switch
3. Access panel for SODIMM RAM
4. Battery
5. Battery ejector switch
6. Access panel for CMOS battery

**Figure 1-1** The Underside of a Typical Laptop, with Removable Panels



1. Hard disk
2. Wireless card
3. SODIMM RAM
4. CMOS battery
5. Main battery compartment after battery removal

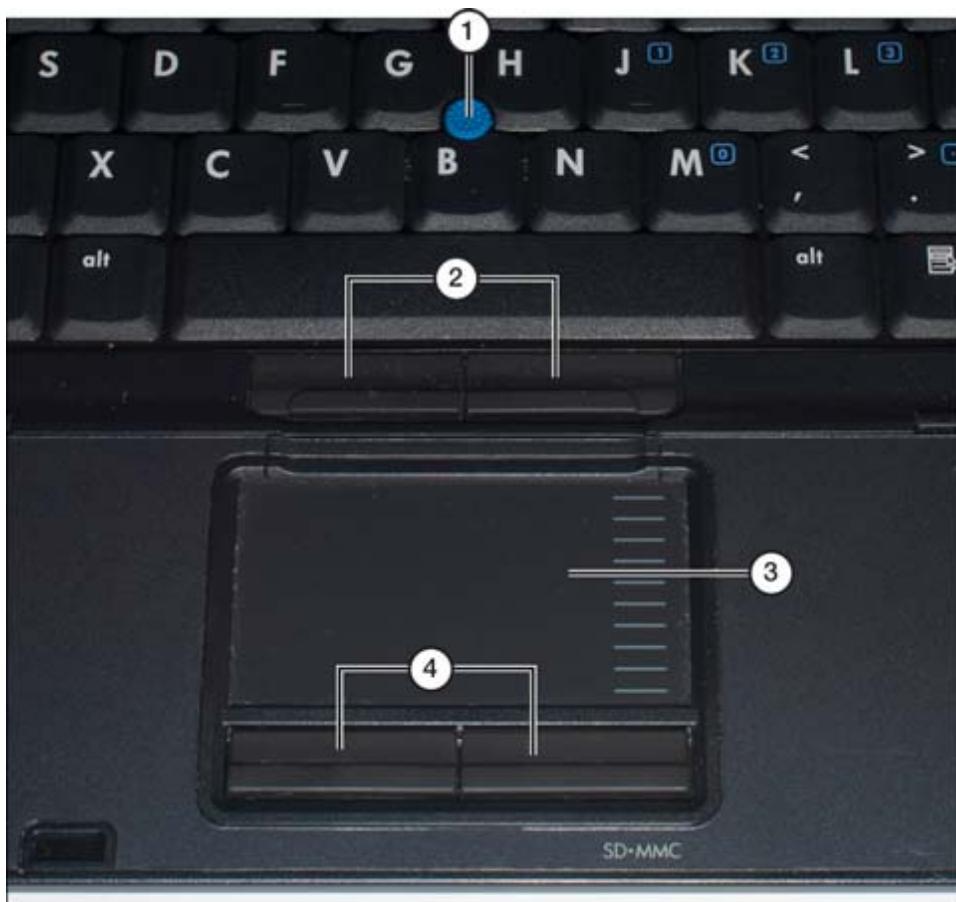
**Figure 1-2** The Same Laptop as in [Figure 1-1](#) After Opening Access Panels to Permit Component Replacements or Upgrades

## Note

Some laptops use a single cover instead of multiple covers for all upgradable components. Some laptops require disassembly to access the hard disk drive or SSD mass storage. Check the system documentation for details.

# Keyboard

If a laptop **keyboard** or its **pointing device** (touchpad or pointing stick) fails, the unit must be replaced. A laptop with a touchpad has a keyboard that is separate from the touchpad, whereas a laptop with a pointing stick has a pointing stick that is integrated with the keyboard. Some laptops have both types of pointing devices (see [Figure 1-3](#)).



1. Pointing stick
2. Buttons for pointing stick
3. Touchpad
4. Buttons for touchpad

**Figure 1-3** A Business-Class Laptop with a Pointing Stick and a Touchpad

## Note

Touchpads are generally located in the palm rest (which extends below the keyboard). Pointing sticks, such as the IBM/Lenovo TrackPoint and Toshiba AccuPoint, are located in the middle of the keyboard (with buttons located in the palm rest).

To replace a keyboard (with or without a pointing stick), follow this basic procedure:



- Step 1.** Disconnect the laptop from AC power and remove the battery.
- Step 2.** Remove the screws that hold the keyboard in place.
- Step 3.** Turn the laptop upright.
- Step 4.** Open the screen so that the keyboard is visible.
- Step 5.** If necessary, remove the bezel that holds the keyboard in place.
- Step 6.** Lift up the keyboard to expose the keyboard cable.
- Step 7.** Remove any hold-down devices used to hold the keyboard cable in place.
- Step 8.** Disconnect the keyboard cable from the system board (see [Figure 1-4](#)).



**Figure 1-4** Removing the Keyboard Cable

**Step 9.** Remove the keyboard.

To install a replacement, reverse these steps.

### Note

It is a good idea to look for instructions on the manufacturer's website. For example, some laptops require that the display be removed before the keyboard.

## Hard Drive Storage

Most laptop computers use one 2.5-inch storage drive that comes in one of three common choices: HDD, SSD, or SSHD. Each has strengths and weaknesses, and each could be the right choice, depending on the scenario presented:

- **Hard disk drive (HDD):** These magnetic disks have been a standard option for years and combine low cost with large capacity. However, they are slower than the other options. Because they use magnetic disks and moving parts that can wear down, they are the least reliable of the three options.
- **Solid-state drive (SSD):** SSD is a flash memory drive with no moving parts. It is much faster than an HDD when booting and storing or retrieving data. Although SSDs currently cost more than HDDs, their prices are dropping and their capacity is improving. Many newer laptops have M.2 expansion ports and can support an M.2 SSD card that is directly mounted to the circuit board for even faster reading.
- **Solid-state hybrid drive (SSHD):** An SSHD combines a solid-state cache with magnetic capacity. It uses a memory manager to choose the most common files for the fast cache.

[Table 1-2](#) highlights the differences among these three hard drive options.



**Table 1-2** Comparison of HDD, SSD, and SSHD

Type of Hard Drive	Cost	Capacity	Speed	Reliability
HDD	Least expensive and readily available	Highest capacity	Slowest because of moving parts and magnetic disks	Has moving parts that can wear over time

Type of Hard Drive	Cost	Capacity	Speed	Reliability
SSD	Most expensive, but price is dropping	Lowest capacity, but improving	Fastest	Has no moving parts
SSHD	Midrange cost	Blends high HDD capacity with fast solid-state cache for most-used files	Blends fast solid-state cache with slower magnetic storage	Has moving parts that can wear out, but spins less than HDD

## Note

Some laptops use the 1.8-inch or 2.5-inch SSD form factor (hard disks or SSD). The larger 3.5-inch drive form factor is used in desktop drive enclosures or in desktop computers.

Although a few laptop computers require removing the keyboard to access the hard drive, most laptops feature storage devices that can be accessed from the bottom of the system. Follow this procedure to remove and replace a storage device (HDD, SSD, or SSHD) accessible from the bottom:



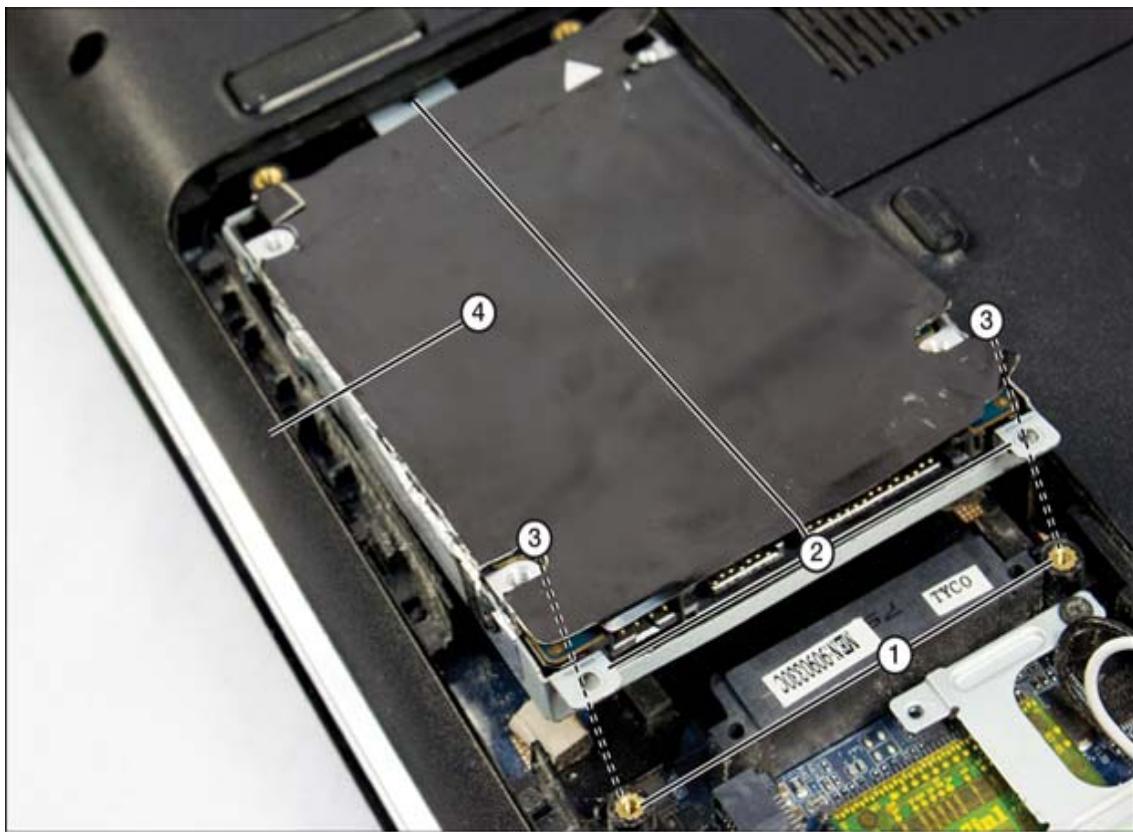
**Step 1.** Disconnect the laptop from AC power and remove the battery.

**Step 2.** Loosen or remove the screw or screws used to hold the drive cover in place.

**Step 3.** Slide the cover away from the retaining lug or clips and remove it.

**Step 4.** Remove the screws holding the drive to the chassis.

**Step 5.** Slide the drive away from the retaining screw holes and lift it out of the chassis (see [Figure 1-5](#)).



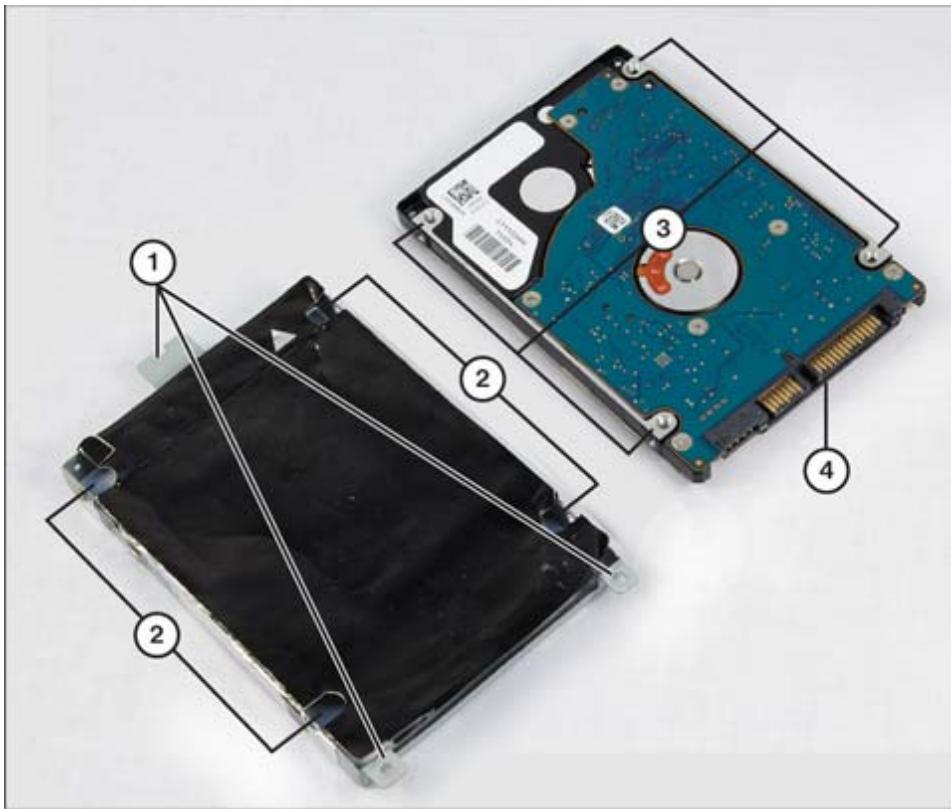
1. Retaining screw holes
2. Drive mounting frame tabs
3. Remove/attach bolts through tabs into screw holes
4. Protective cover over hard disk circuit board

**Figure 1-5** Removing a Laptop Hard Disk After Removing the Retaining Screws

**Step 6.** If the computer uses an interposer—that is, a proprietary connector linking the drive’s SATA connector and the drive bay—remove it and save it for reuse.

**Step 7.** Remove the screws fastening the drive to the drive frame.

**Step 8.** Remove the drive from the drive frame (see [Figure 1-6](#)).



1. Mounting tabs
2. Mounting holes for drive
3. Matching screw holes in drive
4. SATA data and power connectors

**Figure 1-6** A Laptop Hard Disk After Being Removed from Its Mounting Frame (Compare to [Figure 1-5](#))

**Step 9.** Insert the new hard drive into the drive frame.

Reverse these steps to install a new hard drive.

After the system is restarted, start the computer and enter the BIOS or UEFI setup program to verify that the system has properly recognized the new hard drive.

## HDD/SSD Migration

Hard drive migration is the process of copying or cloning data from an old hard drive to a new hard drive. Before cloning a new hard drive, a couple steps need to be taken. First, create a full backup of the computer on an external drive. This ensures that no data is lost if something goes wrong in the migration process. Then check to ensure that the new hard drive has enough space to hold all the data from the old hard drive. Finally, to copy data from one hard drive to another, disk cloning software (either built in or third party) needs to be installed and set up. Remember to set the old hard drive as the source disk and to set the new hard drive as the destination disk. When the cloning process is complete, ensure that everything is operating normally, with all settings correct and all data present.

## Memory

The variety of available computer memory can cause confusion. [Table 1-3](#) provides a brief list of memory types, including memory specifically for laptops.

**Table 1-3** RAM Review

Type of RAM	Description
RAM (random access memory)	Volatile memory that is not used for storage.
SDRAM (synchronous dynamic RAM)	Combination of static RAM and dynamic RAM.
SDR SDRAM (single data rate SDRAM)	Single data rate means that the internal clock rate and input/output are the same.
DDR SDRAM (double data rate SDRAM), DDR3, DDR4, DDR5	Double data rate allows for nearly twice the bandwidth by supporting data transfers on the rising and falling edges

Type of RAM	Description
	of the clock cycle. DDR5 is the latest generation.
DIMM (dual inline memory module)	Form factor used in desktops.
SODIMM (small outline DIMM)	Form factor used in laptops.

When selecting the right memory upgrade for a laptop, note the following:



- **Form factor:** Most laptops in service use DDR3, DDR4, or DDR5 SODIMMs. DDR5 SODIMM, the latest generation, offers twice the transfer rate and operates at a lower voltage, compared to DDR4 SODIMM.
- **Memory speed:** When adding a module, make sure it is the same speed as the existing module. When replacing the modules, buy a matched set of modules in the fastest speed the system supports.
- **Memory timing:** The most common way to refer to memory timing is by its column address strobe (CAS) value. Installing memory modules that use different CAS values can cause the laptop to become unstable and crash or lock up.

To determine the correct memory to use for a memory upgrade, use one of the following methods:

- **Use the interactive memory upgrade tools available from major third-party memory vendors' websites:** These tools list the memory modules suitable for particular laptops and detect the currently installed memory. Crucial System Scanner is a useful tool for showing what is currently installed and what is

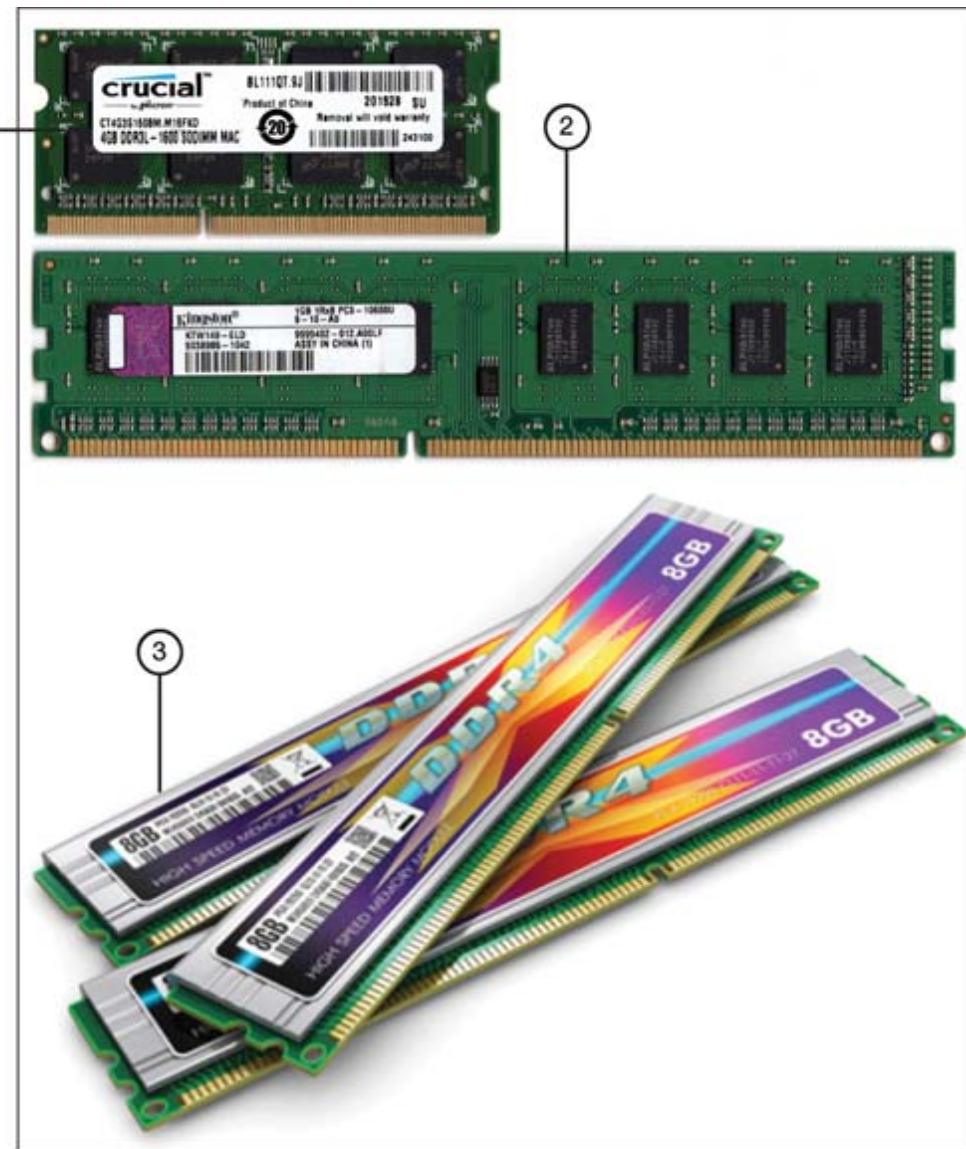
compatible. For more information, visit one of these sites.  
(These are only two of many online memory marketplaces.)

[www.crucial.com/usa/en/systemscanner](http://www.crucial.com/usa/en/systemscanner)

[www.kingston.com/unitedstates/us/configurator](http://www.kingston.com/unitedstates/us/configurator)

- **Check the vendor's memory specifications:** Determining part numbers is possible by using this method, but this method works best if memory must be purchased from the laptop vendor rather than from a memory vendor.

Generally, laptops have two connectors for memory, typically using small outline DIMMs (SODIMMs), which are reduced-size versions of DIMM modules. [Figure 1-7](#) compares a typical DDR3 SODIMM with a DDR3 DIMM and a DDR4 DIMM.



1. DDR3L (low voltage) SODIMM
2. DDR3 DIMM
3. DDR4 DIMM

**Figure 1-7** Comparison of SODIMMs and DIMMs (DDR4 Image)  
© scanrail, 123rf.com)

Table 1-4 compares the major features of SODIMMs (also known as SO-DIMMs).

Key Topic

**Table 1-4** SODIMM Features

<b>Memory Type</b>	<b>Number of Pins</b>	<b>Notch Location</b>	<b>Notes</b>
DDR3	204	After pin 36	67.6mm long and 30mm high
DDR4	260	After pin 144	69.6mm long and 30mm high
DDR5	262	After pin 116	69.6mm long and 30mm high

**TIP**

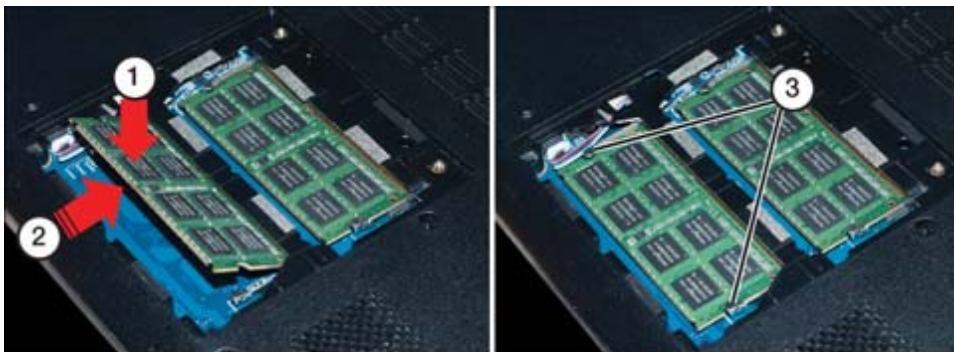
The best memory upgrade for a portable system is to add the largest-capacity memory modules that can be installed in the system. To improve performance, use matched sets on systems that support multichannel memory.

Follow these steps to perform a typical memory upgrade:



- Step 1.** Disconnect the laptop from AC power and remove the battery.
- Step 2.** Remove any screws or hold-down devices.
- Step 3.** Remove the old memory module(s), if necessary. To remove a memory module, pull back the clips on both sides and swing the memory up and out.
- Step 4.** Insert the new memory upgrade, making sure the contacts on the edge of the module make a firm connection with the connector.

**Step 5.** Push down the top of the module until the latches lock into place (see [Figure 1-8](#)).



1. Push the SODIMM into the connector at the appropriate angle
2. Push the SODIMM down until the latches lock into place
3. The latches hold the SODIMM in place

**Figure 1-8** Installing a SODIMM Module on a Typical Laptop

**Step 6.** If the memory socket requires screws to secure the memory in place, install them.

**Step 7.** To complete the upgrade, close the cover and secure it.

**Step 8.** Test the upgrade by starting the system and running a memory diagnostic tool. (Windows includes memory testing software, and you can also download a memory testing program.)

## Mini PCIe

A Peripheral Component Interconnect (PCI) slot in a computer is a slot for plugging in add-on peripherals. This slot provides access to the motherboard for a device such as a Wi-Fi modem, a video graphics processing unit (GPU), or added storage with an M.2 card. miniPCI Express (mPCIe) cards perform functions similar to those of the PCIe card, but they are designed for the compact space of a laptop. The mPCIe slots in a laptop are used for plugging in wireless cards and also for M.2 memory modules. Other examples of modules that can plug into mPCIe slots are GPS units, cellular cards, and analog-to-digital converter (ADC) cards.

## Wireless Card

A laptop with Wi-Fi or Bluetooth support typically uses either an mPCIe expansion card or an M.2 card to provide wireless network support. Additionally, the M.2 card form factor (also called NGFF, for next-generation form factor) is used for SSD and other I/O devices. Note that an M.2 card slot made for SSD cannot be used for Wi-Fi or Bluetooth cards.

Regardless of which **wireless card** a laptop uses, two antennas lead from the Wi-Fi antennas built into the display panel and need to be connected to the card.

To remove a wireless card, follow this basic procedure:



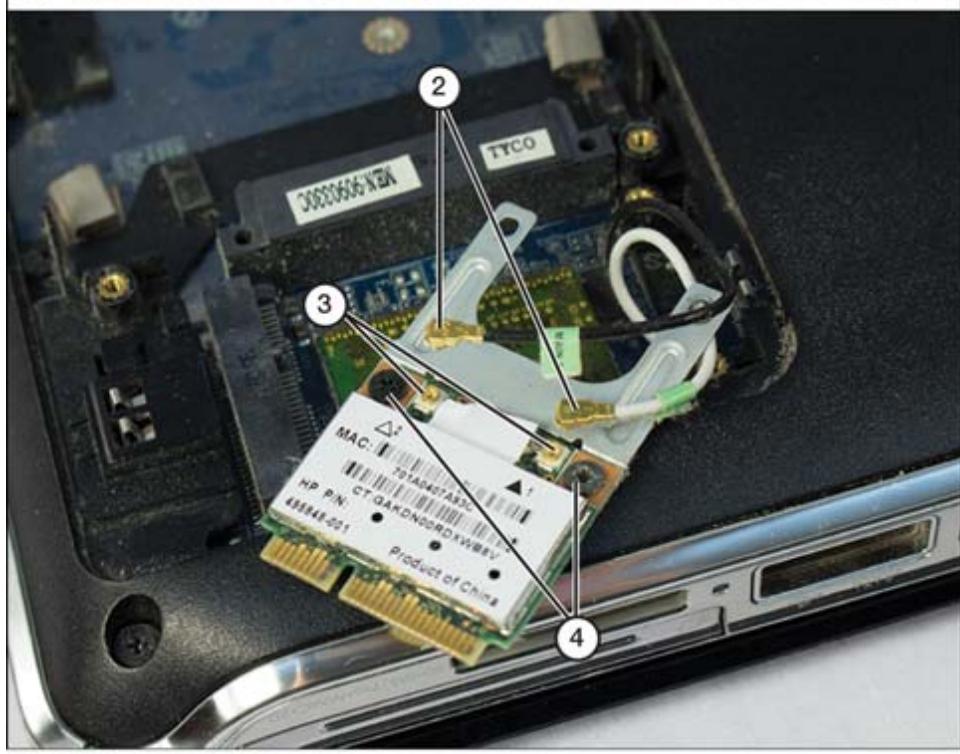
**Step 1.** Verify the location of the card. Some laptops have the card under the keyboard; others have the card under a removable cover on the bottom of the computer.

**Step 2.** Disconnect the laptop from AC power and remove the battery.

- a. If the card is located under the keyboard, remove the keyboard.
- b. If the card is located under an access panel, remove the screws holding the access panel in place.

**Step 3.** Disconnect any wires connected to the adapter. They might be screwed into place or snapped into place. Note their positions.

**Step 4.** Unscrew any bolts holding the card in place. A miniPCIe card (refer to [Figure 1-9](#)) uses two mounting bolts; an M.2 card (refer to [Figure 1-10](#)) uses a single mounting bolt.



1. Unscrew mounting bolts
2. Antenna wires
3. Antenna wire attachment points
4. Unscrew mounting bolts to remove card from bracket

**Figure 1-9** Removing a miniPCIe Wireless Card



1. Mounting screw fits here
2. Antenna connectors
3. M.2 connector

**Figure 1-10** A Typical M.2 Wireless Adapter

**Step 5.** Rotate the card upward at a slight angle and remove it from the slot.

**Step 6.** If the card is attached to a bracket, remove the card from the bracket.

To reinstall the card or replace it with a different card, reverse these steps.

## USB Travel Routers and Wireless WAN Cards

Another option for traveling users is a mobile hotspot. Each cell provider has its own version of a hotspot and can add a hotspot with a data plan to the user's cell account.

## Battery

A failing laptop battery can be a source of all kinds of problems for the user. Most manufacturers have diagnostic software that reports on the health of the battery and estimates how many cycles are left. It is best to be proactive in battery replacement. If you need to purchase a replacement battery for a laptop, consider getting a larger-capacity battery, if one is available for the model being repaired.

Before you replace any internal components, you must remove the system from all power sources. Follow this procedure:



- Step 1.** Turn off the computer.
- Step 2.** Disconnect the AC adapter from the computer.
- Step 3.** Open the battery compartment in the unit; it might be secured by a sliding lock or by screws.
- Step 4.** If the battery is under a removable cover, remove the battery compartment cover.
- Step 5.** Open the lock that holds the battery in place.
- Step 6.** Slide or lift out the battery (see [Figure 1-11](#)). If the battery is a flat assembly, it might be held in place by a clip; if so, push the clip to one side to release the battery.



1. Releasing the battery catch
2. Rotating the battery up and out of the battery compartment

**Figure 1-11** Removing a Battery from a Typical Laptop Computer

**Step 7.** Examine the battery contacts inside the computer for dirt or corrosion, and clean dirty contacts with a soft cloth.

To replace the battery, follow these steps:

**Step 1.** Line up the replacement battery with the contacts inside the battery compartment. Make sure you insert the battery so that the positive and negative terminals are in the right directions.

**Step 2.** Slide or clip the battery into place.

**Step 3.** Replace any cover over the battery compartment.

**Step 4.** If the battery must be charged before use, plug in the AC adapter to both the computer and the wall outlet. Check the computer's manual for the proper charge time for the new battery.

## CAUTION

Take precautions against ESD when you change the battery. Discharge any static electricity in your body by touching a metal

object before you open the battery compartment, and do not touch the contacts on the battery or the contacts in the battery compartment with your hands.

## Physical Privacy and Security Components

The use of mobile devices for personal financial transactions is steadily trending upward. With this increased use comes the need for increased security and reliability when authenticating users who are transferring money.

### Biometrics

**Biometrics** are the physical characteristics of someone that make that person uniquely identifiable in the world. Examples of biometrics are fingerprint readers, retina scanners, and facial recognition software. One or more of these biometrics is scanned into authentication software, and the device then uses the details of those biometrics to validate the user.

Smartphones and tablets commonly include biometric authentication. Although this feature has been slower to arrive in laptops, many newer models now include biometric readers.

### Near-field Scanner Features

**Near-field communications (NFC)** technology is currently most commonly used for peer-to-peer payments and other transactions on newer smartphones. NFC allows secure communication between devices that are physically close. NFC range is about 4 inches (10cm). For example, when making a purchase at a grocery store, a customer might want to pay with a debit card stored on his or her phone. When the customer accesses the digital wallet to pay, the phone will likely ask for biometric verification of identity and then use NFC to communicate between the phone and the store's payment

system. Biometrics and NFC work together this way to keep digital commerce simple and secure.

Devices that use NFC are common. Smartphones after iPhone 6 support Apple Pay. Depending on the manufacturer, devices running Android 4.0 and later support Samsung Pay or Google Pay.

NFC on mobile devices has other uses, too, such as connecting to speakers for music, accessing locked automobiles, controlling door access for some locking systems, and accessing transportation such as busses and trains. As the Internet of Things (IoT) continues to expand, we can expect interactions with NFC applications to expand as well.

## Display Components of Mobile Devices

220-1101  
Exam

**220-1101: Objective 1.2:** Compare and contrast the display components of mobile devices.

## Display Components

A computer display screen typically consists of a liquid crystal display (LCD) or an organic light-emitting diode (OLED) display, and any communication peripherals are added separately. Laptop screens are specially designed to accommodate a webcam, a microphone, Wi-Fi antennas, and often touchscreen digitizers and inverters.

An LCD screen uses a backlight to illuminate light-modulating liquid crystals. When an electric current passes through the crystals, they arrange into patterns that become the image on the screen. LCD screens are customized to different device types, and some have Wi-Fi antennas attached.

In many ways, OLED screens are advanced compared to LED screens. They are brighter, they use less energy (saving on battery

use), and they are both flexible and foldable. However, the screens themselves are much thinner and more subject to cracking or breaking when they are dropped or mishandled.

The display of a laptop is simply known as a **screen**, but there is more to a display than meets the eye. Different types of screens exist, with various components behind the glass that make them work. The following sections cover the essentials of screen technology.

## Screens

Replacing screens can be a difficult task, and it involves expensive and delicate parts. Some vendors provide online documentation of the entire process of reducing an intact portable into many parts and then rebuilding it. However, this information is primarily intended for professional computer service staff.

## LCD

A **liquid crystal display (LCD)** is made with either a passive or active-matrix display grid. Active matrix is considered the better technology and has replaced passive-matrix in current laptops and mobile devices. An active-matrix screen uses a transistor for every dot onscreen; for example, a 1,600 900 active-matrix LCD screen has 1,440,000 transistors. Each pixel intersection in an active-matrix screen has a transistor, and a small current is sent across the screen grid. The transistors can manage the current on the screen very quickly, giving the user an experience of smoothly flowing motion.

There are several types of LCD screens, and each has advantages and disadvantages. The following three are the most common:

- **In-plane switching (IPS):** The *plane* in IPS refers to an area between two glass layers under the screen. This area is the plane that holds liquid crystal cells (or pixels) horizontally. When electrodes in the screen are activated, the cells “switch” by

rotating and allowing light and color to show. These are so close and work so quickly that the screen can appear to display fluid motion when called for. This is the most popular type of active-matrix display in use. The response time with IPS screens is very fast, but they may not offer the deep contrast of other types of screens.

- **Twisted nematic (TN):** This term refers to transparent liquid crystals that cause light to polarize when they are energized. This technology was important in the growth of LCD screens because high quality could come with very low voltage usage. The *twist* refers to the form of the crystal molecules when no power is applied. When turned on, the molecules untwist and allow light through, to be polarized.
- **Vertical alignment (VA):** In the off state, the crystal molecules align perpendicular to the electric field. When energized, they align themselves parallel to the glass plates. VA displays offer high contrast in pictures, but the crystal response time is slower than with TN or IPS screens.

## OLED

An **organic LED (OLED)** offers the highest quality of liquid crystal display because, unlike other LCD types, it uses a layer of organic compounds between two electrodes to emit light. As a consequence, the brightness of each OLED pixel can be individually controlled. OLED displays have been developed in two forms: passive matrix (PMOLED) and active matrix (AMOLED).

The advantages of OLED are as follows:

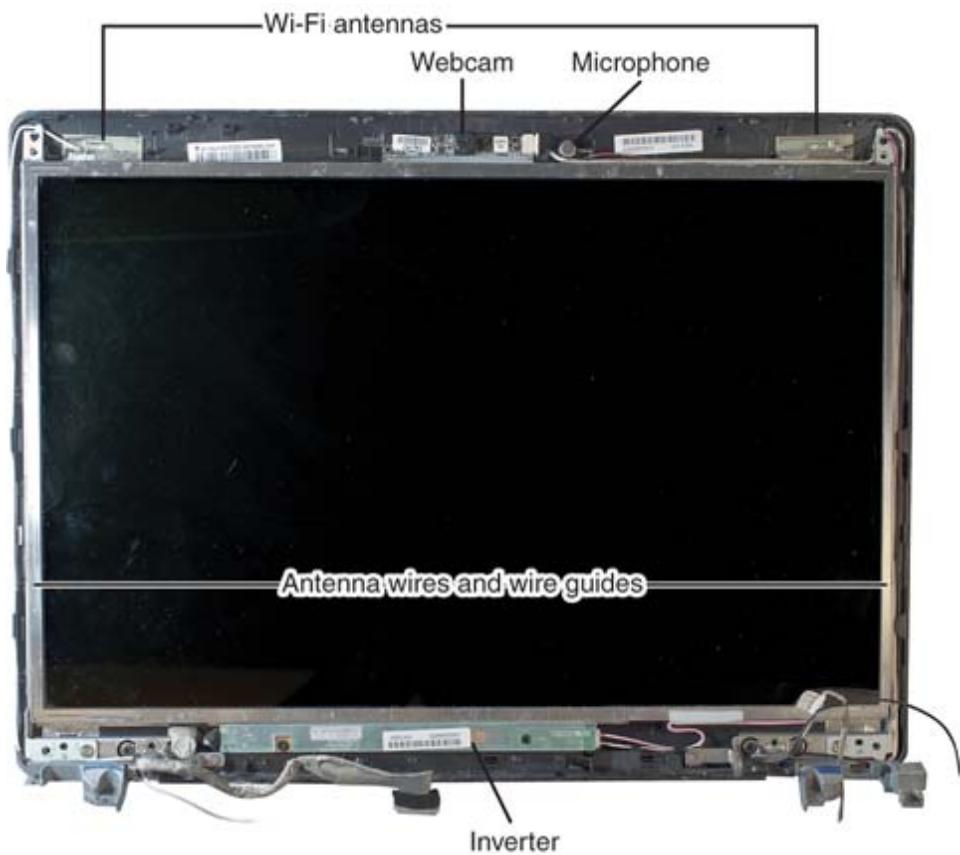
- **Brighter:** OLEDs can be larger than other types of screens and offer higher resolutions.
- **Thinner in size and lighter in weight:** OLEDs are a good choice for smartphones, tablets, and convertible (two-in-one) units that switch between laptop and tablet modes.

- **Energy efficient:** Only the lit pixels draw power; with good application design, this can greatly extend battery life.
- **Faster refresh rates:** OLEDs can refresh quickly, which makes them a favorite of gamers who value quick response time.

## Wi-Fi Antenna Connector/Placement

Although the miniPCIe card that contains the Wi-Fi radio is located in the base of a laptop, the Wi-Fi antenna is usually part of the screen assembly (see [Figure 1-12](#)). If a laptop screen is damaged, the Wi-Fi antennas might also be damaged. In an OLED display, the inverter is not present, but the rest of the components are in the same locations.

Key Topic



**Figure 1-12** Wi-Fi Antennas, Wires, Inverter, Webcam, and Microphone in a Typical LCD Display

## Webcam

Almost every laptop display assembly includes a webcam at the top-center edge of the display assembly (refer to [Figure 1-12](#)). If a webcam fails, it can be replaced after performing a partial teardown of the laptop assembly. However, replacing with a higher-resolution webcam will likely require using an external webcam that plugs into a USB port.

## Microphone

A microphone is also part of the display assembly. It is used by the webcam and works for other recording purposes, as needed (refer to [Figure 1-12](#)). If a microphone fails, it can be replaced after performing a partial teardown of the laptop assembly. However, replacing the original with a higher-quality microphone can require using a microphone as part of a headset that plugs into an audio port or a USB port.

## Inverter

An LCD laptop display is easy to read because of two components: the inverter and the backlight. If either fails, the laptop display becomes so dim that it is almost impossible to use.

The inverter (refer to [Figure 1-12](#)) is a power converter that changes low-voltage DC power into the higher-voltage AC power needed to power a backlight. If the inverter fails, the backlight will not work. Inverter failure is the most common cause of LCD display failure. Inverters are relatively inexpensive to replace, and they can be purchased for do-it-yourself (DIY) replacement.

## Note

Many technicians have uploaded demonstrations of changing inverters to the Web. A good resource for all things LCD is [www.lcdpart.com](http://www.lcdpart.com).

## Touchscreen/Digitizer

A touchscreen display differs from a standard laptop display, in that it has a digitizer layer on top of the display panel. The digitizer detects and transmits touches to the laptop processor. Digitizers are also used on touchscreen smartphones, tablets, fitness monitors, smart watches, phablets, e-readers, and smart cameras.

If the digitizer layer is damaged but the display panel is intact, the digitizer layer can be replaced separately.

## Note

For examples of pricing and availability of digitizers, see [www.touchscreendigitizer.net](http://www.touchscreendigitizer.net). Demonstrations of replacing a digitizer are available online.

## Setting Up and Configuring Accessories and Ports of Mobile Devices

220-1101  
Exam

**220-1101: Objective 1.3:** Given a scenario, set up and configure accessories and ports of mobile devices.

Mobile devices are popular because they can provide the functionality of a connected computer without the wires and cables necessary on a traditional PC. However, some accessories can greatly augment the

use of a mobile device for the user. This section discusses common connection methods for accessories that add function to a mobile device.

## Connection Methods: Wired



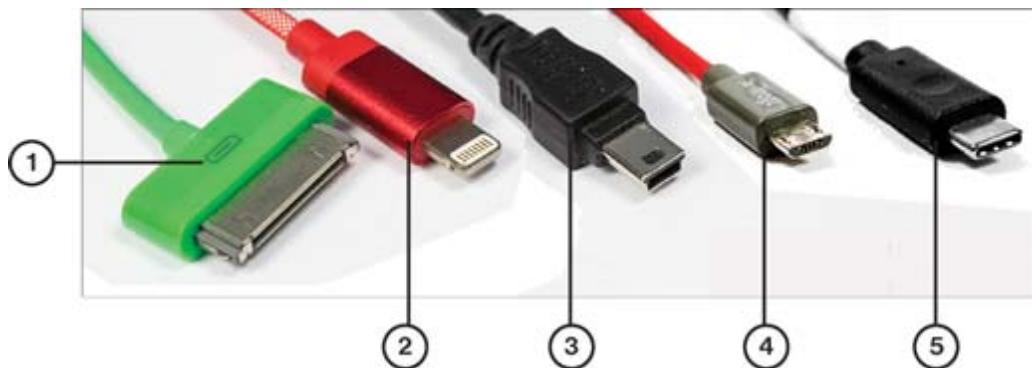
Wired connections have long been moving from proprietary design to universal standards such as USB 3.1, USB 3.2, and USB-C. The following sections describe a few wired connection types that a technician will likely encounter.

### Micro-USB/Mini-USB for Android and Windows

For a brief period, the 5-pin **mini-USB** port was used for Android smartphones. Most recently, the USB-On-The-Go connector has become the de facto standard for both Android smartphones and tablets. However, some recent Android tablets use the reversible USB Type C connector.

Most Android tablets and smartphones (depending on the model) use the USB-On-The-Go (micro-USB) connector or the USB Type C connector.

[Figure 1-13](#) compares 30-pin, Lightning, 5-pin mini-USB, micro-USB, and USB Type C cables. All these cables have the standard USB Type A connector on the other end.



1. 30-pin power/sync cable (iOS)
2. Lightning power/sync cable (iOS)
3. 5-pin miniUSB power/sync cable (Android)
4. microUSB(USB-on-the-Go) power/sync cable (Android smartphones and tablets, Windows tablets)
5. USB Type C power/sync cable (several smartphone brands and the iPad Pro)

**Figure 1-13** The Most Common Mobile Power/Sync Cables

## USB-C

The relationship between USB 3.x USB-C can be confusing, and it is important to know that not all USB-C cables are the same. Different standards of USB, such as USB 3.1 and 3.2 (and even the approaching USB 4.0), might all use the USB-C type connector. The USB-C connector has some important benefits: Most notably, it is easier to plug in because it works with either side of the cable up. The connector is standard, but the cable standards can vary. As a result, it is a good idea to use the USB-C cables and connectors that the manufacturer provides. When purchasing USB-C cables from a source other than the manufacturer, be sure to check the technical specifications for the device and match them to the cable being purchased. Otherwise, a device might be underpowered and the fast charging of some devices might be disabled.

During the last few years, manufacturers have begun using USB-C for power as well. USB-C can deliver up to 100W of power, which is enough to charge and power some laptops. Many manufacturers have replaced standard power cables with USB-C connectors and wall adaptors.

## **Lightning for Apple iOS**

Older iOS devices (up through the iPhone 4 series and the third-generation iPad) used the 30-pin connector. However, starting in 2012, Apple standardized on the 8-pin reversible **Lightning** connector for iPhones, iPads, iPods, and other mobile devices. (The iPad Pro, however, uses USB Type-C.)

## **Hotspot**

Most smartphones can share a cellular data connection by using tethering. Wired tethering involves attaching the phone to a laptop or tablet with a phone cable with a USB connection. When tethering is done wirelessly, the phone becomes a **hotspot** (see the upcoming section under “Connection Types: Wireless”).

## **Serial Interfaces**

Although you might still encounter physical serial interfaces in older laptops, wireless serial interfaces can be equipped on some mobile devices for transferring data. If necessary, some cables can connect USB to serial ports for printing and other data transfer.

## **Proprietary Vendor-Specific Ports (Communication/Power)**

Until recently, every smartphone and tablet used its own proprietary connection for charging and file synchronization. Older Android tablets and smartphones used various proprietary chargers. To support these, multiple-head AC or 12V DC chargers were sold, as were dedicated cables. Some vendors still utilize their own proprietary ports for charging and data transfer, such as with the Apple Lightning connector for iPhones, iPads, and iPods.

# Connection Types: Wireless



Wired connections can offer high-speed data coupled with battery charging benefits, but sometimes wires get in the way or simply are not a practical solution for device connection. Three types of wireless connections are in common use today: NFC, Bluetooth, and hotspots.

## NFC

Near-field communication (NFC) is a feature that is included in many mobile devices, such as smartphones and tablets for data transfer and shopping. When NFC is enabled and a suitable payment system (such as Apple Pay or Google Pay) is installed on a mobile device, the device can be used for payment at any retailer that supports NFC payments.

NFC can also be used to automatically turn on Bluetooth and transfer files between devices (a feature sometimes referred to as “tap and go” or, on Android devices, Android Beam). It can be enabled separately from NFC for payments.

Apple does not currently permit its devices with NFC to work for file transfers, except with iTunes purchasing and Apple Pay. The Apple AirDrop feature uses peer-to-peer Wi-Fi for file sharing.

To set up or reset passcodes and biometrics for NFC on an iPhone, go to Settings and then Face ID & Passcode. On an Android device, go to Settings and then NFC. Use the NFC switch to enable the feature. If a confirmation dialog appears, select Yes to enable it.

## Bluetooth

**Bluetooth** began as a short-range, low-speed wireless network technology primarily designed to operate in peer-to-peer (or ad hoc)

mode between PCs and other devices, such as printers, projectors, smartphones, mouse devices, and keyboards. Before a Bluetooth device can work with your computer or mobile device, it must be paired with the device.

By default, Bluetooth is usually disabled on Android devices but is enabled on iOS devices such as iPads and iPhones. The process of connecting a Bluetooth device to a mobile device follows:

1. Bluetooth first needs to be enabled. This can be done on iOS devices either by swiping the screen to access the Control Center or by going into Settings, tapping on Bluetooth, and manually enabling it. On an Android device, Bluetooth can be enabled by going to Settings and then Wireless and Network Settings.
2. After Bluetooth is enabled, the Bluetooth device needs to be synchronized to the mobile device. This is known as *pairing* or *linking*. To pair devices, the Bluetooth device needs to be set as discoverable. When the device is in a discoverable mode, it appears on the screen. Pairing a device can sometimes require a PIN code.
3. After it is paired, the device should be listed as connected and needs to be tested to ensure that the devices are synchronized.

For more information on Bluetooth, see [Chapter 2, “Networking.”](#)

## Hotspot

When a smartphone enables the sharing of its Internet connection, it becomes a hotspot. Creating a hotspot enables wireless tethering, creating a small Wi-Fi network. The phone generates a default password (which the phone user can change) that other Wi-Fi devices can use to access the network and share the phone’s access to the Web. Setting up a hotspot is covered later in this chapter.

## **Accessories**

Mobile devices can be expensive, and users want to get the most use from a mobile device while protecting their investment. The accessories listed here are aftermarket add-ons that enhance the experience of using a mobile device.

### **Headsets**

For music listening, some mobile devices feature the same 3.5mm mini-jack that is available on computers for headsets or earbuds. However, for hands-free phone use, you can pair a wireless headset with a smartphone using Bluetooth.

### **Speakers**

Portable speakers use rechargeable batteries, and the USB cable on portable speakers is used only for recharging. Some low-cost speakers use a 3.5mm mini-jack speaker cable, but most use Bluetooth. By using Bluetooth, you can place the speaker in the midst of the action while keeping your smartphone or tablet out of harm's way.

### **Touch Pens**

If a tablet or phone's screen allows it, a touch pen or a stylus can be an efficient way to write or draw graphic notes and have them converted to digital formats for editing and sharing. Touch pens also help prevent smudges that fingers leave on the device's screen. To use a touch pen, simply touch the pen to the surface of the device's screen; this works the same as using a finger.

### **Webcam**

Webcams are built into most mobile devices that are currently available. Earlier versions focused on photography, but the

importance of live images for business and school purposes has increased recently. Videoconferencing and film production have become important to consumers; manufacturers have responded by producing much higher-quality video cameras.

## Trackpad/Drawing Pad

Trackpads and drawing pads are touch-sensitive devices that allow a user to interact with a mobile device through finger gestures or a touch pen. A track pad or drawing pad can be connected to a mobile device either wirelessly or through a wired connection. A wireless connection utilizes Bluetooth, whereas a wired connection uses a USB or similar connector. Trackpads and drawing pads can provide additional features that allow for shortcuts or multitouch capabilities, making them ideal for photo editing or drawing.

## Docking Station

A **docking station** expands the capability of a portable computer by adding features such as the following:

- One or more expansion slots
- Additional I/O ports, such as Ethernet, display output ports (for HDMI or DisplayPort), Thunderbolt ports, USB ports (USB 2.0, 3.0, USB 3.1, and USB Type-C), and others
- Power connection for the laptop
- Connectors for a standard keyboard and mouse

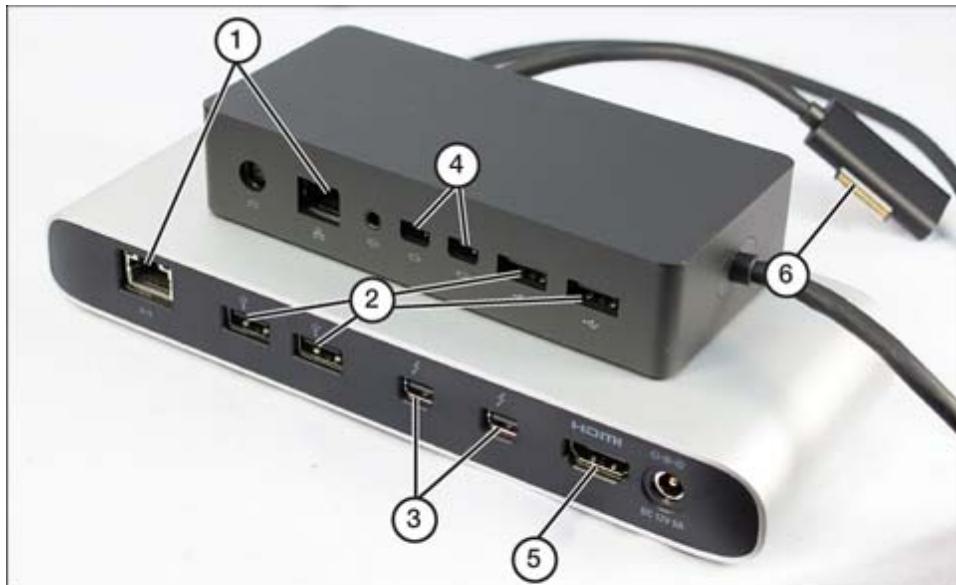
Most docking stations are produced by portable computer vendors, although some third-party products are also available. Business-class laptops that support docking stations might feature a proprietary expansion bus on the rear or bottom of the computer (see [Figure 1-14](#)).



1. Laptop connection to docking station
2. Open door to permit battery charging by docking station

**Figure 1-14** A Typical Proprietary Bus for a Docking Station on a Business-Class Laptop

However, docking stations made for tablets or thin and light laptops might connect via a high-speed bus, such as Thunderbolt or USB 3.0/3.1, or via a proprietary charging/data cable (see [Figure 1-15](#)).



- |                |                                       |
|----------------|---------------------------------------|
| 1. Ethernet    | 4. Mini DisplayPort                   |
| 2. USB         | 5. HDMI                               |
| 3. Thunderbolt | 6. Proprietary charging/docking cable |

**Figure 1-15** Microsoft Dock for Surface Pro 3 and 4 (Top) and a Third-Party Dock for MacBook Air and Pro with Thunderbolt Ports (Bottom)

Wireless docking stations are available for mobile systems running fifth-generation or newer Intel Core vPro (business-class) processors with the Intel Tri-Band Wireless-AC 17265 adapter. Regardless of how a docking station connects to a portable computer, the user can leave desktop-type peripherals connected to the docking station and can access them quickly and easily by connecting the portable computer to the docking station.

## Port Replicator

A **port replicator** is a device that allows a laptop to expand the number of ports so that additional devices can be attached. For example, a user can attach a port replicator to a USB port on a laptop and then attach other devices, such as printers, cameras, mouse devices, speakers, and so on, to the port replicator. The replicator can have DVI and HDMI ports to host additional displays. As features are added, port replicators come to resemble nonproprietary docking stations.

### Note

The terms *docking station* and *port replicator* are often used interchangeably. There is a difference, however. A docking station provides proprietary connections to devices, whereas a port replicator provides industry-standard connections, such as USB and HDMI connections, that work with standard ports in any device.

## Configuring Basic Mobile Device Network Connectivity and Application Support

**220-1101: Objective 1.4:** Given a scenario, configure basic mobile device network connectivity and application support.

Manufacturers are continuously developing new apps and mobile devices that further integrate technology into our daily lives. Many different types of connections, ports, and accessories are available for mobile devices. The following sections review the essential features of several of them.

## Wireless/Cellular Data Network Connectivity for Mobile Devices

This chapter has already introduced the different kinds of connection methods a device can use to send and receive data. The following sections show how to configure these settings.

## Enabling and Disabling 2G/3G/4G(LTE)/5G

Cell providers use the term *generation* to describe the evolution of the wireless technology they provide to customers. First generation was the early analog cellphones, and 2G described the first digital systems developed in the 1990s. Subsequent generations have exponentially improved data rates and services, and phones were improved to take advantage of the service. It is important to note that older phones might not be able to handle updated generations of data, so a 2G phone will be useless on a 3G or 4G network.

4G, also known as Long Term Evolution (LTE), is still the standard for some users today, but 5G is available in many areas and newer phones are 5G capable.

Sometimes changing to a different rate is desirable, such as when troubleshooting connectivity issues or entering an area with slower service.

To check or change the cell data settings on an iPhone 13, simply open the settings and type **Cellular Data Options** in the search area. Select Voice & Data to see the available options. To manually arrive at this page, take the following steps:

- Step 1.** Open the Settings menu and choose **Cellular**.
- Step 2.** From the resulting menu, select **Cellular Data Options**.
- Step 3.** Select **Voice & Data**.
- Step 4.** Choose the preferred connection, such as 5G.

To perform the same function on an Android, follow these steps:

- Step 1.** Go to Apps and select **Settings**.
- Step 2.** Select **Mobile Networks**.
- Step 3.** Select **Preferred Network Type / Preferred Network Mode**.
- Step 4.** Select the preferred option.

## **Enabling/Disabling Hotspots**

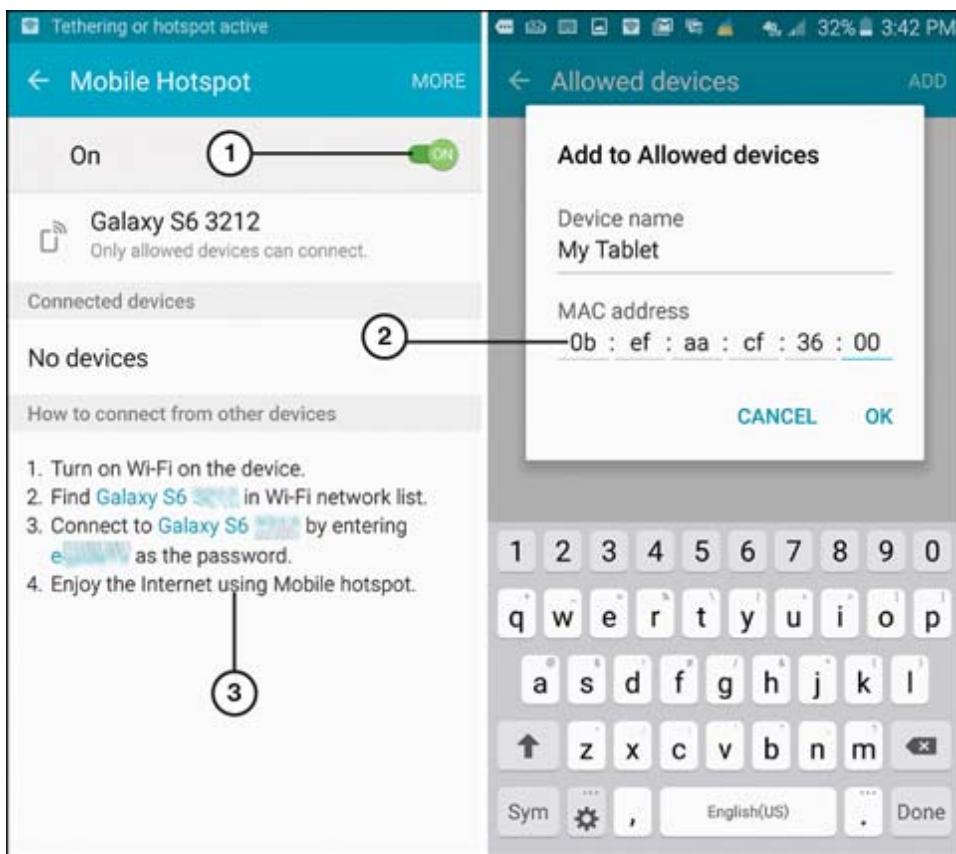


To use the mobile hotspot feature on an Android device, follow these steps (which are based on a Samsung phone running on Android):

- Step 1.** Enable the mobile hotspot feature in the device's setup.
- Step 2.** Select how you want to share the connection wirelessly.  
Provide the SSID and password listed to any devices that will share the connection.
- Step 3.** If you decide to permit only allowed devices to connect, you must provide a name for each device and its MAC address. The MAC address is listed on a label attached to an external adapter. To find the MAC (physical) address for an

internal network adapter, see the sidebar “Finding the Network Adapter’s MAC (Physical) Address.”

**Step 4.** Open the Allowed Devices menu (see [Figure 1-16](#)), click **Add**, enter the device name and address, and click **OK**.



1. Enabling mobile hotspot
2. Entering MAC address of device that will connect to mobile hotspot
3. Instructions for devices that will connect to mobile hotspot

**Figure 1-16** Entering the MAC Address of the Device Sharing the Hotspot’s Internet Connection

## Finding the Network Adapter’s MAC (Physical) Address

If you cannot view the label on an external device, or if your network adapter is internal, use one of these methods to display it. On a Windows device, open a command prompt window and

use the command **ipconfig /all** to see the MAC (physical) address for the device. With macOS 10.4 (Tiger) and newer, the address is located under the Apple menu in the upper-left corner (select System Preferences, Network, Wi-Fi, Advanced). With most Linux distributions, run the command **ifconfig -a**. MAC addresses can be listed in upper or lower case. The MAC address for an iOS device is called its Wi-Fi address. To see it, open **Settings > About**. The MAC address for an Android device is called its Wi-Fi MAC address. To see it, open **Settings > About > Status**.

**Step 5.** Make the connection from your device, just as you would with any other wireless Internet router or hotspot. Enter the password when prompted.

**Step 6.** When your devices are finished using the Internet, disable the hotspot setting in your smartphone or tablet.

## CAUTION

Some cellular providers charge an additional fee if you turn your cellular device into a hotspot or if you use tethering. Check with your mobile service provider for details. Keep in mind that the data usage of every device connected to a mobile hotspot counts toward your total data allocation. If you're not careful, using a mobile hotspot could cost you extra money in overages.

The same process on an iPhone is similar. To use the mobile hotspot feature on an iPhone, follow these steps:

**Step 1.** Select **Settings** and then **Personal Hotspot**. [Figure 1-17](#) shows an iPhone 13 Settings menu with several options pertaining to this section. (Note that the Airplane Mode and Bluetooth options shown here are addressed later in this chapter.)

4:58

LTE

## Settings



Airplane Mode



Wi-Fi

Off >



Bluetooth

On >



Cellular



Personal Hotspot

Off >



Notifications

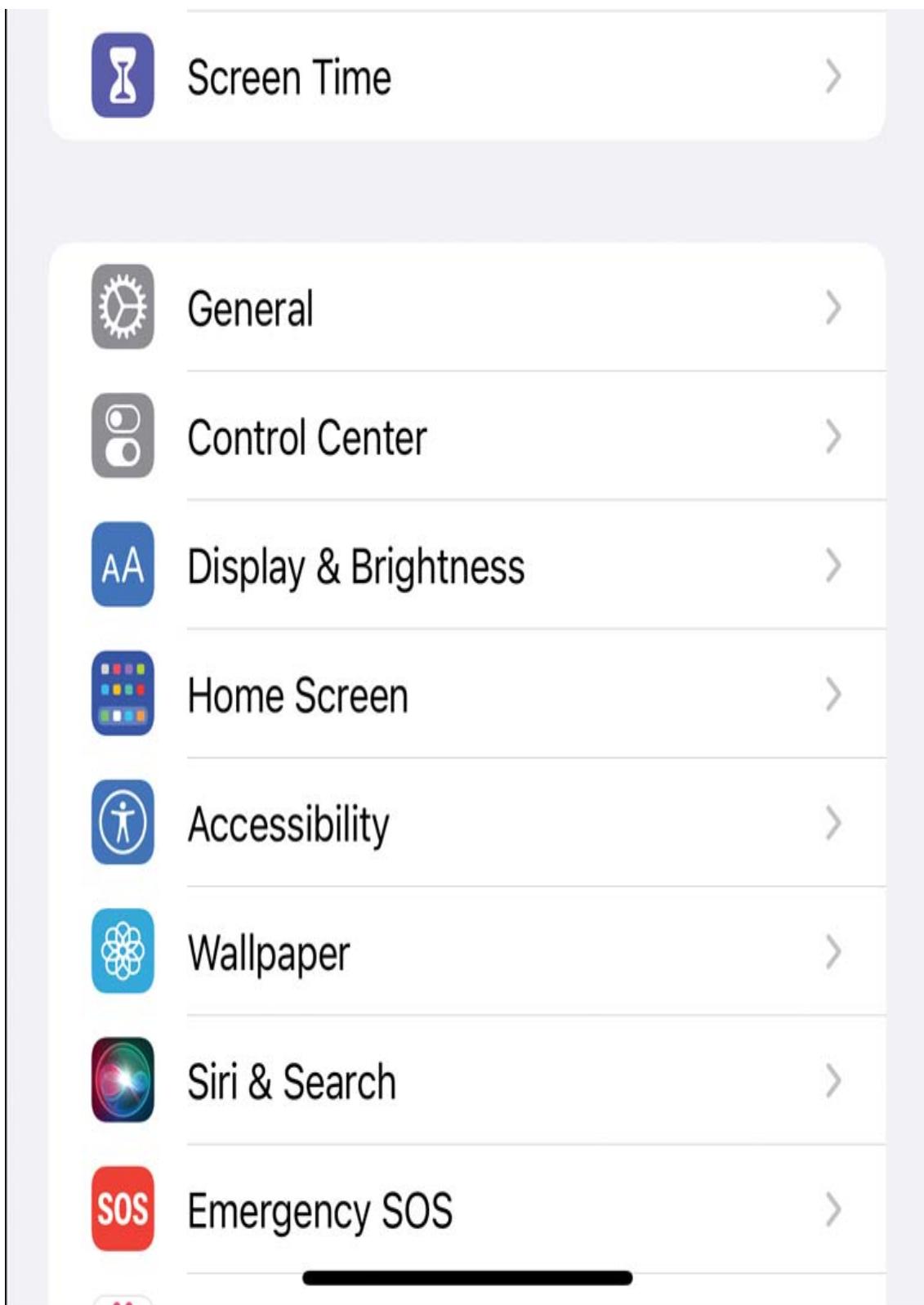


Sounds & Haptics



Focus





**Figure 1-17** iPhone Settings Menu

**Step 2.** Slide the **Personal Hotspot** toggle to turn it on. The menu now shows a Wi-Fi password for the hotspot. The phone generates a password by default, or the user can configure one by selecting the password menu.

**Step 3.** Choose the method of connection. [Figure 1-18](#) shows the options for connecting. For the hotspot, select either Wi-Fi or Bluetooth and follow the instructions for your selection. (An option also is offered for USB, which is used for tethering, as described in the next section.)

4:58



< Settings

## Personal Hotspot

Personal Hotspot on your iPhone can provide Internet access to other devices signed into your iCloud account without requiring you to enter the password.

Allow Others to Join



Wi-Fi Password f19e-t8P4-m0Ht-rD8h >

Allow other users or devices not signed into iCloud to look for your shared network "iPhone" when you are in Personal Hotspot settings or when you turn it on in Control Center.

Maximize Compatibility



Internet performance may be reduced for devices connected to your hotspot when turned on.



#### TO CONNECT USING WI-FI

- 1 Choose "iPhone" from the Wi-Fi settings on your computer or other device.
- 2 Enter the password when prompted.



#### TO CONNECT USING BLUETOOTH

- 1 Pair iPhone with your computer.
- 2 On iPhone, tap Pair or enter the code displayed on your computer.
- 3 Connect to iPhone from computer.



#### TO CONNECT USING USB

- 1 Plug iPhone into your computer.
- 2 Choose iPhone from the list of network services in your settings.

**Figure 1-18** iPhone Personal Hotspot Menu

# Enabling/Disabling Tethering



To use USB **tethering** on an Android, follow these steps:

- Step 1.** Connect a USB cable from your computer to the data port on your device.
- Step 2.** Select the USB tethering option on your device.
- Step 3.** If you are connecting a Windows computer, select the network type (Home) on the computer when prompted.
- Step 4.** Use your computer's web browser and other network features normally.
- Step 5.** When you are finished, disable USB tethering.

## Note

In Windows Device Manager, the tethered USB connection is listed as Remote NDIS Based Internet Sharing Device in the Network Adapters category.

To tether using an iPhone, see the directions in the preceding section, "Enabling/Disabling Hotspots."

## GSM vs. CDMA

*Global System for Mobile Communications (GSM)* and *Code Division Multiple Access (CDMA)* were two methods of cell communication that survived the earlier generations. They still support 2G and 3G phone connectivity. One of the biggest differences between these two systems is that GSM phones use SIM cards to link a particular phone with its network, whereas CDMA phones do not require a SIM card because the phone itself is linked to the network using a

number. When setting up a phone for the first time, the seller uses the IMEI number (for IMEI networks) or the MEID identifier (for CDMA networks). Because these phones have different systems, a phone bought for Verizon (CDMA) cannot be used on an AT&T (GSM) network. GSM/CDMA issues do not apply to 4G and 5G phones, but the systems still reside on phones in case 2G and 3G connections are necessary.

## PRL Updates/Baseband Updates

Updates to your smartphone's **Preferred Roaming List (PRL)** and *baseband* (the portion of the smartphone that makes connections to the cellular network for phone and data) are performed automatically by mobile providers.

When a smartphone or cellular-equipped tablet reports that a system update is available, PRL and baseband are two items that might be updated. Resetting the PRL can help if you are experiencing issues connecting to the cell towers. To reset the connection, go to the phone's dialer (*not* the messaging app) and enter the appropriate code. For example, on an Android, type **##72786#**. On an iOS device, type **##873283#**. Different carriers can have different requirements for phones.

## Bluetooth

As mentioned earlier in the chapter, Bluetooth is a short-range, low-speed wireless network technology that was primarily designed to operate in peer-to-peer (or ad hoc) mode between PCs and other devices. Bluetooth runs in virtually the same 2.4GHz frequency used by IEEE 802.11b, 802.11g, 802.11n, and 802.11ax wireless networks, but it uses a spread-spectrum, frequency-hopping signaling method to minimize interference. Bluetooth devices connect to each other to form a personal area network (PAN).

Some systems and devices include integrated Bluetooth adapters. Others need a Bluetooth module connected to a USB port to enable Bluetooth networking.

Bluetooth 4.0, also known as Bluetooth Low Energy, is designed for use with very low-power applications, such as sensors. Bluetooth 4.1, a software update to 4.0, enables Bluetooth to perform multiple roles at the same time and to work better with LTE cellular devices. Bluetooth 4.2 adds features to support the (IoT). Most Bluetooth mouse devices, keyboards, and headsets on the market today support version 4.0. [Chapter 2](#) covers Bluetooth more extensively.

The most common Bluetooth devices (for example, portable printers, headsets, computer keyboards, and mouse devices) have a range of 10m.

The Bluetooth radios that are built into mobile devices and some laptops can be used for many devices, including headsets, printers, and input devices such as mouse devices and keyboards. By default, Bluetooth is usually disabled on Android devices but is enabled on iOS devices such as iPads and iPhones. To connect a Bluetooth device to a mobile device, Bluetooth first needs to be enabled; then the Bluetooth device must be synchronized to the mobile device. This is known as pairing or linking, and it sometimes requires a PIN code. After it is synchronized, the device needs to be connected. Finally, the Bluetooth connection should be tested.

The following sections show the steps involved in connecting a Bluetooth headset to a typical Android-based device and to an iOS device. Before you begin, make sure the Bluetooth headset is charged.

## **Steps to Configure a Bluetooth Headset on an Android-Based Device**

Follow these steps to connect a Bluetooth headset to a typical Android-based device:



**Step 1.** Go to **Settings > Connections** and then enable **Bluetooth**.

**Step 2.** Tap **Bluetooth** to display the Bluetooth Settings screen.

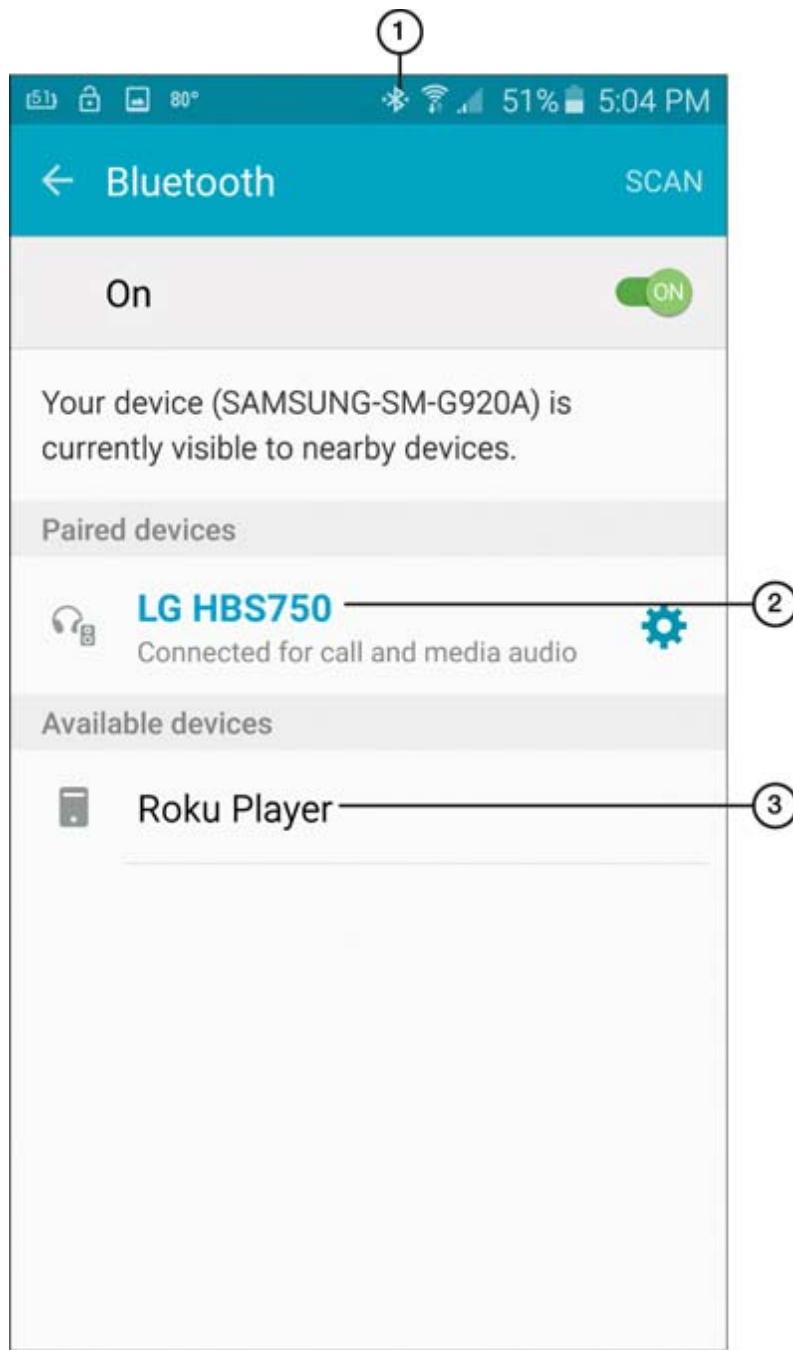
**Step 3.** Prepare the headset. (This process varies from headset to headset.)

**Step 4.** If the Android device is not scanning automatically, tap **Scan**. Keep holding the button on the headset until the Android device finds it.

**Step 5.** On the Android device, tap the device to pair with. Most Android devices pair the Bluetooth headset to the mobile device and then complete the connection automatically, allowing full use of the device.

**Step 6.** Enter a PIN code, if prompted to do so. Many devices come with the default pin 0000.

When finished, the screen on the Android device looks similar to the screen shown in [Figure 1-19](#). Note the Bluetooth icon at the top of the screen. This icon indicates whether Bluetooth is running on the device; it remains even if you disconnect the Bluetooth device. For this headset device, you would test it simply by making a phone call.



1. Bluetooth device connected
2. Newly connected device
3. Other nearby devices

**Figure 1-19** Bluetooth Screen on an Android Smartphone Showing the LG HBS750 Headset Connected

To disconnect the device but retain the pairing, turn off the device. To unpair the device, tap the settings (gearbox) icon on the screen

and tap Unpair. To use it again, pair it again.

Android devices can also connect to other Bluetooth-enabled devices (forming a PAN) or to a computer equipped with a Bluetooth dongle. To create such connections, you must set the mobile device to discoverable (which generally lasts only 2 minutes). In the same way that the headset is discovered by the mobile device in the previous procedure, a mobile device can be discovered by a computer or other mobile device.

## Steps to Configure a Bluetooth Headset on an iOS Device

Following these steps to connect a Bluetooth headset to a typical iOS device:

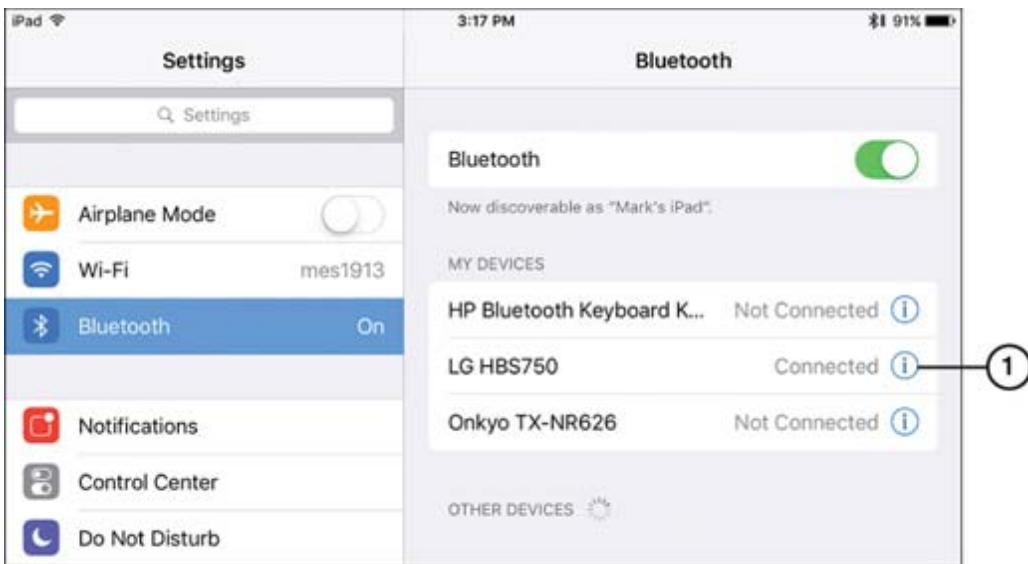


**Step 1.** Go to **Settings** and then tap **Bluetooth** to display the Bluetooth screen.

**Step 2.** Tap **Bluetooth** to enable it (if it isn't enabled already). The device then searches for other devices.

**Step 3.** Prepare the headset. (This process varies from headset to headset. For example, switching on a typical Bluetooth headset or pressing and holding the power button begins the pairing process.) The iOS device automatically recognizes the device and lists it as discoverable.

**Step 4.** Tap the device name, and it automatically connects, as shown in [Figure 1-20](#).



1. Connected device

**Figure 1-20** A Connected Bluetooth Headset on an iOS Device

**Step 5.** Enter a PIN code, if prompted to do so.

To remove the device, tap it. On the next screen, tap Forget This Device. To stop using the device but keep it paired, tap Disconnect. [Figure 1-20](#) shows an example of an iPad that previously paired with several Bluetooth devices and is currently connected to one.

**Note**

Most Bluetooth devices can be connected to only one mobile device at a time. If you need to switch a Bluetooth device from one mobile device to another, be sure to disconnect it or “forget” it from the current connection before you make a new one.

## GPS and Cellular Location Services

When people are connected to mobile devices, they manage to keep moving while staying connected to their networks and Internet. As they move their location between Wi-Fi networks and cell towers, their phones can be tracked by using the phone’s Global Positioning

System (GPS), the phone's Wi-Fi location, or the location of the cell tower providing cellular data and voice to the phone.

Apps designed for your phone can use the location data your phone provides to enhance the app experience. When you are using a map for driving directions, for example, accurate navigation instructions and updated traffic information are available. Ads for local services are also available with location information. Importantly, an emergency service call can share location information with responders to send help.

Sometimes a user does not want to share location information with the companies that have access to the phone, for privacy reasons or other concerns. In that case, the user can easily enable or disable location services and manage app requests to track a location.

On an iPhone 13, navigate to Location Services using the following steps:

**Step 1.** Go to **Settings** and then tap **Privacy** to display the Privacy screen.

**Step 2.** Tap **Location Services**. Services can be toggled on or off. When enabled, a list of installed apps that can take advantage of location services populates.

Note that a link directly below the toggle goes into a more in-depth description of how Apple addresses the use of Location Services and Privacy.

On an Android device, the steps are similar and come with added options for the location tracking method:

**Step 1.** From the Apps screen, select **Settings**.

**Step 2.** Select Connections.

**Step 3.** Select Location. Services can be toggled here.

**Step 4.** Select the location method for accuracy of location. The Apps that are using location services display.

## Mobile Device Management (MDM)

Organizations that have many mobile devices need to administer them so that all devices and users comply with the security practices in place. This is usually done with a suite of software known as **mobile device management (MDM)**. The MDM marketplace is competitive, and several solutions are available from companies such as VMware (AirWatch), Citrix (XenMobile), and SOTI MobiControl. These products push updates and enable an administrator to configure many mobile devices from a central location. Good MDM software secures, monitors, manages, and supports multiple different mobile devices across the enterprise.

## Mobile Application Management (MAM)

Just as organizations need to manage their mobile devices with MDM, it is necessary to manage the applications on those devices with **mobile application management (MAM)**. Each mobile device has software that might need license or security updates, and MAM software enables an organization to manage software across its enterprise network. The purpose of MAM is to allow companies to control the software and data used on its devices, no matter where the users are located.

Examples of secure practices that companies and organizations can enforce with MDM and MAM are as follows:

- Corporate email and communications configurations
- **Two-factor authentication** (2FA) practices and other security measures. 2FA requires the user to provide two different forms of verification. Most forms of 2FA are based on something the user knows and something the user possesses, such as a password and a biometric scan or security token. One example

of 2FA is using a debit card to pay for items. For the transaction to succeed, the user must be in possession of the debit card and provide the correct PIN code.

- Corporate applications management

## Mobile Device Synchronization

Keeping things in sync means having the same information on your different devices. We use synchronization to bring files in line with each other and to force devices to coordinate their data. For example, when a salesperson makes a change to a sales proposal document on a laptop, it is important that the other people involved in the transaction—such as sales managers, ordering specialists, and customers—have access to the updated information when they access the document on their own devices. Synchronizing data to the cloud is how the salesperson updates the other devices.

Synchronizing data from the cloud to the desktop (or another device) is how others gather the updated information.

Each cloud provider carefully designs a system for synchronizing users' data, and different kinds of data might require different levels of synchronization. Most cloud storage providers offer their customers choices in how often data is synchronized. Sometimes transfers are scheduled by time; sometimes they are triggered by events, such as a change to a document or a device coming online. Sometimes, as with Google Drive documents, several users can simultaneously access documents for group editing. It is important to be aware of data caps when considering how often data should be synchronized to and from the cloud. If data is being uploaded and downloaded constantly from the cloud, it can have a substantial impact on data usage.

A mobile device can synchronize by connecting to a PC via USB (or some other serial connection) or, commonly, using cellular data, Wi-Fi, or Bluetooth.

## Types of Data to Synchronize

*Synchronization* is the matching of files, email, and other types of data between two computers. The types of data we synchronize are too numerous to list in one chapter. This section lists data types that commonly need to be synchronized. Brief examples of use are provided, although more are possible.

The types of files that can be synchronized include the following:



- **Contacts:** These come from phones or email applications.
- **Email:** The same messages then appear on all of a user's devices.
- **Calendar:** All attendees then know the right time and place for meetings.

## Synchronization Methods

The main methods are used for synchronization, as briefly discussed in the preceding sections:



- Synchronization to the cloud
- Microsoft 365
- ActiveSync
- Calendar
- Contacts
- Commercial Mail application

With cloud-based synchronization, apps on a mobile device send data to the cloud, where it is downloaded by other mobile apps, web browsers, or programs running on Windows or macOS computers. For example, Microsoft 365 allows synchronization of applications on up to five devices.

Providers that enable cloud-based synchronization include the following:

- Dropbox
- Microsoft 365
- Apple iCloud
- Microsoft OneDrive
- Google Drive ([www.google.com](http://www.google.com))

Data that is synched via cloud-based synchronization is encrypted and secured by passwords and usernames. Mutual authentication is used by each side of the connection to verify its identity to the other side.

If synchronization to a cloud application is interrupted, the problem can usually be resolved by closing and relaunching the application.

## **Commercial Mail Synchronization**

Email synchronization options depend on the commercial email service in use. For example, Microsoft Exchange email uses Exchange ActiveSync. When an email account is configured on a mobile device, synchronization settings are configured as part of the process and can be adjusted, disabled, or reenabled as needed.

Many companies and institutions have enlisted Google to manage their mail services. The employees establish a profile within the Gmail environment, and it is synched among devices but not with other profiles, such as a personal account.

## Exam Preparation Tasks

As mentioned in the Introduction, you have several choices for exam preparation: the exercises here; [Chapter 10, “Final Preparation”](#); and the exam simulation questions in the Pearson Test Prep practice test software.

### Review All the Key Topics

Review the most important topics in the chapter, noted with the Key Topic icon in the outer margin of the page. [Table 1-5](#) lists these key topics and the page number on which each is found.



**Table 1-5** Key Topics for [Chapter 1](#)

Key Topic Element	Description	Page Number
Steps	Replacing a laptop keyboard	10
<a href="#">Table 1-2</a>	Comparison of HDD, SSD, and SSHD	11
Steps	Replacing a laptop storage device (HDD, SDD, and SSHD)	12
List	Laptop memory upgrade considerations	14
<a href="#">Table 1-4</a>	SODIMM Features	15
Steps	Performing a memory upgrade	16
Steps	Removing or replacing a wireless card	18
Steps	Removing a system from all power sources before replacing internal components	20

<b>Key Topic Element</b>	<b>Description</b>	<b>Page Number</b>
Figure 1-12	Wi-Fi Antennas, Wires, Inverter, Webcam, and Microphone in a Typical LCD Display	25
Section	Connection Methods: Wired	27
Section	Connection Types: Wireless	29
Section	Enabling/Disabling Hotspots	34
Section	Enabling/Disabling Tethering	39
Steps	Configuring Bluetooth on Android devices	41
Steps	Configuring Bluetooth on iOS devices	43
List	Files that can be synchronized	46
List	Synchronization methods	46

## Complete the Tables and Lists from Memory

Print a copy of [Appendix C, “Memory Tables”](#) (found online), or at least the section for this chapter, and complete the tables and lists from memory. [Appendix D, “Memory Tables Answer Key,”](#) also online, includes completed tables and lists to check your work.

## Define Key Terms

Define the following key terms from this chapter, and check your answers in the glossary:

[keyboard](#)

[pointing device](#)

[hard disk drive \(HDD\)](#)

[solid-state drive \(SSD\)](#)

wireless card  
biometrics  
near-field communication (NFC)  
liquid crystal display (LCD)  
in-plane switching (IPS)  
twisted nematic (TN)  
vertical alignment (VA)  
organic LED (OLED)  
mini-USB  
Lightning  
hotspot  
Bluetooth  
docking station  
port replicator  
tethering  
Preferred Roaming List (PRL)  
mobile device management (MDM)  
mobile application management (MAM)  
two-factor authentication

## Answer Review Questions

- 1.** Which of the following is best for updating RAM in most laptops?
  - a.** DDRSD4
  - b.** DIMM
  - c.** SODIMM
  - d.** SDR SDRAM
  
- 2.** Which of the following is the term for a smartphone that shares its cellular data connection with a laptop via a USB cable?
  - a.** Pairing

- b.** Tethering
  - c.** NFC
  - d.** Hotspot
- 3.** You have been asked to upgrade an aging laptop without replacing it. Which option can you add to provide the fastest possible update?
  - a.** DIMM
  - b.** HDD
  - c.** SSD
  - d.** SSHD
- 4.** You have been called to check on a laptop that belongs to a user who just returned from vacation. The laptop keeps crashing after a few minutes of use. The documentation for the laptop indicates that additional RAM was added during a system tune-up earlier in the week. What are the considerations worth revisiting when troubleshooting? (Choose two.)
  - a.** Memory speed
  - b.** iOS update history
  - c.** Voltage rating of the power cable
  - d.** Memory timing
- 5.** Which of these converts power from DC to AC for screens?
  - a.** Transformer
  - b.** Inverter
  - c.** Wireless card
  - d.** PCIe card
- 6.** When experiencing issues connecting a phone to cell towers, which can be reset to possibly solve the problem?
  - a.** MAM
  - b.** PRL

- c. OLED
  - d. NFC
- 7. Which of the following are methods of sharing a wireless connection? (Choose all that apply.)
  - a. Twisted nematic
  - b. Hotspot
  - c. Tethering
  - d. Port replicator
- 8. Which statement best describes airplane mode?
  - a. Airplane mode allows mobile devices to communicate safely via Bluetooth and Wi-Fi while in flight but turns off cellular transmission.
  - b. Airplane mode is an FCC regulation that controls the use of mobile devices in airports.
  - c. Airplane mode allows mobile devices to communicate only when they are attached to each other by cable.
  - d. Airplane mode turns off all wireless antennas so that mobile devices cannot transmit or receive data while in flight.
- 9. A user provides both a password and a fingerprint to access a device. What is this called?
  - a. MDM
  - b. MAM
  - c. Pairing
  - d. Two-factor authentication
- 10. Which of the following statements describe Bluetooth? (Choose all that apply.)
  - a. Bluetooth devices form short-range, low-speed wireless networks.

- b.** Bluetooth devices connect to form a PAN.
  - c.** Bluetooth devices create peer-to-peer networks.
  - d.** Bluetooth devices allow dissimilar devices to communicate on the same network.
- 11.** Which of the following most likely needs to be replaced when a touchscreen is unresponsive and no longer detects touch?
  - a.** Inverter
  - b.** Touch pen
  - c.** Battery
  - d.** Digitizer
- 12.** Which of these can a company use to push security updates out to all devices that employees use?
  - a.** MAM
  - b.** MDM
  - c.** PRL
  - d.** NFC
- 13.** Which of these technologies usually has about a 10cm range and can be used to pair a device with speakers?
  - a.** Wi-Fi
  - b.** Cellular
  - c.** Bluetooth
  - d.** NFC
- 14.** When paying with your phone at the store, which of the following communicates with the payment system for the transaction?
  - a.** NFC
  - b.** Wi-Fi
  - c.** Biometrics
  - d.** Bluetooth

**15.** Which of these is *not* a file type to be synchronized?

- a.** Email
- b.** Calendars
- c.** Biometrics
- d.** Contacts

# Chapter 2

## Networking

This chapter covers the eight A+ 220-1101 exam objectives related to knowledge of computer networks. These objectives may comprise 20 percent of the exam questions:

- **Core 1 (220-1101): Objective 2.1:** Compare and contrast Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports, protocols, and their purposes.
- **Core 1 (220-1101): Objective 2.2:** Compare and contrast common networking hardware.
- **Core 1 (220-1101): Objective 2.3:** Compare and contrast protocols for wireless networking.
- **Core 1 (220-1101): Objective 2.4:** Summarize services provided by networked hosts.
- **Core 1 (220-1101): Objective 2.5:** Given a scenario, install and configure basic wired/wireless small office/home office (SOHO) networks.
- **Core 1 (220-1101): Objective 2.6:** Compare and contrast common network configuration concepts.
- **Core 1 (220-1101): Objective 2.7:** Compare and contrast Internet connection types, network types, and their features.
- **Core 1 (220-1101): Objective 2.8:** Given a scenario, use networking tools.

Networking support requires a sound understanding of how different types of computer networking hardware and software work together to enable communication between computing devices. This chapter covers several networking devices and protocols, both wired and wireless, that you will need to master to be a successful network technician.

### “Do I Know This Already?” Quiz

The “Do I Know This Already?” quiz allows you to assess whether you need to read the entire chapter. Table 2-1 lists both the major headings in this chapter and the “Do I Know This Already?” quiz questions covering the material in those headings so that you can assess your knowledge of these specific areas. The answers to the “Do I Know This Already?” quiz appear in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes and Review Questions.”

**Table 2-1** “Do I Know This Already?” Foundation Topics Section-to-Question Mapping

Foundation Topics Section	Questions
TCP and UDP Ports, Protocols, and Their Purposes	1–6
Networking Hardware Devices	7–9
Compare and Contrast Wireless Networking Protocols	10–11
Summarize the Services Provided by Networked Hosts	12–13
Install and Configure a Basic Wired/Wireless SOHO Network	14
Network Configuration Concepts	15–16
Internet Connection Types, Network Types, and Their Features	17

Foundation Topics Section	Questions
Using Networking Tools	18

## CAUTION

The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for the purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Which of the following application tasks would likely require TCP?
  - a. A DHCP request on a network
  - b. Sending an Excel spreadsheet to a coworker**
  - c. A web-based phone conversation
  - d. Streaming a sports event on the Web
  
2. Which statements about UDP are true? (Choose two.)
  - a. UDP is User Data Profile, which is sent in a packet.
  - b. UDP is connection oriented.
  - c. UDP is connectionless.**
  - d. UDP is User Datagram Protocol.**
  
3. Which protocol uses TCP but not UDP?
  - a. IMAP**
  - b. HTTPS**
  - c. FTP
  - d. DNS
  
4. Which protocol requires less processing by networking equipment, TCP or UDP?
  - a. TCP because it is connectionless
  - b. UDP because it is connectionless**
  - c. UDP because it requires reliability
  - d. TCP because it is unreliable
  
5. Which port is used for FTP?
  - a. 35
  - b. 27
  - c. 23
  - d. 21**
  
6. When a file is sent and part of the file is missing, which protocol is used to request that the sender resend the missing parts?
  - a. File Transfer Protocol**
  - b. Simple Network Transfer Protocol
  - c. Transmission Control Protocol

- d. Server Message Block
- 7. Which network devices connect users within a LAN? (Choose three.)
  - a. Router
  - b. Hub
  - c. Switch
  - d. DNS server
  - e. Access point
- 8. Which two devices have functions combined into a standard SOHO router?
  - a. Hub and switch
  - b. Switch and router
  - c. Router and hub
  - d. Wireless bridge and hub
- 9. What is the chief difference between a wireless bridge and a WAP?
  - a. A WAP connects wired devices; a wireless bridge connects wireless devices.
  - b. A WAP is for connecting wireless devices; a bridge is for connecting LANs.
  - c. A WAP uses Ethernet; a bridge uses OSPF.
  - d. There is no difference; these are two names for the same device.
- 10. Imagine that you have been asked to place a switch in a ceiling area where there is no AC outlet. Which technology would be part of a possible solution?
  - a. STP
  - b. TCP
  - c. DNS
  - d. PoE
- 11. On a 2.4GHz network, which channel is the best choice for avoiding interference from other channels?
  - a. 6
  - b. 10
  - c. 5
  - d. 2
- 12. Which technology can assign an IP address to wireless devices in a local coffee shop?
  - a. TCP
  - b. Static IP
  - c. DNS
  - d. DHCP
- 13. Which acronym refers to a feature that makes streaming media and voice services a better experience?
  - a. TCP
  - b. QoS
  - c. PnP
  - d. DNS

- 14.** Which one of the following is a device that enables management of wireless LANs?
- a. Web hub
  - b. SOHO switch
  - c. WLAN controller
  - d. WEB LAN manager
- 15.** Which is an example of a subnet mask?
- a. fe80::
  - b. 10.20.10.1
  - c. 255.255.0.0
  - d. 192.168.1.0
- 16.** Which is an example of a valid IPv6 address?
- a. FF02::2
  - b. 2001:db8:aaaa:1::200
  - c. fe80::c1c6:bd64:f9c7:2c9d
  - d. All of these answers are correct.
- 17.** Which is a secure network connection that is carried on the Internet?
- a. NAT
  - b. VLAN
  - c. PNS
  - d. VPN
- 18.** You have just installed an Ethernet jack in an office and need to connect it to the patch panel in the wiring closet. When you get to the wiring closet, you see that several unused cables are not identified by room number, so you can't tell which one to connect. Which tool in your networking toolkit will best help you solve this problem?
- a. Wi-Fi analyzer
  - b. Toner probe
  - c. Cable tester
  - d. Punchdown tool

## Foundation Topics

### TCP and UDP Ports, Protocols, and Their Purposes



**220-1101: Objective 2.1:** Compare and contrast TCP and UDP ports, protocols, and their purposes.

When humans want to share ideas with each other, they agree to use common communication protocols, or rules, to make sure they are understood. **Protocols** help us know when to speak, when to listen, and how to start and finish conversations. We constantly use protocols but rarely think about them. When people have a communication failure, a protocol failure is likely involved.

Protocols serve the same purpose in computer network communication. Because the processes involved in computer communication can be complex, ways of using protocols and ports have been developed to keep the processes of communication sorted out and flowing smoothly. This section describes some of the protocols and ports that are typically used in networks.

When an application needs to send or receive data, it must use a particular protocol designed for that application and open a **port** on the network adapter to make a connection to another computer. Computers use port numbers to identify protocols and keep the different processes sorted out. For example, if you want to visit [www.google.com](https://www.google.com), you open a browser and type <https://www.google.com>. The protocol being used is HTTPS (short for Hypertext Transfer Protocol Secure), and it makes the connection to the web server: google.com. HTTPS selects an unused port on your computer (known as an *outbound port*) to send and receive data to and from google.com. On the other end, Google's web server has a specific port open at all times, ready to accept sessions. In most cases, the web server's port is 443, which corresponds to HTTPS. This is known as an *inbound port*.

Both TCP and UDP utilize ports to make connections. Remember that the inbound ports are of concern on a server. For example, an FTP server that stores files for customers must have inbound port 21 open by default because that is the common port for FTP. **Table 2-2** displays some common protocols and their default corresponding inbound ports. Most common protocols use the same TCP and UDP port numbers.



**Table 2-2** Common Protocols and Their Ports

Port Number(s)	Protocol	Port Type
20/21	File Transfer Protocol (FTP)	TCP, UDP
22	Secure Shell (SSH)	TCP, UDP
23	Telnet	TCP, UDP
25	Simple Mail Transfer Protocol (SMTP)	TCP, UDP
53	Domain Name System (DNS)	TCP, UDP
67/68	Dynamic Host Configuration Protocol (DHCP)	UDP
80	Hypertext Transfer Protocol (HTTP)	TCP, UDP
110	Post Office Protocol 3 (POP3)	TCP, UDP
137/139	Network Basic Input/Output System (NetBIOS)/NetBIOS over TCP/IP (NetBT)	TCP, UDP
143	Internet Message Access Protocol (IMAP)	TCP
161/162	Simple Network Management Protocol (SNMP)	TCP, UDP
389	Lightweight Directory Access Protocol (LDAP)	TCP, UDP
443	Hypertext Transfer Protocol Secure (HTTPS)	TCP, UDP
445	Server Message Block (SMB)/Common Internet File System (CIFS)	TCP
3389	Remote Desktop Protocol (RDP)	TCP, UDP

**TIP**

Know these protocols and their corresponding port numbers for the 220-1101 exam.

The sections that follow provide more details about these protocols.

## 1. FTP (20 - Data transfer and 21 - Establish connection)

File Transfer Protocol ([FTP](#)) is a protocol that both web browsers and specialized FTP programs use to access dedicated file transfer servers for file downloads and uploads. When accessing an FTP site, the site uses the prefix `ftp://`.

Windows and Linux contain a command-line FTP program; type `ftp`, press Enter, and then type `help` at the FTP prompt to see the available commands. See [https://linux.about.com/od/commands/l/blcmdl1\\_ftp.htm](https://linux.about.com/od/commands/l/blcmdl1_ftp.htm).

For macOS, see <https://osxdaily.com/2011/02/07/ftp-from-mac/> or type `ftp` from the command line.

FTP sites with downloads available to any user support anonymous FTP. If any credentials are required for FTP, they are typically the username anonymous and the user's email address as a password. Some FTP sites require the user to log in with a specified username and password. FTP is not considered secure because FTP users can authenticate in clear-text sign-ins. For greater security, use FTP secured with SSL/TLS (FTPS) or Secure File Transfer Protocol (SFTP). FTP uses ports 20 and 21. Port 21 is used to establish a connection and port 20 is used for data transfer.

**TIP**

It is possible to use an operating system's built-in FTP client for file uploads and downloads with both secured and unsecured FTP sites, but consider using third-party FTP products such as FileZilla (<https://filezilla-project.org>). Such programs enable the creation of a customized setup for each FTP site you visit and store passwords, server types, and other necessary information. They also enable faster downloads than typical web browsers running in `ftp://` mode.

## 2. SSH (22)

Secure Shell ([SSH](#)) enables computers to exchange data on a secured channel. This protocol is more secure than FTP and Telnet. The Secure Shell server housing the data you want to access will have port 22 open. (SSH uses port 22.) Several other protocols use SSH to make secure connections. One of these is Secure FTP (SFTP), as previously mentioned. Regular FTP can be nonsecure. SFTP combats this by providing file access over a reliable data stream, generated and protected by SSH.

## 3. Telnet (TCP 23) - Unsecure ==> Obsolete!!!

[Telnet](#) enables users to make a [text-based connection to a remote computer or networking device](#) and then use that device as if they were sitting in front of it instead of merely downloading pages and files as with an `http://` or `ftp://` connection.

Windows and Linux contain a command-line Telnet program. To open a connection to a remote computer, open a command prompt (Windows) or Terminal session (Linux), type `telnet`, and press

the Enter key. This command opens the Telnet command prompt. For help with commands, type **help** and press the Enter key.

macOS includes a menu-driven Telnet program available from Terminal. Because of the standard practice of using SSH, Telnet has been removed from later versions of macOS. However, if Telnet is still needed, it can be installed. See <https://osxdaily.com/2018/07/18/get-telnet-macos/>.

### Note

A remote computer must be configured to accept a Telnet login. Typically, TCP port 23 on the remote computer must be open before a login can take place.

## 4. SMTP (25)

Simple Mail Transfer Protocol (**SMTP**) is used to send email from a client system to an email server, which also uses SMTP to relay the message to the receiving email server. SMTP uses port 25.

### Note

When configuring email settings on a client, check with the ISP or organization that provides Internet access for the correct settings. You need to know the server type(s) used (SMTP, POP3, or IMAP), the ports used (some ISPs change the default values), the username and password for the email service, and the security settings (for example, whether SSH is used).

## 5. DNS (53)

Domain Name System (**DNS**) is the name for the network of servers on the Internet that translate **domain names**, such as [www.informit.com](http://www.informit.com) or [www.comptia.org](http://www.comptia.org), and individual host names into their corresponding IP addresses. When manually configuring an IP address, you typically provide the IP address of a DNS server (or the IP addresses of multiple DNS servers) as part of the configuration process. DNS uses port 53. Some technicians refer to DNS as the Domain Name Service; this might not be technically correct, but it is understandably a common translation of DNS.

## 6. DHCP (UDP 67 - Inbound on Server and UDP 68 on Client)

Dynamic Host Configuration Protocol (**DHCP**) is used to automatically assign IP addresses to hosts. These hosts can be computers, printers, servers, routers, and so on. In most SOHO networks, a router uses DHCP to assign IP addresses to the client computers. In addition, your ISP uses DHCP to assign an IP address to you, and usually your router gets this address. The DHCP service makes life easier for a network administrator by automatically assigning IP addresses, subnet masks, gateway addresses, DNS servers, and so on. If you get your address from a DHCP server, you are getting your address assigned dynamically, so it might change periodically. However, some computers and printers require a static address—that is, an address that the network administrator assigns manually. In many situations, servers and printers are better served using static addresses that DHCP doesn't change. This way, access to printers and servers is more reliable over time. DHCP uses ports 67 and 68, where UDP port number 67 is the destination port of a server and UDP port number 68 is used by the client.

## **7. HTTP (80) ==> HTTPS (443) 1. HTTP Secure or 2. HTTP over TLS**

Hypertext Transfer Protocol (**HTTP**) is the protocol that web browsers, such as Internet Explorer, Microsoft Edge, Firefox, and Chrome, use to access websites and content. Normal (unsecured) sites use the prefix http:// when accessed in a web browser. Sites that are secured with various encryption schemes such as HTTP Secure or HTTP over TLS (**HTTPS**) are identified with the prefix https://. HTTP uses port 80 and HTTPS uses port 443.

### **Note**

Most browsers connecting with a **secured site** also **display a closed padlock symbol onscreen**.

## **8. POP3 (110) ==> IMAP (See 10.)**

Post Office Protocol version 3 (**POP3**) is one of two leading protocols used for receiving email; IMAP is the other one. In an email system based on POP3, email is downloaded from the mail server to folders on a local system. POP3 is not a suitable email protocol for users who frequently switch between computers and mobile devices because email might be spread over multiple computers. POP3 is the current standard. Users who utilize POP3 servers to retrieve email typically use SMTP to send messages. POP3 uses port 110.

### **TIP**

For users who must use POP3-based email and who use multiple computers, a remote access solution—for example, Windows Remote Desktop Connection or a service such as GoToMyPC—is recommended. A remote access solution enables users to remotely access the system that connects to the POP3 mail server so that they can download and read email messages no matter where they are working.

## **9. NetBIOS/NetBT (137, 138 & 139)**

**NetBIOS**, also known as NetBT (RFC 1001), is a protocol that allows some legacy applications that were developed in the 1980s (before the TCP/IP environment became the standard) to work on larger networks and the Internet. Many of those early applications could not scale to the TCP environment, so the NetBIOS/NetBT protocol was designed in 1987 to provide the needed compatibility. NetBIOS/NetBT uses ports 137–139.

## **10. IMAP (143) and IMAP over SSL/TLS (993)**

Internet Message Access Protocol (**IMAP**) is an email protocol that enables messages to remain on the email server so they can be retrieved from any location. (Recall that POP3, the other leading protocol for receiving email, downloads messages to the mail client.) IMAP also supports folders so that users can organize their messages as desired. IMAP4 is the current version of IMAP.

To configure an IMAP-based email account, you must select IMAP as the email server type and specify the name of the server, your username and password, and whether the server uses SSL/TLS. IMAP uses port 143. IMAP over SSL/TLS uses port 993.

## 11. SNMP (161 / 162)

Simple Network Management Protocol (**SNMP**) is the standard for managing and monitoring devices on a network. SNMP manages routers, switches, and computers and is often incorporated into software known as a *network management system (NMS)*. The NMS is the main software that controls everything SNMP based; it is installed on a computer known as a *manager*. The devices to be monitored are known as *managed devices*. The NMS installs a small piece of software known as an *agent* that allows it to monitor those managed devices. SNMP uses ports 161 and 162.

## 12. LDAP (389) and LDAPS - LDAP over SSL (636)

Lightweight Directory Access Protocol (**LDAP**) is used to access and maintain distributed directories of information such as the kind involved with Microsoft domains. Microsoft refers to this as *directory services*. By default, LDAP traffic is unsecured. LDAP over SSL (LDAPS) secures LDAP by enabling communications over SSL/TLS. LDAP uses port 389 and LDAPS uses port 636.

## 13. SMB/CIFS

Server Message Block (**SMB**) provides access to shared items such as files and printers. SMB uses packets that **authenticate** remote computers through **interprocess communication mechanisms**. SMB uses ports 137–139 for SMB traffic using NetBIOS over TCP (NetBT) and 445 for SMB hosted on TCP.

Port 445 is also used by the Common Internet File System (**CIFS**). CIFS was widely used after its introduction as a standard method for sharing files across corporate intranets and the Internet. CIFS is an enhanced version of Microsoft SMB, which is an open, cross-platform protocol. CIFS has now largely been replaced by updated versions of SMB. The current version is SMB 3.1.1.

### Note

If traffic on ports 137–139 is blocked, you must use the device's IP address to access shared files or printers. When these ports are open, you can use the name of the device to access its shared files or printers.

## 14. RDP (3389)

The Remote Desktop Protocol (**RDP**) port 3389 is used by Remote Desktop Services (RDS), which is the Windows Server-based companion of Remote Desktop Connection. [Chapter 6, "Operating Systems,"](#) discusses RDP in detail.

## TCP vs. UDP

User Datagram Protocol (**UDP**) sessions are known as *connectionless sessions*. This means that the messages are sent without an expectation of communication from the receiver. UDP does its best to send a message, but it does not account for errors. For example, a new device that is looking for an IP address generates DHCP messages as advertisements to all devices on the network. If all the devices that heard the message responded, network traffic would be unnecessarily busy and the network would be less efficient. Similarly, Trivial File Transfer Protocol (**TFTP**) is a protocol that is used to transport file packets that do not need a response.

UDP is used in streaming media sessions, such as Voice over IP (VoIP) and gaming, and for protocols that use a simple query and response, such as DNS. If you have ever been streaming some music and heard a break in the song or a blip of some kind, that likely indicated some missing

packets. TCP tries to replace the missing packets, but you do not really want them back: By the time they might arrive, you would be listening to a totally different part of the music stream and the updated information would be out of place.

**Transmission Control Protocol (TCP)** sessions are known as *connection-oriented sessions*. This means that every packet that is sent is checked for delivery. If the receiving computer doesn't receive a packet, it cannot assemble the message and must ask the sending computer to transmit the missing packet again. No packet is left behind. For example, if a computer sends a picture of a cat but the packets containing part of the picture (say, the nose) don't arrive, TCP allows the receiving computer to tell the sending computer that some expected packets went missing and to send them again. This way, the user application at the receiving end gets the entire picture, not some strange picture of a cat without a nose.

Other examples of protocols that use TCP are HTTPS and SSH. Because they are secure protocols, it is important to verify that the communication has been completed successfully and that any missing packets are re-sent.

The two examples above of the cat picture and the music stream demonstrate that different situations call for different protocols. UDP is the better choice for time-sensitive information, even though it is less reliable than TCP. In other situations, where reliability is important, TCP is beneficial.

## Networking Hardware

220-1101  
Exam

**220-1101: Objective 2.2:** Compare and contrast common networking hardware.

Understanding how computers communicate on a network is essential for any IT professional. Network environments can range from simple home networks to complex corporate designs, but certain essential elements and functions apply to all networks. The following sections cover basic networking hardware devices used to build small networks and describe how they contribute to the communication process.

### Router

A **router** connects one network to another. For example, a router connected to a cable modem or DSL modem enables multiple devices on a LAN to share a single broadband connection to the Web.

Most routers sold for SOHO configurations are Wi-Fi (802.11 family) wireless routers with integrated Fast Ethernet or Gigabit Ethernet switches. Both wired and wireless devices can be on the same network and can share folders and printers, as well as Internet access.

Figure 2-1 shows the rear of a typical 802.11ac router for cable Internet from ASUS.



1. USB 2.0 port for external storage
2. USB 3.0 port for external storage
3. WAN (Internet) port to cable modem
4. Gigabit Ethernet switch for LAN

**Figure 2-1** Many Wireless Routers Can Now Be Used as Hosts for USB Drives for Shared Network Storage

A router used for DSL is similar in appearance to a router used for cable Internet, but it features a DSL port. The switches built into routers are also stackable. If a router needs more ports, you can add a switch.

Routers are specialized computing devices that are controlled by **firmware**. When you log into a router to view or change its configuration, the router's firmware limits the options available. Buggy firmware can cause network problems and make a network more vulnerable to attack.

Use a router's configuration program to determine the firmware date and version it uses. If the router is using an older version of firmware, check the vendor's website for an update. Before downloading the update, read the technical notes to see what issues the firmware affects and whether the update might cause any other problems. Download the update and follow the vendor's instructions for installing the firmware.

If you want more features than the vendor-provided firmware includes, check for third-party firmware. DD-WRT is Linux-based, alternative open source firmware that is suitable for a great variety of WLAN routers and embedded systems. DD-WRT is the most popular replacement firmware for routers, and some vendors now use it in their high-end routers.

## Switch

A **switch** provides connectivity to devices in a local network. Each port on a switch works independently, allowing more than one concurrent session. A switch makes a direct connection between the sending and receiving devices by identifying the Media Access Control (MAC) address of each device. In today's networks, switches are common in 100Mbps, 1000Mbps, 10Gbps, and even 40Gbps networks. Switches can be stacked to increase the number of connection ports in a network. Stacked switches are daisy-chained together and, in theory, no limit governs the number of switches possible in a network.

A switch resembles a hub but creates a dedicated full-speed connection between the two computers that are communicating with each other. A five-port 10/100/1000 switch, for example, provides the full 100Mbps bandwidth to each port connected to a Fast Ethernet or 10/100 card. If the network adapters are configured to run in full-duplex mode (that is, to send and receive data simultaneously) and the switch supports full-duplex mode (as most modern switches do), the bandwidth is doubled; for example, Fast Ethernet bandwidth (100Mbps) on the network would be doubled to 200Mbps, and Gigabit Ethernet (1000Mbps) bandwidth would be doubled to 2Gbps. Low-cost switches used in

small office/home office (**SOHO**) networks (see Figure 2-2) cannot be configured to perform complex switching functions and are considered *unmanaged*. **Managed switches**, which are common in corporate and enterprise networks, also support SNMP for diagnostics and performance measurement, virtual LANs (VLANs) to enable multiple workgroups to use the same physical switch but keep their traffic separate, and redundancy.



1. 100Mbps connection
2. Unused RJ-45 port
3. Ethernet cable

**Figure 2-2 An Unmanaged Fast Ethernet (10/100) Five-Port Switch**

## Wireless Access Point

Whereas hubs and switches deal with wired networks, a **wireless access point (WAP)** extends a wired network to wireless connections. It is also based on Ethernet, but it involves the **IEEE 802.11** group of standards, which define **wireless LANs (WLANS)**. A WAP acts as a central connecting point for computers equipped with **wireless network adapters**; similar to a switch, a WAP identifies each computer by its MAC address.

To turn a wireless router into a WAP (which then needs to connect to a separate router), check the configuration options available for the router.

## Patch Panel

A **patch panel** is a **box** designed as a junction point for **twisted pair (TP) cable** and fiber cable used in networks. Patch panels are typically built into **wiring closets** or added to equipment racks in a 1U or taller form factor.

After any connector on the cable is removed, each wire in the TP cable must be untwisted before it is punched into the appropriate connection on the back of the panel. The twisted cables are color coded so that they can be properly terminated at the other end. The most common standards for **color coding** are known as **T568A** and **T568B**. Be sure to use the color coding that matches the rest of your network. **Chapter 3, “Hardware,”** covers T568A and T568B.

The front of the patch panel uses RJ-45 connectors for short standard network cables.

## Firewall

A **firewall** is a hardware appliance or software application that protects a computer from unwanted intrusion. The networking world is especially concerned with hardware-based devices that protect an entire group of computers, such as a LAN. With small offices and home offices, firewall functionality is usually built into the router. In larger organizations, the firewall is a separate device. A firewall stops unwanted connections from the outside and can block basic network attacks.

## Power over Ethernet (Cat 5+ Twisted Pair cable supports PoE)

A Power over Ethernet (**PoE**) switch has added capability (a built-in *endspan*) to send power out a port using Cat 5 or better grades of twisted pair cable. The switch can send up to 25.5 watts of power on the unused twisted pairs (pins 4–5 and 7–8) in 10Base-T or 100Base-T Ethernet (PoE Mode B) or by using all four wire pairs (PoE Mode A), enabling it to be used with Gigabit Ethernet. PoE enables wireless access points, IP security cameras, VoIP phones, routers, and other Ethernet devices to be installed in areas away from traditional power sources.

A PoE switch *endspan* is built into a switch. Another type of PoE device, known as a *power over Ethernet injector*, is installed between a standard Ethernet switch and a PoE device to provide power only.

The original PoE standard, IEEE 802.3af, was introduced in 2003. It provides up to 15.4 Watts (W) of power to a PoE device; however, only 12.95W is guaranteed because of power dissipation in the cable. In 2009, IEEE 802.3at Type 2 was introduced and improved upon the previous standard. This update provides up to 30W of power, but only 25.5W is guaranteed. Up to this point, the power provided was sufficient enough to power devices such as VoIP phones, security cameras, alarm systems, and wireless access points. In 2018, IEEE 802.3bt was created to help meet the demand for more power capacity. It introduced two new types: Type 3 and Type 4. Type 3 provides up to 60W of power, for devices such as videoconferencing equipment and multi-radio wireless access points. Type 4 provides up to 100W and can support devices such as flatscreen displays or laptops. Table 2-3 compares the four different PoE standards.



**Table 2-3** PoE Standards

Name	IEEE Standard	Power Available to Powered Device (PD)	Maximum Power
PoE	IEEE 802.3af	12.95W	15.4W
PoE+	IEEE 802.3at Type 2	25.5W	30W
2018	PoE++ IEEE 802.3bt Type 3	51W	60W
	PoE++ IEEE 802.3bt Type 4	71W	100W

## Hub

A **hub** is the simplest device used on an Ethernet network for connecting devices to each other. As networks have become more complex, simple hubs have become rare. A hub features multiple RJ-45

ports, a power supply, and signal lights to indicate network activity. Hubs have been used to connect computers and to boost the communication signal between computers.

**Switches** have almost completely replaced hubs because a hub splits the bandwidth of a connection among all the computers connected to it. For example, a five-port 10/100/1000 Ethernet hub divides the 1000Mbps speed of Fast Ethernet among the five ports, providing only 200Mbps of bandwidth to each port for Fast Ethernet and 10/100/1000 adapters. A hub also broadcasts data to all computers connected to it.

## Modems: Cable and DSL

A modem connects a LAN to an Internet service provider (ISP). The term **modem** (short for *modulator/demodulator*) was originally used only for analog (dial-up) modems when most computer networks were connected by phone systems.

Today the term *modem* is typically applied to any device that connects to the Internet. **Cable modems** and **DSL modems**, the devices most commonly used to connect small networks to the Internet, are referred to as modems even though they work quite differently than dial-up modems. These modems are discussed later in the chapter, in the section "Internet Connection Types, Network Types, and Their Features."

## Optical Network Terminal (ONT)

As fiber becomes more affordable as a connection option, its use among end users is growing. An **optical network terminal (ONT)** is similar to a modem, in that it connects the end user to the ISP, but because the communication is light pulses instead of electrical signals, no modulating/demodulating takes place. Thus, an ONT is technically different than a modem.

## Network Interface Card

A **network interface card (NIC)** is the interface on a computer (or other device) that connects to the LAN. A NIC was traditionally a circuit board (card) that mounted to the motherboard, but now NICs are built-in interfaces. A NIC connects to a cable with an RJ-45 connector. The NIC is designed to take communication off the physical cable (or wireless signal from the air) and present it to the computer for processing. A NIC has a unique physical address, known as a MAC address, that identifies the device to other hosts on the network. NICs have evolved to also provide wireless and virtual access to networks.

## Software-Defined Networking

As you have learned so far, computer networks are made up of devices that are connected together and configured by people to enable communication. Over time, the technical capabilities of networking devices have grown in scope, so it is no longer practical to have human interaction to manage every device and configuration on large enterprise networks. A **software-defined network (SDN)** is a network in which a virtual layer created in software controls the data flow over the physical network devices. SDN uses traditional networking devices, such as a router and switches, and breaks down the process of how these devices operate into two planes, called the data plane and the control plane. The **data plane** is in charge of sending, receiving, processing, and forwarding data. The **control plane** controls how the data plane operates. It tells the data plane how networking packets are to be sent and received. In addition, an **SDN controller** allows administrators to make changes to the control plane and manage how data is processed and forwarded. **SDN takes the control plane function out of networking devices**; instead, an SDN controller manages that plane

- a. Data plane
- SDNs
- b. Control plane

for the devices. SDN is changing the world of networking and how administrators manage devices and data flow on the network.

## Compare and Contrast Wireless Networking Protocols

220-1101  
Exam

### 220-1101: Objective 2.3: Compare and contrast protocols for wireless networking.

Computer networking protocols are generally accepted procedures and rules for communication between devices. Different protocols are used for communication, security, data, and so on. When computers communicate on any network, they must follow these strict rules and conventions, to minimize errors. Wireless network protocols are developed by the Institute of Electrical and Electronics Engineers (IEEE), and understanding them and how they have evolved will help you service wireless networks.

### Frequencies

Wireless routers use either the 2.4GHz band or the 5GHz band. Each band offers advantages and disadvantages. The 2.4GHz band has a longer range but can perform at slower speeds. The 5GHz band can provide faster rates but has a shorter range. A couple reasons account for the differences. First, lower frequencies travel better through obstacles such as floors and walls. Second, the 5GHz band is less used and has more channels than the 2.4GHz band, and its channels do not overlap. This means that 5GHz devices do not contend with other devices for bandwidth, as do devices in the more popular 2.4GHz range.

Many wireless routers offer both the 2.4GHz and 5GHz bands, and each can be configured separately; some routers are capable of switching between the two frequencies if a signal becomes weak. [Table 2-4](#) summarizes the two wireless bands.

Key Topic

**Table 2-4** 2.4GHz vs. 5GHz Wireless Bands

Frequency Estimated Range	Channels	Advantages	Disadvantages
2.4GHz	50m (160 feet) indoors	11	Longer range Slower performance, channels easily overlap
5GHz	15m (50 feet) indoors	23	Faster performance, channels do not overlap Shorter range

### Note

The latest Wi-Fi generation, Wi-Fi 6E, supports not only the 2.4GHz and 5GHz bands, but also a new 6GHz frequency. The 6GHz band allows for higher throughputs and lower latency.

### MIMO

The number of antennas supported by the router and the adapters (either built-in or add-on devices) is one reason for different performance levels in a given 802.11n, 802.11ac, or 802.11ax

device. **Multiple input multiple output (MIMO)** devices are available in the following configurations:

- **1x1:** One transmit, one receive antenna
- **2x2:** Two transmit, two receive antennas
- **2x3:** Two transmit, three receive antennas
- **3x2:** Three transmit, two receive antennas
- **3x3:** Three transmit, three receive antennas

The number of **transmit antennas** generally corresponds to the number of **spatial streams (data streams)** the device can support. In the case of a router that supports both 2.4GHz and 5GHz signals, the specifications include this information for each band.

Two types of MIMO exist: single-user MIMO (SU-MIMO) and multiuser MIMO (MU-MIMO). **SU-MIMO** allows wireless routers to communicate with multiple devices, but the router can communicate with only one device at a time. This means that SU-MIMO operates on a first come, first served basis. SU-MIMO was used with 802.11n devices. MU-MIMO allows multiple wireless devices to communicate with a wireless router at the same time. **MU-MIMO** offers significant improvements over SU-MIMO because it breaks up the available bandwidth into individual streams that are shared equally. MU-MIMO was supported in 802.11ac, but only for downlink transmissions. In 802.11ax, MU-MIMO is supported for both the uplink and downlink transmissions. **MU-MIMO routers** come in **2x2, 3x3, 4x4, and even 8x8 configurations.**

## Note

When a device has different numbers of receiving antennas and sending antennas, the device can be identified by the number of **spatial (data) streams** it can send and receive. For example, a device with a 2x3 antenna configuration can also be identified as having a 2x3:2 configuration (two send antennas, three receive antennas, and send/receive support for two spatial [data] streams). **Some smartphones and tablets simply use the term MIMO** (multiple input multiple output) if they support two or more 802.11n or 802.11ac streams.

## Channels



Because frequencies within the radio frequency spectrum exist everywhere, making them available to practically anyone, regulatory bodies were formed to standardize and control how they are used. The United Nations created the International Telecommunication Union Radiocommunication Sector (ITU-R) to manage the international radio frequency spectrum. However, each country can have its own regulations that govern what radio frequencies, channels, and transmission power are allowed. In the United States, the Federal Communications Commission (FCC) regulates what channels and frequencies are allowed and can be used for Wi-Fi LANs. The two frequency ranges that apply to the wireless spectrum are 2.4GHz–2.5GHz and 5.725GHz–5.825GHz. On a 2.4GHz wireless network, the wireless spectrum is divided into 11 **channels**. Installing a router involves selecting an appropriate channel for the signal. For best results, avoid overlapping channels. Only channels 1, 6, and 11 do not overlap with other channels, so it is best to use one of these three channels.

Some routers feature an Auto setting that enables the router to use the least-active channel, but if you prefer to (or must) select a channel manually, use a Wi-Fi diagnostic utility (discussed later in

this chapter) to find the **least-used channel**. (More information on channels follows in the next section.)

To change the channel used by a wireless network, follow these steps:

**Step 1.** Log into the router.

**Step 2.** Navigate to the wireless configuration dialog.

**Step 3.** Select a different channel (typically 1, 6, or 11 when using 2.4GHz networking because they have less interference than other channels).

**Step 4.** Save your changes and exit the wireless configuration dialog.

**Figure 2-3** shows a typical wireless channel configuration dialog on a dual-frequency (2.4GHz and 5.0GHz) Wireless-N router from Western Digital. Most SOHO routers have similar options.



1. Auto channel selection lets router decide which channel works best
2. Mixed mode supports older network devices
3. Default channel width supported by all 2.4GHz devices
4. Auto channel width uses 40MHz channels with Wireless-N or AC clients and 20MHz channels with Wireless-A clients
5. Pre-shared key (blanked out for security)

**Figure 2-3** Configuring Wireless Frequencies and Channels

## Bluetooth

**Bluetooth** began as a short-range, low-speed wireless network technology primarily designed to operate in peer-to-peer (or ad hoc) mode between PCs and other devices, such as printers, projectors, smartphones, mouse devices, and keyboards. Bluetooth runs in virtually the same 2.4GHz frequency that wireless networks use, but Bluetooth uses a **spread-spectrum frequency-hopping signaling method** to **minimize interference**. Bluetooth devices connect to each other to form a personal area network (PAN).

Some systems and devices include **integrated Bluetooth adapters**; others need a Bluetooth module connected to a USB port to enable Bluetooth networking.

Bluetooth version 1.2 offers a data transfer rate of 1Mbps. Version 2 offers 3Mbps. Bluetooth version 3.0 + HS can reach speeds of up to 24Mbps because it uses Bluetooth only to establish the connection; the actual data transfer happens over an 802.11 link. This feature is known as Alternative MAC/PHY (AMP). Bluetooth 4.0, also known as Bluetooth Low Energy, is designed for use

with very low-power applications, such as sensors. Bluetooth 4.1, a software update to 4.0, enables Bluetooth to perform multiple roles at the same time and to work better with LTE and 5G cellular devices.

Bluetooth 4.2 includes additional features to support the Internet of Things (IoT), and Bluetooth 5.0 was designed with the IoT in mind. IoT devices can be spread around a home, factory, or farm and can send a day's worth of stored data back to a network. Bluetooth 5 can provide up to twice the speed and up to four times the range of Bluetooth 4, while keeping power consumption low. As IoT growth continues at a rapid rate, **Bluetooth 5** is a common solution for **IoT gateway** devices.

Bluetooth is divided into **classes**, each with a different range. **Table 2-5** shows these classes, their ranges, and the amount of power their corresponding antennas use to generate signal.



**Table 2-5** Bluetooth Classes

Class	Power (mW)	Range
Class 1	100mW	100m (328 feet)
Class 2	2.5mW	10m (33 feet)
Class 3	1mW	1m (3 feet)

As you can see, Class 1 generates the most powerful signal and, as such, has the largest range. The most common Bluetooth devices are Class 2 devices, with a range of 10m (for example, portable printers, headsets, and computer **dongles**).

The Bluetooth radios that are built into mobile devices and some laptops can be used for many devices, including headsets, printers, and input devices such as mouse devices and keyboards. By default, Bluetooth **is usually disabled on Android devices**, but it **is enabled on iOS devices** such as iPads and iPhones. To connect a Bluetooth device to a mobile device, Bluetooth first needs to be **enabled**; then the Bluetooth device needs to be **synchronized** to the mobile device. This is known as **pairing**, or linking, and it sometimes requires a PIN code. Once synchronized, the device needs to be **connected**. Finally, the Bluetooth **connection should be tested**.

## Wi-Fi Standards

Six Wi-Fi standards are in use:

- **802.11b** has a maximum speed of 11Mbps and can fall back to 5.5Mbps or slower, if necessary. It uses the 2.4GHz frequency band with 20MHz-wide channels.
- **802.11a** has a maximum speed of 54Mbps and supports slower speeds, from 6Mbps to 48Mbps, as needed. It uses the 5GHz frequency band.
- **802.11g** has a maximum speed of 54Mbps and supports slower speeds, from 6Mbps to 48Mbps, as needed. Unlike 802.11a, 802.11g uses the 2.4GHz frequency band, so it is backward compatible with 802.11b.
- **802.11n** (Wi-Fi 4) has a maximum speed of 150Mbps when using a single 20MHz channel, or it can run at up to 300Mbps with channel bonding (40MHz channel). All 802.11n devices use the 2.4GHz frequency by default, but 802.11n can optionally support 5GHz frequencies as well. 802.11n supports MIMO (multiple input multiple output) antennas to improve performance and range, although not all devices include multiple antennas.

- **802.11ac (Wi-Fi 5)** uses only the 5GHz band and supports up to 80MHz-wide channels, compared to 20MHz for 802.11b/g and 40MHz for 802.11n using channel bonding. It supports multiuser MIMO (MU-MIMO). The speed of 802.11ac is up to 433Mbps per stream when 80MHz-wide channels are used.
- **802.11ax (Wi-Fi 6 & Wi-Fi 6E)** has important improvements over Wi-Fi 5 and others. Wi-Fi 6 uses both 2.4GHz and 5 GHz bands, with increased speeds up to 9.6Gbps. Wi-Fi 6E improves upon Wi-Fi 6 by supporting the 6GHz band. Benefits include increased capacity, with up to seven channels at 160MHz wide, better performance, and improved power efficiency.

### Note

Beginning with Wi-Fi 4, the Wi-Fi Alliance ([www.wifi.org](http://www.wifi.org)) now uses Wi-Fi version numbers so that users can identify newer and better devices. These versions appear in the wireless user interface information on the device so that users can identify the type of connection they have.

Table 2-6 compares the six wireless Ethernet standards.



**Table 2-6** Wireless Ethernet Standards

Wireless Ethernet Type	Frequency	Maximum Speed	MIMO Support	Estimated Range Indoors/Outdoors	Channel Width/Number	Interoperable With
802.11a	5GHz	54Mbps	No	35m/120m	20MHz/12*	Requires dual-mode (802.11a/b or 802.11a/g) hardware; 802.11n networks that support 5GHz frequency
802.11b	2.4GHz	11Mbps	No	32m/140m	20MHz/3**	802.11g
802.11g	2.4GHz	54Mbps	No	32m/140m	20MHz/3**	802.11b, 802.11n
802.11n	2.4GHz	72Mbps per stream (20MHz channel)	Yes***	70m/250m	20MHz/3**	802.11b, 802.11g; 802.11a on networks that also support 5GHz frequency
802.11n (optional) (Wi-Fi 4)	5GHz	150Mbps per stream (40MHz channel)	Yes***	70m/250m	20MHz or 40MHz/12*	802.11a (20MHz-wide channels only)

Wireless Frequency Ethernet Type	Maximum MIMO Speed	Estimated Range Support Indoors/Outdoors	Channel Width/Number	Interoperable With Channels
802.11ac 5GHz (Wi-Fi 5)	433Mbps per stream (80MHz channel)	Yes***	70m/250m	20MHz or 40MHz or 80MHz 802.11a, 802.11n (5GHz); 802.11ac routers that also support previous standards
802.11ax 2.4GHz/5GHz (Wi-Fi 6)	Up to 9.6Gbps, 1Gbps (5GHz channel)	Mu-MIMO	Same, but better throughput at longer ranges	160MHz Supports previous standards
802.11ax 2.4GHz/5GHz/6GHz (Wi-Fi 6E)	Up to 9.6Gbps	Mu-MIMO	Same as Wi-Fi 6, but 6GHz has a shorter range	160MHz Supports previous standards

\* Non-overlapping channels; exact number varies by country.

\*\* Non-overlapping channels.

\*\*\* Up to four streams supported. Most devices have up to three antennas but can receive/transmit only two streams at a time.

### Note

Wi-Fi certified hardware is 802.11-family wireless Ethernet hardware that has passed tests established by the Wi-Fi Alliance. Most, but not all, 802.11-family wireless Ethernet hardware is Wi-Fi certified.

## Long-Range Fixed Wireless

Cable modems and DSL have been the traditional method for homes and businesses to connect to the Internet. In cases where physical access to an ISP was not possible, such as rural areas, satellite access has been an option, although it is a slower, less reliable, and more expensive solution. In recent years, another option has emerged: fixed wireless Internet.

Fixed wireless providers send a signal from a wireless tower to customers who have a small antenna in their home or business. For best results, the antenna is placed in direct line of sight to the tower, sometimes aimed out a window or mounted on a rooftop. The antenna is connected via a cable to a router for wired and wireless access to the home or office.

Data rates can be very fast and the service is competitive with wired access, although the ISP usually sets the data rate to coincide with the customer's subscription rate. Figure 2-4 depicts a wireless Internet antenna on the wall of a home.



**Figure 2-4** A Home Antenna for Long-Range Wireless

The majority of the radio spectrum is licensed by the Federal Communications Commission (FCC) for specific uses or organizations such as radio and television broadcasters. An organization can purchase a license for exclusive rights to transmit on a specific frequency within a specific geographical area. This means that no one else is allowed to use or interfere with that frequency. However, certain spectrums can be used without a license. For instance, the wireless spectrum is unlicensed and does not require permission or a license from the FCC to use.

Wireless power transfer (WPT) is the process of using electric power to wirelessly charge a device. Two categories of WPT exist: near field and far field. Much like it sounds, near field transfers power over short distances, such as charging an electric toothbrush or using a wireless charging pad for a smart phone. Far field transfers power over longer distances and has potential application in powering unmanned aircraft and vehicles or solar-powered satellites. The FCC regulates WPT, and any device that uses frequencies above 9kHz is subject to FCC rules.

## A. NFC

Near-field communication (**NFC**) is a feature included in many mobile devices such as smartphones and tablets for data transfer and shopping. When NFC is enabled and a suitable payment system (such as Apple Pay or Google Pay) is installed on a mobile device, the device can be used for secure payments at any retailer that supports NFC payments.

NFC can also be used to automatically turn on Bluetooth and transfer files between devices (a feature sometimes referred to as “tap and go” or, on Android devices, Android Beam). It can be enabled separately from NFC for payments. Apple uses NFC for purchases and other limited functions that require secure data. The technology is widely used and continues to proliferate as the world moves toward contactless transactions.

## RFID

**Radio frequency identification (RFID)** technology consists of an **RFID tag** that can broadcast information about an item, as well as an RFID reader to accept the broadcast information and deliver it to a computer system for use. An example is RFID security badges that allow doors to be unlocked in a secure environment, granting access to some while denying use to others. In some retail environments, an item for sale has an RFID badge identifying the item name and price. The badges on the items in a shopping cart broadcast their information to a checkout reader, and customers can simply walk out the door with their purchases: The items are counted, priced, and paid for just by passing the reader. Passports and other identification documents might also have RFID information embedded in them.

## Services Provided by Networked Hosts

220-1101  
Exam

**220-1101: Objective 2.4:** Summarize services provided by networked hosts.

As computer networks have evolved over time, different technologies have emerged to perform specific tasks, or server roles, for the network. The following sections describe some of the common server roles that perform specialized tasks for the users on a network. A server might not necessarily be a computer. For example, routers often incorporate one or more of the server functions described in the following sections.

### DNS Server

A **Domain Name System (DNS)** server has a database that contains public IP addresses and their associated domain names. The purpose of a DNS server is to translate domain names used in web page requests into IP addresses. DNS server functions are included in SOHO routers. For larger networks, a separate DNS server can be used. A DNS server communicates with other, larger DNS servers if the requested addresses are not in its database.

## DHCP Server

A **DHCP server** supports Dynamic Host Configuration Protocol, the protocol that automatically assigns IP addresses to connected devices on a network. DHCP server functions are included in SOHO routers and are typical roles for domain controllers on small to medium business (SMB) networks. On larger networks, DHCP servers are often separate physical or virtualized servers.

## File Server

A **file server** is used to provide shared storage on a network. A file server is typically a computer with a single large drive or a RAID array for storage. Dedicated servers are used only for storage; a computer that shares storage and also performs standalone tasks (as in a Windows workgroup with 10 or fewer systems) is known as a **nondedicated server**.

A **network-attached storage (NAS)** device is a **special kind of file server** designed to **store large amounts of data in a central location for users on the network**. A NAS is essentially one or more drives fitted with an **Ethernet connection**; **it is assigned its own IP address**.

**Fileshare** is a **specialized data server system** that allows for **efficient processing** of files that many users across a network access at one time.

## Print Server

A **print server** manages the printing tasks for multiple users who share one or more printers in an office. Printing a document in a large office was once a complicated task because printers were expensive and access to them was limited. Eventually, a designated computer and printer became hosts on an office network, and managing printing tasks for the whole office became more efficient. Because print jobs might be requested faster than a printer can deliver them, print servers queue print jobs and deliver them to appropriate printers when they are available. They can also track the usage of printers on the network. Print servers and printers can be either wired or wireless.

## Mail Server

A **mail server** sends or receives email on a network. An **SMTP** (Simple Mail Transfer Protocol) server is used to send outgoing email, and either a **POP3** (Post Office Protocol version 3) or **IMAP** (Internet Message Access Protocol) server is used to receive mail. Mail server platforms are available from many vendors. For example, **Microsoft Exchange Server** is a popular mail server platform that includes email, contacts, calendar, scheduling, and more.

## Syslog Server

**Syslog servers** track and log events that happen on devices (such as routers, switches, and firewalls) and printers on a network. Devices on a network usually have a way to track their system events, such as user logins and crashes, as well as other activities that the network administrator has determined to be important. The reports are sent to a central syslog server for network managers to analyze, as needed.

## Web Server

**Web servers** are specialized computers that host websites and provide various types of content to clients via the Internet. A web server uses **HTTPS** to communicate with computers on other networks that are requesting information. Web hosting is essential in business and education, and setting up a web server has been a common task for an IT professional for many years. Today many

companies use cloud-based web servers such as Amazon Web Services (AWS) Cloud, Microsoft Azure, and Google Cloud.

## **Authentication, Authorization, and Accounting (AAA) Server**

An **AAA server** is used to examine and then authenticate (verify or deny) credentials to a user who is attempting to log into secured networks.

Note. Usernames & permissions are stored in this central server, which provides security certificates to users & records user logins to the network.

After users are authenticated, their level of authorization is determined and enforced.

**Authorization** function refers to making sure users access only areas where they have permission.

**Accounting** function refers to keeping track of the resources & activities a user has performed while on the network. Accessing files and billing for services are examples of accountable activities.

## **Internet Appliances**

Internet appliances are single-purpose devices that are used to perform specific tasks on an IP network.

## **Spam (~50% of email traffic) Gateways**

Email is essential to business. In the past, email spam has comprised up to half of the email traffic on the Web. **Spam gateways** are email filters that can detect almost all spam coming into a system, which increases email efficiency and network security as well. These gateways can be on-premises and attached to the email server or can be cloud based, depending on how email is structured in an institution.

## **UTM - Multi-features (Firewall, Remote access, VPN...)**

**Unified threat management (UTM)** devices provide firewall, remote access, virtual private network (VPN) support, web traffic filtering with anti-malware, and network intrusion prevention. UTM devices can be specialized boxes that are placed between the organization's network and the Internet, but they **can also be virtual machines** that use cloud-based services. UTM devices unite the functions of several earlier devices and have largely replaced IDS and IPS devices (described next). Barracuda Networks, Check Point, Cisco, and other networking equipment manufacturers offer versions of UTM devices.

## **IDS**

An intrusion detection system (**IDS**) device or program detects network intrusions that a firewall might not detect. Typical threats that an IDS can detect include attacks against services, malware attacks, data-driven attacks, and host-based attacks.

To detect these threats, a typical IDS uses:

1. Signature-based detection
2. Detection of unusual activities (anomalies)
3. Stateful protocol analysis.

To maintain protection, an IDS device or program must be **updated frequently** with new signatures & rules.

A true IDS does not block attacks, but some products and services referred to as IDSs actually have characteristics of IPSs (intrusion prevention systems).

## **IPS**

An intrusion prevention system (**IPS**) uses methods similar to those used by an IDS. Unlike an IDS, however, an IPS blocks attacks. Dedicated IDS and IPS devices are not widely used today, but their features are incorporated into UTM devices.

An IPS can also be implemented in software with a package such as the open source Snort ([www.snort.org](http://www.snort.org)) for Windows and some Linux distributions.

## **Load Balancers**

Load balancing refers to sharing tasks and traffic in a network for maximum efficiency. When balancing traffic within a network or handling application processing between servers, the work is shared among all the available resources on a network instead of occurring on only one device. For example, network load balancing occurs when inbound or outbound traffic can be split up and routed to the destination in different ways to enhance speed, with the data reassembled at the destination for processing. A **load balancer** increases redundancy and performance by distributing the load to multiple servers. Network load balancers are often reverse proxy servers configured in a cluster to provide scalability and high availability.

## **Proxy Server**

A **proxy server** is an intermediary between a client and another network, such as the Internet. A proxy server stores web pages that have been requested; if a client requests a web page, the proxy server checks its cache for the page. If the page exists and is up-to-date, the proxy server uses its cached copy to supply the client request. If the proxy server does not have the requested page, it downloads the page on behalf of the client, sends the page to the client, and retains a copy of the page in its cache.

A proxy server reduces traffic between a network and the Internet, and it can also block requests for undesirable traffic. In addition, proxy servers can be used for anonymous surfing. See <https://whatis.techtarget.com/definition/proxy-server> for more information on how proxy servers are used.

## **Legacy and Embedded Systems**

The term *legacy* refers to something handed down from predecessors. **Legacy systems**, therefore, are systems that use outdated operating systems, programming languages, applications, or hardware. Maintaining legacy systems is often necessary when newer products are not compatible with legacy applications (for example, applications that can run only under MS-DOS or old versions of Windows).

If a legacy operating system and its applications can be run in a virtualized environment, the problems of maintaining old hardware are eliminated.

**Embedded systems** are dedicated computing devices used for specific tasks, such as machine control, point-of-sale systems, or ATMs. Embedded systems commonly are found in Supervisory Control and Data Acquisition (SCADA) systems. SCADA systems are designed to provide centralized control for managing industrial equipment, such as in manufacturing or water and waste treatment plants. SCADA systems connect equipment to a typically secure network that facilitates communication between operators and machines. Operators can collect and analyze data from various components, as well as modify configurations or operations. SCADA systems can be complex because many different components are working together to ensure the functionality of the

equipment or process. Embedded systems often also are legacy systems; as long as they work, they are maintained. Embedded systems are very specialized in nature and often run older operating systems because of the way the systems are designed and whether they allow the manufacturer to upgrade the operating system.

Perhaps the biggest risk to both legacy and embedded systems is security. If a legacy system or an embedded system has network or Internet connectivity, it theoretically could be attacked or used as a bot to attack other systems. This is a great concern for organizations that utilize SCADA systems because many manage critical infrastructure equipment in facilities such as power plants, dams, nuclear reactors, and water and waste treatment. Although operating systems designed for embedded uses have more security than standard operating systems, older operating systems face the greatest risks.

Because of the potential for security risks, some organizations have paid for extended security updates for otherwise-legacy systems.

When considering whether and when to update legacy systems or embedded systems, consider these issues:

- Will the existing data be usable with newer apps?
- Can the existing program run with current operating systems?
- Will changes in network security, wireless, or Internet standards (such as a changeover to IPv6) cause problems with the application?
- Can a proprietary application be licensed to run in a virtual machine?
- Does existing hardware used in the embedded system work with the new operating system?
- Does the embedded application run on current embedded operating systems? If not, is an updated version available?

Evaluating, testing, troubleshooting, and running both systems in parallel are highly advisable when updating legacy systems or embedded systems.

## Internet of Things (IoT) Devices

The Internet has long connected people together, but in recent years, the explosive growth of the Web has involved connections between people and the objects that they use. As communication protocols such as Bluetooth and Z-Wave have evolved, production techniques have made it easier to embed communication capability into smaller and less expensive objects that are common in people's everyday life. Markets for **Internet of Things (IoT)** devices are expanding—consider phones, cars, home appliances, door locks, wall outlets, lights, and video-enabled doorbells, among many other devices. Industrial uses are being developed as well, and now devices can measure soil moisture, noise, motion, air pressure, and water pressure. Many billions of objects are now talking to each other and sharing data, and the number of such devices is expected to grow exponentially. Figure 2-5 depicts some of the many IoT functions you might already enjoy on your mobile device.

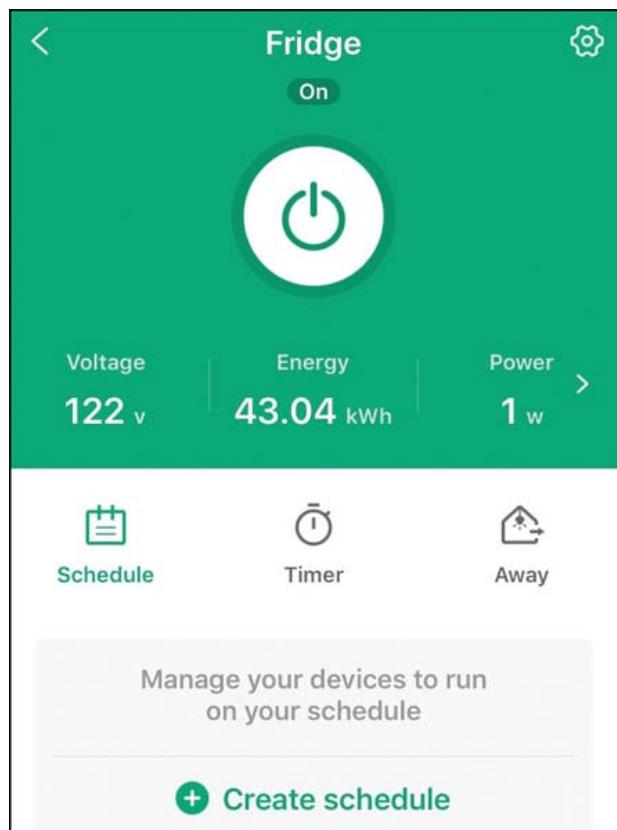


**Figure 2-5** IoT Applications on a Mobile Device (Image © Es sarawuth, Shutterstock)

The software to manage IoT devices can be installed on computers or mobile devices. Typically, a vendor of an IoT product develops a mobile app to monitor and manage the product. Some systems are complex, but many are quite simple and easy to set up on a home network. The following are some items that can participate in the IoT:

- Thermostats
- Light switches
- Security cameras
- Door locks
- Voice-enabled smart speakers/digital assistants

Figure 2-6 shows the user interface for an IoT-enabled wall outlet adapter that is monitoring energy use for a refrigerator. Off/on and scheduling capability are built into the application, and the device can be managed from anywhere on the Web.



**Figure 2-6** IoT Device App Interface

## Install and Configure a Basic Wired/Wireless SOHO Network

220-1101  
Exam

**220-1101: Objective 2.5:** Given a scenario, install and configure basic wired/wireless small office/home office (SOHO) networks.

Wireless Ethernet, also known as IEEE 802.11, is the collective name for a group of wireless technologies that are compatible with wired Ethernet; these technologies are referred to as wireless LAN (WLAN) standards. Wireless Ethernet is also known as Wi-Fi, after the Wireless Fidelity (Wi-Fi) Alliance ([www.wi-fi.org](http://www.wi-fi.org)), a trade group that promotes interoperability among different brands of wireless Ethernet hardware.

The following sections describe factors to consider when implementing these wireless technologies into a SOHO environment.

### IP Addressing

The Internet Protocol (IP) is the communication protocol that computers and other devices use to communicate with computers that reside outside their local networks. IPv4 and IPv6 are two current versions of IP addressing that are commonly in use today. All devices that communicate on a local network have a physical address that is unique and unchanging. IP addresses are changeable, logical addresses and are assigned to devices for communicating outside their local networks.

## IPv4

An IP version 4 (IPv4) address consists of a group of four numbers that each range from 0 to 255 (for example, 192.168.5.1). An IP address is divided into two sections: the network portion, which is the number of the network the computer is on, and the host portion, which is the individual number of the computer. Using the previous IP address as an example, the 192.168.5 portion typically is the network number, and .1 is the host number. A subnet mask distinguishes between the network portion of the IP address and the host portion. For example, a typical subnet mask for the IP address just used is 255.255.255.0. The 255s correspond to the network portion of the IP address; the 0 corresponds to the host portion, as shown in [Table 2-7](#).



**Table 2-7** IPv4 Address and Corresponding Subnet Mask

IP Address/Subnet Mask	Network Portion	Host Portion
192.168.5.1	192.168.5	1
255.255.255.0	255.255.255	0

The subnet mask is also used to define subnetworks, if subnets are being implemented. (Subnetting is beyond the scope of the CompTIA A+ exam.)

Both computers and other networked devices, such as routers and network printers, can have IP addresses. In some cases, a device can have more than one IP address. For example, a router typically has two IP addresses: one to connect the router to a LAN and the other that connects it to the Internet, enabling it to route traffic from the LAN to the Internet and back.

Each number in an IP address is called an *octet*. An octet is an 8-bit byte. This means that, in the binary numbering system, the number can range from 00000000 to 11111111. For example, 255 is actually 11111111 when converted to the binary numbering system. As another example, 192 decimal equals 11000000 binary. Because an IPv4 address has four octets, it is a 32-bit address. IPv4 supports up to 4.3 billion addresses (that is,  $4.3 \times 10^9$ ).

### Note

To convert numbers from decimal to binary and vice versa, use the Windows calculator. Press Windows+R to bring up the Run prompt, and then type **calc** to open the Windows Calculator application. Several types of calculators are available from the Calculator menu in the upper left. Select the Programmer calculator. Now you can see a list on the left that allows you to change between numbering systems. Simply type any number, and then select the numbering system that you want to convert it to.

## Public and Private IP Addresses

*Public IP addresses* can be discovered and seen by anyone on the Web. *Private IP addresses* are not routable to the Web and can be used only inside a local area network (LAN). For most SOHO networks, an ISP provides a single public IP address to a customer. The address provided gives access to the Web and is discoverable by anyone on the Internet. That IP address is usually assigned to the interface of the SOHO router that connects to the ISP.

Inside a SOHO network, private IP addresses are used to identify each device on the network. Private addresses are used for a couple reasons. First, the limited number of available public IPv4 addresses is not nearly sufficient to meet demand. IPv4 was not designed with the explosive growth of connected devices in mind, and private addressing was a solution to the address shortage. Second, using private addresses inside a network adds security because devices cannot be discovered from the Internet.

A few easy clues can help determine whether an IP address is public or private, and those come in the first numbers of the IP address. Private addresses fall in one of three addressing ranges:

- 10.0.0.0–10.255.255.255
- 172.16.0.0–172.31.255.255
- 192.168.0.0–192.168.255.255

Other types of reserved addresses exist, but for a technician working with devices on a private network, knowing the available private addresses is important.

Network address translation (**NAT**) is the process of modifying IP addresses as information crosses a router. Generally, this functionality is built into a router. It hides an entire IP address space (for example, 192.168.0.1 through 192.168.0.255) on the LAN. Whenever an IP address on the LAN wants to communicate with the Internet, the IP address is converted to the public IP address of the router (for example, 68.54.127.95). This way, it appears as if the router is the only device making the connection to remote computers on the Internet, which provides safety for the computers on the LAN. It also allows a single IP address to do the work for many other IP addresses in the LAN.

SOHO routers perform NAT automatically when connected to an IPv4 network. NAT is not necessary on an IPv6 network because IPv6 is much more secure and has no shortage of IP addresses.

Public and private addresses are used in IPv6 as well, but they take a different form.

## IPv6

IP version 6 (IPv6) greatly increases the number of available IP addresses for computers, smartphones, and other mobile devices. IPv6 uses 128-bit source and destination IP addresses (compared to 32-bit for IPv4), theoretically enabling up to 340 undecillion addresses ( $3.4 \times 10^{38}$ ). (This number is largely unimaginable to humans; 340 undecillion is said to exceed the number of grains of sand on Earth.) IPv6 also features built-in security and provides better support for quality of service (QoS) routing, which is important to achieve high-quality streaming audio and video traffic. Windows, macOS, and Linux all support IPv6.

## IPv6 Addressing

IPv6 addresses start out as 128-bit addresses that are each then divided into eight 16-bit blocks. The blocks are converted into hexadecimal, and each block is separated from the following block by a colon. Leading zeros are typically suppressed, but each block must contain at least one digit.

Consider a typical IPv6 address:

21DA:D3:0:2F3B:2AA:FF:FE28:9C5A

A contiguous sequence of 16-bit blocks set to zero can be represented by the double colon (::). This technique is also known as *zero compression*. To determine the number of zero bits represented by

the double colon, count the number of blocks in the compressed address, subtract the result from 8, and multiply the result by 16. An address can include only one zero-compressed block.

This IPv6 address uses the double colon:

FF02::2.

Two blocks exist here: FF02 and 2. So how many zero bits does the double colon represent? Subtract 2 from 8 ( $8 - 2 = 6$ ) and then multiply 6 by 16 ( $6 \times 16 = 96$ ). This address includes a block of 96 zero bits.

The loopback address on an IPv6 system is 0:0:0:0:0:0:1, which is abbreviated as ::1. Thus, if you want to test your network interface in Windows where IPv6 is enabled by default, you can type **ping ::1** at a command prompt.

## IPv6 Address Types



IPv6 supports three types of addresses: unicast, multicast, and anycast. Five types of unicast addresses exist:

- **Global unicast addresses:** Global unicast addresses are used in the same way as IPv4 public addresses. The first 3 bits are set to 001 and the following 45 bits are used for the global routing prefix; these 48 bits are collectively known as the public topology. The subnet ID uses the next 16 bits and the interface ID uses the remaining 64 bits.
- **Link local addresses:** Link local addresses correspond to the Automatic Private IP Addressing (APIPA) address scheme used by IPv4 (addresses that start with 169.254). The first 10 bits are set to FE80 hex, followed by 54 zero bits and 64 bits for the interface ID. Using zero compression, the prefix is thus FE80::/64. As with APIPA, link local addresses are not forwarded beyond the link.
- **Site local addresses:** Site local addresses use the prefix FEC0:: and correspond to IPv4 private address spaces (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16).
- **Special addresses:** Special addresses include unspecified addresses (0:0:0:0:0:0:0 or ::), which are equivalent to IPv4's 0.0.0.0 and indicate the absence of an IP address; a loopback address (0:0:0:0:0:0:1 or ::1) is equivalent to the IPv4 loopback address 127.0.0.1.
- **Compatibility addresses:** Compatibility addresses are used when both IPv4 and IPv6 are in use. In the following examples, *w.x.y.z* is replaced by the actual IPv4 address. An IPv4-compatible address (0:0:0:0:0:*w.x.y.z* or ::*w.x.y.z*) is used by nodes that support IPv4 and IPv6 communicating over IPv6. An IPv4-mapped address (0:0:0:0:FFFF:*w.x.y.z* or ::FFFF:*w.x.y.z*) represents an IPv4-only node to an IPv6 node. A 6to4 address is used when two nodes running both IPv4 and IPv6 connect over an IPv4 link. The address combines the prefix 2002::/16 with the IPv4 public address of the node. ISATAP can also be used for the connection; it uses the locally administered ID::0:5EFE:*w.x.y.z* (where *w.x.y.z* is any unicast IPv4 address, either public or private). Teredo addresses are used for tunneling IPv6 over UDP through network address translation (NAT); they use the prefix 3FFE:831F::/32.

Both IPv4 and IPv6 support multicasting, which enables one-to-many distribution of content such as Internet TV or other types of streaming media. IPv6 multicast addresses begin with FF.

Anycast addressing sends information to a group of potential receivers that are identified by the same destination address. This is also known as *one-to-one-to-many association*. Anycast addressing can be used for distributed services, such as DNS or other situations in which automatic failover is desirable. IPv6 uses anycast addresses as destination addresses that are assigned only to routers. Anycast addresses are assigned from the unicast address space.

## Viewing IP Address Information

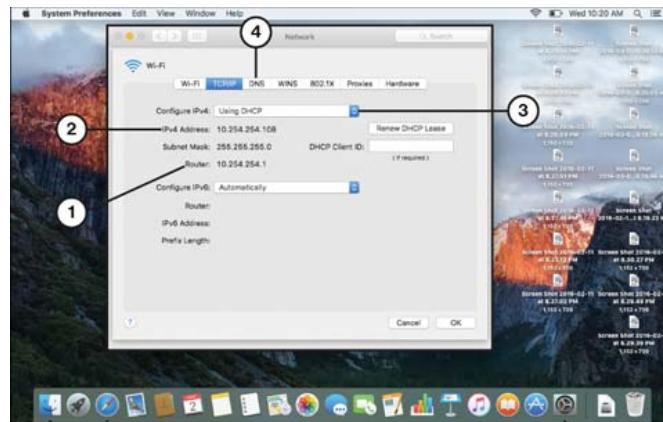
To see the IPv4 and IPv6 addresses assigned to a Windows device using both IPv4 and IPv6, use the command-line **ipconfig** utility at the command prompt. Consider an example of the output from a system using a wireless Ethernet adapter:

[Click here to view code image](#)

```
Wireless LAN adapter Wireless Network Connection:  
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::5cf1:2f98:7351:b3a3%12  
IPv4 Address . . . . . : 192.168.1.155  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.1.1
```

For more information, see [https://technet.microsoft.com/en-us/library/dd392266\(WS.10\).aspx](https://technet.microsoft.com/en-us/library/dd392266(WS.10).aspx).

macOS provides IPv4 and IPv6 address information through the TCP/IP tab of the Network utility (see [Figure 2-7](#)).



1. IPv4 address
2. Router (gateway) address
3. Open this menu to configure IP address manually
4. Click DNS tab to view or edit DNS addresses

**Figure 2-7** The macOS TCP/IP Tab

Many Linux distros include a GUI-based network utility similar to the one used in macOS, but with any Linux distro (as well as with macOS), you can open Terminal and use the command **ifconfig -a** to view this information. [Figure 2-8](#) shows a portion of the output for a wireless connection.

```

viveuser@localhost:~$ ifconfig
loop  txqueuelen 0  [Local Loopback]
      RX packets 1538  bytes 1196888 (116.2 kB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 1538  bytes 1196888 (116.2 kB)
      TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

virbr0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
      inet 192.168.124.1  netmask 255.255.255.0 broadcast 192.168.124.255
        ether 52:54:00:3d:2a:06  txqueuelen 0  [Ethernet]
      RX packets 0  bytes 0 (0.0 B)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 0  bytes 0 (0.0 B)
      TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

wlp8s0f2u2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 10.128.0.154  netmask 255.255.255.0 broadcast 10.128.0.255
        inet6 fe80::2c1:1fffe:ec22:am  prefixlen 64  scopeid 0x20<link>
          RX packets 4  bytes 996 (996.0 B)
          RX errors 0  dropped 0  overruns 0  frame 0
          TX packets 27  bytes 4681 (4.5 kB)
          TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
[1liveuser@localhost ~]$ 

```

1. RUNNING = active connection
2. inet = IPv4 address information
3. inet6 = IPv6 address information
4. ether = MAC (physical) address

**Figure 2-8** Linux **ifconfig** Output for a Wireless Connection

With macOS, use the TCP/IP tab (refer to [Figure 2-7](#)) to configure IPv4 or IPv6 address information. macOS uses the term *router* to refer to the default gateway. Use the DNS tab to configure DNS server information.

With Linux, you can use the network configuration tool provided in the GUI. Alternatively, you can edit the network configuration scripts from Terminal, using the distro’s text editor, if no GUI-based network configuration program is available. Two scripts need to be edited:

- **ifcfg-connection name** identifies IP addresses for IPv4 and IPv6 and the default gateway, as well as other IP settings. It is located in the /etc/sysconfig/network-scripts/ folder. The loopback script is called **ifcfg-lo**. A separate **ifcfg** file exists for each connection (wired, wireless, and so on).
- The file **resolv.conf** identifies DNS servers. It is located in the /etc/ folder.

For the syntax, see the documentation for the distribution in use.

A small office/home office (SOHO) wired or wireless router can provide a secure way for users to access the Internet and local network resources; it can also become a magnet for attack. The difference is in how the router is configured. The following sections look at how to configure SOHO routers to meet typical network requirements.

To configure a router’s settings, connect to the router either with an Ethernet cable or wirelessly, using the manufacturer’s instructions on the default IP address to use. To connect to the router’s web interface, open a browser, enter the IP address of the router in the address bar, and press Enter.

## APIPA IP Addresses/Link Local Addresses

Most IP networks use addresses provided automatically by the Dynamic Host Configuration Protocol (DHCP). However, if the DHCP server becomes unavailable and an alternate IP address has not been set up, devices on the network assign themselves Automatic Private IP Addressing (APIPA) or link local addresses. These addresses are in the IPv4 address range 169.254.0.1 to 169.254.255.254

(with the subnet mask 255.255.0.0); the IPv6 version is called a link local address and has the FE80::/64 prefix. A device with an APIPA address cannot connect to the Internet.

If a DHCP problem causes APIPA/link local addresses to be assigned, you can resolve the problem by checking the device's network connection and using the **ipconfig /release** and **ipconfig /renew** commands at the command prompt. This causes the computer to obtain a new IP address from the DHCP server. If these actions do not solve the problem, the DHCP server (often located in the router on a SOHO network) should be checked and restarted, if necessary.

APIPA was originally developed by Microsoft, but it is now a standard (RFC 3927) that macOS and Linux also support.

## Dynamic vs. Static IP Addresses

The term *static* means “unchanging” or “always the same.” Dynamic means “constantly changing.” These terms describe the two most common ways to configure a computer’s IP address settings:

- **Static IP address:** Assigned to a device by the administrator and not subject to change until reconfigured by the administrator. Note that more than just the IP address must be configured; other areas are the subnet mask, the default gateway, and DNS servers.
- **Dynamic (DHCP server-assigned) IP address:** Assigned by a DHCP server and likely to change each time a device leaves and then rejoins the network, or when the address is used beyond its lease time and expires.

Table 2-8 describes the various settings related to static and dynamic addressing.



**Table 2-8** Static vs. Dynamic IP Addressing

Setting	What It Does	Static IP Address	Dynamic IP Address
IP address	Identifies a computer on the network; unique value for each device	Entered manually on the device	Automatically assigned by the DHCP server
Subnet mask	Determines which bits in the IP address are the network portion and which are the host portion	Entered manually on the device, but a default subnet mask appears when the IP address is assigned	Automatically assigned by the DHCP server
DNS configuration	Identifies Domain Name System servers	IP addresses of one or more DNS servers, hostname, and domain name must be entered	Automatically assigned by the DHCP server
Gateway	Identifies the IP address of the device that connects the computer to the Internet or another network; same values for all devices on the network	IP address for the gateway must be entered	Automatically assigned by the DHCP server

Windows, macOS, and Linux default to using dynamic IP addresses. As [Table 2-7](#) makes clear, this is the preferred method for configuring a TCP/IP network. Use a manually assigned IP address if a DHCP server (which provides IP addresses automatically) is not available on the network or if you need to configure a firewall or router to provide different levels of access to some systems (in this case, you must specify those systems' IP addresses).

### TIP

For the 220-1101 exam, be sure you understand the difference between static and dynamic IP addressing and know where to go within a given operating system to set or change client-side DHCP, DNS, subnet mask, and default gateway settings.

### Note

Routers, wireless gateways, and computers that host a shared Internet connection with Windows Internet Connection Sharing or a third-party sharing program all provide DHCP services to other computers on the network.

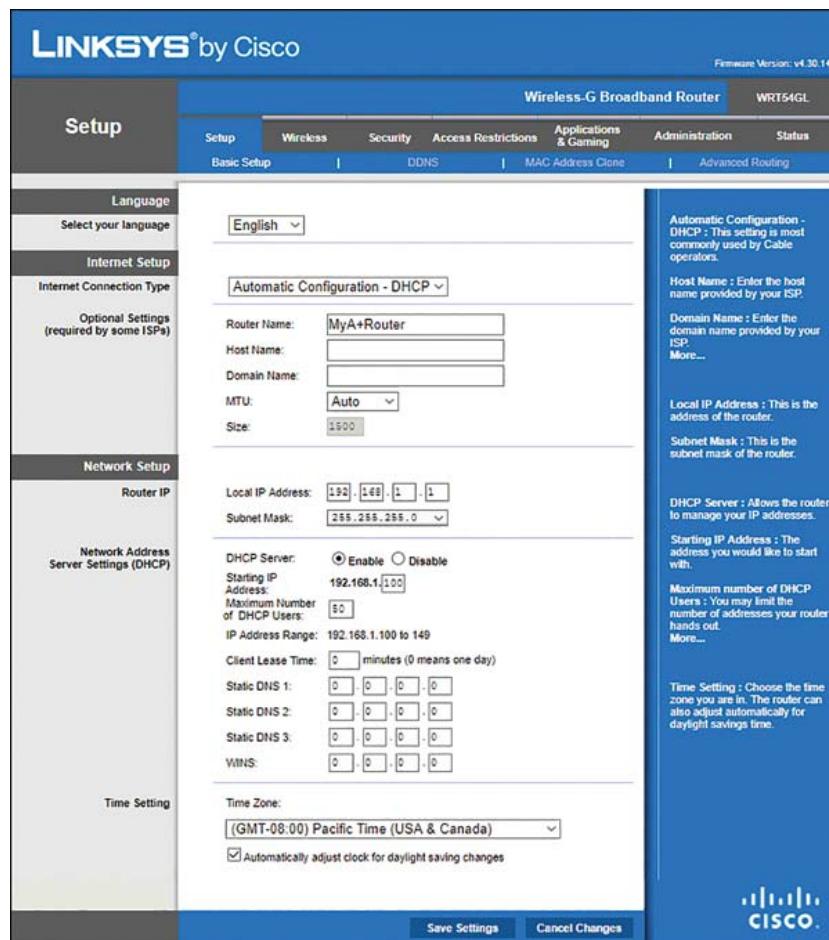
To configure an IP address in Windows, access the Internet Protocol Properties window. This window contains several dialogs used to make changes to an IP address. To open the General tab of the Internet Protocol Properties window, open Network Connections, right-click the network connection, select Properties, click Internet Protocol v4 (TCP/IPv4) or TCP/IPv6 in the list of protocols and features, and click Properties.

IP configuration in Linux is performed by editing the /etc/network/interfaces file. If you use a GUI that features a Network configuration panel, you can use it to make changes for you.

To configure TCP/IP in macOS, go to System Preferences, open the Network panel, and select the appropriate tab.

## DHCP

By default, SOHO routers have the DHCP service turned on so they can provide IP addresses to any wired or wireless devices that connect. Most routers enable you to specify the range and number of IP addresses available via DHCP. [Figure 2-9](#) illustrates a router with DHCP enabled and a range of IP addresses that the DHCP server can assign. In this example, the default address of the router is 192.168.1.1 and the subnet mask is 255.255.255.0. This means that the router has the first address on the 192.168.0 network, which is a private network that cannot be used on the Internet. As shown in the router settings, when devices join the network, DHCP assigns addresses in the range 192.168.1.100 to 192.168.1.149.



**Figure 2-9** Configuring DHCP to Provide a Range of 50 IP Addresses

If a router does not have sufficient IP addresses for the devices that need to connect to it, devices that arrive after the pool of addresses is used up do not receive IP addresses; instead, the router switches to Automatic Private IP Addressing (APIPA), using the nonroutable IP address range 169.254.x.x.

### TIP

When you need to use static IP addresses on some devices, be sure to reserve some IP addresses and keep them out of the range of addresses assigned by the DHCP server. For example, in the network illustrated in Figure 2-9, IP addresses below 100 and above 149 in the 192.168.1.x network could be used for devices that need static IP addresses.

## IP Addressing

A SOHO router comes with a default IP address. This IP address is a special type known as a *private address*.

## NIC Configuration

A PC can have several different NICs, to make it possible to connect to networks over the wire, via Wi-Fi, or virtually. After you select the NIC that matches the method of connecting, you can choose the protocol and configure network access.

## NIC Configuration Steps

The steps for configuring a NIC follow:



- Step 1.** Click the **Windows** icon and select the **Windows Settings** gear.
- Step 2.** In the Windows Settings window, select the **Network & Internet Link**.
- Step 3.** When you see the different connection options, select the one you want and click **Change Adapter Options**, on the right side of the window.
- Step 4.** Choose the adapter you want to configure (in this case, Ethernet) and click the **Properties** button. A list of items available to the NIC appears. In the example, note that both IPv4 and IPv6 are checked, making them available to the NIC.
- Step 5.** Double-click **Internet Protocol Version 4 (TCP/IPv4)**. You now see the window where the IP address is configured either dynamically or statically (see [Figure 2-10](#)).



**Figure 2-10** Configuring a Static IP Address

- Step 6.** By default, the Obtain an IP Address Automatically option is selected. This option dynamically assigns an IP address from a DHCP server. To configure the device with a static IP address, select **Use the Following IP Address** and enter the IP address, subnet mask, and default gateway; click **OK** to accept any changes.

## End-User Device Configuration

The steps for configuring a NIC are essentially the same steps used for other end-user devices, such as printers and mobile phones. If the default on an end-user device is DHCP, the device is likely to autoconfigure. If the device needs to be configured, the process is mostly the same as described for NICs. To access the configuration windows, you might need to visit the manufacturer's support site.

## Cable/DSL Modem

Setting up a cable modem or DSL modem is a fairly simple task on the user's end. Most SOHO networks use a wireless router, and it must be connected to the modem. Simply plug one end of an Ethernet cable into the cable or DSL modem and then plug the other end into the RJ-45 jack labeled as Internet. Attach the local devices to the wireless router with Ethernet cables in the remaining ports or via Wi-Fi.

## Network Configuration Concepts

220-1101  
Exam

**220-1101: Objective 2.6:** Compare and contrast common network configuration concepts.

Computer network technologies evolve at a rapid pace, and keeping track of all the different technologies and protocols can be daunting. Still, a fundamental understanding of communication processes and network configuration concepts is essential for a computer technician. This will become even more true as people increase their computer use for communication and as the number of devices talking to each other grows exponentially. The following sections cover some of the most common networking terms, technologies, and configuration concepts.

### DNS

Domain names are how humans identify web server destinations on the Web. For example, NYT.com, US.gov, and Alaska.edu are all domain names that point to useful websites. Computers, however, use IP addresses, so domain names have to be translated, or mapped, to computer-friendly network addresses. This is not unlike the contacts list on your phone that maps people's names to their phone numbers. Computers and other devices use the Domain Name System (DNS) to map names to addresses on the Internet. Servers throughout the Internet track names and addresses. When a user types in [www.cisco.com](http://www.cisco.com), the DNS protocol sends out messages asking for the network address of cisco.com. A DNS server that knows then responds with the address. This process is often called resolving IP addresses. It generates a lot of traffic on the Web, and DNS traffic can sometimes be generated by viruses that target a server and cause so much traffic with DNS requests that the server shuts down.

DNS stores 32-bit IPv4 address data in A records. DNS accesses A records when resolving IPv4 address requests. IPv6 addresses are bigger (128 bits), and DNS stores them in AAAA records.

Handling email traffic on the Web is a daunting task. One function of DNS is to efficiently map email addresses to the destination email servers. It does this by sending a DNS mail exchange (MX) record that directs email to a mail server. The MX record works with SMTP, the standard mail protocol, to determine mail priority and other settings.

Text (TXT) records enable administrators to enter common text explanations into DNS that usually describe domain ownership or other information. TXT records are also used to counter email spam. Other DNS tools that can protect email from spam follow:

- **DomainKeys Identified Mail (DKIM):** A process that enables a receiving mail system to make sure that the message was authorized by the sending party and was not used for spam or phishing.
- **Sender Policy Framework (SPF):** A tool that lets domain owners list the IP addresses that are authorized to send mail, to control spam.

- **Domain-based Message Authentication, Reporting, and Conformance (DMARC):** A mail authentication process that builds on DKIM and SPF to further enhance security from fraudulent spam.

## DHCP

When a device is configured to receive an IP address dynamically, a DHCP server leases the first available IP address from a specific pool or range of IP addresses. A device is leased an IP address for a certain amount of time and can renew a leased IP address before the lease expires. This process is known as a DHCP leasing. If the lease expires, the device must request an IP address again. The purpose of using a lease is to ensure that any unused IP addresses are put back into the pool of available addresses and can be leased to another device. Otherwise, the pool of addresses could become quickly depleted.

Configuring a DHCP reservation with a specific address from the DHCP pool of addresses is possible. This is a permanent lease that is assigned to a DHCP client. It is similar to a static address, in that it doesn't change, but it is configured into the DHCP server and the address is from the range of addresses that DHCP gives out to clients.

A DHCP scope is a pool or range of IP addresses that the DHCP server can assign or lease to devices. Generally, a scope is a single pool of IP addresses that are assigned to devices on a specific network. In some cases, multiple scopes are configured within the DHCP server to assign to devices on different networks.

## VLAN

A **virtual local area network (VLAN)** is a group of computers on a local area network (LAN) that are configured to behave as if they have their own separate LAN. Usually LANs are separated by a router, but a switch might have the capability to group ports together to behave like a LAN inside the switch. Because the LAN exists in software configuration instead of in hardware, it is considered a VLAN. For example, if a LAN of 10 computers is divided evenly into VLAN 1 and VLAN 2, the computers in VLAN 2 will be able to communicate among themselves, but not with any hosts on VLAN 1. The hosts in each VLAN will even have IP addresses on different networks, and communicating between VLANs will require the services of a router.

## VPN

A **virtual private network (VPN)** is a private (secure) network connection that is carried by an insecure public network, such as the Internet. A VPN connection requires a VPN server at the remote site and a VPN client at the client site. VPN traffic between client and server is encrypted and encapsulated into packets suitable for transmission over the network. VPNs can be used in place of leased lines for connections between locations and for telecommuting workers.

The most common types of VPNs are PPTP and L2TP/IPsec VPNs. PPTP uses 128-bit encryption. L2TP combined with IPsec (L2TP/IPsec) uses 256-bit encryption.

### Note

Remember that a VPN extends a LAN by establishing a remote connection, a connection tunnel, using a public network such as the Internet. Common VPN implementations include site to site, host to site, and host to host.

# Internet Connection Types, Network Types, and Their Features

220-1101  
Exam

**220-1101: Objective 2.7:** Compare and contrast Internet connection types, network types, and their features.

Different methods of accessing the Internet have come and gone over the decades. This section describes the most common methods an A+ technician will likely encounter.

## Internet Connection Types

One of the best reasons to create a network of any size is to provide access to the Internet. The following sections discuss the many types of connectivity technologies that can be used for Internet access.

### Note

As you review the following sections, try to determine which type of Internet connections you use at home and in the workplace. When you are shopping for Internet service, the BroadbandNow website ([www.broadbandnow.com](http://www.broadbandnow.com)) is a useful source for finding the types of broadband Internet access that are available in a specified ZIP code.

For the 220-1101 exam, it is important to know the different network connection types and their speeds. **Table 2-9** compares the network types, from fastest to slowest.

Key Topic

**Table 2-9** Comparison of Network Connection Speeds

Wired	Fiber	Cable	DSL
← Fastest ----- Slowest →			
Wireless	Cellular	Wireless Internet service provider (WISP)	Satellite

## Cable

**Cable** is broadband Internet service that is provided by a cable TV company. Broadband can deliver voice, data, and video at one time. Virtually all cable Internet service today is built on the fiber-optic and coaxial network used for the digital cable and music services that most cable TV vendors provide. In most cases today, separate coaxial cables are used for TV and Internet service into a home or an office. A cable modem is required in the home or office to receive the service.

Cable Internet can reach download speeds anywhere from 3Mbps up to 300Mbps or faster. Upload speeds are typically about 10–20 percent of download speeds, but this varies by vendor. An Internet speed test can be conducted on a device to determine the current upload and download speeds (see **Figure 2-11**). Speed can be impacted by longer distances between the modem and the provider's termination point in the neighborhood. Cable is faster and has more range than DSL.



**Figure 2-11** Speed Test Performed on a Small Office/Home Office (SOHO) Router with Cable Internet Service

### Note

You can have cable Internet service without having cable TV.

Most cable modems connect to a computer or a router via an RJ-45 cable, but some use USB. When a cable provider also provides a telephone service, a special modem is used that also includes a backup battery.

A cable Internet connection can be configured through the standard Network properties sheet in the operating system.

### DSL

**DSL** (Digital Subscriber Line) was originally designed to work on the same telephone line used by a telephone (and a fax machine, if the telephone line can carry a digital signal). For home use, DSL is designed strictly for Internet access. For business use, DSL can be used for additional services and in site-to-site scenarios between organizations.

Although telephone line-based DSL is still available, it is much slower than cable Internet. Newer types of DSL use the same signaling methods but use fiber to provide speed comparable to that of high-performance cable.

Two major types of DSL use telephone lines: **ADSL** (Asynchronous DSL) and **SDSL** (Synchronous DSL). Two newer types of DSL—VDSL (Very High Bit-Rate Digital Subscriber Line) and VDSL2—use fiber for at least part of the signal path. [Table 2-10](#) compares these features.



**Table 2-10** Common DSL Services Compared

Service Type	Line Type	User Installation Option	Typical Downstream Speeds	Typical Upstream Speeds	Supports HDTV Service
ADSL	Existing telephone line	Yes	384Kbps to 24Mbps	128Kbps to 3.3Mbps	No
SDSL	New telephone line	No	384Kbps to 2.0Mbps	384Kbps to 2.0Mbps	No
VDSL	Fiber + telephone line	No	Up to 55Mbps	15Mbps	Yes
VDSL2	Fiber + telephone line	No	Up to 200Mbps	Up to 100Mbps	Yes

### Note

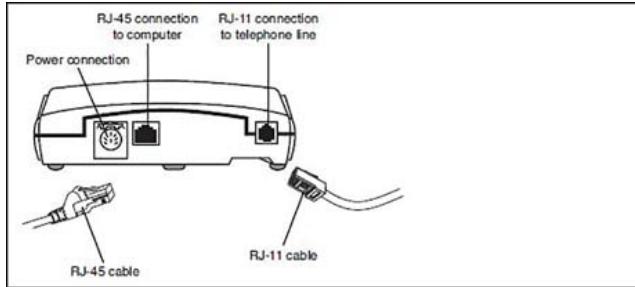
*Downstream* refers to download speed; *upstream* refers to upload speed. SDSL gets its name from providing the same speed in both directions. ADSL is always faster downstream than upstream.

Both VDSL and VDSL2 use fiber for most of the distance from the telephone company's central office (where all DSL services connect to the Internet).

A device known as a *DSL modem* is used to connect a computer to a DSL service. A DSL modem connects to a PC through the RJ-45 (Ethernet) port or the USB port.

Many companies that offer ADSL, VDSL, and VDSL2 services now provide a wireless router with DSL support and an integrated Gigabit Ethernet switch. Some of these devices also support HPNA, which was developed by the Home Phone Networking Alliance and uses either coaxial wiring in the home as a network or connections to a cable modem.

As [Figure 2-12](#) indicates, DSL uses the same telephone lines as ordinary telephone equipment. However, a telephone on the same wire can interfere with the DSL connection. To prevent this, in some cases, a separate DSL line is run from the outside service box to the computer with the DSL modem. However, if the DSL provider supports the self-installation option, small devices called *microfilters* are installed between telephones, answering machines, fax machines, and other devices on the same circuit with the DSL modem. Microfilters can be built into special wall plates but more often are external devices that plug into existing phone jacks, as shown in [Figure 2-12](#).



**Figure 2-12** A Typical Self-Installed DSL Setup

A DSL connection can be configured as an always-on connection, similar to a network connection to the Internet. However, many vendors now configure DSL connections as PPPoE (Point-to-Point Protocol over Ethernet) connections instead. A PPPoE connection requires the user to make a connection with a username and password. PPPoE connections are supported in Windows, macOS, and Linux.

## Fiber

Instead of using a copper connection to a home or business the way dial-up, ADSL/SDSL, or cable Internet do, many companies offer **fiber** (fiber-optic cable) connections to the home (FTTH, also known as fiber to the premises, or FTTP) at their highest service levels. Fiber network download speeds can reach up to 2Gbps, and some vendors provide the same upload speed. DSL vendors such as Verizon, AT&T, and CenturyLink offer fiber connections in some service areas, as does Google Fiber. Contact your ISP to determine whether fiber connections are available in your area now or will be available in the near future.

The conversion between the fiber connection entering a home and the Ethernet or coaxial WAN connection used to connect a router or gateway is performed by an optical network terminal (ONT), which is supplied by the fiber provider and installed in the home.

Fiber users rent the router or gateway, which resembles the router or gateway included with cable or DSL Internet service, from the fiber provider. The fiber router or gateway connects to the ONT. Some vendors offer a network box that incorporates a wireless router as an alternative to a separate ONT and router or gateway.

Fiber has the highest speeds and the longest distances of any network connection type. It is more expensive to install than other types of cable and wire, and it is more fragile as well. A key advantage of fiber is that, because data is carried in light, it is not subject to data interruptions from electrical interference, as the other media can be. [Chapter 3](#) discusses fiber in more detail.

## Satellite

**Satellite** Internet providers, such as HughesNet, StarBand, and WildBlue, use dish antennas similar to satellite TV antennas to receive and transmit signals between geosynchronous satellites and computers. Separate antennas are needed for satellite Internet and TV services. Satellite is ideal for areas where cable infrastructure is unavailable and for ships at sea. Weather such as rain, snow, and fog can impact satellite speeds.

### Note

Geosynchronous satellites orbit Earth's equator at a distance of more than 22,000 miles (approximately 35,000km). Because of their orbits and altitudes, they remain in the same location

in the sky at all times. In the Northern Hemisphere, you need an unobstructed view of the southern sky to make a connection. In the Southern Hemisphere, you need an unobstructed view of the northern sky to make a connection.

Satellite Internet services use external devices that are often called *satellite modems* to connect computers to satellite dishes. A satellite modem connects to the USB or Ethernet (RJ-45) port in much the same way DSL or cable modems do.

The FCC requires professional installation for satellite Internet service because an incorrectly aligned satellite dish with uplink capabilities could cause a service outage on the satellite it is aimed at. Setup software supplied by the satellite vendor completes the process.

### Note

Satellite connections can also be made between buildings to allow for high-speed exchange of data. In this scenario, a satellite dish needs to be installed on each building, and the dishes need to be in direct line of sight of each other. Internet access can also be offered in this manner.

## Cellular

Mobile devices offer many ways to connect to other devices, including sharing their Wi-Fi or cellular connections with one or more computers. The following sections discuss these approaches.

### Note

For the 220-1101 exam, you should know the following:

- Wireless/cellular data network configuration, including enabling and disabling a hotspot, tethering, and using Airplane mode
- Bluetooth configuration, including enabling Bluetooth, enabling pairing, finding a device for pairing, entering the appropriate PIN code, and testing connectivity
- Corporate and ISP email configuration, including POP3, IMAP, port and SSL settings, Exchange, and S/MIME
- Awareness of PRI updates, PRL updates, and baseband updates
- Radio firmware settings
- IMEI vs. IMSI definitions
- VPN configuration

## Wireless/Cellular Data Network

Wi-Fi connectivity is enabled the same way on a smartphone or tablet as with laptops or other types of computers. In addition, smartphones or tablets with cellular radios can share their connections with others.

To enable mobile device use on airplanes, where electronic communications are usually not permitted, Airplane mode is used to turn off Wi-Fi, cellular, and Bluetooth signals.

The following sections cover this more.

## Tethering

To use USB tethering on an Android, follow these steps:



- Step 1.** Connect a USB cable from your computer to the data port on your device.
- Step 2.** Select the USB tethering option on your device.
- Step 3.** If you are connecting a Windows computer, select the network type (Home) on the computer when prompted.
- Step 4.** Use your computer's web browser and other network features as usual.
- Step 5.** When you are finished, disable USB tethering.

### Note

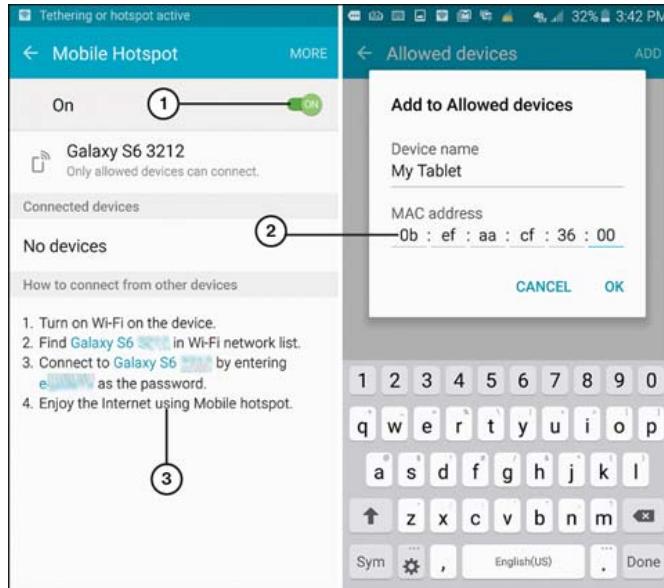
In Windows Device Manager, the tethered USB connection is listed as Remote NDIS-based Internet Sharing Device in the Network Adapters category.

## Hotspots

To use the mobile hotspot feature on an Android, follow these steps:



- Step 1.** Enable the mobile hotspot feature in the device's setup.
- Step 2.** Select how you want to share the connection wirelessly. Provide the SSID and password listed to any devices that will share the connection.
- Step 3.** If you decide to permit only allowed devices to connect, you must provide a name for each device and its MAC address. The MAC address is listed on a label attached to an external adapter. To find the MAC (physical) address for an internal network adapter, see the sidebar "Finding the Network Adapter's MAC (Physical) Address," in [Chapter 1, "Mobile Devices."](#)
- Step 4.** Open the Allowed Devices menu (see [Figure 2-13](#)). Click **Add**, enter the device name and address, and click **OK**.



1. Enabling mobile hotspot
2. Entering MAC address of device that will connect to mobile hotspot
3. Instructions for devices that will connect to mobile hotspot

**Figure 2-13** Entering the MAC Address of the Device That Shares a Hotspot’s Internet Connection

**Step 5.** Make the connection from your device just as you would with any other wireless Internet router or hotspot. Enter the password when prompted.

**Step 6.** When your devices are finished using the Internet, disable the hotspot setting in your smartphone or tablet.

## CAUTION

Some cellular providers charge an additional fee if you turn your cellular device into a hotspot or if you use tethering. Check with your mobile service provider for details. Also keep in mind that the data usage of every device connected to a mobile hotspot counts toward your total data allocation. If you’re not careful, using a mobile hotspot could cost you extra money in overages.

If you prefer to use a standalone mobile hotspot for your home, business, or vehicle, check with your wireless provider.

## Wireless Internet Service Provider

A **wireless Internet service provider (WISP)** is an Internet service provider that offers Internet access through a wireless connection to customers in areas where other options are unavailable. WISP involves installing small receiver antennas to connect users to Internet service that is transmitted from fixed wireless transmission towers. A clear line of sight must be available from the transmission tower to the customer site. In some cases, this means that the customer antenna must be placed on the roof or on its own stand, and trees might need to be trimmed to provide adequate signal quality.

To bring the network signal into the premises, coaxial cable connects from the antenna to a wireless modem, which is similar to a cable modem. To provide Internet access to multiple devices, connect

the modem to a router. Typical download speeds range from 10Mbps up to 100Mbps.

## Network Types

A *network* is a group of computers, peripherals, and software that are connected to each other and can be used together. Special software and hardware are required to make networks work.

### LAN

A **local area network (LAN)** is a group of computers and other devices that are usually located in a small area, such as a house, a small office, or a single building. The computers all connect to one or more switches, and a router grants the computers access to the Internet. A LAN is defined as a group of connected computers under one administrative organization. LANs can contain a wide variety of connected devices, such as computers, servers, routers, switches, printers, intrusion detection appliances, and firewalls.

LANs can be wired or wireless LANS (WLANS). Wired LANs can have high-speed connections with Ethernet unshielded twisted pair cable (UTP), shielded twisted pair cable (STP), or fiber. Legacy LANs were often connected by coax cables. [Chapter 3](#) discusses cables in more detail.

### WAN

A **wide area network (WAN)** is a group of one or more LANs over a large geographic area. Imagine that a company has two LANs, one in New York and one in Los Angeles. Connecting the two would result in a WAN. However, doing this requires the help of a telecommunications company to create the high-speed connection required for the two LANs to quickly communicate with each other. Each LAN requires a router to connect to the other.

WANs are administered by several different Internet service providers (ISPs), and the links are usually slower than with LAN connections.

### PAN

A **personal area network (PAN)** is larger than a LAN and smaller than a WAN. This type of computer network is used for communication by smartphones, tablets, and other small personal computing devices, typically using Bluetooth, IrDA (an infrared technology), wireless USB, Zigbee, or Z-Wave protocols. A PAN can be wired or wireless. Additional examples of devices in a PAN are wireless headsets, keyboards, mouse devices, printers, and bar code readers.

### MAN

A smaller version of a WAN is a **metropolitan area network (MAN)**. This type of network results when a company has two offices in the same city and makes a high-speed connection between them. A telecommunications company or ISP is needed for the high-speed links. MANs often consist of fiber networks around a city, and each one is administered by a single organization.

### SAN

A **storage area network (SAN)** is a special network that consists of computers that store vast amounts of information in blocks of data. The SAN storage servers reside in data centers both near and far, but to the users, it can appear to be attached to their local computer. Several SAN protocols and designs have been implemented.

The amount of data is growing rapidly, and data storage is now a major business for cloud-based storage providers such as Microsoft, Google, and Amazon.

## WLAN

A **wireless local area network (WLAN)** is a network made up of wireless computers and other devices that communicate via wireless transmissions, not cables and wires. A common type of WLAN is a Wi-Fi network in a home or office. A group of network access points that make up the WLAN can be configured to work together and can be managed with a specialized device called a **WLAN controller**.

## Using Networking Tools

220-1101  
Exam

**220-1101: Objective 2.8:** Given a scenario, use networking tools.

Specialized networking tools are needed to build network infrastructure. They can also help in running, terminating, and testing cable. For this short section, imagine that you are the network installer and are required to install a wired network for 12 computers.

To start, check with your local municipality to see if any rules and regulations govern running networking cable. Some municipalities require a person to have an electrician's license to run networking cable, but most require only an exemption of some sort that anyone can apply for at the town or county seat. Because of the low-voltage nature of network wiring (for most applications), some municipalities have no rules about running it. In urban areas, however, you need to apply for a permit beforehand and then, when you have finished the installation, have at least one inspection done.

Every good network starts with a plan. A diagram of the network, called a topology, acts as a map for computer placement. In this scenario, the diagram will have 12 wired connections to computers (known as *drops*), depicting where the cables will be run and where they will terminate. All cables will come out of a wiring closet and will be terminated in a small patch panel. On the other end, they will terminate at in-wall RJ-45 jacks near each of the computers. The next sections discuss each of the tools used to complete this job.

### Note

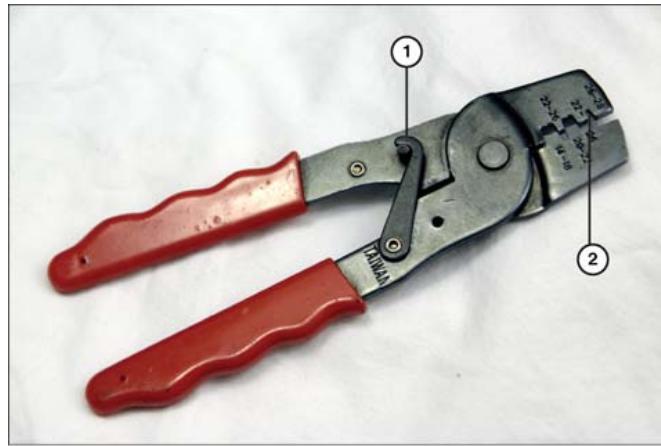
When working with computers and computer network equipment, standard household tools are not adequate for the job. A specialized network technician's toolkit is necessary for quality work. A quick Internet search for "networking toolkit" will return a full range of options in many price ranges. Networking toolkits are also available from nearly every retailer that sells computers and accessories.

## Cutting Tool

A good, sharp cutting tool is essential. You need to make a clean cut on the end of the network cable; scissors will not do. Instead, you need either cut pliers or other cable-cutting tools. Klein Tools ([www.kleintools.com](http://www.kleintools.com)) is an excellent manufacturer of these types of tools.

## Cable Stripper

A **cable stripper** is used to strip a portion of the plastic jacket off the cable to expose the individual wires. When the wires are exposed, you can separate them and get ready to terminate them. [Figure 2-14](#) illustrates a typical cable stripper.

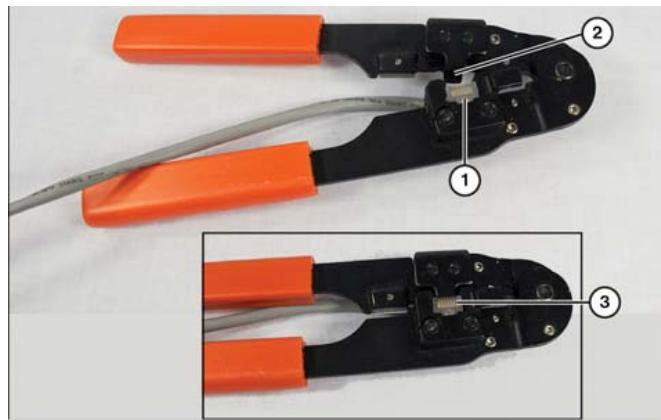


1. Release this clip to use the tool
2. Select the appropriate wire thickness based on the cable type

**Figure 2-14** A Cable (Wire) Stripper

## Crimper

A **crimper** attaches a connector to the end of raw twisted pair (TP) or coaxial cable. Two types of crimpers are available. If you are working with TP, you need an RJ-45 crimping tool (which often also works with RJ-11 telephone cable). After untwisting the wire pairs and aligning them according to the appropriate standard (typically T568B), insert them into an RJ-45 connector and push the cable and connector assembly into the crimper. Line up the crimper jaw with the recessed area of the connector and squeeze (see [Figure 2-15](#)).



1. Connector and cable assembly inserted into crimper
2. Crimping jaw lined up and ready to crimp
3. Squeeze handles to complete crimp

**Figure 2-15** Crimping an Ethernet Cable

If you are working with coaxial cable using F type connectors, a compression-crimping tool is recommended. It produces a better, more water-resistant connection than a hex-type crimper.

## Punchdown Tool

A **punchdown tool** (see [Figure 2-16](#)) punches the individual wires down into the 110 IDC clips of an RJ-45 jack and the patch panel. This “punching down” of the wires is the actual termination. The patch cables connect the various ports of the patch panel to a switch and connect the RJ-45 jacks to the computers.



**Figure 2-16** A Typical Punchdown Tool

## Multimeter

A **multimeter** is a flexible tool that tests both coaxial and TP cabling, as well as AC and DC voltage. (However, testing cables is easier with specially made cable testers.) When set for DC voltage, a multimeter can test computer power supplies and AC adapters. When set for continuity (CONT), it can be used as a cable tester. It can also test ohm (resistance) and ampere (amp, or current) levels.

All multimeters are equipped with red and black test leads. When used for voltage tests, the red lead is attached to the power source to be measured and the black lead is attached to ground.

Multimeters use two different readout styles: digital and analog. Digital multimeters are more common today because their costs have dropped. [Figure 2-17](#) shows a typical digital multimeter.



**Figure 2-17** Typical Digital Multimeter (Image ©fotosv, Shutterstock)

## Toner Probe

A **toner probe** kit consists of two parts:

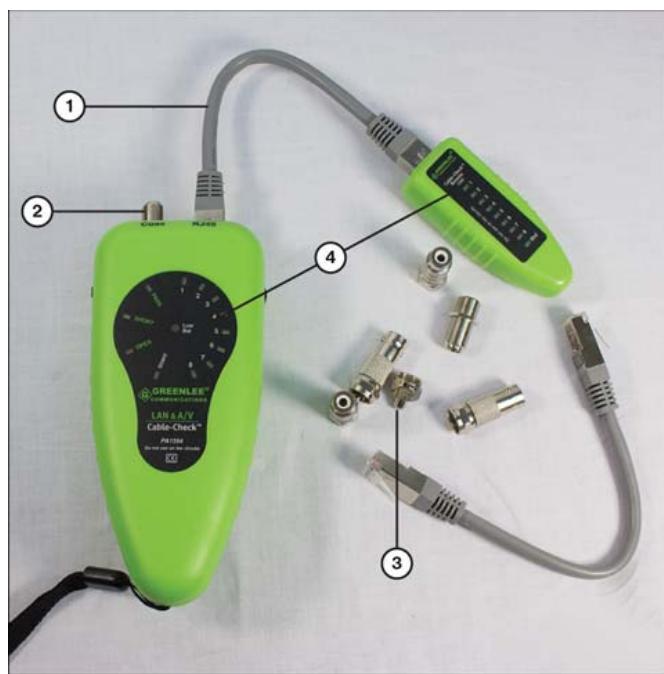
- **Tone device:** This device connects to one end of the network cable. When it is turned on, it sends a tone along the length of the cable.
- **Probing device:** This device, also known as an inductive amplifier, can pick up the tone anywhere along the cable length and at the termination point.

A toner probe is not as handy as a proper network cable tester because it tests only one pair of the wires. However, it is an excellent tool for finding individual phone lines and is commonly used for that.

## Cable Tester

A necessary item for a PC technician's toolkit is a proper network **cable tester**. This device includes a LAN testing unit that you plug into a port on the patch panel and a terminator that you use to plug the other end of the cable into the corresponding RJ-45 jack. This tool tests each wire in the cable and makes sure everything is wired properly.

Some cable testers, such as the one shown in [Figure 2-18](#), can also be used to test coaxial cable using F connectors, BNC connectors, or RCA connectors.



1. STP cable for testing patch panels
2. Threaded connector for testing coaxial cable
3. Adapters for various types of coaxial cable
4. Lights on remote and main unit light up as each line is tested

**Figure 2-18** A Typical Cable Tester Equipped for Testing RJ-45 and Coaxial Cable

## Loopback Plug

A **loopback plug** connects directly to the RJ-45 port of a PC's network adapter. When you use a loopback plug with a network diagnostic program, it simulates a network and tests whether the network adapter and TCP/IP are functioning properly.

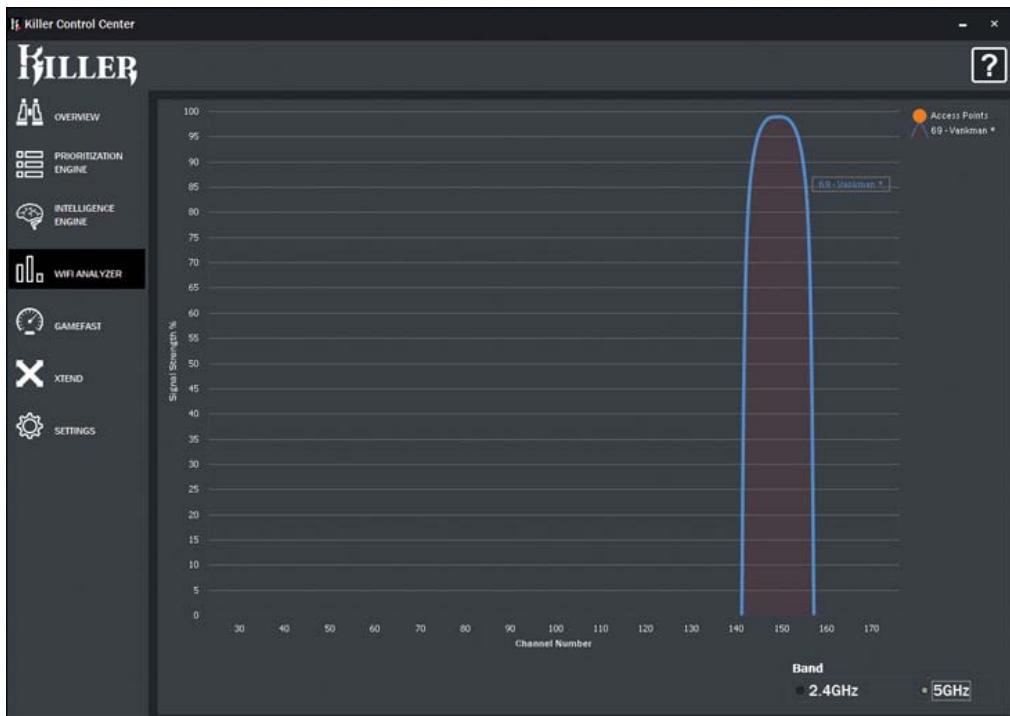
## Wi-Fi Analyzer

A **Wi-Fi analyzer** provides an easy-to-use view of both 2.4GHz and 5GHz wireless networks in the area. A Wi-Fi analyzer can be a standalone device, a program for a desktop computer, or an app on a smartphone.

An example is the Intel Killer Control Center Wi-Fi analyzer program for Windows. Figures 2-19 and 2-20 show the 2.4GHz and 5GHz wireless networks in an office building. Wi-Fi analyzers are helpful when determining what channel is best to use, as well as what channels are currently being used by other wireless access points.



**Figure 2-19** Using the Intel Killer Control Center Wi-Fi Analyzer to View the 2.4GHz Wireless Network in an Office



**Figure 2-20** Using the Intel Killer Control Center Wi-Fi Analyzer to View the 5GHz Wireless Network in an Office

You can also use smartphone apps such as Wi-Fi Analyzer (from olgor.com, available on Google Play), the built-in Wireless Diagnostics feature in macOS, and the **iwlist** command in Linux to learn about the channels used by wireless networks in the vicinity.

## Network Tap

A **network tap** allows network managers to “tap” into the data flowing through a network. A tap is a device that is inserted into the network cable and then makes an exact duplicate of network traffic. While the network traffic is sent on to its destination, the copy of traffic is sent to be stored or analyzed for security purposes. The tapped data allows the network to be analyzed without using software inside the network that could slow performance for users. A network tap also can be used for nefarious reasons by spies or hackers.

### Exam Preparation Tasks

As mentioned in the Introduction, you have several choices for exam preparation: the exercises here; [Chapter 10, “Final Preparation”](#); and the exam simulation questions in the Pearson Test Prep practice test software.

## Review All the Key Topics

Review the most important topics in the chapter, noted with the Key Topic icon in the outer margin of the page. [Table 2-11](#) lists these key topics and the page number on which each is found.



**Table 2-11** Key Topics for Chapter 2

Key Topic Element	Description	Page Number
Table 2-2	Common Protocols and Their Ports	61
Table 2-3	PoE Standards	71
Table 2-4	2.4GHz vs. 5GHz Wireless Bands	73
Section	Channels	75
Table 2-5	Bluetooth Classes	77
Table 2-6	Wireless Ethernet Standards	79
Table 2-7	IPv4 Address and Corresponding Subnet Mask	89
Section	IPv6 Address Types	92
Table 2-8	Static vs. Dynamic IP Addressing	97
Steps	NIC configuration	100
Table 2-9	Comparison of Network Connection Speeds	104
Table 2-10	Common DSL Services Compared	106
Steps	Enabling USB tethering	110
Steps	Enabling mobile hotspots	110

## Complete the Tables and Lists from Memory

Print a copy of [Appendix C, “Memory Tables”](#) (found online), or at least the section for this chapter, and complete the tables and lists from memory. [Appendix D, “Memory Tables Answer Key,”](#) also online, includes completed tables and lists to check your work.

## Define Key Terms

Define the following key terms from this chapter, and check your answers in the glossary:

protocol  
port  
FTP  
SSH  
Telnet  
SMTP  
DNS  
domain names  
DHCP  
HTTP  
HTTPS  
POP3  
NetBIOS

IMAP  
SNMP  
LDAP  
SMB  
CIFS  
RDP  
UDP  
TFTP  
Transmission Control Protocol (TCP)  
router  
firmware  
switch  
SOHO  
wireless access point (WAP)  
patch panel  
firewall  
PoE  
hub  
modem  
cable modem  
DSL modem  
optical network terminal (ONT)  
network interface card (NIC)  
software-defined network (SDN)  
channels  
Bluetooth  
pairing  
802.11b  
802.11a  
802.11g  
802.11n  
802.11ac (Wi-Fi 5)  
802.11ax (Wi-Fi 6 & Wi-Fi 6E)  
NFC  
radio frequency identification (RFID)  
Domain Name System (DNS)  
DHCP server  
file server  
NAS  
fileshare  
print server  
mail server  
syslog server  
web server

AAA server  
spam gateway  
unified threat management (UTM)  
IDS  
IPS  
load balancer  
proxy server  
legacy system  
embedded system  
Internet of Things (IoT)  
NAT  
DomainKeys Identified Mail (DKIM)  
Sender Policy Framework (SPF)  
Domain-based Message Authentication, Reporting, and Conformance (DMARC)  
virtual local area network (VLAN)  
virtual private network (VPN)  
cable  
DSL  
ADSL  
SDSL  
fiber  
satellite  
wireless Internet service provider (WISP)  
local area network (LAN)  
wide area network (WAN)  
personal area network (PAN)  
metropolitan area network (MAN)  
storage area network (SAN)  
wireless local-area network (WLAN)  
WLAN controller  
cable stripper  
crimper  
punchdown tool  
multimeter  
toner probe  
cable tester  
loopback plug  
Wi-Fi analyzer  
network tap

## Answer Review Questions

1. Complete the following chart with the information provided.

---

## **Wired**

---

← Fastest ----- Slowest →

---

## **Wireless**

---

Answer options:

- a.** Wireless Internet service provider (WISP)
  - b.** Satellite
  - c.** DSL
  - d.** Fiber
  - e.** Cable
  - f.** Cellular
- 2.** Which of the following situations requires the use of UDP but not TCP? (Choose all that apply.)
- a.** Video streaming
  - b.** Email
  - c.** Voice
  - d.** Online gaming
  - e.** SMS messaging
- 3.** When you pay online through your browser for an item in a shopping cart, which port is your browser likely using to transport information?
- a.** 68
  - b.** 80
  - c.** 443
  - d.** 53
- 4.** Which device enables communication outside a LAN?
- a.** Router
  - b.** Switch
  - c.** Wireless bridge
  - d.** Hub
- 5.** You have been asked to create a VLAN inside the company LAN. Which device will you configure?
- a.** A wireless bridge
  - b.** A managed switch
  - c.** The router subinterface
  - d.** The central hub
- 6.** Match the following devices with their definitions.

<b>Device</b>	<b>Definition</b>
Wireless access point	
Router	
Switch	

Device	Definition
Modem	
Firewall	
Hub	
Patch panel	

- a. Converts digital signals to analog, and analog signals to digital
  - b. Uses a MAC address to direct data to a specific computer
  - c. Acts as a junction point for network cabling
  - d. Allows networks to communicate with each other
  - e. Broadcasts data to all attached computers
  - f. Extends wired LANs into wireless space
  - g. Prevents unwanted intrusion from outside the network
- 7.** Under what circumstances do you use a WLAN controller?
- a. To extend the LAN to work on adjacent wireless networks
  - b. To improve Internet speeds to the LAN
  - c. For management of wireless LANs
  - d. To control costs of web connectivity at the network operations center
- 8.** Which protocol for accessing the Internet is used by all major operating systems, including Windows, macOS, Linux, Android, and iOS?
- a. APIPA
  - b. DHCP
  - c. Telnet
  - d. TCP/IP
- 9.** 192.168.28.10 is an example of which type of IP address?
- a. IPv6
  - b. Link local
  - c. IPv4
  - d. APIPA
- 10.** Given the IP address 192.168.28.10 and the subnet mask 255.255.0.0, what is the network portion of the address and what is the host portion?
- a. 192. = host, 168.28.10 = network
  - b. 192.168. = network, 28.10 = host
  - c. 192.168.28. = network, 10 = host
  - d. 192.168 = host, 28.10 = network
- 11.** Which of the following is the subnet mask for a network with 255 hosts?
- a. 255.255.255.255
  - b. 255.255.255.0
  - c. 255.255.0.0
  - d. 255.0.0.0

**12.** 127.0.0.1 and ::1 are both IP addresses. Which of the following statements are true? (Choose all that apply.)

- a. 127.0.0.1 is a usable address on a network.
- b. ::1 is an IPv6 address.
- c. 127.0.0.1 is an M.
- d. ::1 is a CIPS address.
- e. Both addresses are loopback addresses.

**13.** 10.0.0.1 is what type of IP address?

- a. Public
- b. Private
- c. APIPA
- d. Loopback

**14.** 169.254.0.1 is what type of IP address?

- a. Loopback
- b. Subnet mask
- c. DHCP
- d. APIPA

**15.** Which of the following statements best describes an advantage of IPv6 over IPv4?

- a. IPv6 is less complicated and easier to use.
- b. IPv6 automatically assigns IP addresses on a network.
- c. IPv6 translates domain names into IP addresses.
- d. IPv6 provides a dramatic increase in the number of available IP addresses.

**16.** Which of the following protocols automatically assigns IP addresses on a network?

- a. APIPA
- b. DHCP
- c. TCP/IP
- d. DNS

**17.** When you enter [www.mycompany.com](http://www.mycompany.com), the address is translated to a numeric IP address to establish a connection. Which of the following is the service that provides the translation?

- a. TCP
- b. UPnP
- c. DNS
- d. DHCP

**18.** As an IT technician, it is important for you to be familiar with the protocols and ports that various applications use to send and receive information across a network. Complete the following chart by adding the port numbers associated with each of the protocols listed.

- a. 443
- b. 80
- c. 22
- d. 21

- e. 110
- f. 143
- g. 53
- h. 25

Protocol	IMAP	FTP	HTTP	HTTPS	SMTP	DNS	SSH	POP3
Port								

- 19.** Which of the following statements best describes SMTP?
- a. SMTP is a protocol for sending email from your computer to a server.
  - b. SMTP is a naming system that links your computer's name with its IP address.
  - c. SMTP is a method for automatically assigning IP addresses to computers on a network.
  - d. SMTP is a protocol used to access the Internet.
- 20.** Which of the following is the family of IEEE standards used by Wi-Fi networks?
- a. 802.5
  - b. 802.11
  - c. 802.9
  - d. 802.3
- 21.** You have been asked to install a web-enabled soil monitor system for an agricultural company. What term describes this kind of device?
- a. Remote sensing router
  - b. Cloud-based network controller
  - c. NAT device
  - d. IoT device
- 22.** Identify the tool in the following figure.



- a. Cable tester
- b. Crimper
- c. Punchdown tool
- d. Cable stripper

# Chapter 3

## Hardware

**Understanding the physical aspects of computing is an essential requirement for a certified support technician. Although most working technicians become specialized in a few areas of hardware support, it is important to demonstrate a broad knowledge of the different components of computing on the A+ exam. This chapter covers the seven A+ 220-1101 exam objectives related to knowledge of hardware. These objectives may comprise 25 percent of the exam questions:**

- **Core 1 (220-1101): Objective 3.1:** Explain basic cable types and their connectors, features, and purposes.
- **Core 1 (220-1101): Objective 3.2:** Given a scenario, install the appropriate RAM.
- **Core 1 (220-1101): Objective 3.3:** Given a scenario, select and install storage devices.
- **Core 1 (220-1101): Objective 3.4:** Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards.
- **Core 1 (220-1101): Objective 3.5:** Given a scenario, install or replace the appropriate power supply.
- **Core 1 (220-1101): Objective 3.6:** Given a scenario, deploy and configure multifunction devices/printers and settings.
- **Core 1 (220-1101): Objective 3.7:** Given a scenario, install and replace printer consumables.

As a computer technician, you will need to know how the hardware components of a PC work together and be able to make appropriate hardware choices that best suit a client's needs. This chapter discusses the fundamental hardware topics covered on the CompTIA A+ exam.

### "Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to assess whether you need to read the entire chapter. [Table 3-1](#) lists both the major headings in this chapter and the "Do I Know This Already?" quiz questions covering the material in those headings so that you can assess your knowledge of these specific areas. The answers to the "Do I Know This

“Do I Know This Already?” quiz appear in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes and Review Questions.”

**Table 3-1** Do I Know This Already?™ Section-to-Question Mapping

Foundation Topics Section	Questions
Basic Cable Types	1–4
Installing RAM Types	5–7
Installing Storage Devices	8–10
Installing Motherboards, CPUs, and Add-on Cards	11–13
Power Supplies	14–16
Multifunction Devices/Printers and Settings	17–19
Print Technologies	20–22

## CAUTION

The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for the purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

- 1.** What is the most commonly used cable in an Ethernet network?
  - a.** STP
  - b.** Coax
  - c.** UTP
  - d.** Plenum
  
- 2.** Which of these video cables uses only analog video signals to transmit data?
  - a.** DisplayPort
  - b.** VGA
  - c.** HDMI
  - d.** DVI
  
- 3.** What is the latest version of USB?
  - a.** 3.1 Generation 2
  - b.** 4
  - c.** 3.0 Generation 3
  - d.** 3.5

**4.** Which of the following is not a video cable connector?

- a. S-Video
- b. VGA
- c. RJ-45
- d. HDMI

**5.** Which RAM type is a legacy type?

- a. SODIMM
- b. DDR3
- c. SDRAM
- d. DIMM

**6.** Which RAM type is designed for laptops?

- a. SODIMM
- b. DDR3
- c. SDRAM
- d. DDR5

**7.** Which of the following types of memory enables the system to correct single-bit errors?

- a. ECC
- b. DDR5
- c. Virtual RAM
- d. SODIMM

**8.** Which one of the following is not used with an SSD?

- a. M.2
- b. PCIe
- c. mSATA
- d. HDD

**9.** What is the method for replicating a single drive from two or more physical drives?

- a. RAID
- b. Incremental backup
- c. Hot swappable
- d. Hard drive duplication (HDD)

**10.** Which of the following is not a common RAID level?

- a. RAID 5

- b.** RAID 10
- c.** RAID 15
- d.** RAID 1

**11.** What does every CPU require?

- a.** Multithreading
- b.** Liquid cooling system
- c.** Virtual support
- d.** Heat sink

**12.** You have been asked to overclock a gaming system. Which places might you go to perform this task? (Choose two.)

- a.** System Settings
- b.** BIOS
- c.** Control Panel
- d.** UEFI

**13.** While fixing a PC, you notice that its date and time are wrong. What are the possible problems you should check? (Choose two.)

- a.** Date and Time settings
- b.** System Updates log
- c.** CMOS battery
- d.** Internal power supply connection

**14.** What function does a power supply perform?

- a.** Reduces DC power to protect components
- b.** Converts DC power to AC
- c.** Converts AC power to DC
- d.** Reduces AC power to safe levels for components

**15.** How are power supply capacities rated?

- a.** Watts
- b.** Amps
- c.** Voltage
- d.** Joules

**16.** Which term best describes a power supply that allows for the customization of connections?

- a.** Standard power supply
- b.** Modular power supply
- c.** Redundant power supply

- d.** Portable power supply
- 17.** Which of the following is not a common print configuration option on a multifunction device?

  - a.** Orientation
  - b.** Collation
  - c.** Ink flow
  - d.** Duplex printing
- 18.** Which printer driver is best suited for printing graphics?

  - a.** PCL
  - b.** PostScript
  - c.** Printer Control Language
  - d.** Apple Print
- 19.** Which printer driver is best suited for fast printing?

  - a.** PCL
  - b.** PDF
  - c.** RAM
  - d.** PostScript
- 20.** Which one of these printer types begins printing after the entire page is stored in its memory?

  - a.** Inkjet
  - b.** Impact
  - c.** Laser
  - d.** Thermal
- 21.** Which of the following is not part of the laser imaging process?

  - a.** Exposing
  - b.** Developing
  - c.** Compacting
  - d.** Fusing
- 22.** Which printer type uses filaments?

  - a.** Thermal
  - b.** Impact
  - c.** Inkjet
  - d.** 3D

## Foundation Topics

### Basic Cable Types

220-1101  
Exam

**220-1101: Objective 3.1:** Explain basic cable types and their connectors, features, and purposes.

The array of cable types in computing can be overwhelming, especially because cable technology is in a constant state of evolution. You need to know not only the kinds of cable, but also different versions of some types. This section organizes cables by their purpose, which should help you keep them straight. Some cables are uncommon and rarely encountered, but you need to be familiar with all the types in this section.

### Network Cables

Network cables covered here are different types of Ethernet cable. *Ethernet* is a term that is commonly used but not often completely understood. Briefly, Ethernet is a system of communication rules that allow computers to work together. Ethernet is considered a networking protocol (which is a bit different from an application protocol). It is concerned with physical cables and wireless standards, as well as the computer's network interface card (NIC). Ethernet cables are designed to standards that allow the protocols to send and receive messages between devices. Ethernet is not the only communication protocol in use, but it is by far the most common.

### Ethernet

Ethernet cable companies are always improving their product. Over time, higher data speeds have been achieved through better engineering of both cables and interface cards. This has created the necessity for categories defining the equipment they can be used with. Between the categories are grades of enhancement that are noted with letters (for example, Cat 5 and Cat 5e, or Cat 6 and Cat 6a).

Ethernet cables carry small voltage pulses (1 is voltage, 0 is no voltage) over a single frequency. This is known as *baseband transmission*. It is bidirectional, which means that hosts can send and receive data on one cable. The various capabilities are indicated in the cable categories. For example, 1000BASE-T indicates that the cable carries 1000Mb/s on a baseband signal over twisted pair (TP) cables. Cable categories and TP are explained in the sections that follow.

## Cat 5, Cat 5e, Cat 6, and Cat 6a

Category 5 (**Cat 5**), Category 5e (**Cat 5e**), Category 6 (**Cat 6**), and Category 6a (**Cat 6a**) are the most common of the standard cabling grades. They are suitable for use with both standard 10BASE-T and Fast Ethernet networking, and they can also be used for Gigabit Ethernet networks if they pass compliance testing. Cat 6, Cat 6a, Category 7 (Cat 7), and Category 8 (Cat 8) are capable of supporting 10GBASE-T (10GB) Ethernet networks. Cat 8 is capable of supporting 40GBASE-T (40Gb/s Ethernet) over shorter distances, compared to Cat 6 and Cat 7. [Table 3-2](#) provides the essential information about each of the TP cable types you need to know for the exam. Categories 5 through 6a are covered on the exam; Categories 3 through 8 are included in [Table 3-2](#) to add perspective. You should know the table well and be able to identify the bandwidth of each category.



**Table 3-2** Categories and Uses for TP Cabling

<b>Category</b>	<b>Network Type(s) Supported</b>	<b>Supported Speeds</b>	<b>Notes</b>
Cat 3	10BASE-T Ethernet	Up to 10Mb/s	Legacy; also supports Token Ring networks at up to 16Mb/s.
Cat 5	10BASE-T, 100BASE-T (Fast Ethernet)	Up to 100Mb/s	Uses 24-gauge wires.
Cat 5e	10BASE-T, 100BASE-T, 1000BASE-T (Gigabit Ethernet)	Up to 1000Mb/s	Enhanced version of Cat 5.
Cat 6	10BASE-T, 100BASE-T, 1000BASE-T (Gigabit Ethernet)	Up to 1000Mb/s (1Gb/s). Cat 6 cable can reach 10-Gigabit Ethernet speeds by reducing the length (from 328 ft) to less than 50 meters.	Often uses 22-gauge or 20-gauge wire pairs (both of which are thicker than 24-gauge wire).
Cat 6a*	10BASE-T, 100BASE-T, 1000BASE-T, 10GBASE-T (10Gb/s Ethernet)	Up to 10Gb/s	Enhanced version of Cat 6.
Cat 7	10BASE-T, 100BASE-T, 1000BASE-T,	Up to 10Gb/s	Uses 12-connector GG45 connector

Category	Network Type(s) Supported	Supported Speeds	Notes
	10GBASE-T (10Gb/s Ethernet)		(backward compatible with RJ-45).
Cat 8	10BASE-T, 100BASE-T, 1000BASE-T, 10GBASE-T (10Gb/s Ethernet), and 40GBASE-T (40Gb/s Ethernet)	Up to 40Gb/s	Has faster throughput over a shorter distance. The maximum cable length is 30m at either 25Gb/s or 40Gb/s.

\* Some vendors sold an enhanced version of Cat 6 that they called Cat 6e before the release of Cat 6a. Cat 6e is not an official standard.

No matter how fast they are, all of the copper Ethernet cable categories have a distance limitation of about 100m (about 300 ft.) before the data signal weakens and needs to be boosted by a switch, a hub, or a repeater.

## Plenum, PVC, and Direct Burial Cables

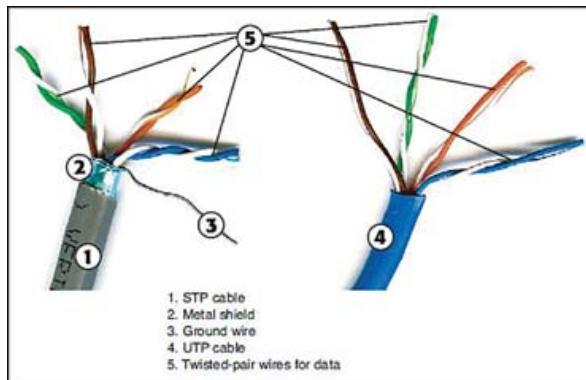
Two categories of TP cable exist, in terms of fire rating:

- **Standard:** Standard cable is suitable for patch cables between a NIC and a network jack or in a patch panel. This type of cable typically has a PVC jacket, which can create a lot of smoke when burned.
- **Plenum:** **Plenum** cable is designed for use in plenum space (that is, space used for HVAC air exchanges), such as in ventilator shafts, under floors, or between suspended ceilings and the permanent ceiling. Plenum cable produces less smoke when burned, produces a lower level of toxic chemicals when burned, and is typically self-extinguishing. Plenum cable jackets might be made from Teflon or from a modified version of PVC that produces less smoke than standard PVC when burned.

## Shielded Twisted-Pair (STP) vs. Unshielded Twisted-Pair (UTP)

Twisted-pair (TP) cabling is the most common of the major cabling types. The name refers to its physical construction: four twisted pairs of wire surrounded by a flexible jacket (**unshielded twisted pair**, or UTP) or various types of metal foil or braid (**shielded twisted pair**, or STP). STP uses the same RJ-45 connector as UTP but includes a metal shield for electrical insulation between the wire pairs and the outer jacket. STP is stiffer and more durable, but also more expensive and harder to loop through tight spaces than UTP. STP is used where electromagnetic interference (EMI) prevents the use of UTP cable.

Figure 3-1 compares the construction of STP and UTP cables.



**Figure 3-1** An STP Cable (Left) Includes a Metal Shield and a Ground Wire for Protection Against Interference, While a UTP Cable (Right) Does Not

UTP and STP cable can be purchased in prebuilt assemblies or can be built using bulk cable and connectors.

**Direct burial** cables are versions of UTP and STP cables designed with enough protection on the outer jacket (commonly known as a CMX jacket) to withstand weather, ground moisture, and even placement directly in water. The cable can be made to withstand the elements in a few ways. Some are double jacketed, some are filled with a waterproofing gel, and some have a waterproofing tape encasing the twisted pairs. If possible, it is better to run cable through electric conduit, for the most protection. These cables are for normal Ethernet use outdoors with IoT devices or security systems.

## T568B (EIA-568B) and T568A (EIA-568A) Standards

The de facto wire pair standard for all types of Ethernet UTP cables is known as **T568B**, or EIA-568B. This is the wire order, from left to right when looking at the top of the connector:

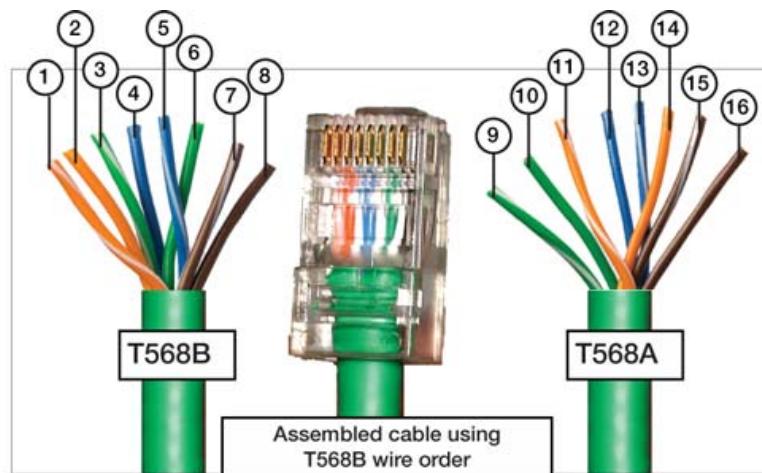
1. Pin 1—Orange/white stripe
2. Pin 2—Orange
3. Pin 3—Green/white stripe
4. Pin 4—Blue
5. Pin 5—Blue/white stripe
6. Pin 6—Green
7. Pin 7—Brown/white stripe
8. Pin 8—Brown

The **T568A** (EIA-568A) standard swaps the positions of the orange and green wires used in T568B. This is the wire order, from left to right when looking at the top of the connector:

1. Pin 1—Green/white stripe
2. Pin 2—Green
3. Pin 3—Orange/white stripe
4. Pin 4—Blue
5. Pin 5—Blue/white stripe
6. Pin 6—Orange
7. Pin 7—Brown/white stripe
8. Pin 8—Brown

[Figure 3-2](#) illustrates cable pairings for a T568B cable, a T568B cable with a vconnector, and a T568A cable.

**Key Topic**



1. Pin 1 – Orange/white stripe
2. Pin 2 – Orange
3. Pin 3 – Green/white stripe
4. Pin 4 – Blue
5. Pin 5 – Blue/white stripe
6. Pin 6 – Green
7. Pin 7 – Brown/white stripe
8. Pin 8 – Brown
9. Pin 1 – Green/white stripe
10. Pin 2 – Green
11. Pin 3 – Orange/white stripe
12. Pin 4 – Blue
13. Pin 5 – Blue/white stripe
14. Pin 6 – Orange
15. Pin 7 – Brown/white stripe
16. Pin 8 – Brown

**Figure 3-2** T568B (Left) and T568A (Right) Wire Pairs and an Assembled T568B Cable

### Note

You can create a crossover cable by building one end to the T568B standard and the other end to the T568A standard.

## Fiber

**Fiber-optic cabling** transmits signals with light instead of with electrical signals, which makes it immune to electrical interference. Fiber is more expensive than copper and requires more experience to install, but it offers the benefit of longer distances for large amounts of data and can be used in areas where electrical interference makes copper cable problematic. Because of the expense, fiber is used primarily as a backbone between networks.

Fiber-optic cable comes in two major types:

- **Single-mode fiber:** Has a thin core (between 8 and 10 microns) and is designed to carry a single light ray long distances (60km or farther). Single-mode cable uses a laser diode as a light source. It is typically used by cable TV and telephone companies.
- **Multimode fiber:** Has a thicker core (62.5 microns) than single-mode fiber and carries multiple light rays for short distances (up to 10km). Multimode cable uses an LED light source. It is typically used in local area networks (LANs) and metropolitan area networks (MANs).

An important point to remember about the two fiber types is that single-mode fiber, with its smaller core, carries less data up to 60km (36 miles) before the signal needs to be boosted. Multimode fiber carries much more data, but only for about 10km (6 miles).

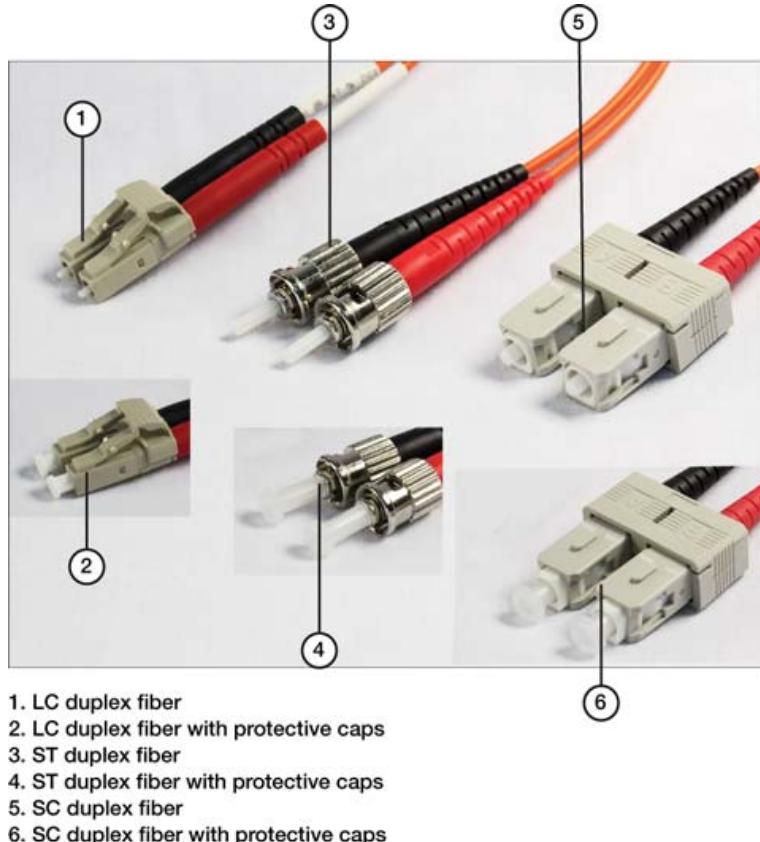
Fiber-optic cabling can be purchased prebuilt, but if you need a custom length, it should be built and installed by experienced cable installers because of the expense and risk of damage. Some network adapters built for servers are designed to use fiber-optic cable. Otherwise, media converters are used to interconnect fiber-optic cable to conventional cables on networks.

Fiber-optic devices and cables use one of several connector types. The following are the most common:

- **Subscriber connector (SC):** Uses square connectors
- **Lucent connector (LC):** Uses square connectors
- **Straight tip (ST):** Uses round connectors

These connectors can be used singly or in pairs, depending on the implementation. Figure 3-3 illustrates duplex (paired) SC, LC, and ST multimode cables.

**Key Topic**



**Figure 3-3** SC, LC, and ST Fiber-Optic Cable Connectors Compared

### Note

If you need to interconnect devices that use two different connector types, use adapter cables that are designed to match the connector types and other characteristics of the cable and device.

## Coaxial

**Coaxial** cabling is the oldest type of network cabling; its data wires are surrounded by a wire mesh for insulation. Coaxial cables, which resemble cable TV connections, are not popular for network use today because they must be run from one station directly to another station instead of to or from a hub/switch. However, coaxial cabling is used for most cable TV, cable Internet, and satellite TV installations, as well as CCTV cameras used for security.

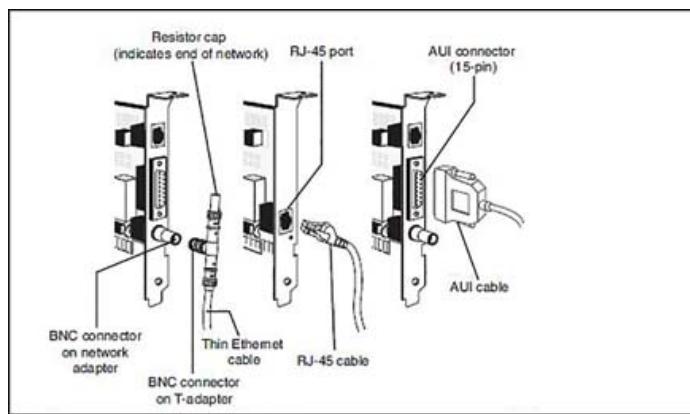
## Legacy 10Mb/s Ethernet Coaxial Cable Standards

Coaxial cabling creates a bus topology. With an Ethernet bus topology, all network members are added to the same physical coaxial cable line to communicate with each other. Each end of the cable must be terminated so that signals are contained. A big disadvantage of the bus is that if any part of the bus fails, the entire network fails.

The oldest Ethernet standard, 10BASE5, uses a very thick coaxial cable (RG-8) attached to a NIC through an AUI transceiver that uses a “vampire tap” to connect the transceiver to the cable. This type of coaxial cable is also referred to as *Thick Ethernet*, or *Thicknet*.

*Thin Ethernet*, also referred to as *Thinnet*, *Cheapernet*, and *10BASE2 Ethernet*, was used for low-cost Ethernet networks before the advent of UTP cable. The coaxial cable used with 10BASE2 is referred to as RG-58. This type of coaxial cable connects to network cards through a T connector that bayonet-mounts to the rear of the network card using a BNC connector. The arms of the T are used to connect two cables, each running to another computer in the network.

If the workstation is at the end of a network, a terminating resistor is connected to one arm of the T to indicate the end of the network. If a resistor is removed, the network fails; if a station on the network fails, the network fails. [Figure 3-4](#) shows both of these connection types. Note that some 10Mb/s Ethernet cards are combo cards that might feature both legacy connector types and, on some models, an RJ-45 jack.



**Figure 3-4** Combo UTP/BNC/AUI Ethernet Network Cards (Left and Right), Compared with a UTP/STP-Only Ethernet Card (Center) and Cables

## RG-59 and RG-6 Coaxial Cable

Two other types of coaxial cable are common in cable Internet, satellite Internet, and fixed wireless Internet installations:

- **RG-59:** This cable is used in older cable TV and satellite TV installations, as well as in CCTV security installations; it uses 75-ohm resistance. RG-59 uses a 22-gauge (AWG) center conductor and a single outer shield. It is designed for signals up to 50MHz.
- **RG-6:** This cable uses the same connectors as RG-59 but has a larger diameter with dual shielding. It is used in cable TV/Internet, satellite TV/Internet, fixed wireless Internet/TV service, and closed-circuit (security) TV; it uses 75-ohm resistance. RG-6 uses an 18-gauge (AWG) center conductor, which can carry a signal farther than RG-59. RG-6 is also available in quad-shielded versions. RG-6 can carry signals up to 1.5GHz, making it much better for HDTV signals.

BNC connectors are used for CCTV cameras and for some types of video projectors. BNC connectors are crimped to the coaxial cable and use a positive-locking bayonet mount.

**F type** connectors are used for cable, satellite, and fixed wireless Internet and TV service. F type connectors can be crimped or attached via compression to the coaxial cable. High-quality cables use a threaded connector. However, some F type connector cables use a push-on connector, which is not as secure and can lead to a poor-quality connection. [Figure 3-5](#) compares BNC and F type connectors on an RG-6 coaxial cable.



1. F type connector  
2. BNC connector

**Figure 3-5** F Type Connector and BNC Connector on RG-6 Cables

A two-way splitter such as the one shown in [Figure 3-6](#) reduces signal strength by 50 percent (3.5dB) on each connection. Splitting the signal only once usually does not cause issues with your TV or Internet signal. However, if you need to split your signal, contact your TV or Internet provider for a splitter, or ask what type of booster is recommended for your installation.



**Figure 3-6** A Two-Way Coaxial Splitter

### Note

Many antennas used for over-the-air digital TV now include a small inline booster that is powered by a 500mA USB connection or a small AC adapter. The booster helps improve range and bring in more stations.

## Video Cables

When selecting a monitor or projector for use with a particular video card or integrated video port, it is helpful to understand the physical and feature differences between different video connector types, such as VGA, DVI, HDMI, DisplayPort component/RGB, BNC, S-video, and composite. [Table 3-3](#) provides an overview of these connector types.



**Table 3-3** Video Connector Types Overview

Connector	Signal Type	Base Resolution	Maximum Resolution (60Hz Refresh Rate)	HDCP Support	3D Support	Audio Support
VGA	Analog	640×480 graphics, 720×480 text	2048×1536*	No	No	No
HDMI	Digital, analog	VGA	7680×4320 8K <sup>†</sup>	Yes	Yes‡	Yes
DVI	Digital, analog <sup>§</sup>	VGA	1920×1200** 2560×1600 <sup>††</sup>	Varies	No	No
DisplayPort	Digital, analog	VGA	8K	Yes	Yes	Yes
BNC	Analog	VGA	1080p	No	No	No
Composite	Analog	480i	480i	No	No	No
S-Video <sup>#‡</sup>	Analog	480i	480i	No	No	No
Component	Analog	720p	1080i	No	No	No

\* Recommended resolutions are lower because of excessive interference

† HDMI 2.1 or higher

§ DVI-D is digital only; DVI-I supports analog and digital signals; DVI-A is analog only

\*\* Single-link

†† Dual-link

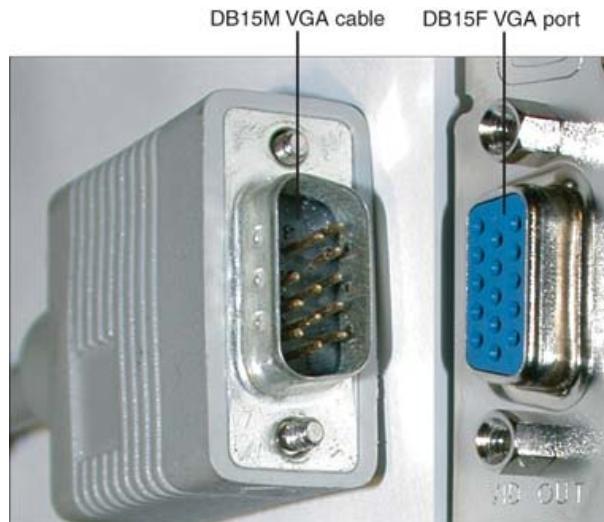
#‡ S-video splits luma and chroma signals for a better picture than composite; composite combines these signals

## VGA

**Video Graphics Array (VGA)** is an analog display standard. It is largely a legacy technology, but you might still encounter it on older systems. By varying the levels of red, green, or blue per dot (pixel) onscreen, a VGA port and monitor can display an unlimited number of colors. However, practical color limits are based on the video card's memory and the desired screen resolution.

The base resolution (horizontal × vertical dots) of VGA is 640×480. An enhanced version of VGA is Super VGA (SVGA), which typically refers to 800×600 VGA resolution.

A VGA card made for use with a standard analog monitor uses a DB15F 15-pin female connector, which plugs into the DB15M male connector used by the VGA cable from the monitor. [Figure 3-7](#) compares these connectors.



**Figure 3-7** DB15M (Cable) and DB15F (Port) Connectors Used for VGA Video Signals

Most video cards with DVI ports use the DVI-I dual-link version, which provides both digital and analog output and supports the use of a VGA/DVI-I adapter for use with analog displays. (See [Figure 3-22](#) in the “DVI-I to VGA” section, later in this chapter, to see some adapters and refer to [Figure 3-11](#) in the “DVI” section, later in this chapter, to see a DVI-D cable and DVI-I port.)

The less common DVI-A version supports analog signals only. The maximum length for DVI cables is 5m.

## HDMI

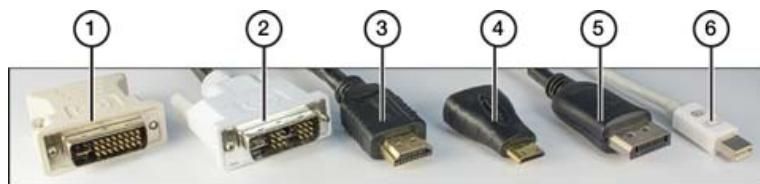
Video cards and systems with integrated video that are designed for home theater use support a standard known as ***High-Definition Multimedia Interface (HDMI)***. HDMI has the capability to support both digital audio and video through a single cable. HDMI ports are found on HDTVs, as well as home theater hardware such as amplifiers and Blu-ray and DVD players, and many recent laptop and desktop PCs running Windows or Linux. All versions of HDMI support HDCP and digital rights management (DRM) for copyright protection.

The most recent HDMI standard, version 2.1a, supports video resolutions and refresh rates including 8K60 and 4K120, as well as resolutions up to 10K. The most common HDMI port is Type A, which has 19 pins. It is used to achieve high-definition resolutions such as  $1920 \times 1080$  (known as 1080p or 1080i). For more about HDMI specifications, visit [www.hDMI.org](http://www.hDMI.org).

## Mini-HDMI

The HDMI 1.3 and later specifications also define a mini-HDMI connector (Type C). It is smaller than the Type A plug but has the same 19-pin configuration. The HDMI 1.4 specification defines a micro-HDMI connector (Type D), which uses the same 19-pin configuration, but in a connector the size of a micro USB plug.

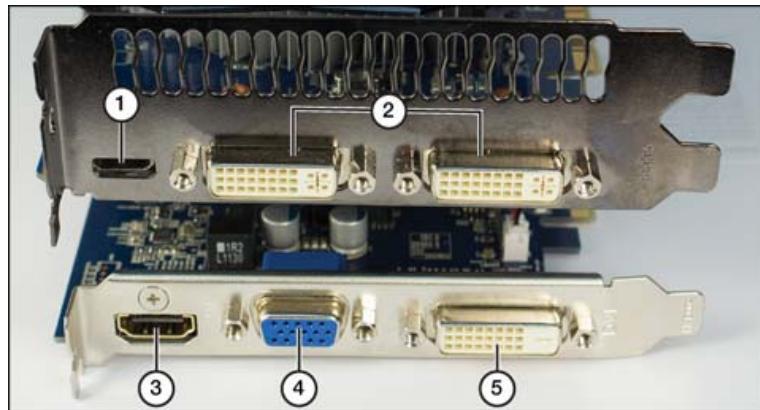
Regardless of the version in use, HDMI hardware uses connectors similar to the ones shown in [Figure 3-8](#) and the ports shown in [Figure 3-9](#). Typical cable lengths range up to 40 feet, but higher-quality copper cables can be longer.



1. DVI-I dual-link
2. DVI-D single-link
3. HDMI
4. Mini-HDMI
5. DisplayPort
6. Mini DisplayPort

**Figure 3-8** HDMI Cable Connectors Compared to DVI and DisplayPort Cable Connectors





1. Mini HDMI
2. DVI-I Dual-link
3. HDMI
4. VGA
5. DVI-D Dual-link

**Figure 3-9** HDMI, DVI, and VGA Ports on the Rear of Two Typical PCIe Video Cards

## DisplayPort

**DisplayPort** was designed by the Video Electronics Standards Association (VESA) as a royalty-free digital interface to replace DVI and VGA. It offers similar performance to the HDMI standard.

Unlike HDMI or DVI, which can connect only one display per port, DisplayPort enables multiple displays to be connected via a single DisplayPort connector.

DisplayPort utilizes packet transmission, similar to Ethernet and USB. Each packet transmitted has the clock embedded (whereas DVI and HDMI use a separate clocking signal).

DisplayPort connectors are not compatible with USB, DVI, or HDMI; however, devices that support dual-mode DisplayPort (DisplayPort++) technology are capable of sending HDMI or DVI signals with the use of the appropriate adapter. DisplayPort offers a maximum transmission distance of 3m over passive cable and, in theory, up to 33m over active cable. A DisplayPort connector has 20 pins, with pins 19 and 20 being used for 3.3V, 500mA power on active cables. The mini-DisplayPort cable shown in [Figure 3-8](#) also uses a 20-pin connector.

DisplayPort cables can be up to 15m long, but quality decreases with length.

[Figure 3-10](#) shows a high-performance video card with a DisplayPort connector.



1. DisplayPort
2. HDMI
3. DVI-I dual-link
4. DVI-D dual-link

**Figure 3-10** DisplayPort, HDMI Port, and DVI Ports

DisplayPort is available in the following versions:

- **DisplayPort 1.1:** Maximum data transfer rate of 8.64Gb/s.
- **DisplayPort 1.2:** Maximum data transfer rate of 17.28Gb/s. Introduces mini-DisplayPort connector and support for 3D.
- **DisplayPort 1.3:** Maximum data transfer rate of 32.4Gb/s, with support for 4K, 5K, and 8K UHD displays.
- **DisplayPort 1.4:** Maximum data transfer rate of 32.4Gb/s. Introduces Display Stream Compression (DSC) 1.2 support.
- **DisplayPort 2.0:** Maximum data transfer rate of 80Gb/s. Introduces support for resolutions beyond 8K, improved configurations for multiple displays, and 4K and beyond for VR.

The Thunderbolt digital I/O interface is backward compatible with mini-DisplayPort, so you can connect mini-DisplayPort displays to either a Thunderbolt or mini-DisplayPort connector. [Figure 3-10](#) depicts various display ports. Thunderbolt is explained further in the upcoming section “Thunderbolt.”

## DVI

The **Digital Visual Interface (DVI)** port is a digital video port that is used by many LED and LCD displays with a 25-inch or smaller diagonal measurement. The DVI-D supports only digital signals and is found on digital LCD displays. Most of these displays also support analog video signals through separate VGA ports. [Figure 3-11](#) depicts DVI-I digital and DVI-D analog cable.

**Key Topic**



**Figure 3-11** DVI-I Video Port and DVI-D Video Cable

**Note**

DVI single-link omits some of the connectors in the DVI interface, limiting the maximum resolution. DVI dual-link uses all the connectors, enabling higher resolutions than are possible with DVI single-link.

## Peripheral Cables

Cables are highly engineered for the specific tasks they are intended to perform, but the growing number of cable types can become a burden. Designing cables that perform more than one function, such as combining the capability to charge batteries and transfer data, is an option that technology users appreciate.

## Thunderbolt

**Thunderbolt** is a high-speed interface capable of supporting hard disk drives, SSDs, HDTVs up to 4K resolution, and other types of I/O devices. Thunderbolt includes PCIe and DisplayPort digital signals into a compact interface that runs from 2x to 8x faster than USB 3.0, and 2x to 4x faster than USB 3.1 Gen 2. Intel introduced Thunderbolt in 2011. Thunderbolt was initially adopted by Apple, which uses it in the recent and

current MacBook product lines. Thunderbolt is also available on some high-end desktop motherboards that use Intel chipsets.

Thunderbolt is available in three versions that use two different port types: Thunderbolt 1 and Thunderbolt 2 use the same physical port as mini-DisplayPort. The newest version, Thunderbolt 3, uses the same physical connector as USB Type C. All three versions support up to six Thunderbolt devices per port and use daisy chaining to connect devices to each other.

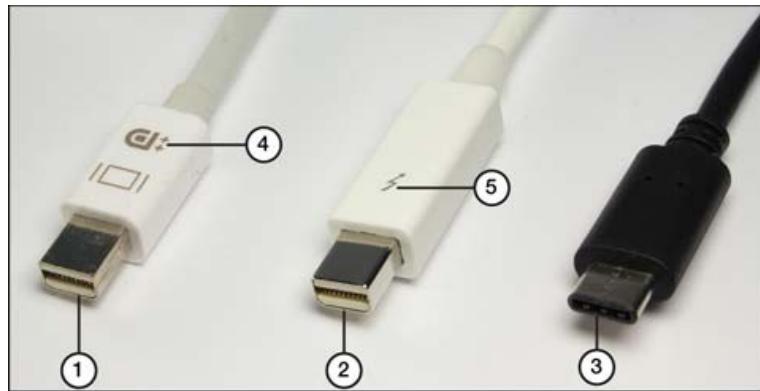
[Table 3-4](#) compares Thunderbolt versions to each other.

**Table 3-4** Thunderbolt Interface Overview

Interface Version	Maximum Interface Speeds	Connection Type	Supported Protocols	Maximum Cable Length*
Thunderbolt 1	10Gb/s	Thunderbolt 1*	Thunderbolt 1, DisplayPort	3m (9.8 ft.)
Thunderbolt 2	20Gb/s	Thunderbolt 1*	Thunderbolt 1–2, DisplayPort 1.2	3m (9.8 ft.)
Thunderbolt 3	40Gb/s	USB Type C	Thunderbolt 1–3, DisplayPort 1.2, PCIe 3, USB 3.1, USB Power Delivery	3m (9.8 ft.)
Thunderbolt 4	40Gb/s	USB Type C	Thunderbolt 3–4, DisplayPort 2.0, USB4, 4x PCI Express 3.0	3m (9.8 ft.)

\* Using copper cable. Some vendors are now shipping optical cable in lengths up to 30m.

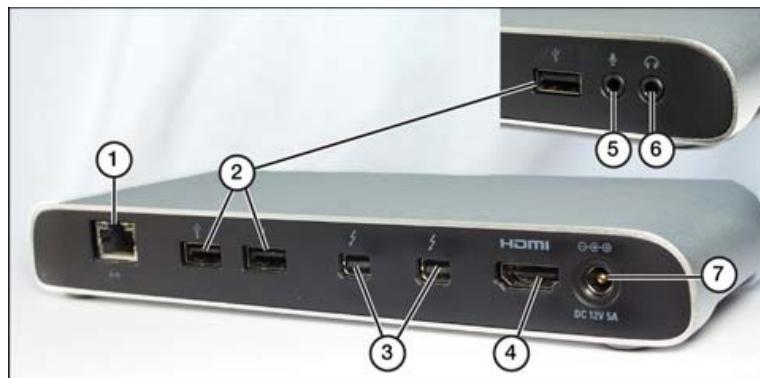
[Figure 3-12](#) compares a Thunderbolt 2 cable with a USB Type C cable (the cable used by Thunderbolt 3) and a mini-DisplayPort cable, which uses the same physical connector as a Thunderbolt cable. USB is explained in greater detail in the next section.



1. Mini-DisplayPort+ cable
2. Thunderbolt 1/Thunderbolt 2 cable
3. USB Type C – Thunderbolt 3 cable
4. DisplayPort++ icon
5. Thunderbolt icon

**Figure 3-12** Mini-DisplayPort, Thunderbolt 1/Thunderbolt 2, and USB Type-C/Thunderbolt 3 Cables

Because of Thunderbolt's high bandwidth, it can be connected to docks that feature multiple port types. [Figure 3-13](#) shows a typical Thunderbolt 2 dock that also provides USB 3.0 ports, an HDMI video port, a Gigabit Ethernet port, and audio headphone and microphone jacks.



1. Gigabit Ethernet port
2. USB 3.0 ports
3. Thunderbolt 2 ports
4. HDMI port
5. Microphone port
6. Headset port
7. AC power jack

**Figure 3-13** A Typical Thunderbolt 2 Dock

## USB

Universal Serial Bus (USB) ports have long since replaced PS/2 (mini-DIN) mouse and keyboard ports on recent systems. They can be used for printers, mass storage, and other external I/O devices. Some form of USB port is also used by most mobile devices,

game consoles, many network devices, cars and trucks, smart TVs, and other electronics, making USB truly universal.

Most recent desktop systems have at least 8 USB ports, and many systems support as many as 10 or more front- and rear-mounted USB ports. Laptops typically have three or four USB ports, and Windows and Android generally have at least one USB or USB-On-the-Go port.

USB ports send and receive data digitally.

## USB-C

The traditional USB Type A (USB-A) has been the standard USB connector for years, but USB Type C (USB-C) is now the industry standard for transmitting power and data. Hundreds of technology companies came together to develop the initial USB-A connector; the same group, known as USB Implementers Forum (USB-IF), has moved forward with **USB-C**, a connector that is easier to connect (reversible, with no up or down side to the plug); the appropriate adapter allows backward compatibility to USB 2.0. (USB-C connectors are shown previously in [Figures 3-12](#) and [3-13](#), and are shown again in [Figures 3-15](#) and [3-16](#) in the following sections.)

The USB-C standard refers to the connector type on the cable, not the data transfer rate of the cable. USB-C can handle any data rate, from USB-2 to USB-3.2.

## USB 2.0, USB 3.0, USB 3.1, USB 3.2, and USB4

The following USB ports are included on the A+ certification exam:

- **USB 2.0** (Hi-Speed)
- **USB 3.0** (SuperSpeed), also known as USB 3.1 Generation 1
- USB 3.1 (SuperSpeed+), also known as 3.1 Generation 2
- USB 3.2 Gen 2x2 (SuperSpeed+), rated at 20Gb/s

There are four versions of USB in common use. The industry uses the term *Hi-Speed USB* for USB 2.0, *SuperSpeed USB* for USB 3.0, and *SuperSpeed+ USB* for USB 3.1 Gen 2. USB 1.0 is legacy and is not on the A+ exam.

With any version of USB, a single USB port on an add-on card or motherboard is designed to handle up to 127 devices through the use of multiport hubs and daisy-chaining hubs. USB devices are Plug and Play (PnP) devices that are hot swappable (which means they can be connected and disconnected without turning off the system).

Additional USB ports can be added with any of the following methods:

- Motherboard connectors for USB header cables
- Hubs
- Add-on cards

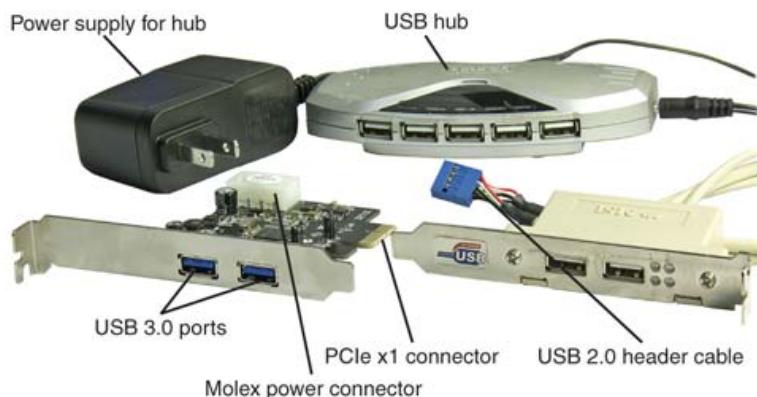
Some motherboards have USB header cable connectors, which can enable additional USB ports on the rear or front of the computer. Most recent cases also include front-mounted USB ports, which can also be connected to the motherboard. Because of vendor-specific differences in how motherboards implement header cables, the header cable might use separate connectors for each signal instead of the more common single connector for all signals.

USB generic hubs are used to connect multiple devices to the same USB port, distribute both USB signals and power via the USB hub to other devices, and increase the distance between the device and the USB port. Two types of generic hubs exist:

- **Bus powered:** Bus-powered hubs can be built into other devices, such as monitors and keyboards, or they can be standalone devices. Different USB devices use different amounts of power, and some devices require more power than others. A bus-powered hub provides no more than 100 milliamps (mA) of power to each device connected to it. Thus, some devices fail when connected to a bus-powered hub.
- **Self-powered:** A self-powered hub, on the other hand, has its own power source; it plugs into an AC wall outlet. A self-powered hub designed for USB 1.1 or USB 2.0 devices provides up to 500mA of power to each device connected to it, whereas a self-powered hub designed for USB 3.0/3.1/3.2 devices provides up to 900mA of power to each device. USB4 devices provide up to 5A to each device. Note that USB hubs are backward compatible with previous USB versions. A self-powered hub supports a wider range of USB devices than a bus-powered hub.

Add-on cards can be used to provide additional USB ports as an alternative to hubs. One advantage of an add-on card is its capability to provide support for more recent USB standards. For example, you can add a USB 3.0 card to a system that has only USB 1.1/2.0 ports, to permit use of USB 3.0 hard drives at full performance. Add-on cards for USB 1.1 or USB 2.0 ports connect to PCI slots on desktop computers and CardBus or ExpressCard slots on laptop computers, whereas USB 3.0 cards connect to PCIe x1 or wider slots on desktop computers and ExpressCard slots on laptop computers.

[Figure 3-14](#) illustrates a typical USB 3.0 card, a USB 2.0 self-powered hub, and a USB 2.0 port header cable.



**Figure 3-14** USB 2.0 and 3.0 Hardware

Table 3-5 provides an overview of USB standards.



**Table 3-5** USB Standards Overview

Version	Marketing Name	Speeds Supported	Maximum Cable Length*	Notes
1.1 (legacy)	USB	12Mb/s 1.5Mb/s	3m	
2.0	Hi-Speed USB	480Mb/s	5m	Also supports USB 1.1 devices and speeds
3.2 Gen 1 (also known as USB 3.0 and USB 3.1 Gen 1)	SuperSpeed USB	5Gb/s	† 15m	Also supports USB 1.1 and 2.0 devices and speeds
3.2 Gen 2 (also known as USB 3.1 Gen 2)	SuperSpeed+ USB	10Gb/s	†	Also supports USB 1.1, 2.0, 3.0/3.1 Gen 1 devices and speeds
USB 3.2 Gen 1x2	Superspeed +	10Gb/s	†	Uses two lanes of data
3.2 Gen 2x2	Superspeed+ USB	20Gb/s	†	Uses two lanes of data USB-C only
USB4 Gen 2x2	USB4	20Gb/s	20Gb/s	2m

<b>Version</b>	<b>Marketing Name</b>	<b>Speeds Supported</b>	<b>Maximum Cable Length*</b>	<b>Notes</b>
USB4 Gen3x2	USB4 40Gb/s	40Gb/s	2m	

\* To exceed recommended or maximum cable lengths, connect the cable to a USB hub or use an active USB extension cable.

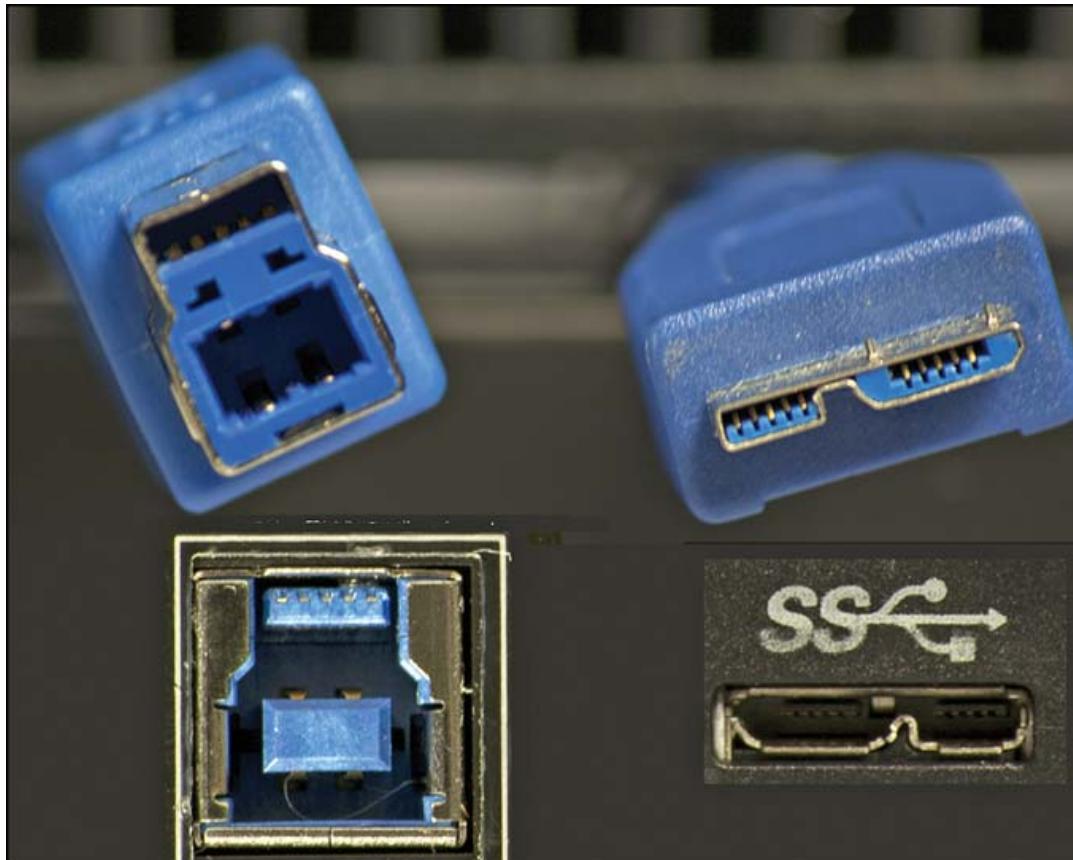
† 3m is the recommended length, but no maximum cable length has been established for these versions of USB.

## USB 3.2

USB 3.2 is actually two standards in one:

- *USB 3.2 Gen 1* is the new name for USB 3.0 and USB 3.1. Anytime you see a reference to USB 3.2, keep in mind that USB 3.1 Gen 1 and USB 3.0 is the same standard. Although USB 3.1 Gen 1 is the same standard as USB 3.0, vendors continue to use the original USB 3.0 name.
- *USB 3.2 Gen 2* has new USB 3.1 features. USB 3.2 Gen 2 (often referred to simply as USB 3.2) runs at speeds up to 10Gb/s (2x the speed of USB 3.0/USB 3.1 Gen 1). It is backward compatible with USB 1.1, 2.0, and 3.0/3.1 Gen 1.

Both USB 3.2 Gen 1 and Gen 2 use the same cables and connectors as USB 3.0. However, some USB 3.2 Gen 2 ports support the newer reversible connector, USB Type C, which can be used by both hubs and devices. Some systems, such as the second motherboard similar to the ones shown in [Figure 3-15](#), include both a Type C USB 3.1 port and a standard Type A USB 3.1 Gen 2 port. USB 3.2 Gen 2x2 is available only in the USB Type C connector.



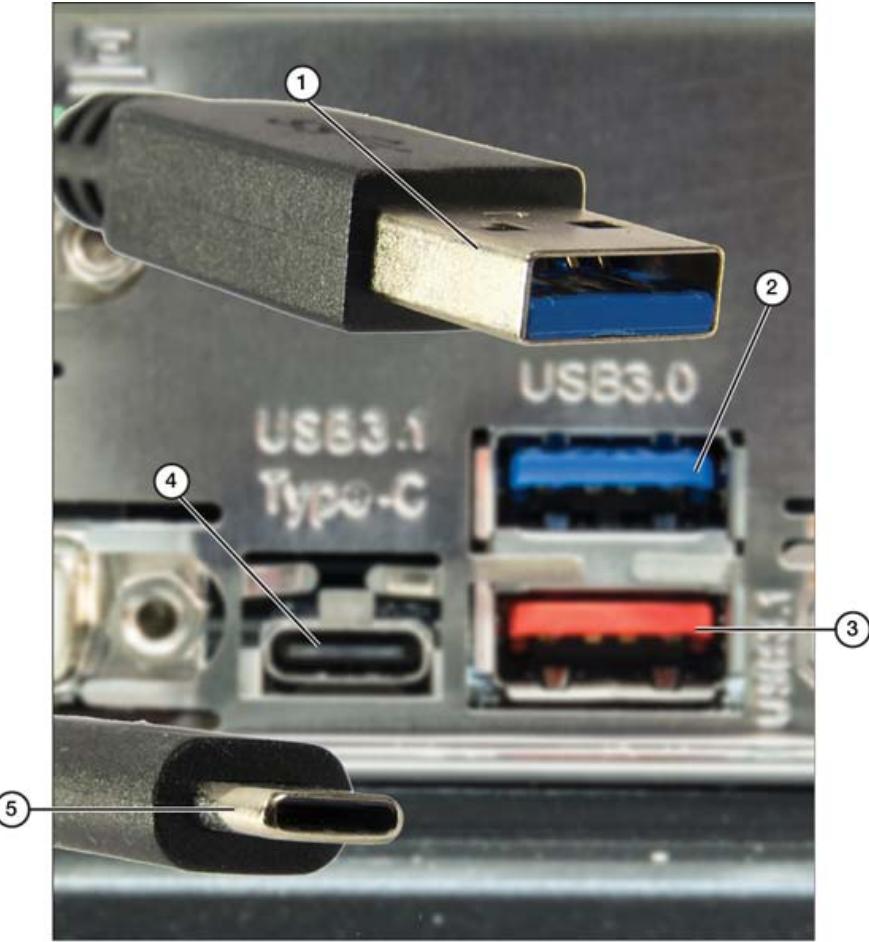
**Figure 3-15** USB 3.0 Standard-B (Left) and Micro-B (Right) Cables and Receptacles

### Note

Although USB Type C connectors also support older USB standards, it is unlikely that vendors would use it for USB 3.0, USB 2.0, or USB 1.1 ports.

Other USB standards, such as USB Power Delivery and USB Battery Charging, take advantage of other features in the USB Type C port. For more information about USB 3.2, USB Type C, USB Power Delivery, or USB Battery Charging, see the official USB website, [www.usb.org](http://www.usb.org).

Figure 3-16 illustrates USB 3.0 Type A and Type C cable and USB 3.1 Gen 2 ports.



1. USB 3.0/3.1 Type A cable
2. USB 3.0 Type A port
3. USB 3.1 Type A port
4. USB 3.1 Type C port
5. USB 3.1 Type C cable

**Figure 3-16** USB 3.0/3.1 Type A and Type C Ports and Cables

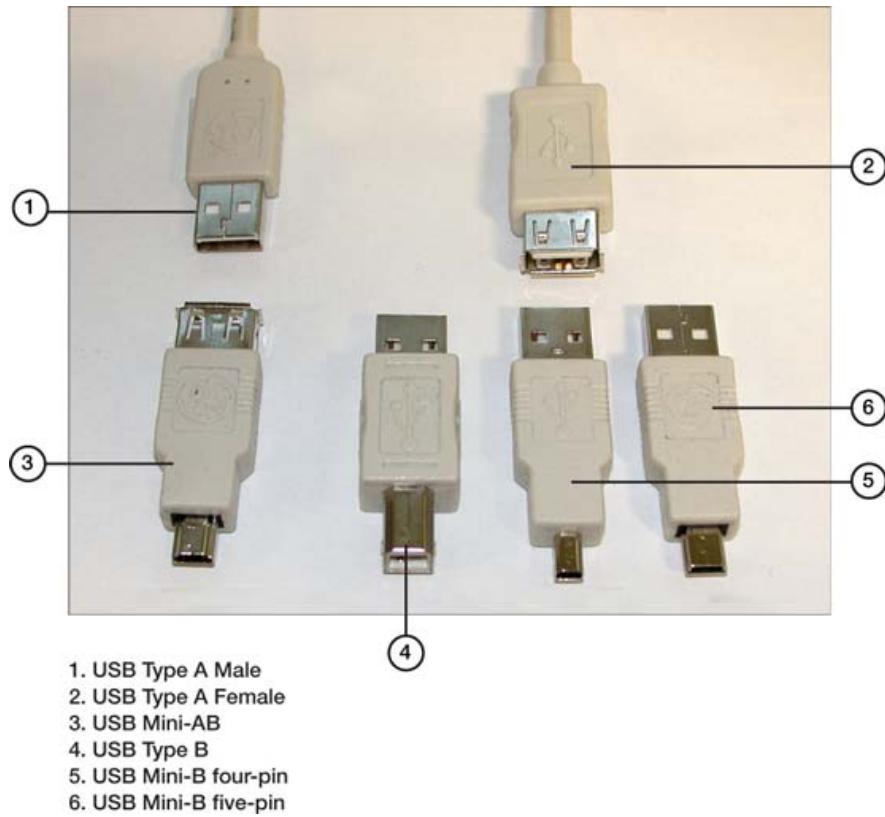
## USB4

Although USB4 is not on the A+ exam, it is important to keep up with new technologies and protocols. USB4 was introduced in 2019 and has two versions, USB4 2x2 and USB4 3x2. USB4 2x2 has a maximum data transfer speed of 20Gb/s, and USB4 3x2 has a maximum data transfer speed of 40Gb/s. Both versions are available only in USB Type C connectors.

## USB Adapters

USB cable adapter kits enable a single cable with replaceable tips to be used for the following tasks:

- Type A male to female, to extend a short cable
- Type A female to Type B connectors, to enable a single cable with multiple adapter tips to work with various types of peripherals (see [Figure 3-17](#))



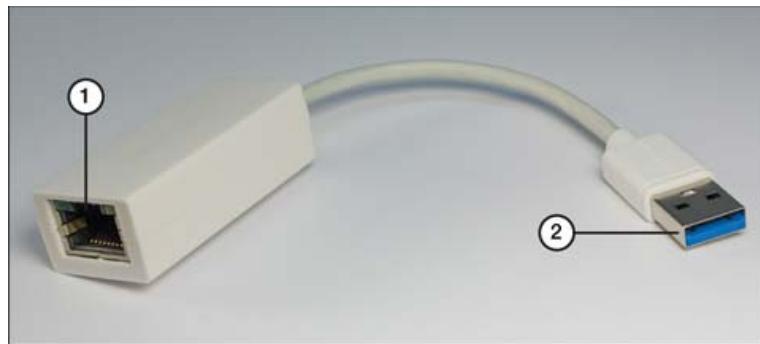
**Figure 3-17** USB 2.0 Cable Kit, Including a Type A Male/Female Cable and Several B-Type Connectors

- Type A female to USB-On-the-Go, for use with tablets or smartphones (see [Figure 3-18](#))



**Figure 3-18** USB-On-the-Go to Type A Adapter, which Enables a Standard USB Cable to Work with Devices That Use the Micro-A Connector

- USB to Ethernet, to enable a device without an Ethernet port to connect to a wired network (see [Figure 3-19](#))



1. Gigabit Ethernet  
2. USB 3.0 Type A

**Figure 3-19** A Typical USB 3.0 to Gigabit Ethernet Adapter

## Peripheral Cables: Serial

In years past, a device connected to a computer via a serial cable plugged into a serial port. **Serial** means that the data bits flow in a line, one after the other, over the cable. Serial connections were designed for the relatively low speed of telephone modem communication but were also used for other devices, such as keyboards, mouse devices, and other peripheral devices.

Serial ports and cables were usually compared to parallel ports and cables, where multiple bits flow at once. Serial cables conformed to the RS-232 standard. Printers were the most common devices to be connected with parallel ports, but now most printers are connected with USB cables or via Ethernet cables on networks.

USB cables have replaced serial cables, but it is possible to use a USB-to-serial adapter to connect to an older machine, if necessary.

## Hard Drive Cables

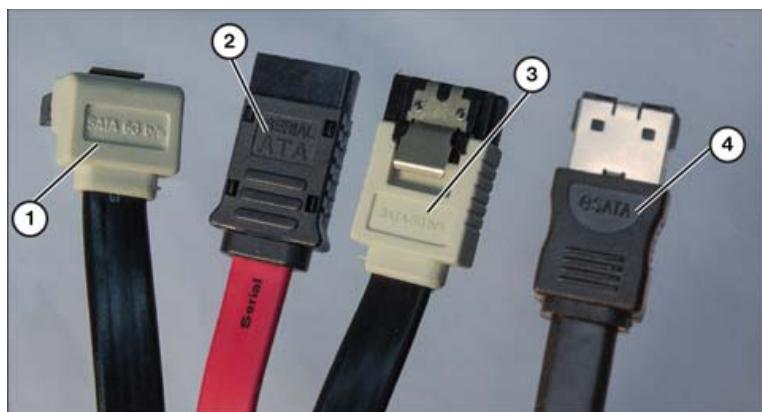
Hard drive cables are built to carry data to and from the motherboard. As data rates have increased, cable designs have changed to keep up with the data speeds. This section describes some of the hard drive cables technicians encounter.

## SATA Cables

At one time, hard drives were connected to motherboards with Advanced Technology Attachment (ATA) cables. These cables had a ribbonlike appearance, with multiple wires carrying data between the bus and the hard drive.

**Serial Advanced Technology Attachment (SATA)** cables are next-generation serial cables that carry high-speed data. SATA cables are used inside computer cases and offer not only the advantage of high speed, but also the benefit of better airflow inside the box.

External SATA (eSATA) cables allow for external drives to be mounted at the same data rate. eSATA has better shielding to protect the cable and the data. To prevent the use of thinner SATA cables from being used outside the case, eSATA cables have a different connector. [Figure 3-20](#) depicts SATA and eSATA cables. (Note the thicker cable and different keying between cables 3 and 4.)



1. Right-angle SATA 6Gb/s cable end with locking clip
2. Standard SATA 1.5-3Gb/s cable end
3. Straight SATA 6Gb/s cable end with locking clip
4. eSATA cable end

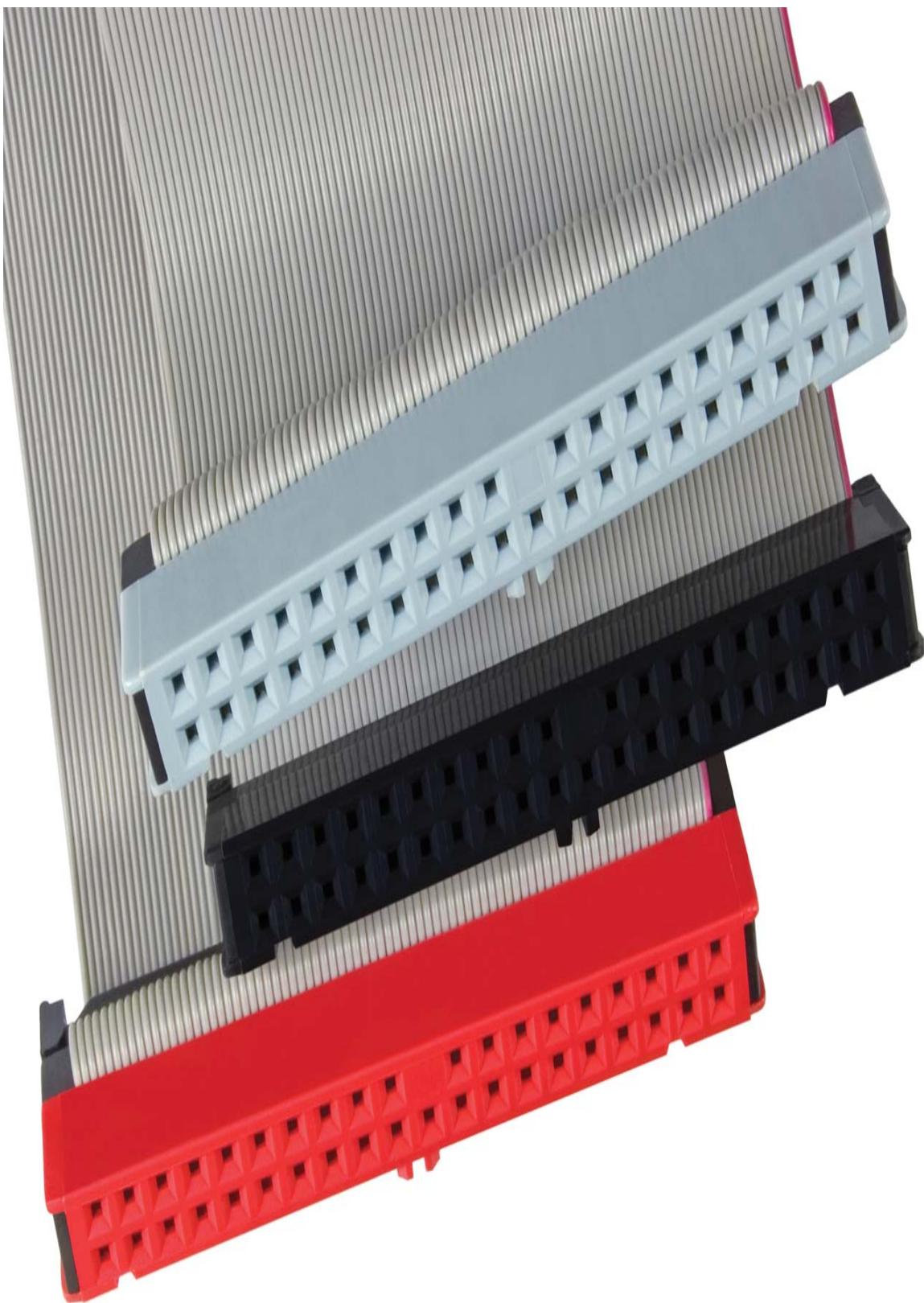
**Figure 3-20** SATA and eSATA Cables Compared

## IDE Cable

An **Integrated Drive Electronics (IDE)** cable is a standard cable type for connecting devices to a motherboard inside a computer case. Older hard drives have IDE connectors, and an IDE cable is one that accommodates them. SATA and SSD storage drives are more common, but you should be able to recognize an IDE hard drive and an IDE connector on a motherboard so that you know whether you need an IDE cable to get them working.

An IDE cable typically has three: one for the motherboard that splits into two connectors. This way, you can attach two hard drives to a motherboard with only one cable.

If you need to service an older computer that has only IDE connectors, but you have a SATA drive, you can solve the problem with a SATA-to-IDE adapter. [Figure 3-21](#) depicts a typical IDE connector.



**Figure 3-21** A Typical IDE Cable (Image © Kaspri, Shutterstock)

## **SCSI**

As with their IDE cable cousins, **Small Computer System Interface (SCSI)** cables have been replaced by SATA cables inside computers. Most motherboards were designed for SATA and IDE connections, but because SCSI is less common, it requires an **expansion card** to connect a hard drive.

The advantages of a SCSI drive system is that up to 7 (or sometimes 15) SCSI drives can be daisy-chained together; for comparison, an IDE connector supports only 2 drives. At one time, SCSI drives were the fastest option, but that is no longer the case: SATA and SSD are faster. On the downside, SCSI was more expensive to purchase and more complicated to configure. Of course, these advantages and disadvantages have been rendered moot by the newer technologies.

## **Adapters**

With any advance in technology, there tends to be a period of time when the old overlaps with the new, or when competing technologies need to find a way to get along. Physical cable adapters are often the short-term (and economical) answer to technical compatibility problems during an upgrade cycle. This section briefly explains the adapters listed in the A+ objectives.

### **DVI to HDMI**

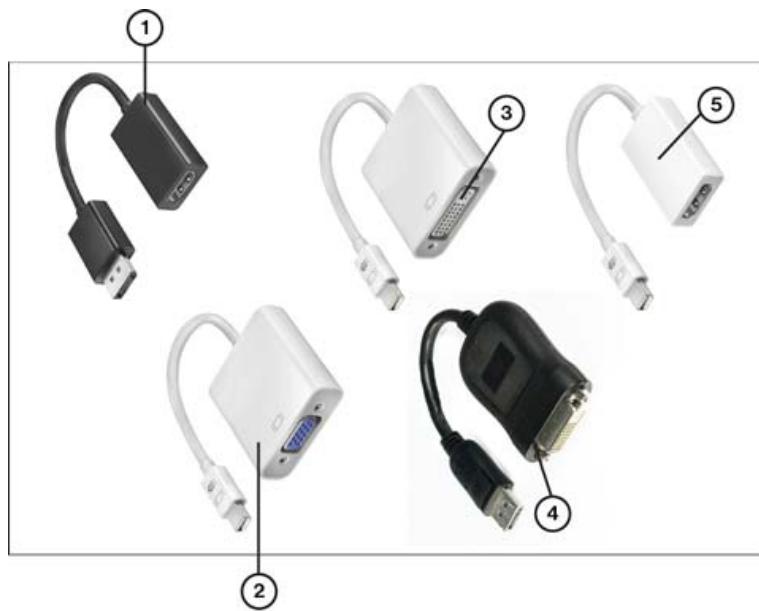
Because HDMI uses the same video signals as DVI, DVI-to-HDMI cables or adapters are widely available. Usually only the video transmits through these adapter cables, but some newer graphics cards allow for HDMI audio over DVI, which eliminates the need for a separate sound cable connection.

### **USB to Ethernet**

USB-to-Ethernet adapters (refer to [Figure 3-19](#)) enable a device without an Ethernet port to connect to a wired network. These common connectors are available in a wide range of prices and qualities.

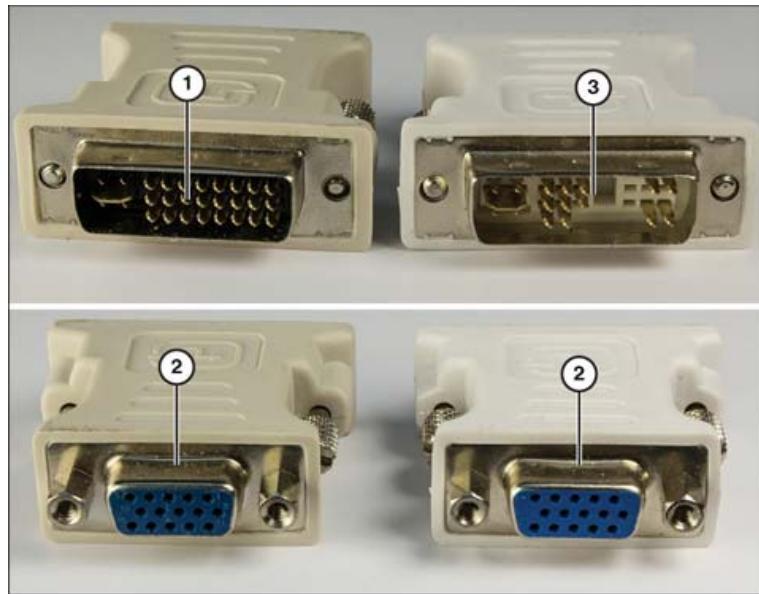
### **DVI-I to VGA**

DVI-I includes both VGA-compatible analog video and DVI digital video. The DVI-I-to-VGA adapters in [Figures 3-22](#) and [3-23](#) enable VGA displays to work with DVI-I ports on video cards.



1. DisplayPort to HDMI
2. Mini-DisplayPort to VGA
3. Mini-DisplayPort to DVI-I
4. DisplayPort to DVI-D
5. Mini-DisplayPort to HDMI

**Figure 3-22** Adapters for Mini-DisplayPort and DisplayPort to Other Display Types



1. DVI-I dual-link
2. VGA (DB15)
3. DVI-I single-link

**Figure 3-23** Single-Link and Dual-Link DVI-I-to-VGA Adapters

## Connector Types

As mentioned earlier, the array of cable types in computing can be daunting. This is even more so with the connector types because many cables can use more than one connector type. To help keep them straight, this section reviews all the networking connector types listed in the A+ objectives. Some of them are legacy types—and they are identified as such—but you might encounter a lot of legacy equipment and, therefore, should be familiar with all the types listed.

**Table 3-6** briefly summarizes the connector types you should know. Most are discussed in this chapter. If a figure is available to show each connector, it is listed in the last column of the table.



**Table 3-6** Network Connector Types

Type	Description/Application	Status	Figure
<b>RJ-11</b>	Standard phone jack. Smaller than RJ-45.	Current	
<b>RJ-45</b>	Standard Ethernet cable connector.	Current	<a href="#">Figures 3-2 and 3-4</a>
F Type	Type of coax connector used with satellite boxes, set-top boxes, and CATV.	Current	<a href="#">Figure 3-5</a>
Straight Tip (ST)	The standard fiber-optic connector with a bayonet-style insert and clip. Usually used in pairs with one fiber of inbound data and one fiber of outbound data. Uses round connectors.	Current and most common in use	<a href="#">Figure 3-3</a>
Subscriber Connector (SC)	Similar to ST, but uses square connectors.	Current	<a href="#">Figure 3-3</a>
Lucent Connector (LC)	Similar to ST, but uses square connectors.	Current	<a href="#">Figure 3-3</a>
Punch-down Block	Used for Ethernet cable connections to wall jacks and cross-connect racks in telecom closets. (See <a href="#">Chapter 2</a> .)	Current	<a href="#">Figure 2-16</a>
USB	Universal Serial Bus. Most common connector currently in use	Current	<a href="#">Figures 3-15 and 3-16</a>

Type	Description/Application	Status	Figure
<b>microUSB</b>	Smallest of the USB connector types. The USB type for many non-Apple phones.	Current/to be displaced by USB-C	
<b>miniUSB</b>	About half the size of USB-A. Common for external storage, cameras, and so on.	Legacy, but still in use	Figures 3-12 and 3-17
USB-C	Newest reversible USB connector. Should replace other USB types.	Current	Figure 3-12
<b>DB9</b>	Nine-pin serial connector that was once common on PCs. Once used for peripherals such as mouse devices and keyboards. Can be used for serial communications to networking equipment. Also used with a DB9-to-USB adapter to PCs without DB9 ports.	Legacy, but still in specialized use	
<b>Lightning</b>	Apple mobile device connector used for data and power.	Current	
SCSI	Used internally (hard drives) or externally (printers, storage, and so on).	Legacy	
eSATA	Used for connecting external storage. Thicker than internal SATA cables.	Current	Figure 3-20
<b>Molex</b>	Not a networking connector. Delivers power from the power supply to various drives and the motherboard inside a PC.	Legacy, but still around; replaced by SATA	

## Installing RAM Types

**220-1101: Objective 3.2:** Given a scenario, install the appropriate RAM.

220-1101  
Exam

RAM is like a work table, in that it holds every project that the CPU is working on. The operating system, open applications, and all kinds of hidden processes use the RAM workspace when the device is running. If you get too many projects piled up onto a small work table, things get awkward and inefficient; the work will not go as smoothly as it could with more workspace. For a computer, adding more RAM is like getting a bigger table for sorting everything and spreading out for smoother working. Installing more RAM improves transfers between the CPU and both the RAM and hard drives.

The contents of RAM are temporary, and RAM is much faster than magnetic or SSD storage: RAM speed is measured in nanoseconds (billions of a second), while magnetic and SSD storage is measured in milliseconds (thousandths of a second).

Ever-increasing amounts of RAM are needed as operating systems and applications get more powerful and add more features. Because RAM is one of the most popular upgrades to add to any laptop or desktop system during its lifespan, you need to understand how RAM works, which types of RAM exist, and how to add RAM to provide the biggest performance boost to the systems you maintain.

RAM is in a continual state of evolution, and it is no surprise that the list of RAM types has grown to be quite complicated—not just because there are so many developments, but because RAM is so often described in acronyms that do not define the differences of the types. [Table 3-7](#) provides a review of RAM development from [Chapter 1](#).

**Table 3-7** RAM Review

Acronym	Meaning	Note
<b>RAM</b>	Random access memory	Volatile memory that is not for storage
SDRAM	Synchronous dynamic RAM	Combines static RAM and dynamic RAM
SDR SDRAM	Single data rate SDRAM	Legacy
DDR SDRAM <b>DDR3, DDR4, and DDR5</b>	Double data rate SDRAM	DDR3 through DDR5 are currently in use in most computers
DIMM	Dual Inline Memory Module	Form factor used in desktops
<b>SODIMM</b>	Small Outline DIMM	Form factor used in laptops
<b>Virtual RAM</b>	Virtual RAM	Uses part of the hard drive to expand the RAM
ECC RAM	Error correction code RAM	Memory that enables the system to correct single-bit errors and notify if larger errors occur

When you upgrade a computer, you need to know a few important details:

- **Form factor:** Most computers in service use DDR3, DDR4, or DDR5. Laptops use SODIMMs of each DDR type.

- **Memory speed:** If you plan to add a module, make sure it is the same speed as the existing module. If you plan to replace the modules, buy a matched set of modules in the fastest speed supported by the system.
- **Memory timing:** The most common way to refer to memory timing is by its column address strobe (CAS) value. It is usually marked on the label with a CL value. If you install memory modules that use different CAS values, the computer could become unstable and crash or lock up.

Memory modules of the same type with memory chips of the same speed can have different CAS latency (CL) values. CL refers to how quickly memory column addresses can be accessed. A lower CL value provides faster access than a higher CL value. CL values increase when comparing different types of memory.

Most, but not all, memory module labels indicate the CL value. For modules that are not labeled, look up the part number for details.

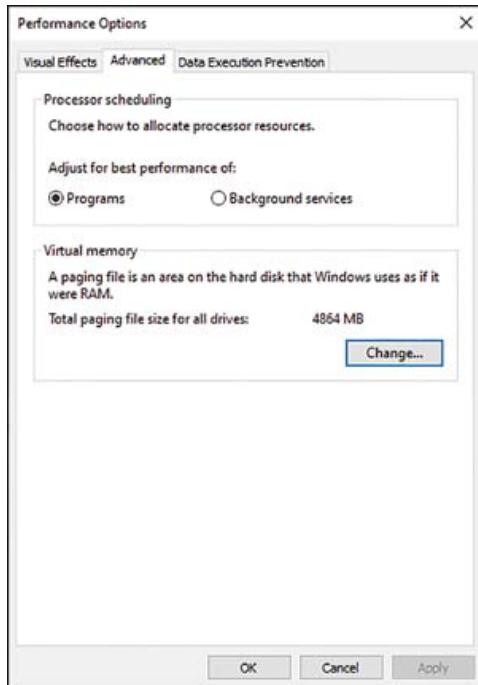
To determine the correct memory to use for a memory upgrade, use one of the following methods:

- **Use the interactive memory upgrade tools available from major third-party memory vendors' websites:** These tools list the memory modules suitable for particular laptops, and some can be used to detect the currently installed memory. Crucial System Scanner is a useful tool for showing what is currently installed and what is compatible. For more information, visit [www.crucial.com/usa/en/systemscanner](http://www.crucial.com/usa/en/systemscanner).
- **Check the vendor's memory specifications:** You can determine part numbers by using this method, but it works best if memory must be purchased from the laptop vendor instead of from a memory vendor.

Synchronous DRAM (SDRAM) and DDR (double data rate) SDRAM were the first two generations of RAM in sync with the processor bus (the connection between the processor, or CPU, and other components on the motherboard). They used 168-pin and 184-pin DIMMs to attach to the motherboard. These are legacy versions and are mentioned here for perspective on the evolution of RAM. The following section discusses the types of RAM that are important to know.

## Virtual RAM

Virtual RAM, or virtual memory (also known as the paging file), uses part of the hard drive to expand the RAM. This allows users to run more apps than the RAM could otherwise handle. To make adjustments to the virtual memory on a Windows 10/11 device, launch the search menu (Windows+S on the keyboard), type **View Advanced System Settings**, and press Enter. A System Property box appears with the Advanced tab active. Click the Settings button under Performance; then select the Advanced tab. From here, the virtual memory size can be changed by clicking the Change button under Virtual Memory (see [Figure 3-24](#)).



**Figure 3-24** Adjusting Virtual Memory on a Windows Device

## SODIMM Memory

As mentioned in [Chapter 1](#), laptops have a more compressed form factor than desktops; therefore, RAM for laptops needs to be smaller to fit the form factor. Laptops use small outline DIMMs (SODIMMs), which are reduced-size versions of DIMM modules. [Figure 3-25](#) compares a typical DDR3 SODIMM with a DDR3 DIMM.

Key Topic



1. DDR3 SO-DIMM
2. DDR3 DIMM

**Figure 3-25** DDR3 SODIMM Module Compared to a DDR3 DIMM Module

[Table 3-8](#) lists DIMM and SODIMM form factors and their uses.



**Table 3-8** RAM Comparison

RAM Type	Pins (DIMM)	Pins (SODIMM)	Common Type and Speed	Defining Characteristic
DDR SDRAM	184	200*	PC3200 = 400MHz/3200Mb/s	Double the transfers per clock cycle, compared to regular SDRAM
DDR3 SDRAM	240 <sup>†</sup>	204	DDR3-1333 (PC3-10600) = 1333MHz/10,600Mb/s	External data bus speed (I/O bus clock) that is 4x faster than DDR SDRAM
DDR4 SDRAM*	288 <sup>‡</sup>	260	DDR4-2400 (PC4-19200) = 2400MHz/19200Mb/s	External data bus speed (I/O bus clock) that is 2x faster than DDR3 SDRAM (8x faster than DDR SDRAM)
DDR5 SDRAM*	288	262	DDR5-7200 (PC5-57600) = 7200MHz/57600Mb/s	External data bus speed (I/O bus clock) that is 2x faster than DDR4 SDRAM (16x faster than DDR SDRAM)

\*DDR SODIMM keying is closer to the middle of the motherboard than with SDRAM SODIMMs.

<sup>†</sup>The keying on DDR3 is offset to one side, compared to DDR2.

<sup>‡</sup>The keying on DDR4 is different from the keying on DDR3, and they are not interchangeable.

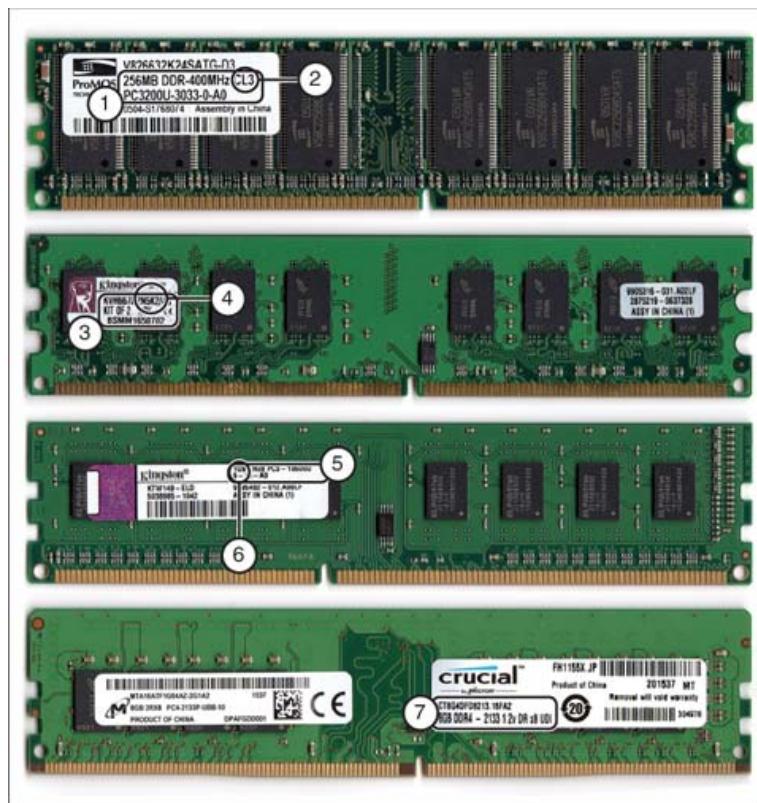
## DDR3 SDRAM

Compared to earlier RAM types, Double Data Rate 3 SDRAM (DDR3 SDRAM) runs at lower voltages, has twice the internal banks, and (with most versions) runs at faster speeds. DDR3 also has an 8-bit prefetch bus. DDR3 has greater latency. Typical latency values for mainstream DDR3 memory are CL7 or CL9, compared to CL5 or CL6 for earlier versions. Although DDR3 modules also use 240 pins, their layout and keying are different from previous types, and they cannot be interchanged.

DDR3 SDRAM memory can be referred to by the effective memory speed of the memory chips on the module (the memory clock speed x4 or the I/O bus clock speed x2)—for example, DDR3-1333 (333MHz memory clock x4 or 666MHz I/O bus clock x2) = 1333MHz). It also can be referred to by module throughput (DDR3-1333 is used in PC3-10600 modules, which have a throughput of more than 10,600MB/s, or 10.6GB/s). *PC3* indicates that the module uses DDR3 memory.

Other common speeds for DDR3 SDRAM modules include PC3-8500 (DDR3-1066; 8500MB/s throughput), PC3-12800 (DDR3-1600), and PC3-17000 (DDR3-2133).

[Figure 3-26](#) compares DDR, DDR2, DDR3, and DDR4 memory modules.



1. 256MB DDR module, PC3200 (DDR400)
2. CL3 latency
3. 2GB DDR2 module (from matched set), DDR2-667 (PC2-5300)
4. CL5 latency
5. 2GB DDR3 module, PC3-10600 (DDR3-1333)
6. CL9 latency
7. 8GB DDR4 module, DDR4-2133 (PC4-17000)

**Figure 3-26** DDR, DDR2, DDR3, and DDR4 DIMM Desktop Memory Modules with Different Notch Locations

## DDR4 SDRAM

DDR4 SDRAM, introduced alongside Intel's X99 chipset for Haswell-E Core i-series processors in 2014, is the fourth generation of DDR memory. Compared to its predecessor, DDR3, DDR4 runs at lower voltage (1.2V) than either DDR3 or the lower-voltage DDR3L. DDR4 supports densities up to 16GB per chip (twice the density of DDR3) and twice the memory banks, and it uses bank groups to speed up burst accesses to memory; however, it uses the same 8-bit prefetch as DDR3. Data rates range from 1600Mb/s to 3200Mb/s, compared to 800Mb/s to 2133Mb/s for DDR3. To improve memory reliability, DDR4 includes built-in support for CRC and parity error checking instead of requiring the memory controller to support error checking (ECC) with parity memory, as in DDR3 and earlier designs.

## DDR5 SDRAM: The Current Standard

DDR5 SDRAM was released in 2020 and is the fifth generation of DDR memory. Although DDR5 DIMMs has the same number of pins as DDR4 (288 pins), they are not compatible because the alignment key is located in an area on the RAM stick. In comparison to DDR4, DDR5 reduces power consumption (1.1V vs. 1.2V), offers twice the data transfer rate (6.4Gb/s vs. 3.2Gb/s) and has four times the memory density per chip (64GB vs. 16GB). DDR5 can include an onboard voltage regulator to gain higher speeds. In addition, the burst length in DDR5 is increased from DDR4's 8 to 16. *Burst length* refers to the amount of data that is read/written after a single read/write command in SDRAM. The increase of burst length in DDR5 results in increased read/write efficiency.

### Single Channel

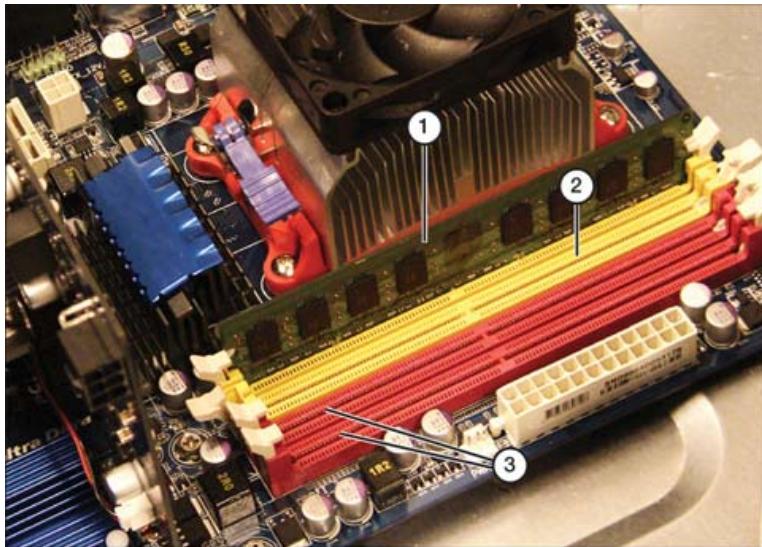
Originally, all systems that used SDRAM were **single-channel** systems. Each 64-bit DIMM or SODIMM module was addressed individually.

Because RAM services the CPU, it is best to have RAM with enough speed to match the processing that the CPU performs. Dual-channel (and, later, triple-channel and quad-channel) RAM represents efforts to increase RAM speed for more efficient performance.

### Dual Channel

Some systems that use DDR and most systems that use DDR2 or newer memory technologies support **dual-channel** operation. When two identical (same size, speed, and latency) modules are installed in the proper sockets, the memory controller accesses them in interleaved mode for faster access. This is why almost all RAM upgrades are done in pairs of chips.

Most systems with two pairs of sockets marked in contrasting colors implement dual-channel operation in this way: Install the matching modules in sockets of the same color (see [Figure 3-27](#)). See the instructions for the system or motherboard for exceptions.



1. Installed DIMM
2. Install identical module here for dual-channel operation
3. Use a matched pair (same speed and CL value as the first pair) in these sockets for best performance.  
This pair need not be the same size as the first pair.

**Figure 3-27** Adding an Identical Module to the Light-Colored Memory Socket to Use Dual-Channel Operation on a Motherboard

## Triple Channel

**Triple-channel** RAM is designed to triple the speed of the RAM bandwidth. Some systems that use the Intel LGA series chipsets support triple-channel addressing. Most of these systems use two sets of three sockets. Populate at least one set with three chips that have identical memory. Some triple-channel motherboards use four sockets, but for best performance, the last socket should not be used on these systems.

## Quad Channel

Some systems that use the Intel LGA series chipset support **quad-channel** addressing. Most of these systems use two sets of four sockets. As in dual- and triple-channel systems, with quad-channel operation, you populate one or both sets with four chips of identical memory.

### Note

One point to remember about dual, triple, and quad memory is that the chips are not different for each; the difference is in the way the motherboard accesses the chips. Thus, it is technically possible (although not technically resourceful) to use only two of the same RAM chips in a quad system.

## Parity vs. Nonparity

Two methods have been used to protect the reliability of memory:

- Parity checking
- ECC (error-correcting code or error correction code)

Both methods depend on the presence of an additional memory chip over the chips required for the data bus of the module. For example, a module that uses eight chips for data would use a ninth chip to support parity or ECC. If the module uses 16 chips for data (two banks of 8 chips each), it would use the 17th and 18th chips for parity. Parity checking, which goes back to the original IBM PC, works like this: Whenever memory is accessed, each data bit has a value of 0 or 1. When these values are added to the value in the parity bit, the resulting checksum should be an odd number. This is called *odd parity*. A memory problem typically causes the data bit values plus the parity bit value to total to an even number. This triggers a parity error, and the system halts with a parity error message. Note that parity checking requires parity-enabled memory and support in the motherboard. On modules that support parity checking, a parity bit exists for each group of 8 bits.

The method used to fix this type of error varies, depending on the system. On museum-piece systems that use individual memory chips, you must open the system, push all memory chips back into place, and test the memory thoroughly if you have no spares (using memory-testing software). If you have spare memory chips, you must replace the memory. If the computer uses memory modules, replace one module at a time and test the memory (or at least run the computer for a while), to determine whether the problem has disappeared. If the problem recurs, replace the original module, swap out the second module, and repeat.

### TIP

Some system error messages tell you the logical location of the error so that you can refer to the system documentation to determine which module or modules to replace.

### Note

Parity checking has always been expensive because of the extra chips involved and the additional features required in the motherboard and chipset. It fell out of fashion for PCs starting in the mid-1990s. Systems that lack parity checking freeze up when a memory problem occurs and do not display any message onscreen.

Because parity checking “protects” you from bad memory by shutting down the computer (which can cause you to lose data), vendors created a better way to use the

parity bits to solve memory errors: using a method called ECC.

## Error Correction: ECC vs. non-ECC Memory

For critical applications, network servers have long used a special type of memory called **error correction code (ECC)**. This memory enables the system to correct single-bit errors and notify you of larger errors.

Although most desktops do not support ECC, some workstations and most servers do offer ECC support. On systems that offer ECC support, ECC support might be enabled or disabled through the system BIOS/UEFI, or it might be a standard feature. The ECC feature uses the parity bit in parity memory to determine when the content of memory is corrupt and to fix single-bit errors. Unlike parity checking, which only warns you of memory errors, ECC memory actually corrects errors.

ECC is recommended for maximum data safety, although parity and ECC do incur a small slowdown in performance in return for the extra safety. ECC memory modules use the same types of memory chips that standard modules use, but they also use more chips and might have a different internal design to support ECC operation. As with parity-checked modules, ECC modules have an extra bit for each group of 8 data bits.

To determine whether a system supports parity-checked or ECC memory, check the system BIOS/UEFI memory configuration (typically on the Advanced or Chipset screens). Systems that support parity or ECC memory can use non-parity-checked memory when parity checking and ECC are disabled. Another name for ECC is EDAC (error detection and correction).

## Installing Memory



As mentioned earlier, upgrading RAM is one of the most (if not *the* most) common tasks a technician performs to improve a computer's performance. When upgrading RAM, note that not all different types are compatible or interchangeable. For instance, a DDR3 RAM stick cannot be used in a DDR4 slot, and vice versa. A DDR3 DIMM has 240 pins, and a DDR4 DIMM has 288 pins. In addition, DDR4 DIMM and DDR5 DIMM are not compatible even though they have the same number of pins; the notches on both RAM sticks are in different locations, preventing installation into an incompatible slot. Different SODIMM types are also not compatible because they all have a different number of pins. This is an essential skill to learn and understand, so it is covered here. This section largely applies to both desktops and laptops.

### Installing Memory Safely

When you install memory, be sure to follow the important safety procedures listed in Objective 4.4 of the 220-1102 Core 2 exam (see [Chapter 9](#)).

## Preparations for Installing DIMM Memory

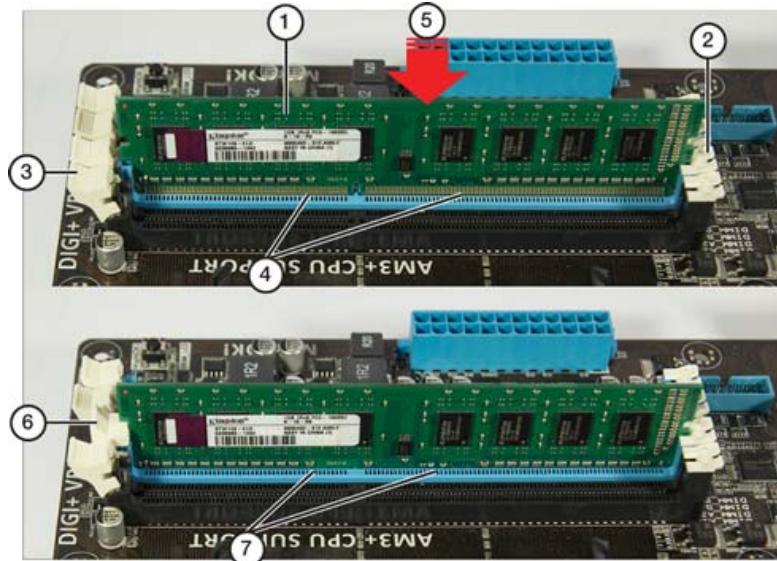
Before working with any memory modules, turn off the computer and unplug it from the AC outlet. Be sure to employ electrostatic discharge (ESD) protection in the form of an ESD strap and ESD mat. Use an antistatic bag to hold the memory modules while you are not working with them. Before actually handling any components, touch an unpainted portion of the case chassis, in a further effort to ground yourself. Try not to touch any of the chips, connectors, or circuitry of the memory module; hold them from the sides.

To install a DIMM module, follow these steps:

- Step 1.** Line up the modules' connectors with the socket. DIMM modules have connections with different widths to prevent backward insertion of the module.
- Step 2.** Verify that the locking tabs on the socket are swiveled to the outside (open) position. Some motherboards use a locking tab on only one side of the socket.
- Step 3.** After you verify that the module is lined up correctly with the socket, push the module straight down into the socket until the swivel locks on each end of the socket snap into place at the top corners of the module (see [Figure 3-27](#)). A fair amount of force is required to engage the locks. Do not touch the metal-plated connectors on the bottom of the module; doing so can cause corrosion or ESD.

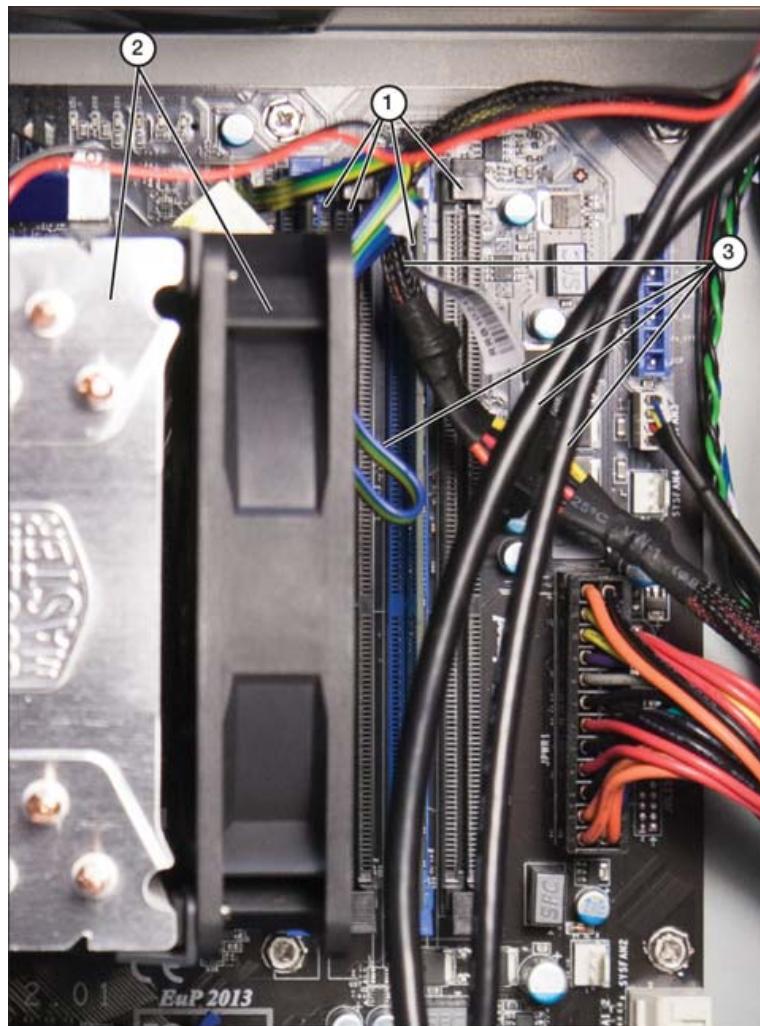
For clarity, the memory module installation pictured in [Figure 3-28](#) was photographed with the motherboard out of the case. However, the tangle of cables and components around and over the DIMM sockets in [Figure 3-29](#) provides a much more realistic view of the challenges you face when you install memory in a working system.





1. DIMM module lined up for installation
2. Many recent motherboards use fixed guides on one side.
3. Motherboards have at least one locking tab per module.
4. Connectors visible when module is not fully inserted.
5. Push module firmly into place.
6. Locking tab holds module in place when fully installed.
7. Connectors are no longer visible when module is fully inserted.

**Figure 3-28** A DIMM Partly Inserted (Top) and Fully Inserted (Bottom)



1. Memory sockets (some blocked by fan and heat sink)
2. Aftermarket fan and heat sink for CPU
3. Power and data cables

**Figure 3-29** DIMM Sockets Surrounded and Covered Up by Power and Data Cables or Aftermarket CPU Fans and Heat Sinks, Making It Difficult to Properly Install Additional Memory

When you install memory on a motherboard inside a working system, use the following tips to help your upgrade go smoothly and get the module to work properly:

- If the system is a tower system, consider placing the system on its side to make the upgrade easier. Doing this also helps keep the system from accidentally tipping over when you push on the memory to lock it into the socket.
- Use a digital camera or smartphone set for close-up focusing so that you can document the system's interior before you start the upgrade process.

- Move the locking tab on the DIMM sockets to the open position before you try to insert the module (refer to [Figure 3-28](#)). The memory module must be pressed firmly into place before the locking tab (left) will engage. The sockets shown in [Figure 3-29](#) have closed tabs.
- If an aftermarket heat sink blocks access to memory sockets, try to remove its fan by unscrewing it from the radiator fin assembly. This is normally easier to do than removing the heat sink from the CPU.
- Move power and drive cables away from the memory sockets so that you can access the sockets. Disconnect the cables, if necessary.
- Use a flashlight to shine light into the interior of the system so that you can see the memory sockets and locking tabs clearly; this enables you to determine the proper orientation of the module and to make sure the sockets' locking mechanisms are open.
- Use a flashlight to double-check your memory installation, to make sure the module is completely inserted into the slot and locked into place.
- Replace any cables that you moved or disconnected during the process before you close the case and restart the system.

## TIP

Note the positions of any cables before you remove them to perform an internal upgrade. You can use self-stick colored dots on a drive and its matching data and power cables. Marking masking tape with matching symbols works as well.

## Installing Storage Devices

220-1101  
Exam

**220-1101: Objective 3.3:** Given a scenario, select and install storage devices.

Many ways to store computer data are discussed throughout this book. In this section, the focus is on hardware storage attached to the computer—specifically, optical storage, magnetic storage, and flash memory. Optical drives are not as prevalent as they once were, but they are still being used and are listed on the A+ objectives. Each type of storage can be a viable solution for a storage problem, and you should be able to discuss the differences among them.

## Optical Drives

**Optical drives** fall into three major categories:

- Drives based on CD technology, including CD-ROM, CD-R (recordable CD), and CD-RW (rewritable CD)
- Drives based on DVD technology, including DVD-ROM, DVD-ROM/CD-RW combo, DVD-ROM/DVD-RW/DVD-RW DL, DVD-RAM, DVD-R/RW, DVD+R/RW, DVD±R/RW, and DVD±R/RW DL
- Drives based on Blu-ray technology, including BD-ROM, Combo BD-ROM/DVD Super Multi, BD-R, and BD-RE

All three types of drives store data in a continuous spiral of indentations called *pits* and *lands* that are burned into the nonlabel side of the disc from the middle outward to the edge. All these drives use a laser to read the data.

The difference in the storage capacities of Blu-ray, DVD, and CD results from the differences in laser wavelengths. The shorter the wavelength, the smaller the pits and lands on the disc—and shorter wavelengths enable more data to be stored in the same space. Each type has a different capacity:

- Blu-ray, which has the highest capacity, uses a blue laser with a shorter wavelength than DVD or CD.
- DVD uses a red laser with a longer wavelength than Blu-ray but shorter than that of CD.
- CD, which has the lowest capacity, uses a near-infrared laser with the longest wavelength.

Most CD, DVD, and Blu-ray drives are tray loading, but some use a slot-loading design (especially in home and automotive electronics products).

## **CD-ROM/CD-RW**

CD-R and CD-RW drives use special media types and a more powerful laser than the one used on CD-ROM drives to write data to the media. CD-R is a “write-once” media type; that is, the media can be written to during multiple sessions, but older data cannot be deleted. CD-RW media can be rewritten up to 1,000 times. The 80-minute CD-R media has a capacity of 700MB, whereas the older 74-minute CD-R media has a capacity of 650MB. CD-RW media capacity is up to 700MB but is often less, depending on how the media is formatted. CD-RW media is available in four types:

- CD-RW 1x–4x
- High-speed CD-RW 4x–12x
- Ultra-speed CD-RW 12x–24x
- Ultra-speed+ CD-RW 32x

Drives compatible with faster media types can usually work with slower media types, but not the other way around.

## DVD Recordable and Rewritable Standards



DVD-R and DVD+R media is recordable but not erasable, whereas DVD-RW and DVD+RW media use a phase-change medium similar to CD-RW and can be rewritten up to 1,000 times.

Consider these characteristics of the many members of the DVD family:

- **DVD-R:** A single-sided, single-layer, writable/nonerasable medium similar to CD-R. Capacity of 4.7GB. Some DVD-RAM and all DVD-RW drives can use DVD-R media.
- **DVD-R DL:** A single-side writable/nonerasable medium similar to CD-R, but with a second recording layer. Capacity of 8.4GB.
- **DVD-RW:** A single-sided rewritable/erasable medium similar to CD-RW. Capacity of 4.7GB. DVD-RW drives can also write to DVD-R media.
- **DVD+RW:** A rewritable/erasable medium. Also similar to CD-RW, but not interchangeable with DVD-RW or DVD-RAM. Capacity of 4.7GB.
- **DVD+R:** A single-side, single-layer writable/nonerasable medium. Also similar to CD-R, but not interchangeable with DVD-R. Capacity of 4.7GB.
- **DVD+R DL:** A writable/nonerasable medium with a second recording layer. Also similar to CD-R, but not interchangeable with DVD-R DL. Capacity of 8.4GB.

SuperMulti DVD drives can read and write all types of DVD media, as well as CD media. Sometimes these drives are also referred to as DVD± R/RW. Some early DVD+R/RW and DVD-R/RW drives cannot write to DL media.

## Blu-ray Disc (BD)

Blu-ray disc (BD) technology is an enhancement of the DVD technology that offers greater storage capacity. It was developed by a consortium of electronics companies. BD drives are compatible with BD-ROM (read-only Blu-ray media), such as the media used for Blu-ray movies. To play back Blu-ray movies, you must have a compatible player app installed. Standard-capacity BD media types include the following:

- **BD-R:** Recordable, not erasable. Similar to CD-R, DVD+R, DVD-R. 25GB capacity.
- **BD-R DL:** Dual-layer recordable media. Similar to DVD+R DL, DVD-RW DL. 50GB capacity.
- **BD-RE:** Recordable and rewritable. Similar to CD-RW, DVD-RW, DVD+RW. 25GB capacity.

- **BDXL:** BDXL drives and media represent a large jump in capacity over standard BD drives and media. The BDXL specification was released in April 2010. It supports multilayer 100GB and 128GB recordable media (BD-R 3.0) and multilayer 100GB rewritable media (BD-RE Revision 4.0). Many, but not all, BD-RE compatible drives are compatible with BDXL standards. Check the drive's specifications to determine compatibility.

## Drive Speed Ratings

Drive speeds are measured by an X-rating:

- **CD media:** 1X equals 150KB/s, the data transfer rate used for reading music CDs. Multiply the X-rating by 150 to determine the drive's data rate for reading, writing, or rewriting CD media.
- **DVD media:** 1X equals 1.385MB/s; this is the data transfer rate used for playing DVD-Video (DVD movies) content. Multiply the X-rating by 1.385 to determine the drive's data rate for reading, writing, or rewriting DVD media.
- **Blu-ray Disc (BD) media:** 1X equals 4.5MB/s; this is the data transfer rate for playing Blu-ray movies. Multiply the X-rating by 4.5 to determine the drive's data rate for reading, writing, or rewriting Blu-ray media.

### Note

Blu-ray drives are also compatible with CD and DVD media. Check the specifications for a particular drive to determine the specific types of media it supports and the maximum read/write/rewrite speeds for each media type.

## Recording Files to Optical Discs

You can use the following methods to record files onto optical discs:

- Built-in recording features in Windows or other operating systems
- Third-party disc mastering programs
- Third-party drag-and-drop programs

All optical media must be formatted, but depending on how you write to the media, the formatting process might be incorporated into the writing process or might require a separate step. Because of digital rights management, significant differences exist between Windows 8 and 10 when writing copyright-protected files. Third-party software such as VLC is commonly used to play and manage media.

## Hard Drives

Hard drives are the most important storage devices used by personal computers. A hard drive stores the operating system (Windows, macOS, Linux, or others) and loads it into the computer's memory (RAM) at startup. Hard drives also store applications, system configuration files used by applications and the operating system, and data files created by the user.

Hard disk drives (HDDs) have traditionally been magnetic drives, but in recent years, solid-state drives (SSDs) and hybrid magnetic/SSD (SSHDs) have become viable options for storage. These are discussed in the sections that follow.

## Solid-State Drive (SSD)

An SSD is a flash memory drive with no moving parts. Because the drive does not spin to retrieve data, it is much faster than a magnetic hard drive for storing and retrieving data. SSD is currently more expensive, with less capacity than HDD, but SSD capacity is improving and costs are dropping.

A typical SSD (see [Figure 3-30](#)) has a 2.5-inch form factor, but an optional 2.5-inch-to-3.5-inch adapter enables it to be installed in desktop computers that lack 2.5-inch drive bays. SSDs placed in drive bays are faster, but they still connect via the hard drive cables to connect to the motherboard.



**Figure 3-30** An SSD with Optional Data Transfer Cable and 2.5-Inch-to-3.5-Inch Bay Adapter

A common upgrade to improve speed and capacity for a computer is to install an SSD to replace an older, slower, and smaller HDD. Because only newer motherboards and chipsets support M.2 drives (pronounced “M-dot-2”), adapting an SSD into a desktop is a common solution. (A good time to do this is when upgrading to Windows 10 or Windows 11 because loading the OS on the SSD makes the booting and updating processes much faster and avoids a cloning process to migrate the OS to the new drive.) Having the OS image copied to a USB flash drive makes installation easy.

M.2 is an SSD that can mount directly onto the motherboard or an expansion card, giving the drive more direct access to the CPU for much faster reading than is possible with an SSD. An M.2 has an appearance closer to that of a RAM chip than to that of a standard hard drive. A motherboard must be specifically designed to accept an M.2 SSD, so M.2s are not a likely option for a legacy system.

Although M.2 SSDs are currently more expensive, they have the potential to be both faster and lighter than standard SSDs. Depending on the motherboard and operating system, upgrading to either an SSD or an M.2 SSD (pictured later in this section, in [Figure 3-32](#)) is possible. The M.2 SSD requires an available PCIe slot. If the motherboard does not have a PCIe slot, a PCIe adapter can be purchased to enable the drive. In BIOS/UEFI, the M.2 drive can be enabled by locating the drive in the PCI drive settings.

The following steps describe how to install an SSD in a desktop with a new OS image:

**Step 1.** Be sure the desktop has room for another drive, a bay to hold the drive and a SATA connection on the motherboard, and a Molex cable to power the SSD. If you are replacing the hard drive, back up files first. Follow the safety procedures outlined in [Chapter 9](#).

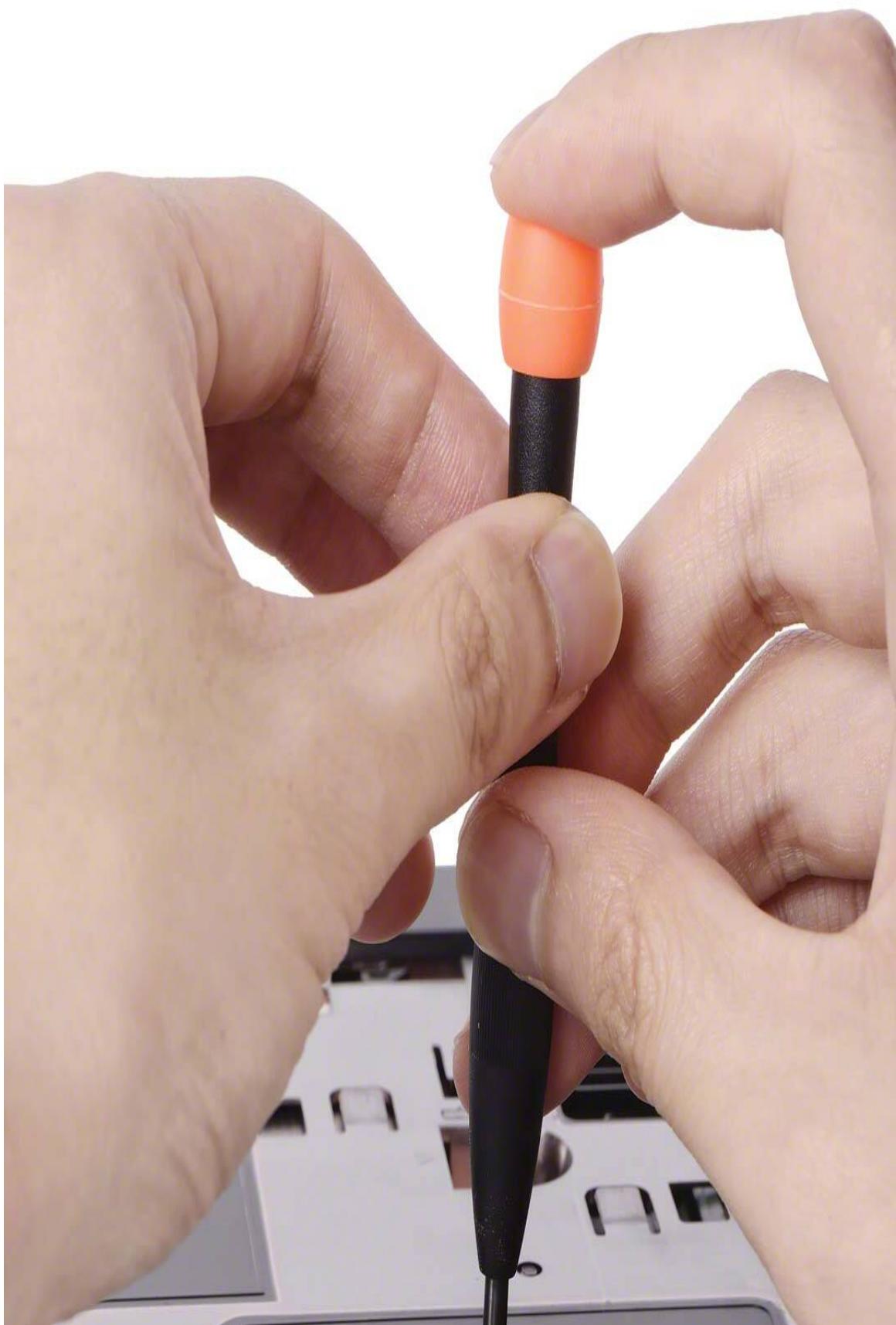
**Step 2.** Gather a new SSD, adapter bracket, and, if necessary, SATA cable. The bracket screws are very small, so be sure to also have a quality small Phillips screwdriver. Follow the instructions to mount the SSD into the bracket.

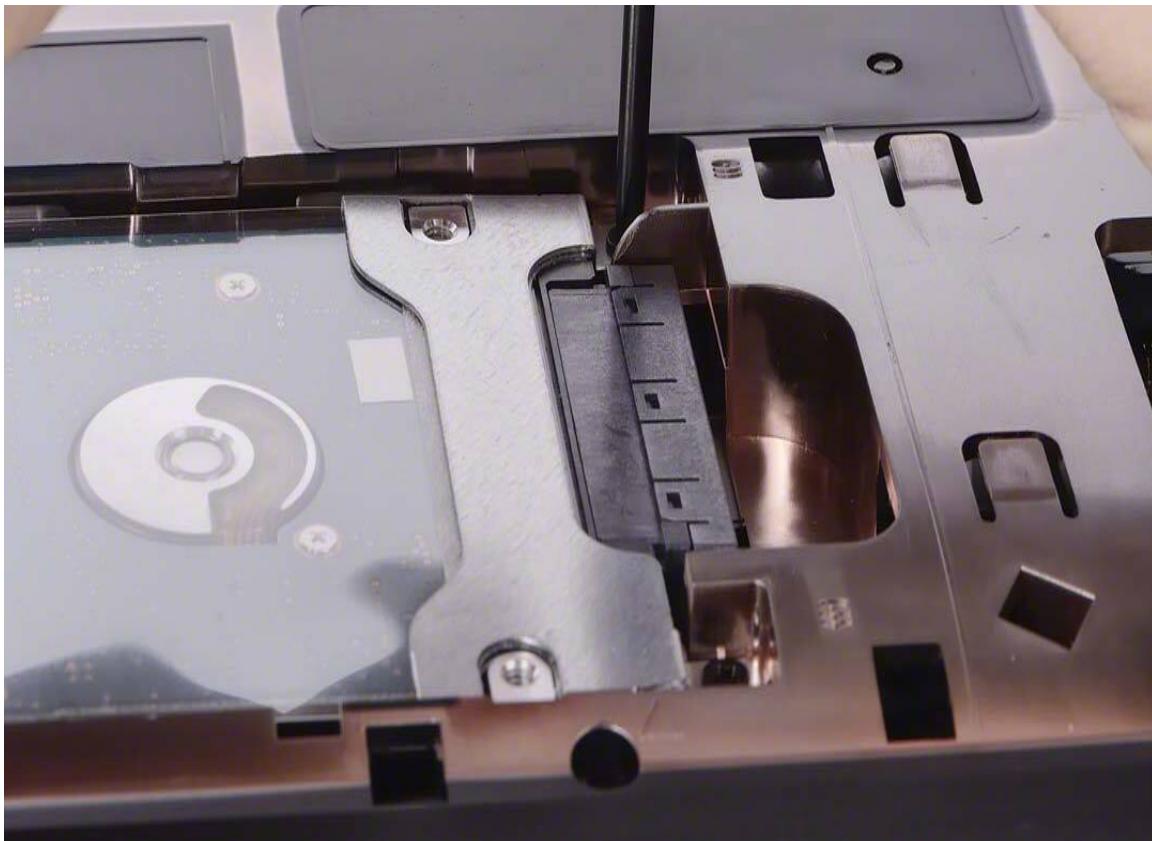
**Step 3.** Mount the bracket into the spare drive bay. Attach the SATA cable from the SSD to the motherboard. Attach the Molex power connector to power the drive. Tuck away the cables, close up the box, and reconnect the external power.

**Step 4.** Boot the computer and enter the BIOS/UEFI settings to set the boot drive to the USB flash with the new OS. If you are installing Windows 10/11, when you see the prompt for choosing which drive for the installation, choose the new SSD drive. Let the install run.

**Step 5.** Upon reboot, enter the BIOS/UEFI and set the boot order to boot from the new SSD with the OS.

To perform this process in a laptop, you might need to visit the manufacturer support page to determine the best method to access the hard drive. The process is mostly the same, but on a smaller scale. Laptops do not have room for additional drives, so backing up to an external drive is necessary. [Figure 3-31](#) depicts the tight workspace encountered when removing a hard drive from a laptop.



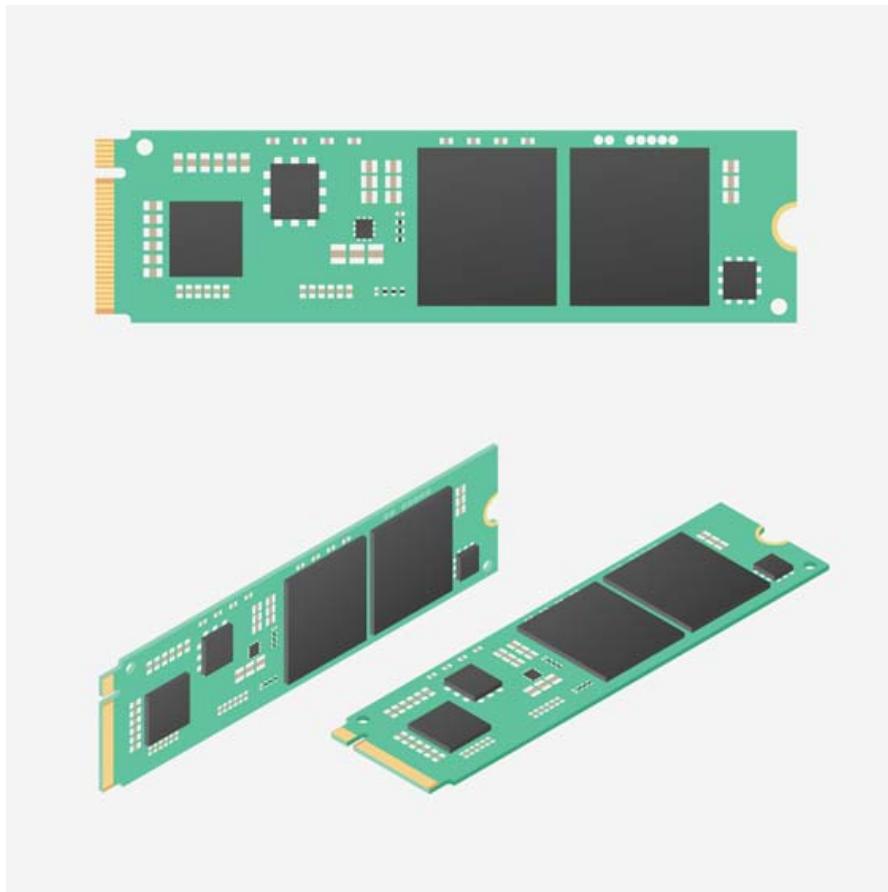


**Figure 3-31** Laptop HD Removal (Image © JIPEN, Shutterstock)

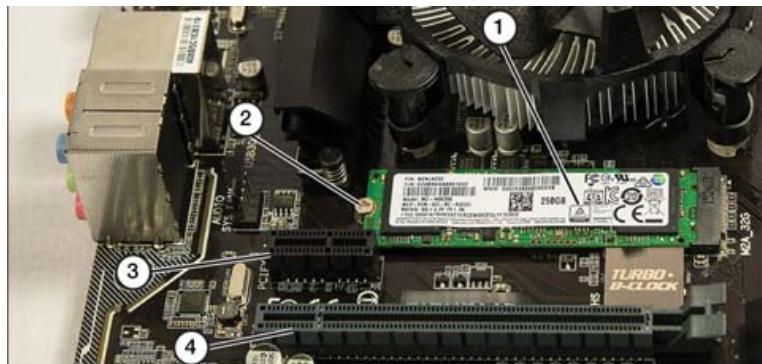
SSDs are also available in these form factors:

- **mSATA (miniPCIe form factor):** Used by some high-performance laptops and desktops.
- **M.2 (smaller than miniPCIe; pronounced “M-dot-2”):** Faster than mSATA. Used in some high-performance desktops and laptops, but becoming increasingly popular as prices drop. Needs a specific form factor because it attaches directly to the motherboard.
- **PCIe card:** For high-performance desktops. This is a way for SSDs to access the CPU by directly attaching to the motherboard and bypassing the traditional hard drive infrastructure.

[Figure 3-32](#) depicts an M2 card, and [Figure 3-33](#) illustrates an M.2 card installed in a high-performance desktop computer.



**Figure 3-32** An M.2 SSD (Image © Andrush, Shutterstock)



1. M.2 SSD installed in slot
2. Retaining screw for M.2 SSD
3. PCIe x1 slot (for comparison)
4. PCIe x16 slot (for comparison)

**Figure 3-33** An M.2 SSD Installed in a High-Performance Desktop Computer

SSDs use one of two types of flash memory: multilevel cell (MLC) or single-level cell (SLC). MLC memory has lower performance than SLC and does not support as many write cycles, but it is much less expensive per gigabyte than SLC memory. Almost all SSDs sold in the consumer space use MLC flash memory. The differences in

performance for similarly sized drives are based on the controller used, the firmware version in use, and whether the drive uses separate memory for caching or uses a portion of the SSD.

Although SSDs emulate hard disks, there are differences in their operation. Because unnecessary writing to flash memory causes premature failure, SSDs should not be defragmented. Newer SSDs use a feature known as TRIM to automatically reallocate space used by deleted files and make it available for reuse. TRIM is supported by modern Windows versions, but older SSDs require you to use vendor-supplied utilities to perform this task.

When Windows detects an SSD, it enables TRIM (if the drive supports this command), disables defragment, and disables other utilities, such as SuperFetch and ReadyBoost, that are designed for use with traditional hard disks.

## SSHD

A solid-state hybrid drive (SSHD) combines a solid-state cache with magnetic capacity. It uses a memory manager to choose the most common files for the fast cache. An SSHD can be a good choice if improved performance and high capacity are desired, but the cost of large SSDs is prohibitive, especially in laptops that lack the capacity for multiple drives.

Table 3-9 highlights the differences among the three types of hard drives.



**Table 3-9** Comparison of the Three Hard Drive Types

Type	Cost	Capacity	Speed	Reliability
HDD	Least expensive and readily available	Highest	Slowest due to moving parts and magnetic storage	Moving parts that can wear over time
SSD	Most expensive, but price is dropping	Lowest, but improving	Fastest	Solid state; no moving parts
SSHD	Midrange	Blends high HDD capacity with fast SSD cache for most-used files	Blends fast solid-state cache with slower magnetic storage	Moving parts that can wear out, but spins less than HDD

## NVMe

One of the big reasons SSD is faster than HDD is the lack of moving parts. However, this benefit created another problem: With all the available capacity to access data, the SSDs still had to funnel all the data through a communication infrastructure designed for much slower HDDs. To solve this problem, a consortium of electronics companies pooled their resources to develop **Non-Volatile Memory Express (NVMe)**. NVMe is a protocol designed to allow SSDs to transfer data between the motherboard and the SSD at staggeringly higher rates. It involved redesigning the command queueing method AHCI to create NVMe.

NVMe is not a physical form factor like M.2, nor is it an interface like PCIe; in fact, both of these can use NVMe. It is a protocol (or set of communication rules) that allows SSD data to bypass the bottleneck that happens with HDD infrastructure. The older protocol Advanced Host Controller Interface (AHCI) uses a process called *command queuing* to send requested data to the controller and motherboard. It is capable of handling one command queue with 32 commands at a time. NVMe, in contrast, can process more than 65,000 queues at one time, with each queue containing up to 65,000 commands. Needless to say, such data rates are having a huge impact on the kinds of applications being designed.

For NVMe to work, the computer's BIOS/UEFI and hardware needs to be designed for the high traffic, so only newer computers can physically support NVMe. On the software side, NVMe is supported by Windows, macOS, Linux, and Chrome OS.

## SATA 2.5

**SATA** 2.5 refers to an HDD with a 2.5-inch form factor. These are usually found in laptops, and larger 3.5-inch HDDs are found in desktops. The 2.5 inches refers to the size of the spinning platters inside the HDDs. They are connected to the motherboard internally with a SATA cable.

## PCIe

Peripheral Component Interconnect Express (PCIe) is a common expansion slot on a motherboard that provides peripheral devices such as SSDs and graphic processing units (GPUs) direct access to the CPU. This gives PCIe SSDs an edge over SATA SSDs because data does not need to go through RAM before reaching the CPU. This results in faster data transfer times compared to SATA SSDs.

## Magnetic Hard Disk Drives

Traditional hard disk drives use one or more double-sided platters formed from rigid materials such as aluminum or glass. These platters are coated with a durable

magnetic surface divided into sectors. Each sector contains 512 bytes of storage, along with information about where the sector is located on the disk medium. Sectors are organized in concentric circles, from the edge of the media inward toward the middle of the platter. These concentric circles are called *tracks*.

Hard disk drives are found in many desktop PCs; many newer PC systems and most newer mobile computers typically use some form of SSD.

External drives typically include SATA hard disks with a bridge controller for use with USB 2.0, USB 3.0, or USB4 ports. Drives made for macOS include USB or Thunderbolt ports. Some external drives can also connect to eSATA ports. External drives that use 3.5-inch desktop hard disks require AC power, but most external drives that use 2.5-inch or smaller mobile hard disks can be bus powered, receiving power from the USB port on the host computer.

## Speeds/Spin Rate

The speed at which hard disk media turns, its spin rate, is measured in revolutions per minute (rpm). Hard drives have four common speeds:

- Low-performance hard disks typically spin at 5400rpm.
- Midperformance drives spin at 7200rpm.
- High-performance desktop drives spin at 10000rpm.
- Drives designed for use in enterprise computing, such as servers, spin at rates up to 15000rpm.

### Note

It is generally felt that the 15000rpm drives are being built mostly for existing system replacements because their speed comes with higher power use. SSDs are leaping forward in speed and capacity, with a fraction of the energy use of the 15000rpm drives.

[Table 3-10](#) is a quick-reference table of hard disk spin rates with examples.

**Table 3-10** Hard Disk Spin Rate Comparison

Spin Rate (RPM)	Typical Use	Desktop Drive Example	Laptop Drive Example
5400	"Green" power-saving drives	WD Blue Seagate 4TB Desktop HDD*	WD Blue Seagate Laptop HDD
7200	Midrange performance	WD Black	WD Black

Spin Rate (RPM)	Typical Use	Desktop Drive Example	Laptop Drive Example
		Seagate Barracuda	Seagate Laptop Thin
10000	High performance	WD VelociRaptor	—
15000	Servers and enterprise	Servers	—

\* Actual spindle speed 5900RPM

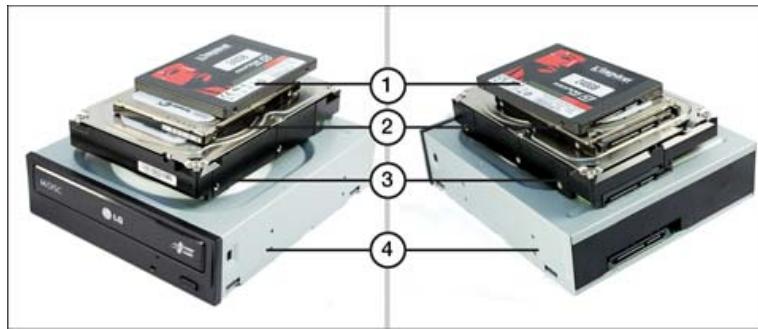
## Form Factors

Internal hard disk drives for desktop computers use 3.5-inch form factors. Their capacities range up to 8TB, but most installed desktop drives in recent systems have capacities ranging from 500GB to 2TB.

Internal hard disk drives or SSDs for laptop computers use the SATA 2.5-inch form factors. Their capacity ranges up to 3TB, but most laptop drives in recent systems have capacities ranging from 500GB to 1TB.

[Figure 3-34](#) compares front and rear views of a DVD drive, 3.5-inch desktop hard disk, SATA 2.5-inch laptop hard disk, and 2.5-inch laptop SSD.

Key Topic



1. 2.5-inch laptop SSD
2. 2.5-inch laptop hard disk
3. 3.5-inch desktop hard disk
4. 5.25-inch DVD rewriteable drive

**Figure 3-34** Front (Left) and Rear (Right) Internal Optical, Desktop, and Mobile Internal Hard Disks, and Mobile Internal SSD Drives

## Cache Sizes and Performance

Aside from interface type and spin rate, the drive's cache size also influences hard disk performance. In a hard disk, the cache is used to hold recently read

information for reuse. As with processor cache memory, which often enables the CPU to read cache memory instead of the slower main memory to reuse previously read information, hard disks with larger buffers can reread recently transferred information more quickly from cache than from the drive's magnetic storage.

In general, high-performance drives have larger caches than lower-performance drives. The larger-capacity drives in any given series typically have larger caches than the smallest-capacity drives in the same drive series.

## Hybrid Drives

A hybrid drive combines a standard SATA hard disk with up to 8GB of the same type of solid-state (SS) memory used in SSDs. The SATA hard disk is used for most of the storage, but the recent files are kept in the SS cache for fast access. Just as in SSD drives, the SS memory provides much faster data access than do purely mechanical hard disk drives. Consequently, when information needed by the CPU is available in the hybrid drive's flash memory, it is read from that memory, which boosts performance. Hybrid hard disk (also known as SSHD) drives are available in both 3.5-inch and 2.5-inch form factors. SSHDs are the middle ground in terms of cost and performance between HDDs and SSDs. Refer to [Table 3-9](#) to review how SSHD compares to other drive types.

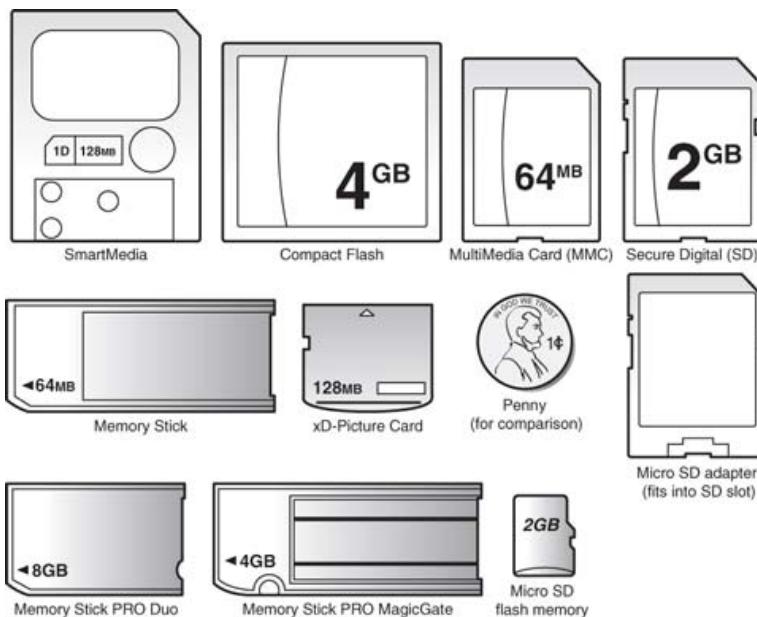
## Flash Drives/Memory Cards



Flash memory is a type of memory that can retain its contents without electricity. It has no moving parts, so it is very durable. Standard flash memory is used in digital media players, memory cards for cameras and digital media devices, digital camcorders, and USB thumb drives.

SSDs and **flash drives** are related, but they are not the same. SSD means *solid-state drive*, which defines the drive as having no moving parts. Flash is a type of memory that SSDs currently use. SSD flash also operates at a much higher level than the flash drives discussed here. (Refer to the earlier section "Solid-State Drive (SSD)" for information on SLC and MLC.)

[Figure 3-35](#) illustrates the most common types of flash memory cards.



**Figure 3-35** Common Flash Memory Card Types

[Table 3-11](#) describes the most common types of flash memory.

**Table 3-11** Flash Memory Card Capacities and Uses

Media Category	Common Capacity	Common Uses	Notes
SmartMedia (SM)	Up to 128MB	Digital cameras	Now obsolete. Replaced by xD-Picture Card.
CompactFlash (CF)	Up to 512GB	Professional digital SLR cameras	Check the manufacturer's speed rating for the best performance in burst mode.
MultiMedia Card (MMC)	Up to 4GB	Various devices	Obsolete. Replaced by SD, SDHC, and SDXC.
Memory Stick	Up to 128MB	Older Sony point-and-shoot digital cameras and digital media devices; also PlayStation 3 (PS3)	Obsolete. Replaced by SD, SDHC, and SDXC.
Memory Stick PRO MagicGate	Up to 4GB	Older Sony point-and-shoot digital cameras and digital media devices, including PlayStation Portable (PSP) and PS3	Obsolete. Replaced by SD, SDHC, and SDXC.

<b>Media Category</b>	<b>Common Capacity</b>	<b>Common Uses</b>	<b>Notes</b>
Memory Stick PRO Duo	Up to 32GB**	Older Sony point-and-shoot digital cameras and camcorders, and digital media devices, including PSP and PS3 (but not PS4)	Obsolete. Replaced by SD, SDHC, and SDXC.
Secure Digital (SD)	Up to 2GB	Most models of point-and-shoot digital cameras, some digital SLR cameras, and many flash memory-based media players	Has the write-protect switch on the left side of the media. Can also be used in place of SDHC or SDXC memory.
Secure Digital High Capacity (SDHC)	4GB to 32GB	Many models of point-and-shoot digital cameras, digital SLR cameras, and flash memory-based media players	SDHC media has the same physical form factor as SD; however, only devices made for SDHC can use SDHC. These devices are also compatible with SD. Check with the device vendor for details.
Secure Digital Extended Capacity (SDXC)	64GB to 512GB	Some high-performance digital SLR cameras	SDXC media has the same physical form factor as SD and SDHC; however, only devices made for SDXC media can use it.
miniSD	2GB	Mobile phones and cameras	Obsolete. Replaced by microSD. Can be used in SD or SDHC slots with an optional adapter.
miniSDHC	32GB	Mobile phones and cameras	Obsolete. Replaced by microSDHC. Can be used in SDHC slots with an optional adapter.
microSD	2GB	Various portable devices: smartphones, video games, and expandable USB flash memory drives	Can also be used in place of microSDHC; can be used in SD or SDHC slots with an optional adapter.

<b>Media Category</b>	<b>Common Capacity</b>	<b>Common Uses</b>	<b>Notes</b>
microSDHC	32GB	Various portable devices: smartphones, video games, and expandable USB flash memory drives	Device must support microSDHC; can be used in SDHC slots with an optional adapter.
xD-Picture Card	Up to 512MB (standard) Up to 2GB (Type M, Type M+, Type H)	Older Fujifilm and Olympus digital point-and-shoot cameras	Obsolete. Replaced by SD Card. Some cameras also support SD Card.

\*\* Original version up to 8GB; Mark 2 version up to 32GB

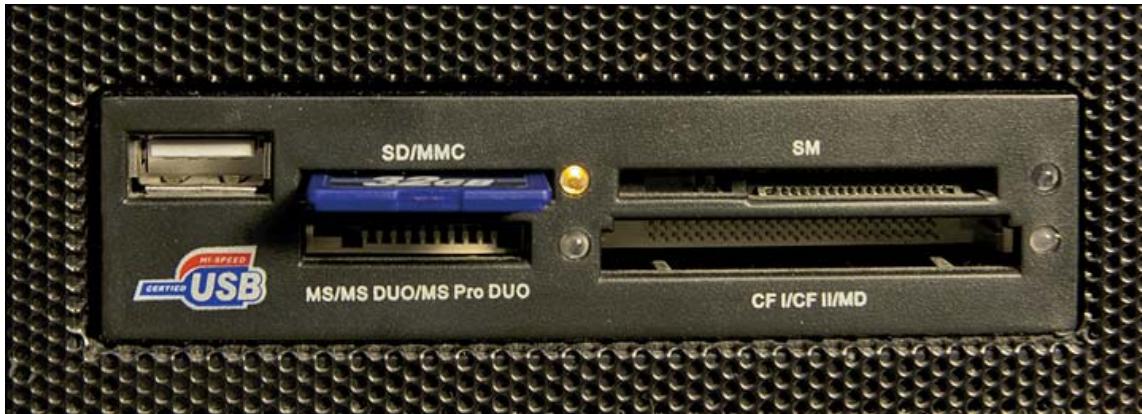
## Flash Card Reader

A card reader enables flash memory cards to be used with a computer. [Figure 3-36](#) shows a typical external multislots card reader, and [Figure 3-37](#) shows a typical internal multislots card reader. Most card readers assign a separate drive letter to each slot.



1. SDHC card inserted into card reader

**Figure 3-36** An External Multislot Card Reader That Supports a Wide Variety of Flash Memory Cards and Connects to a USB 3.0 Port



**Figure 3-37** An Internal Card Reader That Connects to an Unused USB 2.0 Port Header on the Motherboard

### Note

Do not confuse flash card readers with smart card readers. Smart card readers are used as part of a security system to read ID cards with embedded security.

### NOTE

Some printers and multifunction devices also include card readers. Some card readers built into printers and multifunction devices are used only for printing, whereas others can be used to transfer files to and from the host computer.

When you insert a flash memory card containing files in Windows, Windows might display a simplified AutoPlay dialog box (see [Figure 3-38](#)). If AutoPlay does not appear, open File Explorer and navigate to the appropriate drive letter to use the files on the card.



**Figure 3-38** A Typical AutoPlay Menu Displayed by Windows When a Flash Memory Card Containing Files Is Inserted into a Card Reader

## Storage Device Configurations

When adding or replacing a storage drive, it is necessary to optimize it for its intended purpose. A common reason for adding storage is to create a fault-tolerant set of drives that will protect data in case a drive fails. This section details the process of building data security into a system using RAID and hot-swappable drives.

### RAID Types

**Redundant Array of Independent (or Inexpensive) Disks (RAID)** is a method for creating a faster or safer single logical hard disk drive from two or more physical drives. The most common RAID levels include the following:

- **RAID Level 0 (RAID 0):** Two drives are treated as a single drive, and both drives are used to simultaneously store different portions of the same file. This method of data storage is called **striping**. Striping boosts performance, but if either drive fails, all data is lost. Do not use striping for data drives.
- **RAID Level 1 (RAID 1):** Two drives are treated as mirrors of each other, and changes to the contents of one drive are immediately reflected on the other drive. This method of data storage is called **mirroring**. Mirroring provides a built-in backup method and delivers faster read performance than a single drive. It is suitable for use with program and data drives.
- **RAID Level 5 (RAID 5):** Three or more drives are treated as a logical array, and parity information (used to recover data in the event of a drive failure) is spread across all drives in the array. It is suitable for use with program and data drives.
- **RAID Level 1+0 (RAID 10):** Four drives combine striping plus mirroring for extra speed plus better reliability. It is suitable for use with program and data drives. RAID 10 is a striped set of mirrors.

Most PCs with RAID support include support for Levels 0, 1, and 10. Some high-performance desktop systems also support RAID 5. Systems that lack the desired level of RAID support can use a RAID add-on card. [Table 3-12](#) provides a quick comparison of these types of RAID arrays.



**Table 3-12** Comparisons of Common RAID Levels

RAID Level	Minimum Number of Drives Required	Data Protection Features	Total Capacity of Array	Major Benefit over Single Drive	Notes
0	2	None	Twice the capacity of either drive (if same size) OR twice the capacity of the smaller drive	Improved read/write performance	Also called <i>striping</i>
1	2	Changes to the contents of one drive are immediately performed on the other drive.	Capacity of one drive (if they are same size) OR the capacity of smaller drive	Automatic backup; faster read performance	Also called <i>mirroring</i>
5	3	Parity information is saved across all drives.	Capacity of smallest drive (where $x$ equals the number of drives in the array)	Full data redundancy in all drives; hot swap of the damaged drive supported in most implementations	
10	4	Changes on one two-drive array are immediately performed on the other two-drive array.	Capacity of the smallest drive $\times$ the number of drives / 2	Improved read/write performance and automatic backup	Also called <i>striped and mirrored</i>

## Creating a SATA RAID Array

The advent of SSDs has disrupted the normal acceptance of RAID as the most reliable backup method, but RAID is still in widespread use. Many argue that because SSDs are several times more reliable than HDDs, using an SSD with an HDD backup could be the more reliable and cost-effective option. This thinking will likely change again as SSD prices continue to fall while capacity improves.

That said, here are the basics of setting up RAID on a PC.

Many recent desktop systems include SATA RAID host adapters on the motherboard. SATA RAID host adapter cards can also be retrofitted to systems that lack onboard RAID support. These types of RAID arrays are also referred to as *hardware RAID arrays*. RAID arrays can also be created through operating system settings and are sometimes called *software RAID arrays*. However, software RAID arrays are not as fast as hardware RAID arrays.

Motherboards that support only two drives in a RAID array support only RAID 0 and RAID 1. Motherboards that support more than two drives can also support RAID Level 1+0 (also known as RAID 10), and some support RAID 5 as well. RAID-enabled host adapters support varying levels of RAID.

### Note

A nonstandard definition of “RAID 10” was created for the Linux MD driver; Linux RAID 10 can be implemented with as few as two disks. Implementations supporting two disks, such as Linux RAID 10, offer a choice of layouts. Arrays of more than four disks are also possible.

A SATA RAID array requires the following:

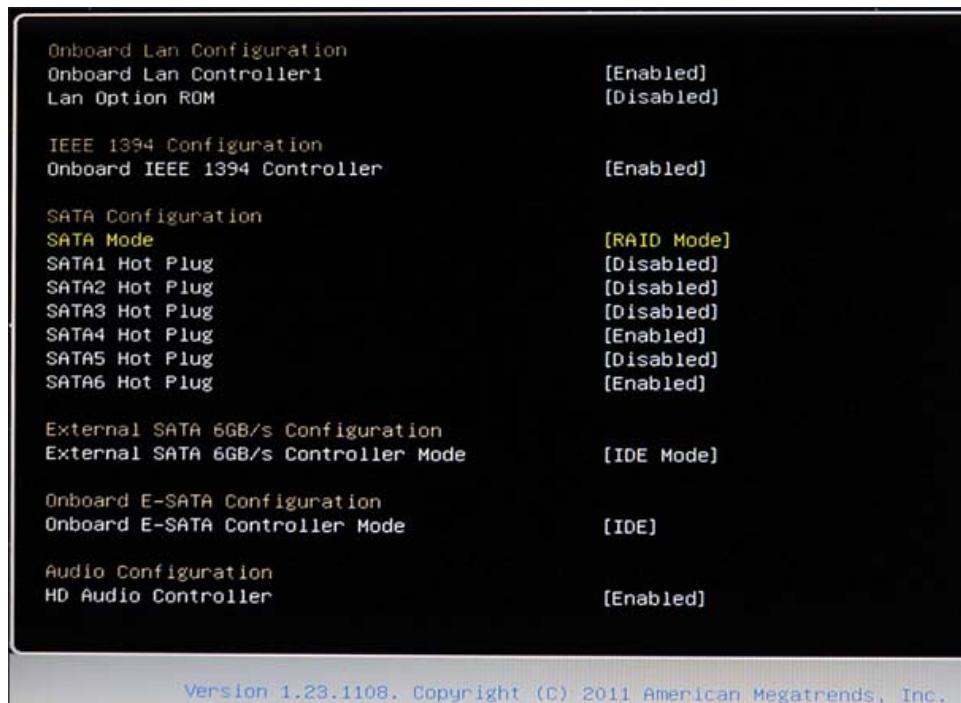
- **Two or more drives:** It's best to use identical drives (with the same capacity, buffer size, and RPMs). However, you can mix and match drives. If some drives are larger than others, the additional capacity will be ignored. You can use standard hard disk drives, hybrid hard disks, or SSDs.
- **A RAID-compatible motherboard or add-on host adapter card:** Both feature firmware that supports RAID.

Because RAID arrays typically involve off-the-shelf drives, the only difference in the physical installation of drives in a RAID array is where they are connected. They must be connected to a motherboard or an add-on card that has RAID support.

### Note

Sometimes RAID connectors are made from a different color of plastic than other drive connectors. However, the best way to determine whether a system or motherboard supports SATA RAID arrays is to read the manual for the system or motherboard.

When the drives used to create the array are connected to the RAID array's host adapter, restart the computer. If you are using the motherboard's RAID interface, start the system BIOS/UEFI setup program and make sure the RAID function is enabled (see [Figure 3-39](#)). Save the changes and exit the BIOS/UEFI setup program.



**Figure 3-39** Enabling SATA RAID in a Typical System BIOS

When you restart the computer, watch for a prompt from the RAID BIOS to start the configuration process (see [Figure 3-40](#)).



**Figure 3-40** A Typical Prompt to Start RAID Array Setup

Specify the desired RAID setting and any optional settings that you want to use (see [Figure 3-41](#)). After the RAID array is configured, the system handles the drives as a single physical drive. If drivers for the array are not already installed, you need to install them when prompted by the computer. For Windows, you can provide driver files via USB or on optical discs, if necessary.



**Figure 3-41** Preparing to Create a RAID 1 Array

## CAUTION

If one or more of the drives to be used in the array already contains data, back up the drives before you start the configuration process. Most RAID array host adapters delete the data on all drives in the array when creating an array—sometimes with little warning.

If you do not have RAID adapters in a system, you can create a software RAID volume, also known as a *disk array*, by using Windows.

## Note

Some hard disk drive vendors now produce drives especially made for SOHO RAID arrays of eight or fewer drives. Compared to normal SATA hard disk drives, RAID-optimized drives (also known as NAS drives) typically include features such as vibration reduction, optimization for streaming, disabled head parking, intelligent recovery from errors, and longer warranties.

To add a RAID array to a laptop, convertible (two-in-one), or all-in-one PC, use an external RAID drive or drive enclosure that connects to a USB 3.0 (or greater), Thunderbolt, or eSATA port. An external RAID drive contains two hard disks that can be configured as RAID 0 or RAID 1. Enclosures with support for three or more drives can also be configured as RAID 5. Enclosures with support for four drives can be configured

as RAID 10. Use the program provided with the drive or enclosure to configure the RAID array.

## Hot-Swappable Drives

Hot-swappable drives are drives that can be safely removed from a system or connected to a system without shutting down the system. In Windows, the following drives can be hot-swapped:

- USB drives
- eSATA drives
- SATA drives
- Flash memory drives

### Note

eSATA and SATA drives must be configured as AHCI in the system BIOS/ UEFI firmware.

In most enterprise systems, the RAID drives are hot swappable.

## Safely Ejecting a Drive in Windows

To safely eject a hot-swappable drive from a Windows system, follow these steps (see [Figure 3-42](#)):

**Step 1.** Open the Eject/Safely Remove Hardware and Eject Media icon in the notification area. If the icon is not visible, click the up arrow to display hidden icons.

**Step 2.** Select the drive to eject from the menu.

**Step 3.** When the Safe to Remove Hardware message appears, disconnect the drive.



**Figure 3-42** Safely Ejecting a Hot-Swappable Drive from a System Running Windows 10

If the drive is still in use, a Problem Ejecting type Storage Device dialog box appears, informing you that the drive is in use. Click OK, make sure no apps or processes are using the drive, and then try the process again.

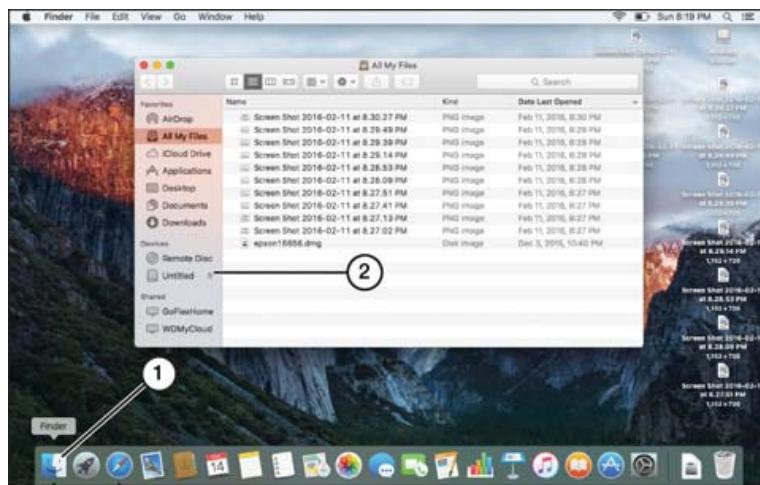
## Safely Ejecting a USB Drive in macOS

To safely eject a USB drive in macOS, follow these steps:

**Step 1.** Open Finder.

**Step 2.** Click the up arrow next to the USB drive icon in the left pane.

**Step 3.** When the drive icon is removed from the left pane of Finder, disconnect the drive (see [Figure 3-43](#)).



1. Click to open Finder
2. Click to eject USB drive

**Figure 3-43** Safely Ejecting a Hot-Swappable Drive from a macOS System

## Safely Ejecting a USB Drive in Linux

Some Linux distributions include support for safely ejecting a USB drive. However, the terminal command **df** can be used to list mounted devices. If the USB drive is not listed as mounted, it can be removed immediately. If the USB drive is listed as mounted, you can use the following command:

```
sudo umount /dev/sdb1 (where sdb1 is the mounted USB drive)
```

When the drive access light goes out, disconnect the drive.

# Installing Motherboards, CPUs, and Add-on Cards

220-1101  
Exam

**220-1101: Objective 3.4:** Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards.

Everything on a computer connects to the motherboard, where the CPU, the brains of a computer, resides. With so many different uses of computers, it follows that there are many different designs for how parts and devices attach to the motherboard to access the CPU. The A+ objectives cover the form factors that you will most likely encounter at some point as a technician.

## Motherboard Form Factors

*Form factor* refers to the size, shape, and other specifications of a motherboard. These other specifications can include the location of the mounting holes, the type of power supply, the external ports, and so on. Computer chassis are designed to accommodate specific form factors, and knowing these common standard form factors is essential for an A+ technician:

- ATX (Advanced Technology eXtended)
- mATX (microATX)
- ITX (Information Technology eXtended)
- mITX (Mini-ITX)

## ATX and mATX

The **Advanced Technology eXtended (ATX)** family of motherboards has dominated desktop computer designs since the late 1990s. An ATX motherboard has the following characteristics:

- A rear port cluster for I/O ports
- Expansion slots that run parallel to the short side of the motherboard
- Left-side case opening (as viewed from the front of a tower PC)

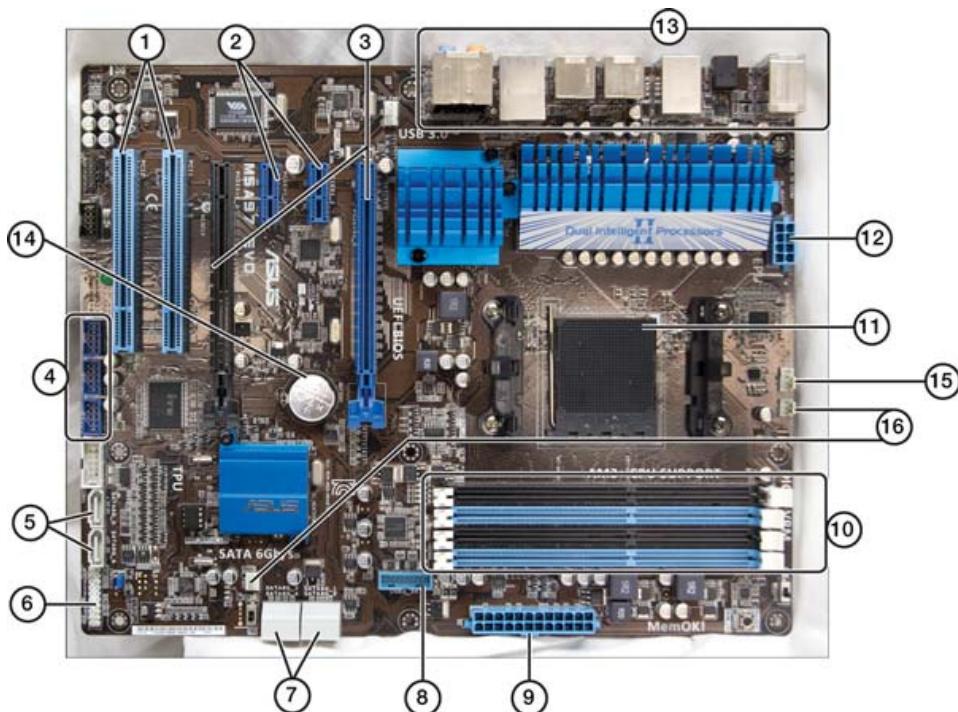
The ATX family has two members; see [Table 3-13](#).

Key  
Topic

**Table 3-13** ATX Motherboard Family Comparison

Motherboard Type	Maximum Width	Maximum Depth	Maximum Number of Expansion Slots	Typical Uses
ATX	12 in. (30.5cm)	9.6 in. (24.4cm)	7	Full tower
mATX	9.6 in. (24.4cm)	9.6 in. (24.4cm)	4	Mini tower

Figure 3-44 illustrates a typical ATX motherboard.



1. PCI slots
2. PCIe x1 slots
3. PCIe x16 slots
4. USB Port headers
5. SATA ports
6. Front-panel cable headers
7. Front-facing SATA ports
8. USB 3.0 header
9. ATX 24-pin power connector
10. DDR3 memory slots (dual-channel)
11. CPU socket
12. EPS12V power connector
13. Port cluster
14. CMOS battery (CR2032)
15. CPU fan header
16. Case fan header

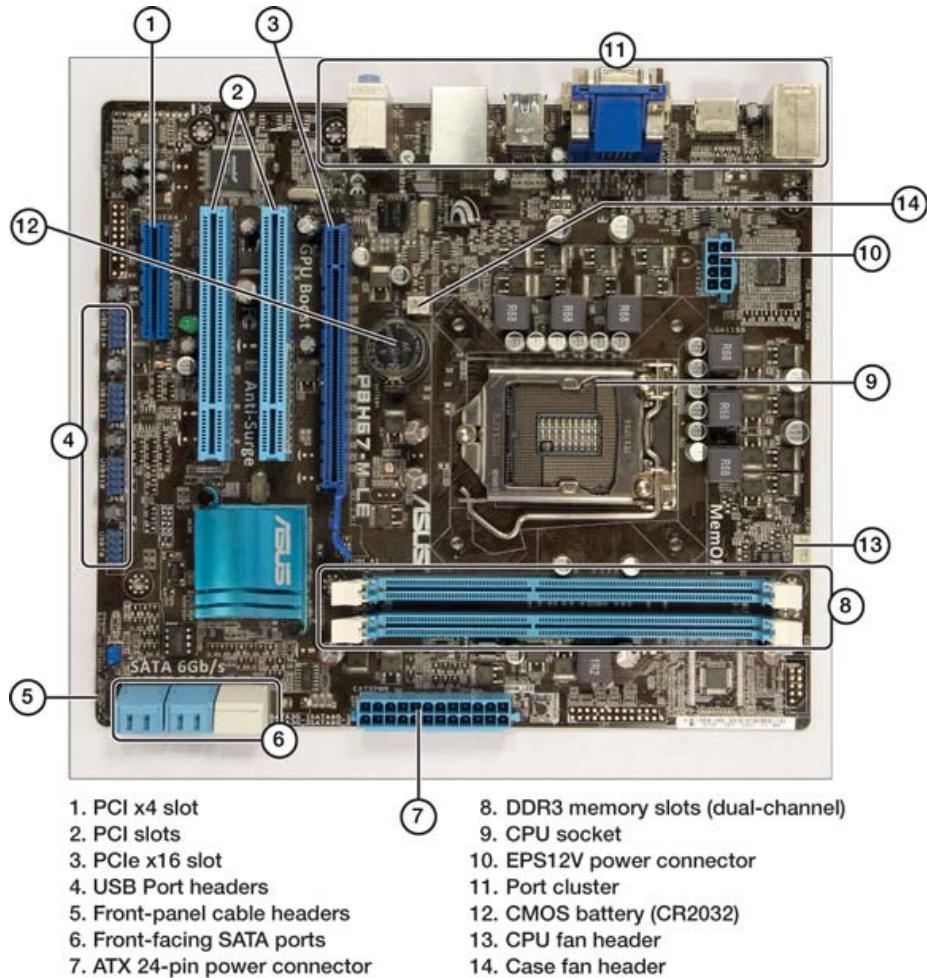
**Figure 3-44** A Typical Late-Model ATX Motherboard

## Note

mATX and ATX have matching mounting holes, and an mATX usually can be placed in an ATX case.

Figure 3-45 illustrates a typical *microATX (mATX)* motherboard.

Key Topic



**Figure 3-45** A Typical Late-Model *microATX (mATX)* Motherboard

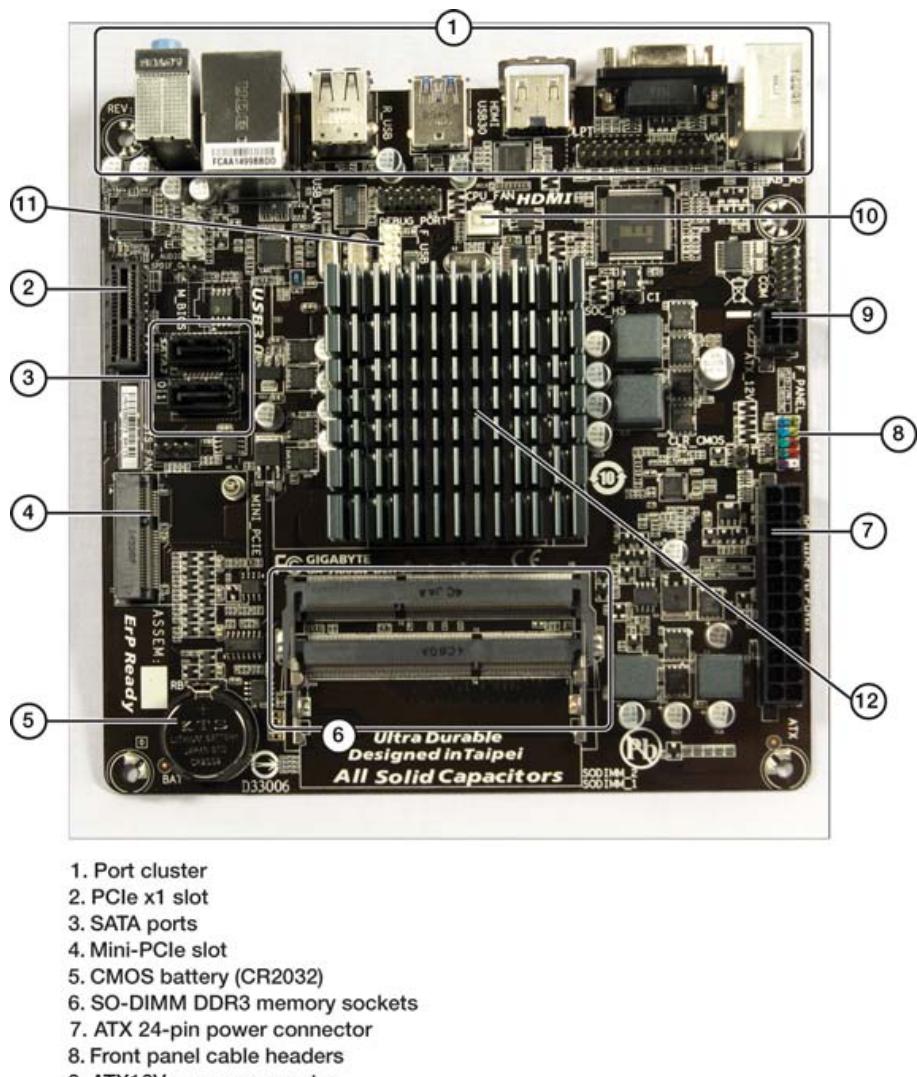
## ITX Family

The **Information Technology eXtended (ITX)** family of motherboards was originally developed by VIA Technologies in 2001 for use with its low-power x86 C3

processors. The original ITX motherboard form factor was quickly superseded by the smaller Mini-ITX form factor. Mini-ITX (mITX) measures 6.7×6.7 inches and has been adopted by many vendors for use with Advanced Micro Devices (AMD) and Intel processors. These processors can be socketed or soldered in place. Original designs featured a single PCI expansion slot, but most recent designs include a PCIe x1 or x16 expansion slot instead. A Mini-ITX motherboard can typically fit into a case made for ATX-family motherboards and uses a similar port cluster; however, Mini-ITX motherboards are used in small form factor PCs and in home theater applications.

[Figure 3-46](#) shows a typical Mini-ITX motherboard optimized for home theater applications. It uses a low-power CPU soldered to the motherboard, a fanless passive heat sink, and SODIMM memory to reduce heat and allow for very quiet operation. It includes a miniPCIe slot (normally found in laptops) for use with a Wi-Fi card. Some Mini-ITX motherboards feature socketed processors and a PCIe x16 slot for high-performance 3D video, making them suitable for gaming.



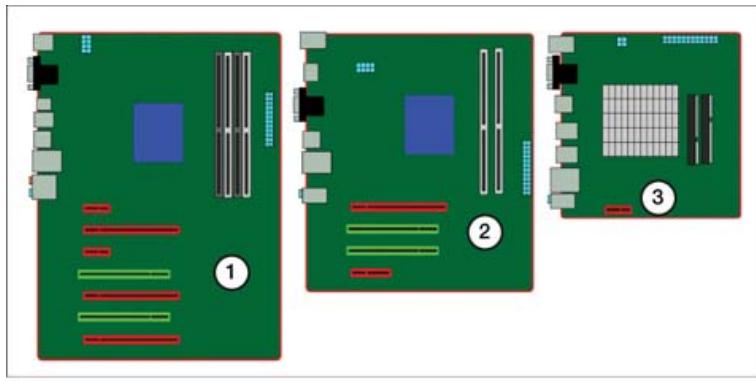


**Figure 3-46** A Typical Mini-ITX (mITX) Motherboard Optimized for Home Theater Applications

## Comparing ATX, microATX, and Mini-ITX Motherboards

Figure 3-47 compares the general sizes and layouts of ATX, microATX (mATX), and Mini-ITX (mITX) motherboards.

Key Topic



1. ATX motherboard
2. microATX motherboard
3. Mini-ITX motherboard

**Figure 3-47** ATX, microATX, and Mini-ITX Motherboard Component Layouts Compared

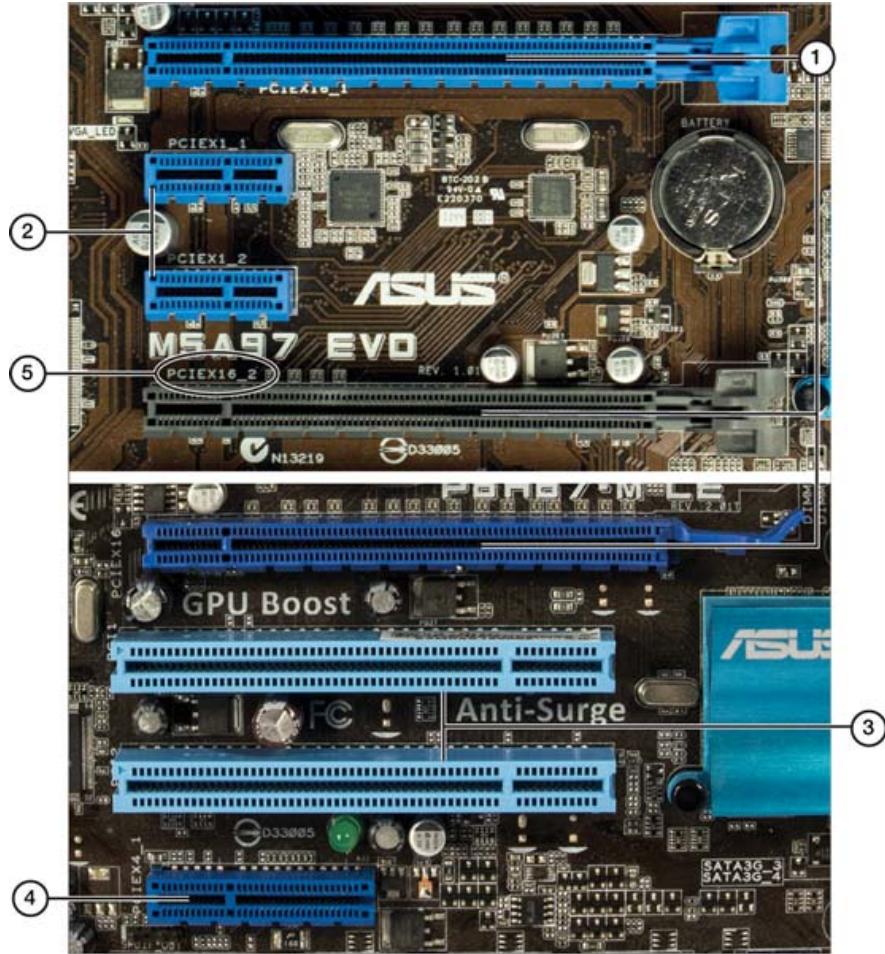
## Motherboard Connector Types

Motherboards use connectors to attach peripheral components to expand computing options. These are commonly known as expansion slots to provide support for additional input/output (I/O) devices and high-speed video/graphics cards. The most common expansion slots are PCI Express (also known as PCIe).

## Peripheral Component Interconnect (PCI) Slots

A **Peripheral Component Interconnect (PCI)** slot (developed in 1992) mounts to the motherboard and is used for many types of add-on cards, including network, video, audio, I/O, and storage host adapters for SATA drives. Several types of PCI slots exist, but the one found in desktop computers is the 32-bit slot running at 33MHz (see [Figure 3-48](#) in the next section). PCI slots are also available in 66MHz versions and in 64-bit versions.





1. PCIe x16 slots
2. PCIe x1 slots
3. PCI slots
4. PCIe x4 slot
5. Slot identification

**Figure 3-48** PCI Express Compared to PCI Slots

### Note

Early PCI cards used 5V DC power, but virtually all 32-bit PCI cards in use for a number of years have used 3.3V DC power. Note that although PCI slots are mostly obsolete, they are still found on many motherboards for backward compatibility.

## PCIe (PCI Express) Slots

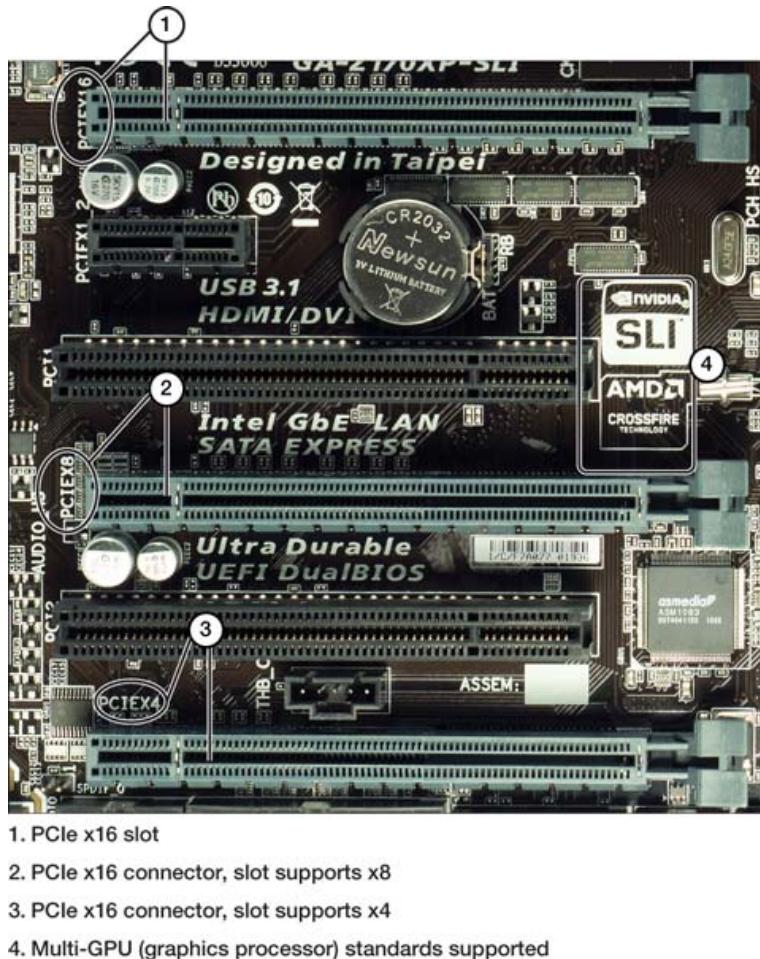
**Peripheral Component Interconnect Express (PCIe) slots** began to replace both PCI and Accelerated Graphics Port (AGP) slots in system designs starting in 2005. PCIe slots are available in four “lane” configurations:

- x1

- x4
- x8
- x16

Each x refers to an I/O lane. The most common versions include the x1, x4, and x16 designs, as shown in [Figure 3-48](#).

Some motherboards have two or more slots that use the x16 connector; however, the additional slots might actually support only x4 or x8 transfer rates (see [Figure 3-49](#)).



**Figure 3-49** A Motherboard Built for Multi-GPU Gaming That Has Three PCIe x16 Physical Connectors but Only One That Actually Provides x16 Speeds

PCI Express has evolved over the years to keep up with processing and data transfer needs for improvements in NICs, Wi-Fi, graphics, and storage. Each generation doubles the performance of the previous generation in bandwidth and frequency. PCIe speeds are represented in both bandwidth (gigabytes per second, expressed as GBps or GB/s) and gigatransfer (the theoretical speed per lane used on the card). For example, PCIe

version 3.0 used 4 I/O lanes of 8GB to reach an aggregate bandwidth of 32GB/s. [Table 3-14](#) compares the recent versions of PCIe.

**Table 3-14** Comparison of Recent PCIe Versions

Version/Year	Bandwidth	Gigatransfer	Suggested Uses
PCIe 3.0/2010	32GB/s	8GT/s	Ethernet, graphics SSD, NIC
PCIe 4.0	64GB/s	16GT/s	Ethernet, graphics SSD, NIC
PCIe 5.0/2019	128GB/s	32GT/s	Storage SSD, enterprise
PCIe 6.0	256 GB/s	64GT/s	Storage, enterprise
PCIe 7.0			In development

### NOTE

*GT* stands for *gigatransfers*. In the tables throughout this chapter, *GT/s* stands for *gigatransfers per second*, which differs from *Gb/s*, or gigabits per second. *GT/s* has to do with clocking embedded into the data of PCIe traffic. Using *GT* clarifies that some of the data being counted is “overhead” data used to make the transfer reliable. The nature of GTs is beyond the scope of the A+ exam.

### Note

miniPCI and miniPCIe are reduced-size versions of the PCI and PCIe standards. They are used in laptop computers.

## Power Connectors

Most motherboards feature headers for the power supply to connect and to supply added power for the drives, fans, lights, and CPU. Other headers will be lower voltage for data. For more information, see the section “Power Supplies,” later in the chapter.

## SATA

The motherboard’s Serial Advanced Technology Attachment (SATA) connectors are adjacent to the CPU. SATA connectors replaced IDE connectors, which were ribbonlike cables that were slower and more cumbersome and that needed to be assigned priority to hard drives.

The most important improvement was speed, with first-generation SATA cables transferring data up to 1.5Gb/s. As SSDs came to market, SATA specifications improved

to 3Gb/s, to match the faster data capabilities of the solid-state drives. The latest SATA version transfers data at 6Gb/s and can be up to 1m (3 ft.) in length.

Each generation of SATA cable had some differences in connectors, but the speed difference came from the controllers on the devices they connected to the motherboard and the capability of the motherboard controllers to handle the faster speeds.

## eSATA

**External SATA (eSATA)** connectors meet SATA standards for data, but the connectors are different from the internal SATA connectors. The eSATA cables have more sheathing, to protect data from interference for up to 2m (6 ft.) in length.

## Headers

The term **headers** on a motherboard refers to the pin headers that the connectors plug into. Some user manuals use the terms interchangeably.

## M.2

As noted earlier, an **M.2** (pronounced “M-dot-2”) is an SSD that can mount directly onto the motherboard or an expansion card, giving the drive more direct access to the CPU for much faster reading than is possible with an SSD. Motherboards must be specifically designed to accept an M.2 SSD.

## Motherboard Compatibility

When selecting a motherboard and installing or upgrading components on a motherboard, it is important to ensure that the components are compatible with the motherboard. The following sections discuss important aspects of motherboard compatibility that are covered on the CompTIA A+ exam.

## Processor Compatibility

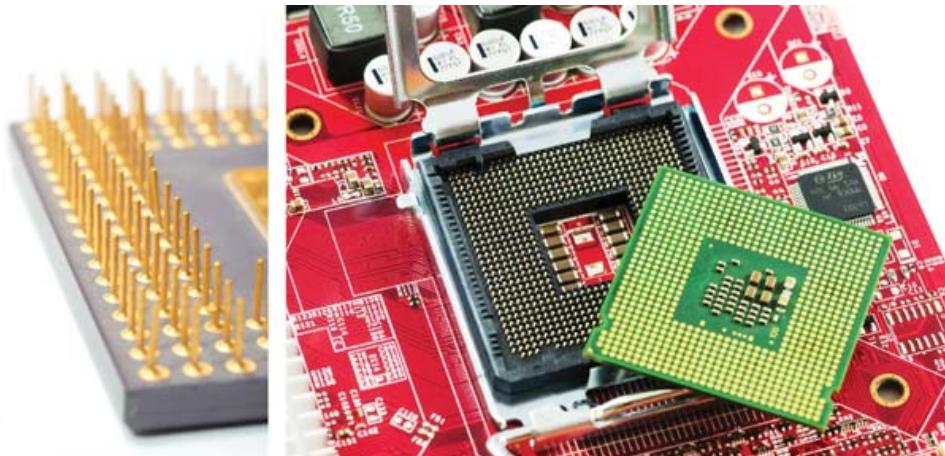
Intel and AMD, the two main manufacturers of desktop CPUs, use different form factors for attaching the processor to the motherboard. Differences in how the CPUs physically attach and how they work internally means one brand’s CPU is not compatible with the other brand’s motherboard. Because Intel and AMD use different socket types on their motherboards, CPUs from Intel will not fit an AMD form factor, and vice versa.

Independent manufacturers of motherboards, such as ASUS and ASRock, make several different boards that support CPUs from both companies.

Intel uses a Land Grid Array (LGA) form factor for CPUs. The pins that connect the CPU to the motherboard are mounted on the motherboard’s socket. Because of the grid protruding from the socket, careful handling of the motherboard is essential; damage to any pin can ruin the motherboard.

AMD, on the other hand, uses a Pin Grid Array (PGA) form factor, in which the contact pins that insert into the socket are mounted to the CPU itself. Of course, careful handling of the CPU is important here as well. When an AMD chip is installed, the pins and the socket should be carefully aligned; then the CPU must be gently dropped into the socket without any force applied by hand. The CPU is locked into place using a zero insertion force (ZIF) lever that acts as a retention arm that holds the chip in place.

Figure 3-50 shows an AMD CPU with a PGA.



**Figure 3-50** An AMD CPU with PGA (Left) and an Intel CPU with LGA (Right)  
(Images © S. Rimkuss, Shutterstock and © RMIKKA, Shutterstock)

AMD and Intel CPUs are also fundamentally different from one generation to the next. The CPU form factor must match the socket form factor when building a PC or when changing out a motherboard or CPU. For example, Intel's Core i7 CPU uses an LGA 1151, meaning that it has 1,151 pins. The newer Core i9 uses an LGA 2066, with 2,066 pins. Because of the pin difference, each CPU needs a different motherboard. Similar differences occur between AMD generations.

CPUs have evolved over time, and each generation of CPU, whether Intel or AMD, can make different demands of a motherboard. For example, earlier CPUs could support 32-bit processing but not 64-bit processing. When 64-bit CPUs became available, they did not work on motherboards designed for 32 bit because those motherboards could not support the additional RAM capabilities and other features. Current CPUs have graphics features that were not available in the previous generation, and the chipsets might need to be enhanced as well.

When upgrading a system, it is wise to start with the speed and features you want from a CPU and then shop for a motherboard that supports it. Checking with the manufacturer is the only way to know for sure whether a new version of CPU will work with the current motherboard's chipset.

## Central Processing Unit (CPU) Socket Types

The socket on a motherboard holds the central processing unit (CPU). The CPU takes in instructions from the software and runs calculations to process them into meaningful output for the application. (CPUs are discussed in more detail later in this section.)

Intel and AMD are the most prolific chip makers, and they design chips to efficiently perform certain tasks. For example, gaming chips might have one architecture, and chips for mining crypto currency might use another; desktops and mobile devices also have their own variations of chip design.

Although Intel and AMD processors share two common architectures—x86 (used for 32-bit processors and for 64-bit processors running in 32-bit mode) and x64 (an extension of x86 that enables larger files, larger memory sizes, and more complex programs)—these processor families differ in two important ways:

- Different processor sockets
- Differences in multicore processor designs (discussed later in this section)

The sockets used by these two companies are both physically and logically different, so they are not interchangeable. One will not physically fit into the motherboard of the other, and since CPUs are designed for certain motherboards, they cannot work together even if they could physically connect.

### Intel

Intel has used many processor sockets over the years. Note that the number of sockets has increased over time to accommodate more cores and improved architectures. Intel uses a connecting pattern called a Land Grid Array (LGA), which refers to the more than 1,000 connecting surfaces, or *lands*, that fit onto the Intel socket pins that wire into a motherboard. Common LGA models include the following:

- LGA 775
- LGA 1155
- LGA 1156
- LGA 1366
- LGA 1150
- LGA 2011
- LGA 2066

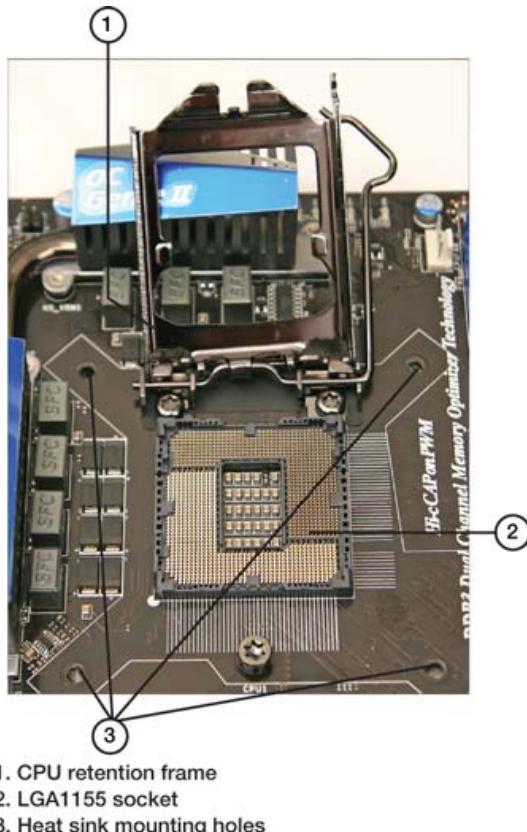
### Note

So many types of specialty CPUs exist (along with a maddening number of code names) that keeping it all straight is difficult. Before you buy any CPU from the vendor, be sure that what you are buying will work with what you have. For example, see the Automated Relational Knowledgebase, also known as the Intel ARK website (<https://ark.intel.com>).

## Land Grid Array Sockets



The LGA design uses spring-loaded lands in the processor socket (see [Figure 3-51](#)) that connect to bumps on the backside of the processor (see [Figure 3-52](#)). The number of lands in the processor socket is used for the numeric part of the socket name. For example, LGA 1150 has 1150 lands in the processor socket.



1. CPU retention frame
2. LGA1155 socket
3. Heat sink mounting holes

**Figure 3-51** An LGA 1155 Socket Prepared for Processor Installation



1. Processor notch for assuring proper installation
2. Pin 1 triangle marking

**Figure 3-52** The Front and Back Sides of an LGA Processor Before Installation

### Note

An excellent resource for information about currently available Intel processors and discontinued models is the Intel ARK website (<https://ark.intel.com>), mentioned earlier. To learn how to decode processor model number series, see “About Intel Processor Numbers,” at [www.intel.com/content/www/us/en/processors/processor-numbers.xhtml](http://www.intel.com/content/www/us/en/processors/processor-numbers.xhtml). Mobile processors with similar model numbers can vary in features.

### Note

The latest Intel socket for desktop processors, Socket LGA2066, supports the Intel X-Series processors. To learn more about X-Series processors and matching chipsets, visit <http://ark.intel.com>.

## AMD

AMD has used many processor sockets over the years, but the current desktop standard is the AM4.

All these sockets use the micro Pin Grid Array (mPGA) design.

### Note

In the following sections, only processors with thermal design power (TDP) over 25 Watts are covered. Processors with 25 Watts or less TDP are typically used in laptops or all-in-one units rather than typical desktops.

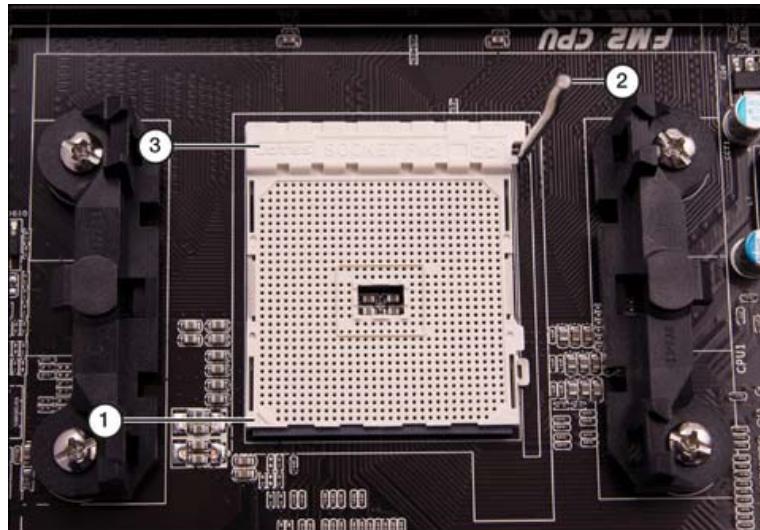
## mPGA Sockets

**Key Topic**

The micro Pin Grid Array (mPGA) design uses pins on the back side of the CPU to connect to pins in the processor socket. To hold the CPU in place, a zero insertion force (ZIF) socket mechanism is used. Open the arm and insert the processor; then close the arm to clamp the CPU pins in place.

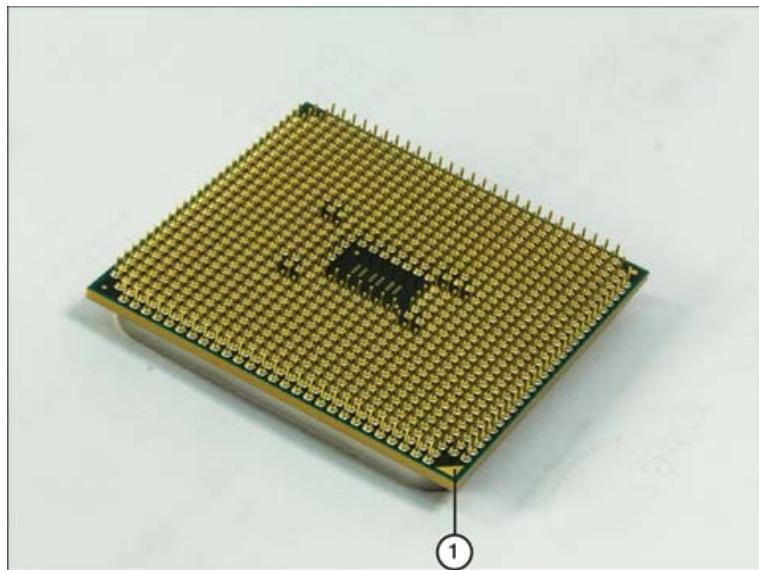
The heat sink clips to mounting lugs on two sides of the processor socket. All the mPGA sockets listed at the beginning of this section work in the same way.

[Figure 3-53](#) shows Socket FM2, which uses mPGA. [Figure 3-54](#) shows the back side of a processor designed for Socket FM2.



1. Triangle corresponds to pin 1 marking on processor
2. ZIF socket locking lever raised to unlock clamping mechanism
3. Processor socket name embossed here

**Figure 3-53** Socket FM2 Before Processor Installation



1. Pin 1 triangle also visible on top side of processor

**Figure 3-54** The Back Side of an AMD A10 5800K Processor Made for Socket FM2

The CPU series numbers contain codes and naming conventions for features or strengths of the chips, or they might indicate when a new generation of chip was developed. For example, features in an Intel i9 Core were developed later than an i7 Core, even though their production time overlapped. Each CPU can be compatible with chipsets on many compatible boards, so the manufacturer's online database is invaluable.

[Table 3-15](#) provides a quick reference to Intel and AMD sockets and processor family code names. The following sections provide additional detail.



**Table 3-15** Examples of Intel and AMD Desktop and Mobile Series CPUs

CPU	Cores	Threads	PCIe Version/Lanes	Socket	Maximum RAM
Intel i9-10920X	12	24	3.0/28	LGA2066	256GB
Intel i9-10940X	14	28	3.0/28	LGA2066	256GB
Intel i9-10980XE	18	36	3.0/28	LGA2066	256GB
Intel i9-10900X	10	20	3.0/28	LGA2066	256GB
AMD Ryzen Threadripper	16	32	4.0/64	AM4	

CPU	Cores	Threads	PCIe Version/Lanes	Socket	Maximum RAM
AMD Ryzen Threadripper	12	24	4.0/64	AM4	
AMD Ryzen Threadripper	8	16	4.0/64	AM4	
AMD 3015Ce from MD 3000 Series Mobile Processors	2	8	3.0/Chromebook	FT5	4GB/DDR4

## Servers

Data center servers are specially designed for their main task of data retrieval and storage. Graphics and other tasks common to a desktop are not required of a server, but high performance and lower power consumption are. CPU manufacturers therefore create special server CPUs for these machines.

The latest generation of servers has multisocket support, with Intel Xeon CPU and AMD Threadripper allowing two CPU sockets to work together. Newer models support up to eight sockets. [Table 3-16](#) depicts two high-end products in the race for server power and performance.

**Table 3-16** Server CPU Comparison

Name	Cores	Threads	TDP/Watts	RAM	Security	Notes
AMD 773X	64/128	128	280W	4TB/16DIMM	Yes	Encryption for security
Intel HNS2600BPBRCT/3rd Gen Xeon	32x2		165W	2.8TB/16 DIMMs	Yes	Up to 8 sockets

Having more than one CPU on a motherboard means having more physical sockets and more supporting design, which is not practical for desktop or even gaming machines.

## Mobile

Laptops, tablets, and phones each have motherboard standards. CPUs generate heat, and mobile devices rarely include fans, so mobile CPUs are made to run on lower voltage and to sleep when not needed. The motherboards are much smaller than the AMD and Intel designs mentioned earlier. [Table 3-17](#) depicts different ITX dimensions.

**Table 3-17** Comparison of ITX Dimensions for Mobile Devices

Form Factor	Dimensions
Mini-ITX	6.7 × 6.7 in.
Nano-ITX	4.7 × 4.7 in.
Pico-ITX	3.9 × 2.8 in.
Mobile-ITX	2.4 × 2.4 in.

## Basic Input/Output System (BIOS)/Unified Extensible Firmware Interface (UEFI) Settings

The Basic Input/Output System (BIOS) is an essential component of the motherboard. This boot firmware, also known as System BIOS or, on most recent systems, Unified Extensible Firmware Interface (UEFI), is the first code run by a computer when it is booted. It prepares the machine by testing it during bootup and paves the way for the operating system to start. It tests and initializes components such as the processor, RAM, video card, hard drives, optical drives, and USB drives. If any errors occur, the BIOS/UEFI reports them as part of the testing stage, known as the power-on self-test (POST). The BIOS/UEFI resides on a ROM chip and stores a setup program that you can access when the computer first boots up. From this program, it is possible to change settings in the BIOS and upgrade the BIOS as well.

### Note

From this point on in the chapter, the term *BIOS/UEFI* refers to both traditional BIOS and UEFI firmware, except when they differ in function.

## BIOS/UEFI Configuration



The system BIOS/UEFI has default settings provided by the system or motherboard maker, and these settings work fine for most people out of the box. However, as a system is built up with storage devices, memory modules, adapter cards, and other components, it is sometimes necessary to alter the default settings to get the best use of the devices.

The changes to BIOS/UEFI are made using the BIOS/UEFI setup program and then saved to the CMOS (complementary metal-oxide semiconductor) chip on the motherboard.

## Note

macOS provides operating system menus for making changes to system devices instead of permitting direct access to the BIOS.

## Accessing the BIOS/UEFI Setup Program

The BIOS/UEFI configuration program is stored in the BIOS/UEFI chip itself. Just press the key or key combination displayed onscreen (or described in the manual) when the system starts booting to access the BIOS/UEFI program menu.



Although these keystrokes vary from system to system, the most popular keys on current systems include Escape (Esc), Delete (Del), F1, F2, and F10.

Most recent systems display the key(s) necessary to start the BIOS/UEFI setup program at startup (see [Figure 3-55](#)). If you do not know which key to press to start your computer's BIOS/UEFI setup program, however, check the system or motherboard manual for the correct key(s).



1. Keystrokes for configuration options at startup

**Figure 3-55** A Typical Splash Screen That Displays the Keystrokes Needed to Start the BIOS Setup Program

## Note

Because the settings you make in the BIOS/UEFI setup program are stored in the nonvolatile CMOS, the settings are often called CMOS settings or BIOS/UEFI settings. The contents of CMOS are maintained by a battery.

## CAUTION

BIOS/UEFI configuration programs vary widely, but the screens used in the following sections are representative of the options available on typical recent systems; your system might have similar options but place the settings on different screens than those shown here. Laptops, corporate desktops, and tablets generally offer fewer options than those shown here.

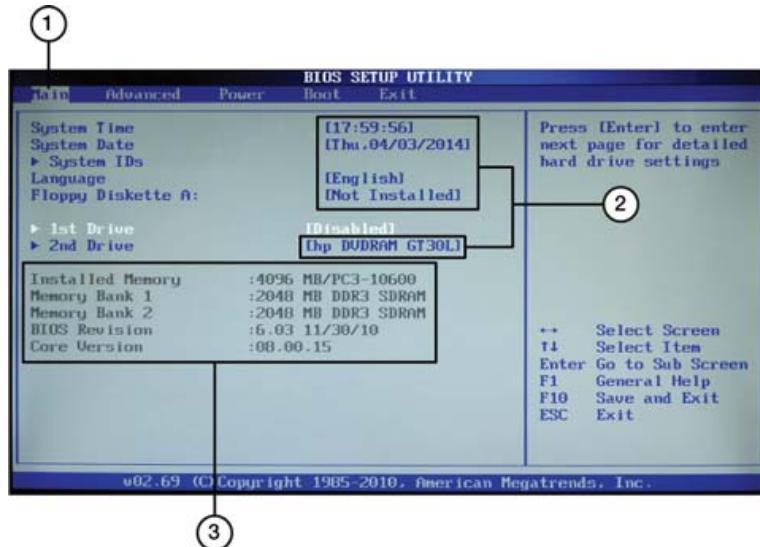
Be sure to consult the manual that came with your computer or motherboard before you change the settings you find here. Fiddling with the settings can improve performance, but it can also wreak havoc on an otherwise healthy device if settings are changed in error.

## UEFI and Traditional BIOS

All desktop and laptop computers from 2014 on use a new type of firmware called the Unified Extensible Firmware Initiative (UEFI) to display a mouse-driven GUI or text-based menu for BIOS setup. macOS computers all use UEFI firmware. Compared to a traditional flash ROM BIOS, UEFI has the following advantages:

- Support for hard drives of 2.2TB and higher capacity. These drives require use of the GUID Partition Table (GPT) to access full capacity.
- Faster system startup (booting) and other optimizations.
- Larger-size ROM chips used by UEFI to make room for additional features, better diagnostics, the capability to open a shell environment for easy flash updates, and the capability to save multiple BIOS configurations for reuse.

UEFI firmware offers similar settings to those used by a traditional BIOS (see [Figure 3-56](#)), along with additional options (see [Figures 3-57](#) and beyond). Most desktop systems with UEFI firmware use a mouse-driven graphical interface. However, many laptops with UEFI firmware use a text-based interface similar to BIOS.



1. Selected menu
2. Editable items
3. Reported by system; not editable

**Figure 3-56** A Computer That Uses a Traditional BIOS

To learn more about UEFI, visit [www.uefi.org](http://www.uefi.org).

## BIOS/UEFI Settings Overview

The following sections review the typical setup process using various UEFI firmware versions on systems running Intel Core i3 3227U, Intel Core i5 i6600, AMD FX-8350, and AMD A10-5800K processors.

Table 3-18 provides detailed information about the most important CMOS/BIOS settings. Use this table as a quick reference to the settings you need to make or verify in any system. The following sections provide examples of these and other settings.



**Table 3-18** Major CMOS/BIOS/UEFI Settings

Option	Settings	Notes
Boot Sequence	Hard drive, optical (CD/DVD, Blu-ray), USB, network ROM; order as wanted	To boot from bootable OS or diagnostic CDs or DVDs, place the CD or DVD (optical) drive before the hard drive in the boot sequence. To boot from a bootable USB device, place the USB device before the hard drive in the boot sequence. You can enable or disable

<b>Option</b>	<b>Settings</b>	<b>Notes</b>
		additional boot devices on some systems.
Memory Configuration	By SPD or Auto (default); manual settings (Frequency, CAS Latency [CL], Fast R-2-R turnaround, and so on) also available	This option provides stable operation using the vendor settings stored in memory. Use manual settings (frequency, CAS latency, and so on) for overclocking (running memory at faster than normal speeds) or to enable memory of different speeds to be used safely by selecting slower settings.
CPU Clock and Frequency	Automatically detected on most recent systems	Faster or higher settings overclock the system but could cause instability. Some systems default to low values when the system does not start properly.
Hardware Monitor	Enable display for all fans plugged into the motherboard	This is also known as PC Health on some systems. It can be monitored from within the OS with vendor-supplied or third-party utilities.
Onboard Audio, Modem, or Network	Enable or disable	Enable this when you do not use add-on cards for any of these functions; disable each setting before installing a replacement card. Some systems include two network adapters.
USB Legacy	Enable when USB keyboard is used	This option enables a USB keyboard to work outside the OS.
Serial Ports	Disable unused ports; use default settings for ports you use	Serial ports are also known as COM ports. Most systems no longer have serial ports.
Parallel Port	Disable unused port; use EPP/ECP mode with default IRQ/DMA when a parallel port or device is connected	A parallel port is compatible with almost any parallel printer or device; be sure to use an IEEE-1284-compatible printer cable. Most recent systems no longer include parallel (LPT) ports.
USB Function	Enable	When the motherboard supports USB 2.0 (Hi-Speed USB) ports, be sure to enable USB 2.0 function and load USB 2.0 drivers in the OS.

<b>Option</b>	<b>Settings</b>	<b>Notes</b>
USB 3.0 Function	Enable	USB 3.0 ports also support USB 3.1, 2.0, and USB 1.1 devices. Disable this function when USB 3.0 drivers are not available for the operating system.
Keyboard	NumLock, autorepeat rate/delay	Leave this at the default (NumLock On) unless the keyboard has problems.
Plug-and-Play OS	Enable for all except some Linux distributions	When this is enabled, Windows configures devices.
Primary VGA BIOS	Varies	Select the primary graphics card type (PCIe or onboard).
Shadowing	Varies	Enable shadowing for video BIOS; leave other shadowing disabled.
Quiet Boot	Varies	Disable this to display system configuration information at startup.
Boot-Time Diagnostic Screen	Varies	Enable this to display system configuration information at startup.
Virtualization	Varies	Enable this to run hardware-based virtualization programs such as Hyper-V or Parallels so that you can run multiple operating systems, each in its own window.
Power Management (Menu)	Varies	Enable and disable various power settings, as well as manage voltages. Voltages should be set to Auto. Enable CPU fan settings to receive warnings of CPU fan failure.
Fan Settings	Varies	Manage CPU fan settings and chassis fan settings.
S1 or S3 standby	Enable S3	Use S1 (which saves minimal power) only when you use devices that do not properly wake up from S3 standby.
AC Pwr Loss Restart	Enable restart or full on	This prevents the system from staying down when a power failure takes place.
Wake on LAN (WOL)	Enable when you use WOL-compatible	WOL-compatible cards use a small cable between the card and the motherboard.

Option	Settings	Notes
	network card or modem	Some integrated network ports also support WOL.
User/Power-On Password	Blocks system from starting when password is not known	Enable this when physical security settings are needed, but be sure to record the password in a secure place.
Setup Password	Blocks access to setup when the password is not known	Both passwords can be cleared on both systems when CMOS RAM is cleared.
Write-Protect Boot Sector	Varies	Enable this for normal use, but disable it when installing drives or using a multiboot system. This helps prevent accidental formatting but might not stop third-party disk prep software from working.
Boot Virus Detection (Antivirus Boot Sector)	Enable	This stops true infections but allows multiboot configuration.
SATA Drives	Varies	This autodetects the drive type and settings at startup time. Select CD/DVD for a CD/DVD/Blu-ray drive; select None when a drive is not present or to disable an installed drive.
SATA Drive Configuration	IDE, AHCI, RAID	The IDE setting emulates now-obsolete PATA drives. To take advantage of hot swapping and native command queuing (NCQ) to improve performance, select AHCI. Use RAID when the drive will be used as part of a RAID array.

As you can see in [Table 3-18](#), you have many options to select from when configuring BIOS settings. Many BIOS firmware versions enable you to automatically configure your system with a choice of these options from the main menu:

- BIOS defaults (also referred to as Original/Fail-Safe on some systems)
- Setup defaults (also referred to as Optimal on some systems)

These options primarily deal with performance configuration settings in the BIOS firmware, such as memory timings and memory cache. The settings used by each BIOS setup option are customized by the motherboard or system manufacturer.

Use BIOS defaults to troubleshoot the system because these settings are conservative in memory timings and other options. Normally, the setup defaults provide better performance. As you view the setup screens in this chapter, you'll see that these options are listed.

### **CAUTION**

If you use automatic setup after you make manual changes, all your manual changes will be overridden. Use the setup defaults and then make any other changes you want.

With many recent systems, you can select optimal or setup defaults, save your changes, and then exit; the system will then work acceptably. However, to configure drive settings or USB settings, or to enable or disable ports, you also need to work with individual BIOS settings, such as the ones shown in the following sections.

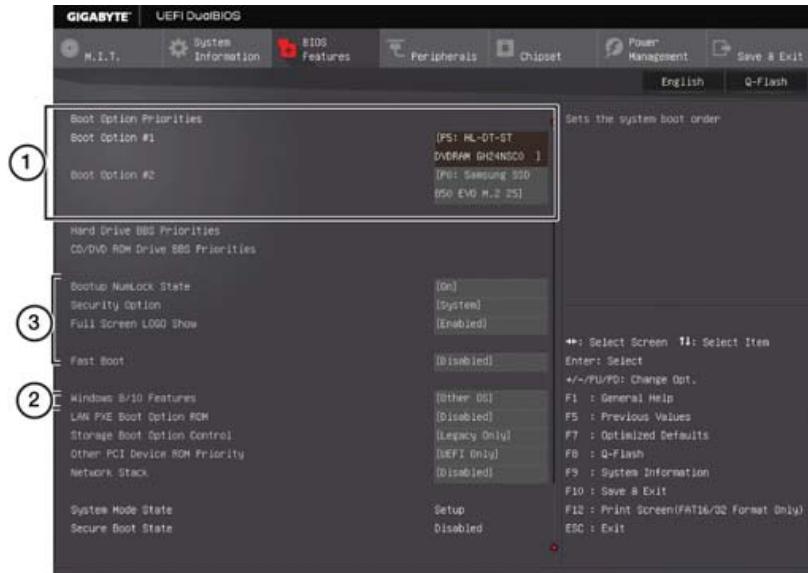
### **TIP**

On typical systems, you set numerical settings, such as date and time, by scrolling through allowable values with keys such as + and – or Page Up/Page Down. However, to select settings with a limited range of options, such as to enable/disable or choose from a menu, press Enter or the right-arrow key on the keyboard and then choose the option you want from the available choices.

## **Boot Options: Settings and Boot Sequence**

Most computers include settings that control how the system boots and the sequence in which drives are checked for bootable operating system files. Depending on the system, these settings might be part of a larger menu, such as an Advanced Settings menu, a BIOS Features menu (see [Figure 3-57](#)), or a separate Boot menu (see [Figure 3-58](#)).

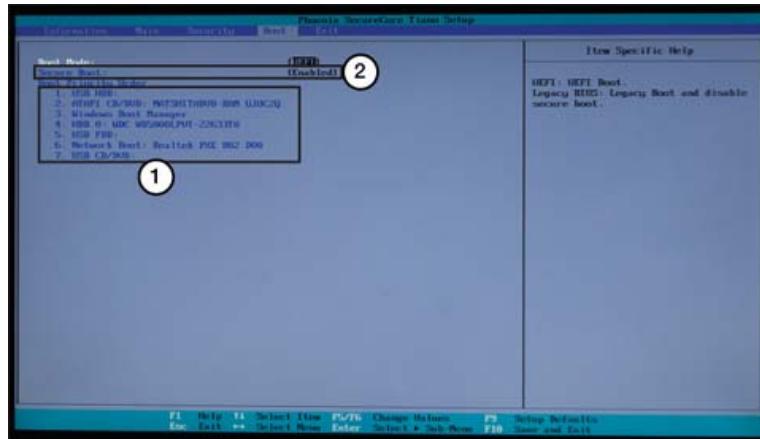




1. Boot sequence
2. Other OS setting secure boot disabled
3. Other boot options

**Figure 3-57** Boot Sequence and Other Boot Settings in the UEFI/BIOS Features Menu

**Key Topic**



1. CD/DVD and USB flash boot before windows boot manager or hard disk drive
2. Secure boot enabled

**Figure 3-58** A Typical Boot Menu Configured to Permit Booting from a CD/DVD or USB Flash Drive Before the Hard Drive

Enabling Fast Boot skips memory and drive tests to enable faster startup. Enabling Boot Up NumLock turns on the keyboard's NumLock option.

The menus shown in [Figures 3-57](#) and [3-58](#) are used to adjust the order in which drives are checked for bootable media. For faster booting, set the hard drive with

system files as the first boot device. However, when you want to have the option to boot from an optical (CD/DVD/Blu-ray) disc or from a USB flash or hard drive for diagnostics or operating system installations, put those drives before SATA hard drives in the boot order.

### Note

Even when the first boot drive is set up as CD/DVD, some discs prompt the user to press a key to boot from the CD/DVD drive when a bootable disc is found. Otherwise, the system checks the next available device for boot files.

## Firmware Updates



Interestingly, a flash BIOS update is not available from BIOS manufacturers (Phoenix, Insyde, AMI, and Award/Phoenix). They do not sell BIOS updates because their basic products are modified by motherboard and system vendors. Following are the general steps to locate a flash BIOS update and install it:

**Step 1.** For major brands of computers, go to the vendor's website and look for links to downloads or tech support. The BIOS updates are listed by system model and by version; avoid beta (prerelease) versions.

### TIP

If your system is a generic system (that is, it came with a mainboard or motherboard manual and other component manuals instead of a full system manual), you need to contact the motherboard maker.

You can also buy a replacement flash BIOS file from [www.eSupport.com](http://www.eSupport.com) if you cannot get an updated BIOS code from your system or motherboard vendor.

To determine the motherboard's make and model, you can download and run Belarc Advisor (free for personal use) from [www.belarc.com/free\\_download.xhtml](http://www.belarc.com/free_download.xhtml).

See the following websites for additional help:

- Wims BIOS page ([www.wimsbios.com](http://www.wimsbios.com))
- BIOSAgentPlus ([www.biosagentplus.com](http://www.biosagentplus.com))
- AMI (American Megatrends International LLC, formerly American Megatrends Inc.): <https://www.ami.com>

**Step 2.** Locate the correct BIOS update for your system or motherboard. For generic motherboards, the Wims BIOS page also has links to the motherboard vendors' websites.

**Step 3.** Determine the installation media needed to install the BIOS image. Many recent systems use a Windows-based installer, but some use a bootable CD or USB flash drive.

**Step 4.** Be sure to download all the files needed to install the BIOS image. In most cases, a download contains the appropriate loader program and the BIOS image. For some motherboards, you might also need to download a separate loader program. If the website has instructions posted, print or save them for reference.

**Step 5.** If you need to create bootable media, follow the vendor's instructions to create the media and place the loader and BIOS image files on the media.

**Step 6.** To install from bootable media, follow step 6a. To install from within Windows, follow step 6b.

**Step 6a.** To install from bootable media, make sure the drive is the first item in the BIOS boot sequence. Insert or connect your media, and restart the system. If prompted, press a key to start the upgrade process. Some upgrades run automatically, others require you to choose the image from a menu, and still others require the actual filename of the BIOS. The BIOS update might also prompt you to save your current BIOS image. Choose this option, if possible, so that you have a copy of your current BIOS, in case a problem arises. After the process starts, it takes approximately 3 minutes to rewrite the contents of the BIOS chip with the updated information.

**Step 6b.** For installation from Windows, close all Windows programs before you start the update process. Navigate to the folder containing the BIOS update, and double-click it to start the update process. Follow the prompts onscreen to complete the process. It takes approximately 3 minutes to rewrite the contents of the BIOS chip with the updated information.

## CAUTION

While performing a flash upgrade, make sure you do not turn off the power to your PC and that you keep children or pets away from the computer, to prevent accidental shutdown. Wait for a message indicating that the BIOS update has been completed before you touch the computer. If the power goes out during the flash update, the BIOS chip could be rendered useless.

**Step 7.** Remove the media and restart the system to use your new BIOS features. Reconfigure the BIOS settings, if necessary.

## Recovering from a Failed BIOS Update

If the primary system BIOS is damaged, keep in mind that some motherboard vendors offer dual BIOS chips on some products. The secondary BIOS performs the same functions as the primary BIOS so the system can continue to run.

If you use the wrong Flash BIOS file to update your BIOS, or if the update process does not finish, your system cannot start. You might need to contact the system or motherboard maker for service or purchase a replacement BIOS chip.

In some cases, the BIOS contains a “mini-BIOS” that can be reinstalled from a reserved part of the chip. Systems with this feature have a jumper on the motherboard called the *flash recovery jumper*.

To use this feature, download the correct flash BIOS, make a bootable disc from it, and take it to the computer with the defective BIOS. Set the jumper to Recovery, insert the bootable media, and then rerun the setup process. Because the video will not work, you need to listen for beeps and watch for the drive light to run during this process. Turn off the computer, reset the jumper to Normal, and then restart the computer.

If the update cannot be installed, your motherboard might have a jumper that write-protects the flash BIOS. Check the manual to see whether your system has this feature. To update a BIOS on a system with a write-protected jumper, you must follow these steps:

- Step 1.** Disable the write protection.
- Step 2.** Perform the update.
- Step 3.** Reenable the write protection to keep unauthorized people from changing the BIOS.

## Security Features



Security features of various types are scattered around the typical system BIOS/UEFI dialog boxes. Features and their locations vary by system and might include the following:

- **BIOS/UEFI password:** BIOS Settings Password or Security dialog boxes
- **Power-on password:** Configured through the Security dialog box
- **Chassis intrusion:** Various locations
- **Boot sector protection:** Advanced BIOS Features dialog box

These features support drive encryption:

- **TPM (trusted platform module):** Security dialog box
- **LoJack for laptops:** An after-market product embedded in firmware or installed by the end user; not managed with BIOS dialog boxes
- **Secure Boot:** Boot or other dialog boxes

Enable the BIOS password feature to permit access to BIOS setup dialog boxes only for those with the password. The power-on password option prevents anyone without the password from starting the system. Note that these options can be defeated by opening the system and clearing the CMOS memory.

When intrusion detection/notification, also known as chassis intrusion, is enabled, the BIOS displays a warning on startup that the system has been opened.

Boot sector protection, found primarily on older systems, protects the default system drive's boot sector from being changed by viruses or other unwanted programs. Depending on the implementation, this option might need to be disabled before an operating system installation or upgrade.

Windows editions that support the BitLocker full-disk encryption feature use the **Trusted Platform Module (TPM)** to protect the contents of any specified drive. Although many corporate laptops include a built-in TPM module, desktop computers and servers might include a connection for an optional TPM.

LoJack for laptops (and other mobile devices) is a popular security feature embedded in the laptop BIOS of a number of systems, and it can be added to other systems. It consists of two components: a BIOS-resident component and the Computrace Agent, which is activated by LoJack when a computer is reported as stolen. To learn more about LoJack for laptops, tablets, and smartphones, see <https://homeoffice.absolute.com>.

**Secure Boot** (refer to [Figures 3-57 and 3-58](#))—blocks installation of other operating systems and also requires the user to access UEFI setup by restarting the computer in a special troubleshooting mode from within Windows 10/11. Secure Boot is enabled by default on systems shipped with Windows 10/11. Linux users or those who want more flexibility in accessing UEFI/BIOS (for example, technicians making changes in UEFI firmware) should disable Secure Boot.

## Interface Configurations

Typical desktop systems are loaded with onboard ports and features, and the menus shown in [Figure 3-59](#) through 3-63 are typical of the BIOS menus used to enable, disable, and configure storage, audio, network, and USB ports.



**Figure 3-59** Fan Settings Shown in ASUS UEFI BIOS Utility's Advanced Mode



1. SATA ports enabled
2. SATA ports configured to run in AHCI mode
3. Port 0 is connected to a 250GB SSD
4. Port 1 is connected to a DVD optical drive

**Figure 3-60** A UEFI Configuration Dialog Box for SATA Ports



1. USB 3.0 host adapter enabled
2. Charging option being edited

**Figure 3-61** Configuring a USB Host Adapter for Battery Charging



1. HD Audio enabled
2. Change to HDMI to permit HDMI cable to carry audio as well as video signals

**Figure 3-62** Configuring Onboard HD Audio



1. Ethernet network adapter enabled
2. LAN Option ROM (for booting from network) disabled

**Figure 3-63** Configuring an Onboard Network Adapter

## Fan Considerations

Internal fan-related settings can be accessed in BIOS/UEFI. Adjustments can be made to CPU fans and, in some cases, other fans such as chassis fans. Fans that bypass the motherboard and connect directly into the power supply cannot be adjusted from BIOS/UEFI. Fans that connect directly into the motherboard, such as Pulse Width Modulation (PWM) fans, are typically adjustable from BIOS/UEFI settings. The fan settings options vary among motherboard vendors. Some BIOS/UEFI settings offer generic options, such as Quiet or Performance. Others offer options that can adjust the speed or percentage at which the fans are operating (see [Figure 3-59](#)). In some BIOS/UEFI models, settings can be implemented that adjust the fan speed based on the temperature inside the case.

## SATA Configuration

Use the SATA configuration options (such as those shown in [Figure 3-60](#)) to enable or disable SATA and eSATA ports and to configure SATA host adapters to run in compatible (emulating PATA), native (AHCI), or RAID modes. AHCI supports native command queuing (NCQ) for faster performance and permits hot swapping of eSATA drives.

## USB Host Adapters and Charging Support

Most systems have separate settings for the USB (2.0) and USB 3.0/3.1/3.2 (a.k.a. SuperSpeed) controllers (on systems that have USB 3.0/3.1/3.2 ports). If you don't enable USB 2.0 or USB 3.0/3.1/3.2 in your system BIOS, all your system's USB ports will run at the next-lower speed.

Some USB configuration utilities can also be used to enable a specified USB port to output at a higher amperage than normal, to enable faster charging of smartphones. [Figure 3-61](#) illustrates a system with USB 3.0 support enabled and battery charging support being enabled.

## Audio and Ethernet Ports

Depending on the system, audio and Ethernet ports and other integrated ports might be configured using a common menu or separate menus. In [Figure 3-62](#), the HD Azalia onboard audio is enabled; with a separate sound card installed, onboard audio should be disabled. SPDIF audio can be directed through the SPDIF digital audio port (default) or the HDMI AV port (optional) using this menu.

In [Figure 3-63](#), the option Onboard LAN Option ROM is disabled on this system. Enable it when you want to boot from an operating system that is stored on a network drive.

## CMOS Battery



The system BIOS is responsible for configuring the ports and features controlled by the chipset, and the CMOS chip on the motherboard stores the settings. The CMOS battery provides power to maintain the contents of the CMOS chip (see [Figure 3-64](#)). Battery life is several years, but a low CMOS battery can cause problems with drivers and sometimes booting. Because date and time settings are stored in CMOS, date and time errors can be a good indication that it is time to check or change the battery.





1. CR2032 CMOS battery
2. Jumper block for clearing CMOS memory

**Figure 3-64** A Typical CMOS Battery (CR2032)

To clear CMOS on most systems, place a jumper block over two jumper pins.

### Note

Some systems feature a port cluster-mounted push button to clear the CMOS. If you need to clear the CMOS on a particular system, check the documentation for details.

## Encryption

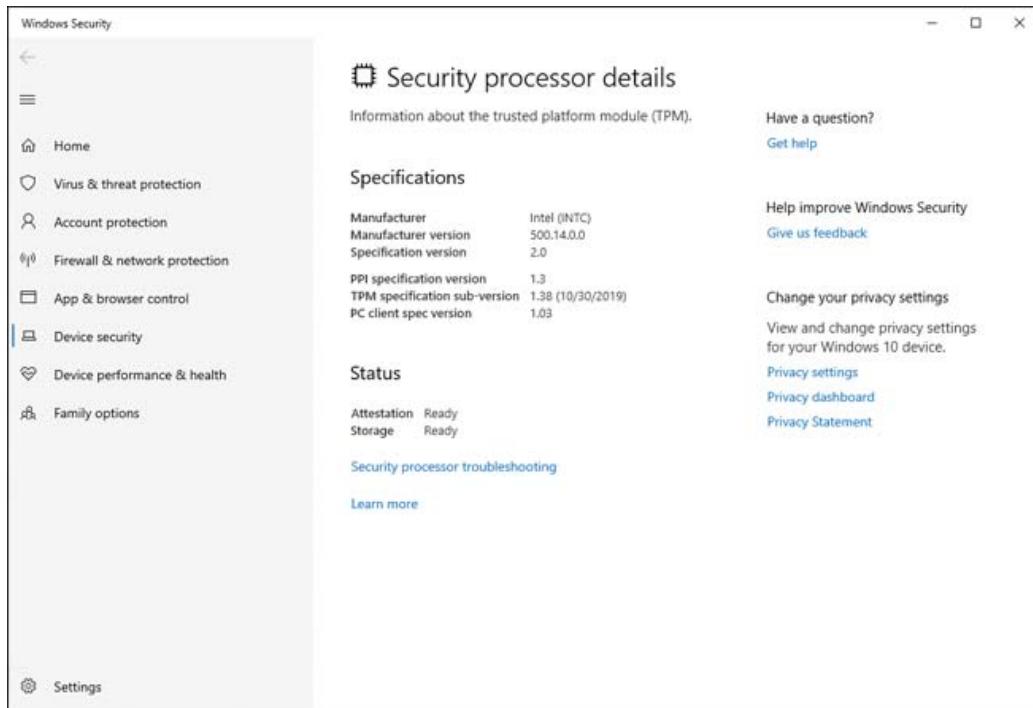
Security has become the major concern in the design, manufacturing, and use of computers. Hackers find vulnerabilities in software to get into computers and compromise data. One method of mitigating the security threats is to have security processes separate from the software. To do this, specialized chips have been developed to manage hardware security away from the CPU. TPMs and HSMs are designed for different tasks, but both are important to desktop and laptop security.

## Trusted Platform Module (TPM)

As previously mentioned, a Trusted Platform Module (TPM) is a chip embedded into the motherboard of a desktop or laptop that enhances hardware security. The tasks it performs include generating and storing cryptographic keys to be used by the operating system, and managing authentication of the user booting up the system. Because they are processed separately from the CPU, there is little chance that the CPU can be hacked to acquire the keys.

The TPM provides full disk encryption capabilities and protects disks during the boot process until the operating system can complete authentication. The TPM chip actually has its own small operating system for generating encryption keys separately from the CPU.

TPMs are enabled in the BIOS/UEFI settings and are designed to be sure that the operating system is authentic and that the correct owner is booting the computer, but they do not manage other security keys needed by applications. Every certified Windows 11 system comes with a TPM chip. To view information about the TPM, open the Windows Defender Security application, select Device Security from the left menu, and then select Security Processor Details (see [Figure 3-65](#)).



**Figure 3-65** Information About the TPM on Windows

## Hardware Security Module (HSM)

A **hardware security module (HSM)** is not embedded into the motherboard. Instead, it is an added module or external device that can be added for storing security keys for general use.

An important difference between TPMs and HSMs is that HSMs can store encryption data, but they do not generate the encryption keys as the TPMs do. Because HSMs are not embedded into the motherboard, they must access the CPU via USB, mounted in an extension slot, or, if being used by a network, via TCP/IP.

Smartphones have similar chips on their motherboards for isolating security data, but they are beyond the scope of the current A+ exam.

## CPU Architecture

The architecture of a CPU refers to how it is designed to process data with its instruction set architecture (ISA). The ISA tells the CPU what to do and how to

accomplish it. CPU manufacturers have adopted similar architectures, which are discussed in this section.

## x64/x86

Early CPUs from Intel were developed on the x86 architecture, which eventually allowed for 32-bit processing by the CPU. This means that 32 bits of data could be processed at one time and the CPU could address up to 4GB of RAM.

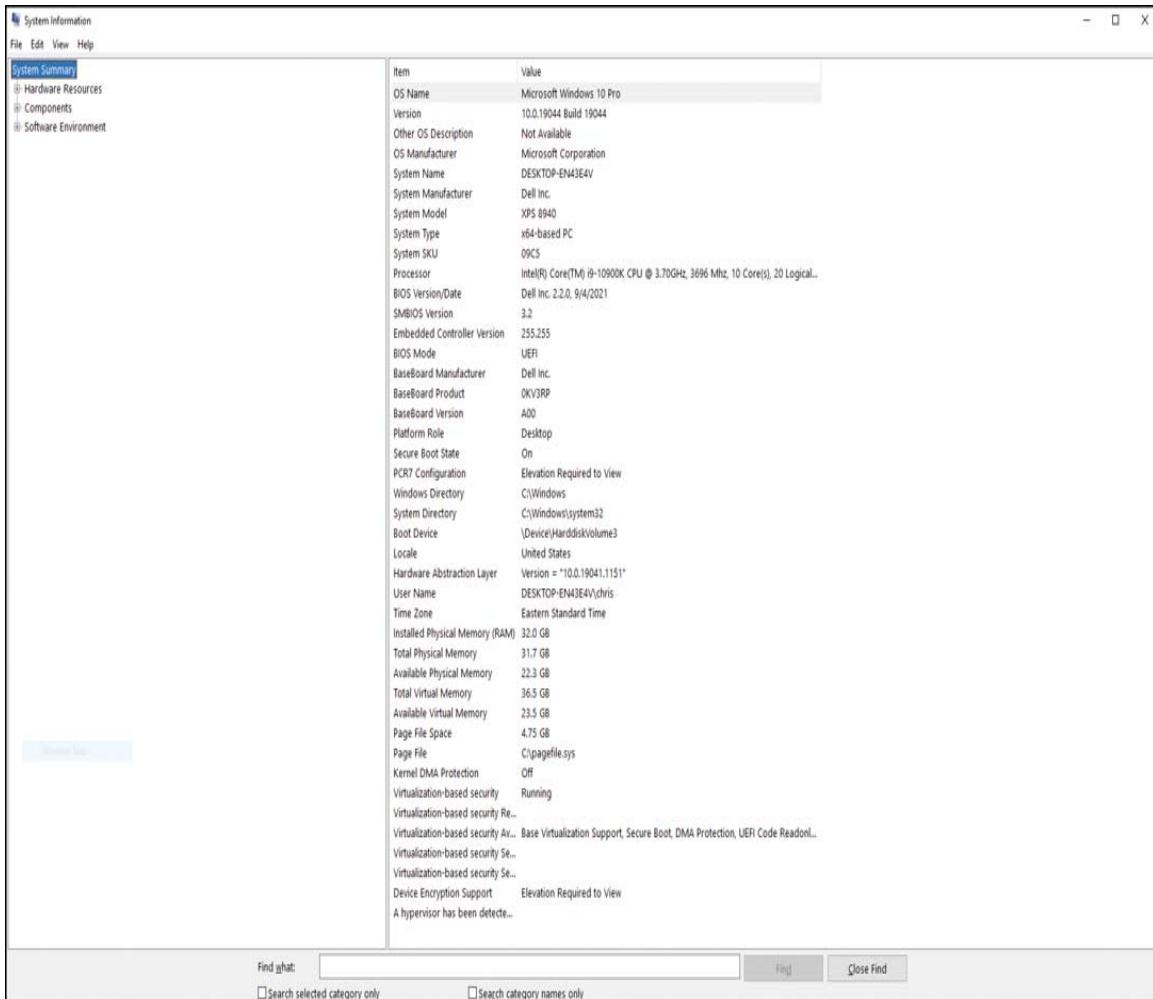
This worked well for years, until more complex software needed more memory and faster processing. AMD developed the x64 CPU (also known as the x86-64), which greatly expanded the speed and memory access. The two most common architectures in use today by CPU manufacturers are the x86 and the x64.

[Table 3-19](#) outlines the key differences between the x86 and the x64.

**Table 3-19** Comparison of x86 and x64 CPUs

Architecture x86	x64
Bit processing	32
RAM access	4GB
Common uses	Tablets, lower-end laptops, mobile devices
	Most desktops and laptops, gaming, 3D rendering

It is important to note that x64 CPUs can easily run the 32-bit x86 architecture, but the reverse is not true. To see if your Windows machine is running in 32- or 64-bit mode, search for “system information” to retrieve the data in [Figure 3-66](#).



**Figure 3-66** Determining CPU Type

## Advanced RISC Machine (ARM)

Reduced Instruction Set Computer (RISC) was designed to simplify CPUs from the x86 standards. Making the instruction set smaller for tasks enabled chip manufacturers to use fewer transistors, improving the efficiency of the computing process.

**Advanced RISC Machines (ARM)** is a processor architecture that is based on RISC. ARM is the most widely used instruction set architecture. ARM processors are low cost, have minimal power consumption, and generate lower heat, making them ideal for devices such as smartphones, tablets, laptops, and other embedded systems. However, ARM processors are also utilized in desktops and servers. Additionally, ARM architecture is implemented on operating systems such as Windows, UNIX, Apple iOS, and Android.

## CPU Cores: Single Core and Multicore



A processing core is the part of the CPU that gets instructions from software and performs the calculations for output. Early computers had **single-core** processors to do all the work. As demands on CPUs grew, single-core processors could not keep up.

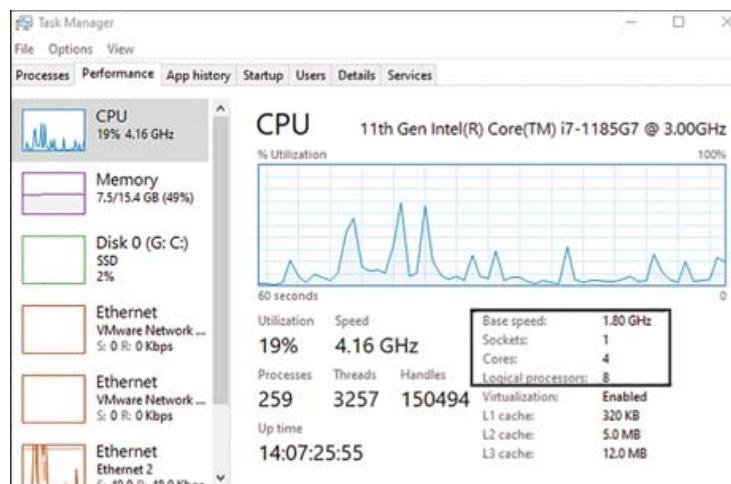
Two or more physical processors in a system enable it to perform much faster when multitasking or running multithreaded applications. However, as mentioned earlier, systems with multiple processors are expensive to produce and are best used in server and enterprise computing. **Multicore** processors, which combine two or more processor cores into a single physical processor, provide virtually all the benefits of multiple physical processors, are lower in cost, and work with any operating system that supports traditional single-core processors. The operating system sees each core as a CPU.

## Multithreading

CPUs process the data from the operating systems, and delays in moving data in and out of the CPU meant there was downtime. Designers found an elegant way to “thread” additional work into the CPU while it was waiting for other operating instructions. This way, one physical core could behave like two logical cores. This process, known as hyperthreading, allowed much more processing than with one core alone.

As CPUs developed and added cores, **multithreading** was designed as a method to allow multiple threads on each core. This works differently from hyperthreading: Multithreading breaks each core into logically smaller CPUs to handle more sets of operating instructions, resulting in higher CPU performance.

The relationship between the motherboard socket, the cores in the CPU, and the logical processing from multithreading can be easily seen in the Task Manager in Windows, on the Performance tab. [Figure 3-67](#) depicts a typical laptop or desktop CPU at work.



**Figure 3-67** Task Manager Depicting One Socket Holding a CPU with Four Cores Being Threaded, with the Capacity of Eight Logical Processors

## Virtualization Support

Creating and managing a virtual version of a computer (or any device) is a rapidly growing sector in computing. (See [Chapter 4, “Virtualization and Cloud Computing,”](#) for further discussion of virtualization.) Most current AMD and Intel processors feature virtualization support, also known as hardware-assisted virtualization. Virtualization support allows a physical CPU to be emulated as multiple individual CPUs that can be used in a virtualized operating system. This enables virtualized operating systems and applications to run faster and use fewer system resources. The benefits are too many to discuss here, but think of it as getting two or more computers running in software, but buying only one piece of hardware to run them. To check whether a Windows device has virtualization support enabled or disabled, navigate to the Task Manager; the Performance tab shows those details (see [Figure 3-67](#)). Virtualization is enabled and disabled through BIOS/UEFI firmware settings.

## CPU Speeds

Different components of the motherboard—such as the CPU, memory, chipset, expansion slots, storage interfaces, and I/O ports—connect with each other at different speeds. The term *bus speeds* refers to the speeds at which different buses in the motherboard connect to different components. On a motherboard, the bus is the path data takes between the internal components of the computer.

Some of these speeds, such as the speed of I/O ports and expansion slots (USB, Thunderbolt, and SATA ports, as well as PCI and PCIe slots), are established by the design of the port or by the capabilities of the devices connected to them. However, depending on the motherboard, you might be able to fine-tune the bus speeds used by the processor, the chipset interconnect, and memory. These adjustments, where available, are typically performed through BIOS/UEFI firmware settings in menus such as Memory, Overclocking, and AI Tweaker.

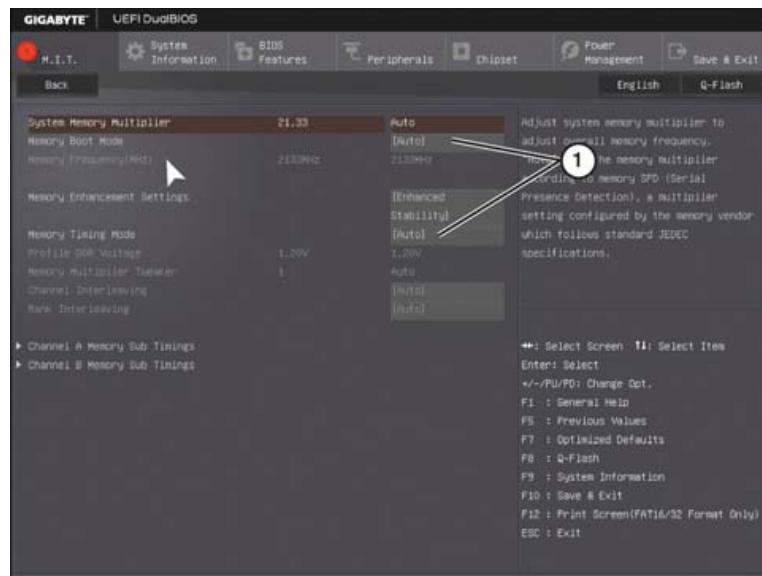
[Figure 3-68](#) shows the dialog box for the CPU (processor) overclocking UEFI firmware for a system with an Intel i5 processor. The dialog box indicates the current CPU and memory multipliers that can be adjusted.



1. Enter this menu to overclock processor (CPU)
2. CPU clock speed based on current base clock speed and ratio
3. Memory speed based on current base clock speed and ratio
4. CPU base clock speed

**Figure 3-68** CPU and Memory Speed Information on a System That Allows Speed Adjustment

Figure 3-69 illustrates the dialog box for memory overclock adjustments on the same system. To change the CPU speed, memory timing, or other adjustments, change the Auto setting and enter the desired values. On this system and others, you can select a CPU overclocking value; other settings are adjusted automatically as needed.



1. Change from [Auto] to overclock memory

**Figure 3-69** Preparing to Overclock Memory

## **Expansion Cards**

Most new CPUs come with integrated video, which is sufficient for everyday use. However, users of graphics applications and gamers will likely find a benefit in upgrading to an onboard graphics card that has dedicated memory space for graphics.

The more integrated graphics processors are called upon, the more memory is used for processing and the more heat is generated by the CPU. A good video card has a separate processing chip and a cooling system that takes the load off the CPU and frees up space for the CPU to run more efficiently.

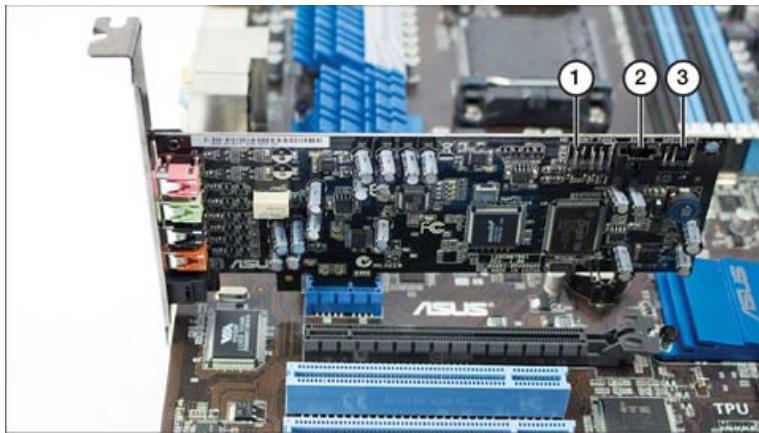
## **Installing Sound Cards**

A sound card converts the digital sound signal into an analog sound experience preferred by the human ear. For most users, the onboard sound card that is integrated into the motherboard is fine, but some users want high-fidelity sound for home theaters and music mixing. Purchasing an internal sound card that is more powerful and has more input/output options makes sense for professionals who work with sound.

Installing a sound card is similar to installing a video card. Before installing a sound card, be sure to disable onboard audio with the system BIOS/UEFI setup program and uninstall any proprietary mixer or configuration apps used by onboard audio.

To install a sound card, follow these steps:

- Step 1.** Shut down the computer and disconnect it from AC power.
- Step 2.** Open the case to gain access to the PC's expansion slots.
- Step 3.** Select an empty PCIe or PCI expansion slot that is appropriate for the form factor of the sound card to be installed.
- Step 4.** Remove the corresponding bracket from the back of the case.
- Step 5.** Insert the card into the slot (see [Figure 3-70](#)).



1. Front panel audio header
2. Aux in (from optical drive)
3. SPDIF out digital audio header

**Figure 3-70** A Typical PCIe Sound Card with 5:1 Surround Audio After Being Inserted into an Expansion Slot

**Step 6.** Secure the card bracket into place, using the screw or locking mechanism you removed or released in step 4.

**Step 7.** Connect any header cables as needed (refer to Figure 3-70).

**Step 8.** Connect speakers, microphone, and line-in and line-out cables as needed to support your audio or home theater subsystem.

**Step 9.** Close the system.

**Step 10.** Reconnect AC power and restart the system.

**Step 11.** Install the driver files provided with the sound card, or install updated versions provided by the vendor.

**Step 12.** If they were not already installed in step 11, install the mixer and configuration utilities provided with the new sound card.

## External USB Audio Sound Cards

An external USB sound card can allow for higher-quality sound and multiple adapter input/output jacks. These sound cards really look more like USB-attached devices than cards, but they perform the same task as cards (for an example, see [Sewelldirect.com](http://Sewelldirect.com)). You can also add surround audio with a USB-based audio device. This is a good solution for laptops and for systems with limited or no expansion slots.

### Installing a USB Audio Sound Card

To install a USB audio device, follow these steps:

**Step 1.** Turn off the computer.

**Step 2.** Connect the USB audio device to the computer's USB 2.0, USB 3.0, or USB4 port.

**Step 3.** Turn on the computer and then turn on the device. The computer installs audio drivers automatically.

**Step 4.** If needed, install additional or updated drivers downloaded from the vendor's website or provided with the device.

## Configuring a Sound Card with Windows

To configure a sound card, onboard audio, or USB audio with Windows, follow these steps:

**Step 1.** Type **Sound Settings** in the search box.

**Step 2.** Select the **Sounds** icon in the Control Panel.

**Step 3.** Select the **Playback** tab and adjust the settings.

**Step 4.** Select the **Recording** tab and adjust the settings.

**Step 5.** To specify sounds to play during Windows events (startup, shutdown, errors, and program events), use the **Sounds** tab.

**Step 6.** Click **Apply** and then click **OK** to accept changes.

If the sound card or onboard audio includes proprietary management or configuration programs, run them from the Start menu.

## Configuring a Sound Card with macOS

To configure a sound card, onboard audio, or USB audio with macOS, follow these steps:

**Step 1.** Open the Apple menu.

**Step 2.** Open System Preferences.

**Step 3.** Select the **Sound** icon.

**Step 4.** Select the **Output** tab.

**Step 5.** Select the device to use for sound output.

**Step 6.** Adjust the balance and volume, and then close the window.

## Configuring a Sound Card with Linux

To configure a sound card, onboard audio, or USB audio with Linux (Ubuntu 21.x), follow these steps:

- Step 1.** Open System Settings.
- Step 2.** Open Sound.
- Step 3.** Under the Output section, select the device to use for sound output.
- Step 4.** Adjust the balance and volume.
- Step 5.** Select the speaker mode (stereo or surround options).
- Step 6.** Click **Test Sound** to verify proper operation.
- Step 7.** Close the window to save the changes.

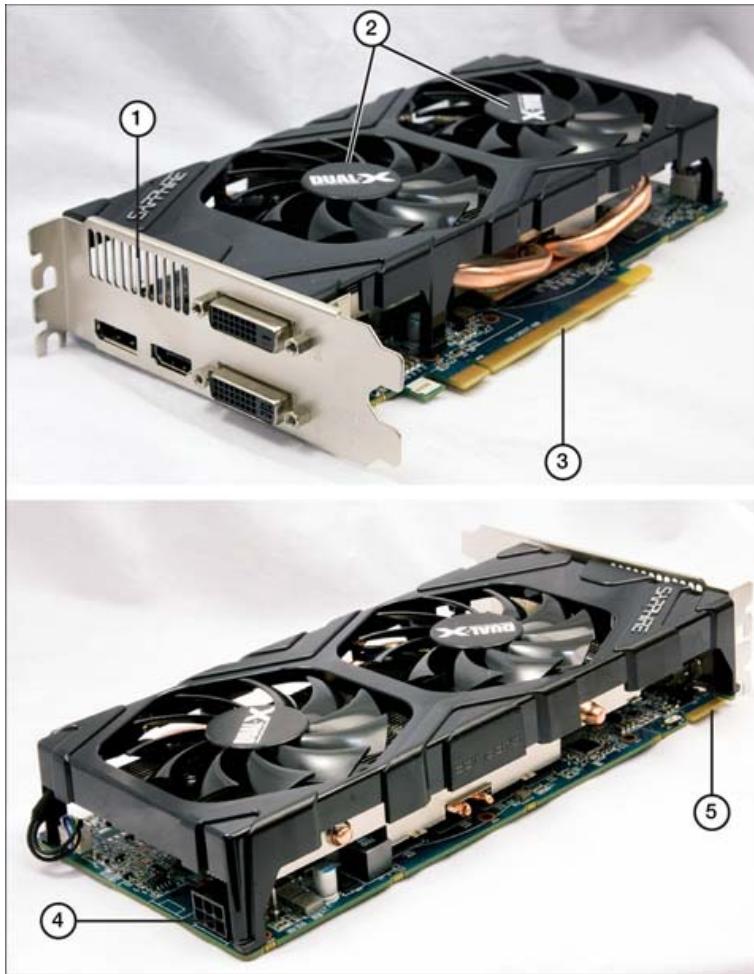
## Installing Video Cards

The installation process for a video card includes three phases:

- Step 1.** Configure the BIOS for the video card being installed.
- Step 2.** Physically install the video card.
- Step 3.** Install drivers for the video card.

[Figure 3-71](#) illustrates a typical high-performance video card that uses an AMD GPU.





1. Exhaust panel for fans
2. Cooling fans
3. PCIe x16 connector
4. PCIe 6-pin power connector
5. Connector for CrossFire multi-GPU cable

**Figure 3-71** A PCIe x16 Video Card Designed for Multi-GPU (CrossFire) Support

## BIOS/UEFI Configuration for Video Cards

Video cards interact differently, depending on the motherboard and BIOS/UEFI settings. When adding a card, you might need to enter BIOS/UEFI to disable the onboard video; some other systems allow both video systems to interact, for better efficiency. These are the basic steps for BIOS/UEFI configuration for video cards:

- Step 1.** Check and adjust the primary VGA BIOS setting (for the primary graphics adapter), as needed:
- Step 2.** Choose **PCIE** or **PCIE > PCI** if you use a PCIe video card. On some systems, the term NB PCIe Video Slot is used for PCIe.
- Step 3.** Choose **PCI** or **PCI > PCIE** if you use a PCI video card.

For onboard video (integrated graphics), see the manufacturer's recommendation. (Onboard video can use PCI or PCI Express buses built into the motherboard.) On some recent systems, Auto is the default setting.

If the installed video card and driver are not working well, but the screen is still visible, remove the card and use the Device Manager Driver Rollback feature to restore the previous driver.

## Removing Drivers for an Old Video Card or Onboard Video



Although all video cards created since the beginning of the 1990s are based on VGA, virtually all of them use unique chipsets that require special software drivers to control acceleration features (faster onscreen video), color depth, and resolution. Whenever you change video cards, you must thus change the video driver software as well. Otherwise, your operating system will drop into a low-resolution mode and might give you an error message because the driver does not match the video card.

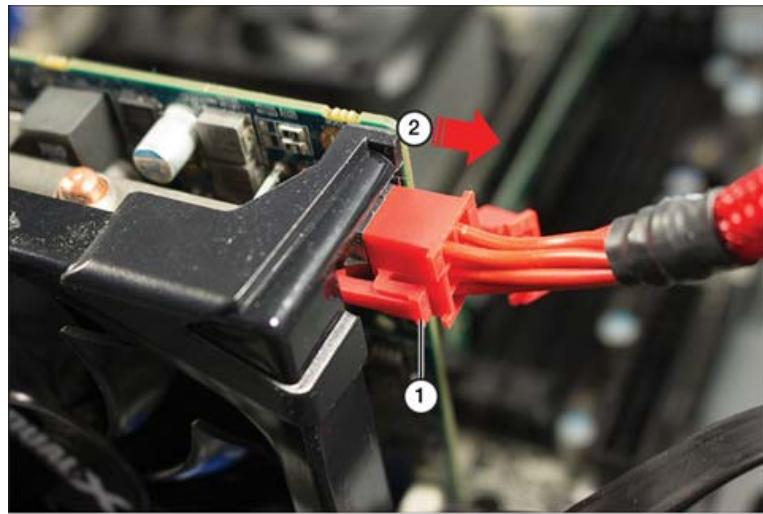
To delete an old video driver in Windows, open **Control Panel > Device Manager** and delete the listing for the current video card. Right-click on a program and select Uninstall in Programs and Features; then uninstall the driver or configuration apps used by the current video card.

It is not necessary to delete old drivers in macOS or Linux.

## Removing the Old Video Card

Follow these steps to remove an old video card (if present):

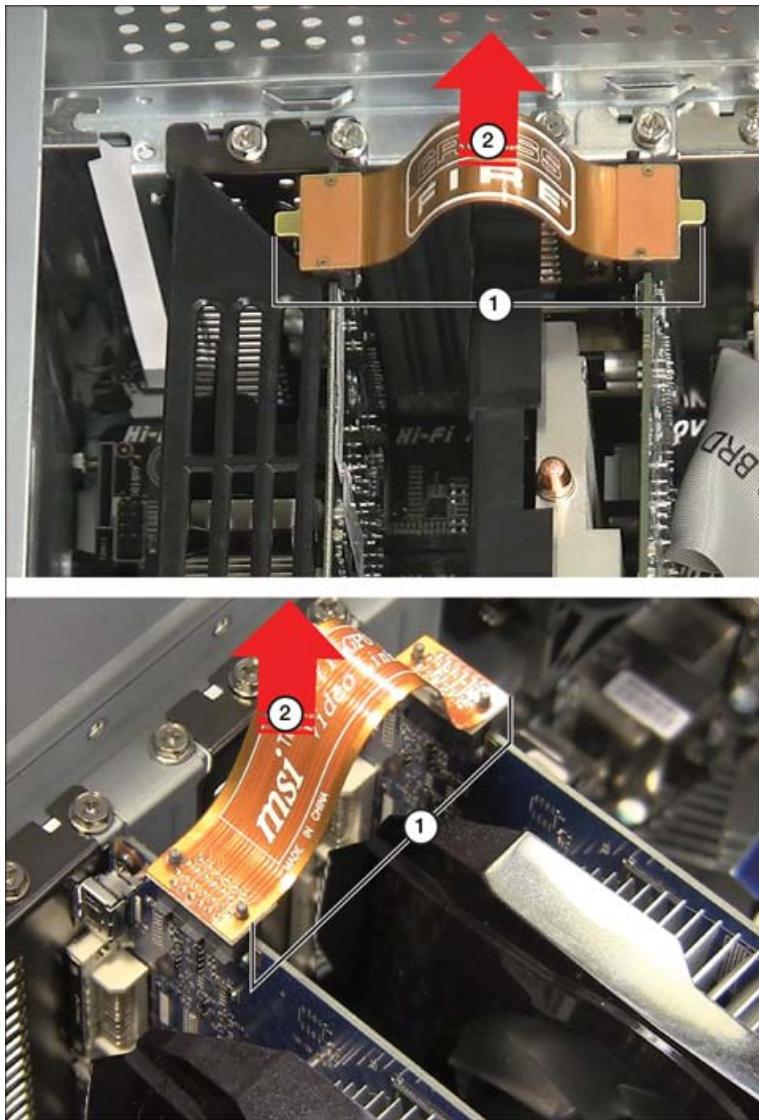
- Step 1.** Shut down the computer and disconnect it from AC power.
- Step 2.** Turn off the display.
- Step 3.** Disconnect the data cable attached to the video card.
- Step 4.** Open the case.
- Step 5.** Disconnect any power cables running to the video card (see [Figure 3-72](#)).



1. Push locking tab in
2. Pull power cable away from card

**Figure 3-72** Removing the PCIe Power Cable from a Video Card

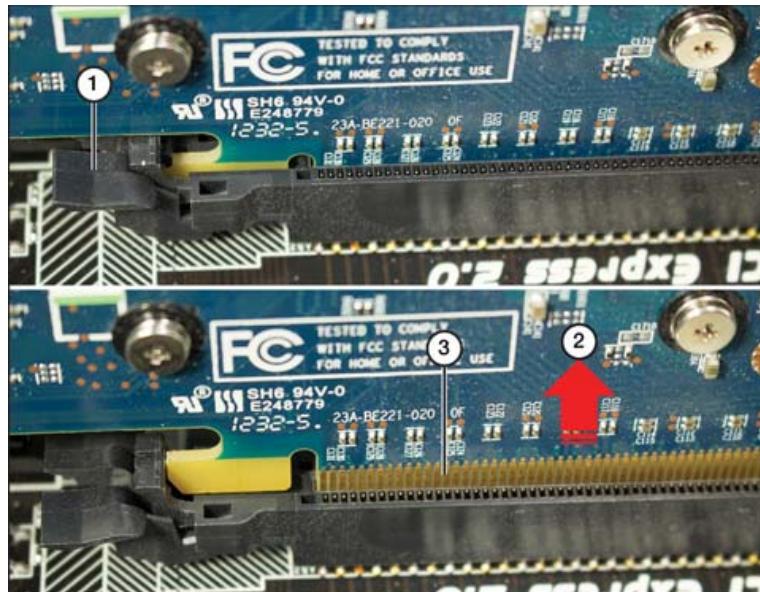
**Step 6.** Remove SLI (NVIDIA) or CrossFire (AMD) cables connected to any card(s) you are removing (see [Figure 3-73](#)).



1. Lift up ends of connector cable to release
2. Lift connector cable out of system

**Figure 3-73** SLI and CrossFire Cables, which Should Be Removed Before Removing the Video Cards for Replacement

**Step 7.** Remove the old video card(s) by removing the screw holding a card bracket in place and releasing the card-retention mechanism that holds video card in place (see [Figure 3-74](#)). Repeat for each video card.



1. Push down on locking tab
2. Pull up on card
3. Card connectors now visible

**Figure 3-74** Releasing the Card-Retention Mechanism Before Removing a PCIe x16 Video Card

### Note

Card-retention mechanisms vary widely among motherboards. In addition to the design shown in [Figure 3-74](#), some use a lever that can be pushed to one side to release the lock; others use a knob that is pulled out to release the lock.

To complete a CrossFire or SLI installation, use the configuration apps supplied with the video card drivers to enable CrossFire or SLI, and select specific 3D performance settings.

## Video Card Physical Installation



Follow these steps to install the new video card:

- Step 1.** Insert the new video card into a PCIe x16 slot. If the motherboard has two or more PCIe x16 slots, use the slot closest to the port cluster for the primary (or only) card.
- Step 2.** Lock the card into position with the card-retention mechanism and with the screw for the card bracket.

**Step 3.** If the card uses power, connect the appropriate PCIe power connector to the card (refer to [Figure 3-72](#)).

**Step 4.** If the card is running in multi-GPU mode and uses SLI or CrossFire, connect the appropriate bridge cable between the new card and a compatible existing (or new) card in the system (refer to [Figure 3-73](#)).

**Step 5.** Reattach the data cable from the display to the new video card.

## Driver Installation

Driver installation takes place when the system is restarted:

**Step 1.** Turn on the display.

**Step 2.** Reconnect power to the system and turn on the computer.

**Step 3.** Provide video drivers as requested; you might need to run an installer program for the drivers. If you are installing the card under Linux, check with the card vendor for downloadable Linux drivers for your distribution.

**Step 4.** If the monitor is detected not as a Plug and Play monitor but as a default monitor, install a driver for the monitor.

### Note

A driver disc or thumb drive might have been packed with the monitor, or you might need to download a driver from the monitor vendor's website. If you do not install a driver for a monitor identified as a default monitor, you will not be able to choose from the full range of resolutions and refresh rates the monitor actually supports.

## Integrated Graphics Processing Unit (GPU)

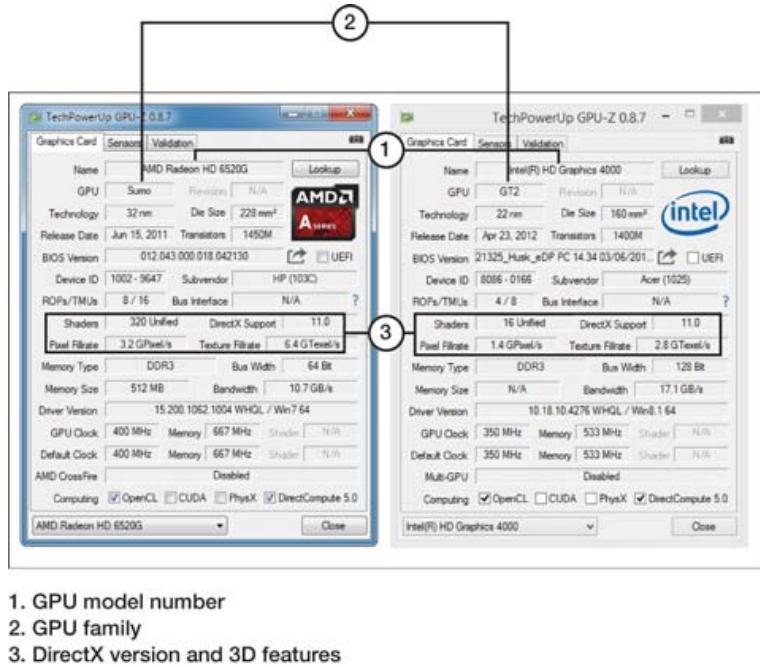
Integrating the GPU into the processor facilitates faster video processing, easier access to memory, and lower-cost systems. The Intel Core i3, i5, and i7 CPUs and the AMD A-series advanced processing units (APUs) are the first processors to have integrated GPUs. The newer series from AMD, Ryzen 5 and Ryzen 7, and Intel i9 continue to improve on GPU processing.

Intel uses three different names to refer to its processor-integrated graphics:

- HD Graphics refers to base-level 3D graphics in any given processor family. Specific features vary by processor family.
- Intel UHD Graphics for 12th generation, formerly code-named Alder Lake, was released in 2021.
- Intel Iris Xe Graphics, formerly code-named Alder Lake, was released in 2022.

Several families of CPUs exist; you can find information about their GPUs at [www.intel.com](http://www.intel.com).

The GPU-Z reporting app from TechPowerUp ([www.techpowerup.com](http://www.techpowerup.com)) can be used to display information about discrete or integrated GPUs. **Figure 3-75** displays information about the HD Graphics 4000 GPU built into an Intel Core i3-2770U processor and the Radeon HD 6520G built into an AMD A6-3420M processor.



1. GPU model number
2. GPU family
3. DirectX version and 3D features

**Figure 3-75** GPU-Z Reports on Intel and AMD Processors with Integrated GPUs

AMD, which also manufactures Radeon GPUs for video cards, integrates Radeon GPU features into its line of APUs, which integrate the CPU and GPU:

- APUs in the Llano and Trinity series use Radeon HD 6xxxD, 7xxxD, and 8xxxD graphics using stream processor technology for 3D graphics. These support OpenGL 4.1 or better and OpenCL 1.1 or better.
- Radeon R7 graphics in the 7000 series use Compute Cores, which permit both CPU and GPU cores to access the same memory. These support OpenGL 4.3 and OpenCL 1.2.
- Radeon R5 graphics in the 7000 series feature fewer Compute Cores and run more slowly than R7, but are otherwise similar.

For more information about APU specifications, see [www.amd.com](http://www.amd.com).

Although the fastest CPU-integrated graphics are suitable for casual gaming as well as general office use, high-performance graphics cards are still recommended for 3D gaming. If a high-performance card is installed, the GPU must be disabled in the BIOS/UEFI.

## Video Capture Cards

Although many TV tuner cards and USB devices are designed to work with analog video sources (S-Video or composite), they are not designed to work with HD video or high-resolution computer or video game sources. A true video **capture card** is equipped to receive HDTV or higher-quality signs via HDMI, DVI, or Component. Video capture cards have built-in hardware support for MPEG-4 recording and can be used to capture video for training, game recording, YouTube, or broadcast purposes. Some video capture devices connect to a USB port.

To install a video capture card, follow these steps:

- Step 1.** Turn off the computer, unplug it, and remove the case cover.
- Step 2.** Locate an available PCIe expansion slot.
- Step 3.** Remove the slot cover and insert the card into the slot. Secure the card in the slot.
- Step 4.** Connect the appropriate cable between the video source (computer, video game, and so on) and the video capture card.
- Step 5.** Close the system, reattach AC power, restart the computer, and provide the driver media when requested by the system.
- Step 6.** Start the capture utility, and capture video or still images from the video source.

## Installing Network Cards

Although most computers include a 10/100/1000 Ethernet port or a Wireless Ethernet (Wi-Fi) adapter, you sometimes need to install a network card (**network interface card [NIC]**) into a computer that you want to add to a network.

To install a Plug and Play (PnP) network card, follow these steps:

- Step 1.** Shut down the computer, disconnect it from AC power, and remove the case cover.
- Step 2.** Locate an available expansion slot that matches the network card's design. (Most use PCIe, but some servers and workstations might use PCI-X and some older desktop systems might use PCI.)
- Step 3.** Remove the slot cover and insert the card into the slot. Secure the card in the slot.
- Step 4.** Reconnect power to the system, restart the system, and provide drivers when requested by the system.
- Step 5.** If you are prompted to install network drivers and clients, insert the operating system disc.

**Step 6.** Connect the network cable to the card.

**Step 7.** Test for connectivity (check LED lights, use a command such as **ping**, and so on), and then close the computer case.

If no slots are available, or if you need to add (or upgrade) network connectivity on a laptop, use a USB-to-Ethernet or USB-to-wireless adapter. Although USB network adapters are also PnP devices, you might need to install the drivers provided with the USB network adapter before you attach the adapter to your computer. After the driver software is installed, the device is recognized as soon as you plug it into a working USB port.

### Note

If you are using a wireless USB adapter, you can improve signal strength by using an extension cable between the adapter and the USB port on the computer. Using an extension cable enables you to move the adapter as needed to pick up a stronger signal.

Most USB network adapters are bus powered. For best results, they should be attached to a USB port built into your computer or to a self-powered hub. Most recent adapters support USB 3.1 Gen 2 (10Gb/s), which provides support for 100BASE-TX (Fast Ethernet, 100Mb/s) and 1000BASE-T (Gigabit Ethernet, 1000Mb/s) signal speeds. A USB 2.0 port (480Mb/s) is adequate for Fast Ethernet but does not run fast enough for Gigabit Ethernet. USB4 offers two versions with differing speeds of 20Gb/s and 40Gb/s.

## Cooling Mechanisms

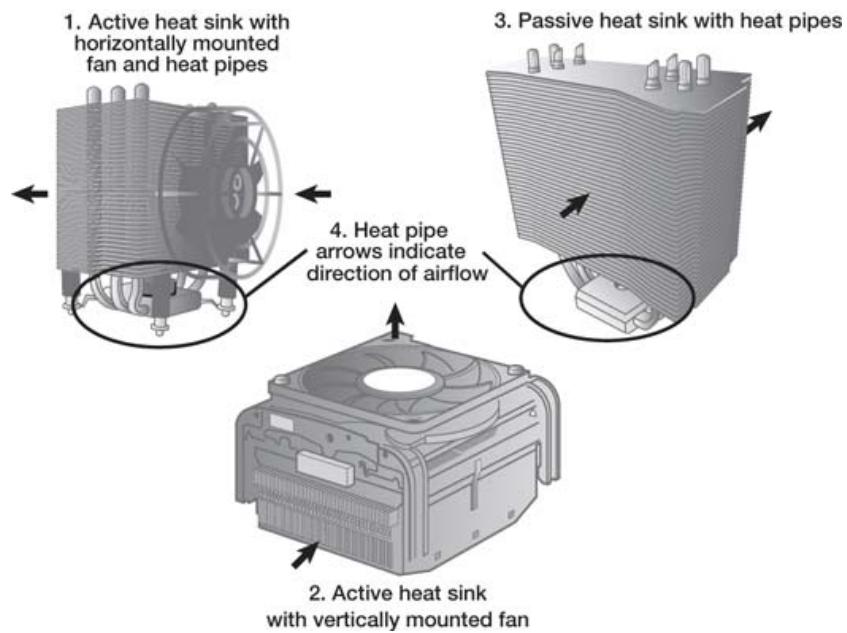
A CPU is one of the most expensive components in any computer, and keeping it cool is important. The basic requirements for proper CPU cooling include the use of an appropriate active heat sink (which includes a fan) and the application of an appropriate thermal material (grease, paste, or a preapplied thermal or phase-change compound). Advanced systems sometimes use liquid cooling instead.

## Fans

A traditional active heat sink includes a cooling fan that rests on top of the heat sink and pulls air past the heat sink in a vertical direction (see [Figure 3-76](#)). However, many aftermarket heat sinks use other designs (see [Figure 3-77](#)).



**Figure 3-76** Stock (Original Equipment) Active Heat Sinks Made for AMD (Left) and Intel (Right) Processors



**Figure 3-77** Typical Third-Party Active and Passive Heat Sinks

## Fanless/Passive Heat Sinks

A passive heat sink does not include a fan, but it has more fins than an active heat sink, to help dissipate heat. One typical use for fanless heat sinks is on low-power processors that are soldered in place on Mini-ITX or similar small form factor motherboard designs, such as the one shown in [Figure 3-78](#).



1. Passive heat sink

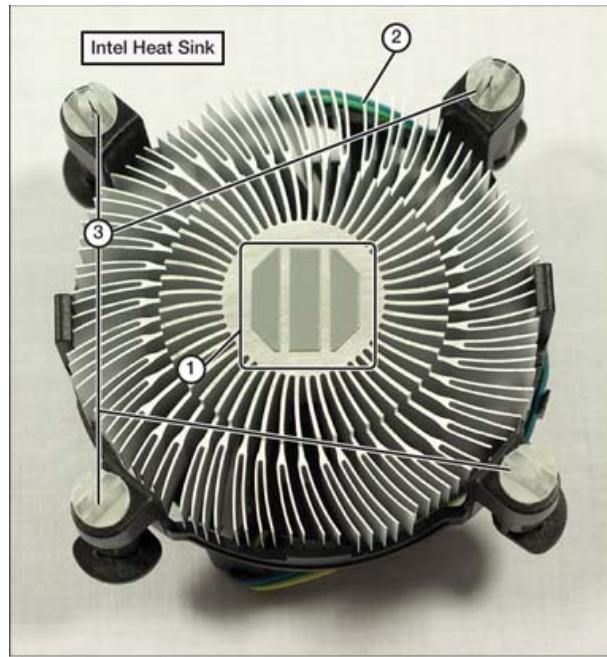
**Figure 3-78** A Low-Power Mini-ITX Motherboard Designed for Home Theater and Media Streaming

## Heat Sink

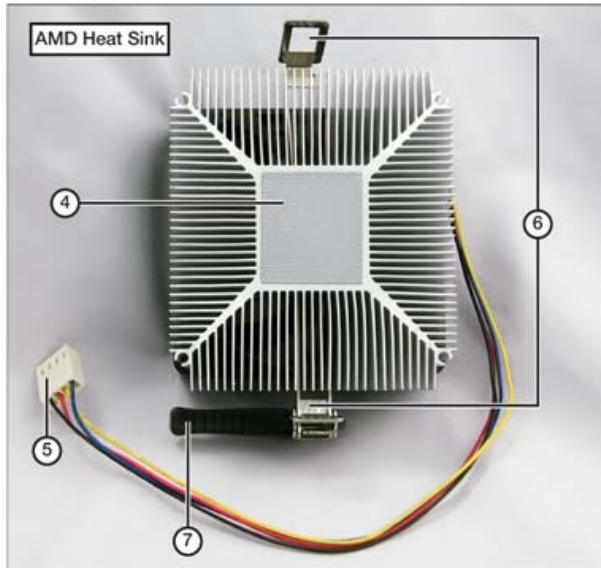


Every processor requires a heat sink. A **heat sink** is a finned metal device that radiates heat away from the processor. In almost all cases, an active heat sink (a heat sink with a fan) is required for adequate cooling. However, if a system case (chassis) is specially designed to move air directly over the processor, then a fanless passive heat sink can be used instead.

Aluminum has been the most common material used for heat sinks, but copper has better thermal transfer properties. Many designs therefore mix copper and aluminum components. ([Figure 3-79](#) in the next section shows two examples of heat sinks.)



1. Preapplied thermal compound
2. Power cable for fan
3. Locking pins for mounting heat sink to motherboard



4. Preapplied thermal compound
5. Power connector for fan
6. Clamping mechanism for mounting heat sink to frame
7. Clamping lever

**Figure 3-79** Bottom View of OEM (Original Equipment Manufacturer) Active Heat Sinks Made for Intel and AMD Processors

## Phase-Change Material/Thermal Paste

Before installing a heat sink bundled with a processor, remove the protective cover over the preapplied thermal material (also known as *phase-change material*) on the heat

sink. When the heat sink is installed on the processor, this material helps ensure good contact between the CPU and the heat sink, to maximize heat transfer away from the CPU. [Figure 3-79](#) illustrates a preapplied thermal material on the bottom of typical Intel and AMD active heat sinks.

### TIP

When you remove a heat sink, keep in mind that the thermal compound acts as an adhesive. Make sure you have loosened the locking mechanism before you remove the heat sink. You might need to exert some force to remove it from the processor.

If you need to remove and reapply a heat sink, be sure to remove all residue from both the processor and the heat sink using isopropyl alcohol, and apply new thermal paste or a thermal pad to the top of the CPU. **Thermal paste** is applied with a syringe; it is important to use the correct amount, about the size of a pea. Applying too little or too much thermal paste will lead to less than effective results; applying too much involves the risk of the material spilling out onto the motherboard. **Thermal pads** can be an easier, less messy option because the material can be cut to size.

## Liquid-Based Cooling

Liquid-based cooling systems for processors, motherboard chipsets, and GPUs are available. Some are integrated into a custom case, whereas others can be retrofitted into an existing system that has openings for cooling fans.

A liquid cooling system involves attaching a liquid cooling unit instead of an active heat sink to the processor and other supported components. A pump moves the liquid (which might be water or a special solution, depending on the cooling system) through the computer to a heat exchanger, which uses a fan to cool the warm liquid before it is sent back to the processor. Liquid cooling systems are designed primarily for high-performance systems, especially overclocked systems. It is essential that only approved cooling liquids and hoses be used in these systems (check with cooling system vendors for details); unauthorized liquids or hoses could leak and corrode system components.

[Figure 3-80](#) illustrates a typical liquid cooling system, compared to a typical Intel OEM heat sink.



1. Radiator
2. Cooler for processor
3. Intel OEM active heat sink (for comparison)

**Figure 3-80** A Typical Liquid Cooling System and Active Heat Sink

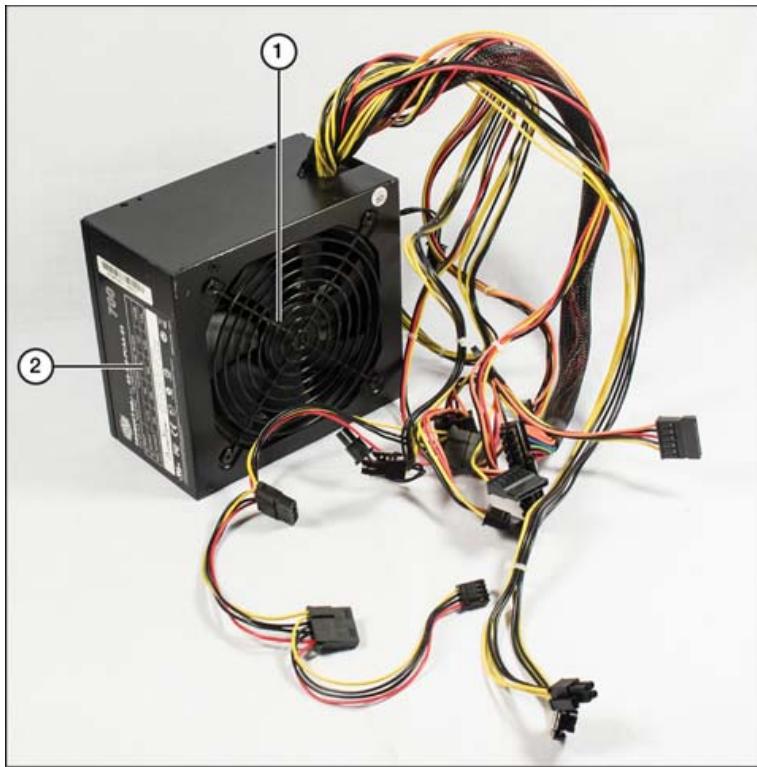
## Power Supplies

**220-1101: Objective 3.5:** Given a scenario, install or replace the appropriate power supply.

220-1101  
Exam

Power supplies vary widely in features and ratings. When building a custom configuration or updating a system to perform a specific task, the power supply is a critical factor in the success of that system.

The power supply is so named because it converts power from high-voltage alternating current (AC) to low-voltage direct current (DC). Many wire coils and other components inside the power supply do the work, and during the conversion process, a great deal of heat is produced. Most power supplies include one or two fans to dissipate the heat created by the operation of the power supply; however, a few power supplies designed for silent operation use passive heat sink technology instead of fans. On power supplies that include fans, fans also help to cool the rest of the computer. [Figure 3-81](#) shows a typical desktop computer's power supply.



1. Power supply intake fan (faces into system)
2. Specification and safety information label

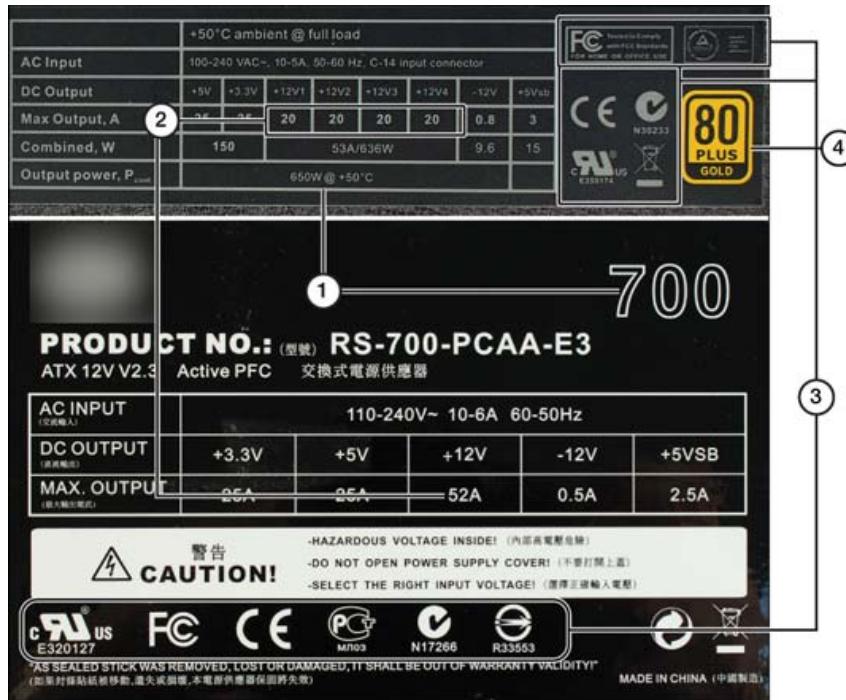
**Figure 3-81** A Typical ATX Power Supply

## Power Supply Ratings



Power supply capacity is rated in Watts; and the more Watts a power supply provides, the more devices it can safely power.

You can use the label attached to a power supply, as shown in [Figure 3-82](#), to determine its wattage rating and see important safety reminders.



1. Rated maximum output (watts)
2. +12V amperage
3. Safety approvals
4. 80 PLUS Gold rating

**Figure 3-82** Typical Power Supply Labels

A power supply with two separate +12V rails is a dual-rail design. Some high-performance power supplies feature more than two +12V outputs, such as the 650-Watt model shown in [Figure 3-82](#). Another term for two or more +12V outputs is *split rail*.

### Note

Power supplies with two or more separate +12V power sources are common today for providing adequate power for CPUs (which use voltage regulators on the motherboard or in the CPU itself to reduce +12V power to the power level needed) and other devices, such as PCIe video cards, fans, and drives. Add together the values of the +12V rails to get the total +12V output in amps.

### Note: Wattage vs. Amperage

The power supply label shown at the top of [Figure 3-82](#) is rated at 650 Watts, whereas the power supply label shown at the bottom of [Figure 3-82](#) is rated at 700 Watts. Take a closer look at the amperage ratings, though, and it becomes

clear that the 650-Watt power supply provides much more of the +12V power needed by processors and motors.

The 650-Watt power supply provides a total of 80A on the +12V lines (20A each on four +12V lines). The 700-Watt power supply provides only 52A on its +12V line. The 700-Watt power supply provides no information about the temperature or load factor at which its rating is calculated, whereas the 650-Watt power supply indicates that its calculations are made at 50° Celsius (about 122° Fahrenheit) at full load. Despite the rating difference, the 650-Watt power supply shown in [Figure 3-82](#) clearly provides more useful power than the 700-Watt power supply in the same figure.

## **Input 115V vs. 220V Multivoltage Power Supplies**

Most power supplies are designed to handle two different voltage ranges:

- 115–120V/60Hz
- 220–240V/50Hz

Power supplies that support these ranges are known as dual-voltage power supplies. Standard North American power is now 115–120V/60Hz-cycle AC. (The previous standard was 110V and is still covered in the A+ exam.) The power used in European and Asian countries is typically 230–240V/50Hz AC (previously 220V).

How can you tell whether a power supply meets minimum safety standards? Look for the appropriate safety certification mark for your country or locale. For example, in the United States and Canada, the backward UR logo indicates that the power supply has the UL and UL Canada safety certifications as a component. (The familiar circled UL logo is used for finished products only.) Both power supplies shown in [Figure 3-82](#) meet the safety standards for the U.S. and other nations.

### **Note**

The CompTIA A+ exam covers 110–120 VAC vs. 220–240 VAC.

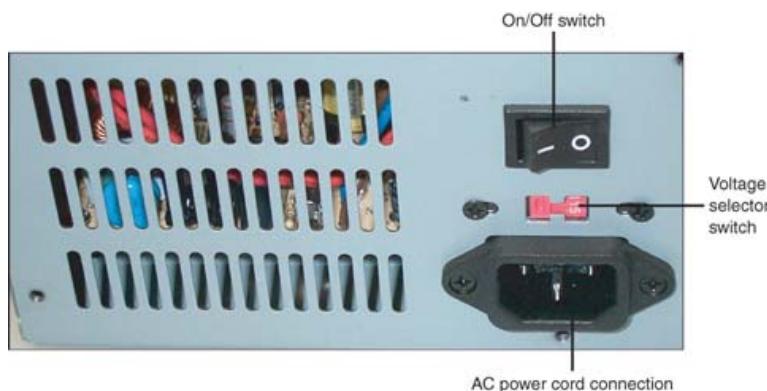
### **CAUTION**

Power supplies that do not bear the UL or other certification marks should not be used because their safety is unknown.

Typically, power supplies in recent tower case (upright case) machines use 500-Watt or larger power supplies, reflecting the greater number of drives and cards that can be installed in these computers. Power supplies used in smaller desktop computers have

typical ratings of around 220 to 300 Watts. The power supply rating is found on the top or side of the power supply, along with safety rating information and amperage levels produced by the power supply's different DC outputs.

Some older power supplies have a slider switch with two markings: 115 (for North American 110–120V/60HzAC) and 230 (for European and Asian 220–240V/50Hz AC). [Figure 3-83](#) shows a slider switch set for correct North American voltage. If a power supply is set to the wrong input voltage, the system will not work. Setting a power supply for 230V with 110–120V current is harmless; however, feeding 220–240V into a power supply set for 115V will destroy the power supply and possibly other onboard hardware.



**Figure 3-83** An Older Power Supply's Sliding Voltage Switch Set for Correct North American Voltage (115V)

### Note

Most recent power supplies for desktop and laptop computers can automatically determine the correct voltage level and cycle rate. These are referred to as *autoswitching* power supplies, and they lack the voltage/cycle selection switch shown in [Figure 3-83](#).

The on/off switch shown in [Figure 3-83](#) controls the flow of current into the power supply. It is not the system power switch, which is located on the front or top of desktop systems and is connected to the motherboard. When you press the system power switch, the motherboard signals the power supply to provide power.

### CAUTION

Unless the power supply is disconnected from AC current or is turned off, a small amount of power can still be flowing through the system even when it is not running. Do not install or remove components or perform other types of service to the inside of a PC unless you disconnect the AC power cord or turn off the power supply. Wait a few seconds afterward to ensure that the power is completely off. A

desktop motherboard might have indicator lights that turn off when the power has completely drained from the system.

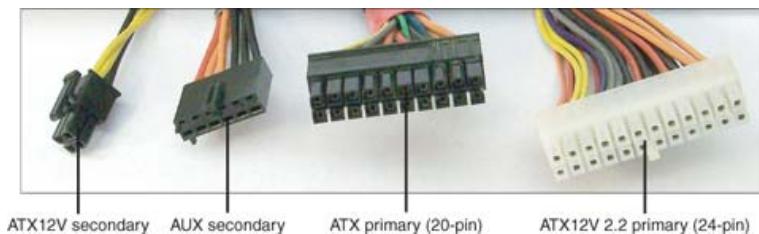
## 20-Pin-to-24-Pin Motherboard Adapter



When shopping for a power supply, make sure it can connect to your motherboard. Almost all power supplies sold today have a 24-pin connector, but you could encounter a legacy 20-pin connector used by older motherboards in the ATX family. The 24-pin is used by recent ATX/microATX/Mini-ITX motherboards requiring the ATX12V 2.2 power supply standard.

Most motherboards use power supplies that feature several additional connectors to supply added power, as follows (see [Figure 3-84](#)):

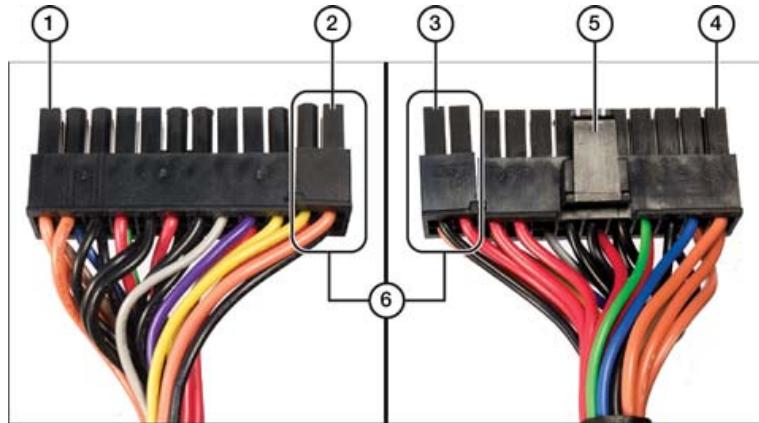
- Some high-wattage power supplies with 20-pin connectors might also include a 20-pin-to-24-pin adapter. Some 24-pin power supplies include a split connector to support either 24-pin or 20-pin motherboard power connectors (refer to [Figure 3-85](#)).



**Figure 3-84** 20-Pin ATX and 24-Pin ATX Power Connectors, Compared to 4-Pin ATX12V and 6-Wire AUX Power Connectors

- The four-wire square ATX12V connector provides additional 12V power to the motherboard. This connector is sometimes referred to as a P4 or Pentium 4 connector.
- Most recent power supplies use the 4/8 pin +12V (EPS12V) connector (see [Figure 3-84](#)) instead of the ATX12V power connector. The EPS12V lead is split into two four-wire square connectors to be compatible with motherboards that use either ATX12V or EPS12V power leads.
- Some very old motherboards use a six-wire AUX connector to provide additional power.

[Figure 3-85](#) shows both sides of a convertible 24-pin/20-pin ATX power supply connector.



1. Pin 1 (+3.3V, orange wire)
2. Pin 12 (+3.3V, orange wire)
3. Pin 24 (ground wire, black)
4. Pin 13 (+3.3V, orange wire)
5. Retaining clip
6. Used only on motherboards that use a 24-pin ATX power supply

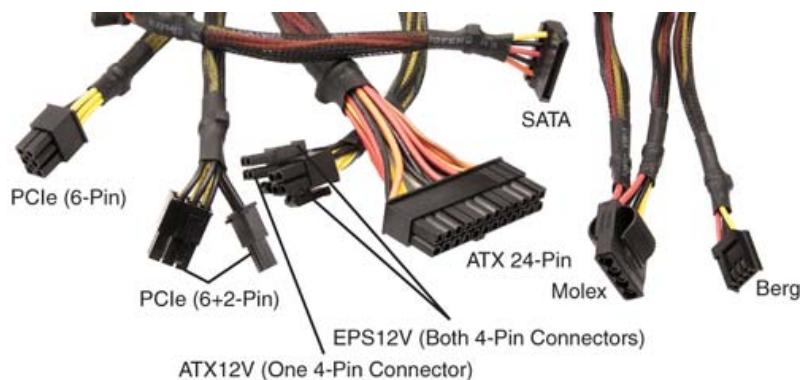
**Figure 3-85** Both Sides of a 24-Pin ATX Power Supply Cable (Also Compatible with 20-Pin Motherboards)

The power supply also powers various peripherals:

- Hard disks and CD/DVD/BD optical drives
- Case fans that do not plug into the motherboard and that use a four-pin Molex power connector
- An L-shape, 15-pin thinline power connector for Serial ATA (SATA) hard disks
- A PCI Express six-pin or eight-pin power cable (PCIe 6/8-pin) for high-performance PCI Express x16 video cards that require additional 12V power

[Figure 3-86](#) illustrates these power connectors and the EPS12V motherboard power connector.

**Key Topic**



**Figure 3-86** Power Supply Connectors for Peripherals and Modern Motherboards

## Output 3.3V vs. 5V vs. 12V

Because different peripherals have varying voltage requirements, three different voltages are delivered to the motherboard from the power supply. Different connector types carry different voltages. [Table 3-20](#) lists the power levels carried by each connector type.



**Table 3-20** Power Levels for Different Connector Types

Connector	+5V	+12V	+3.3V	Notes
Molex	Yes	Yes	No	Used today primarily for case fans that do not connect to the motherboard or that can be adapted to SATA drives
Berg	Yes	Yes	No	Used for power by some add-on cards
SATA	Yes	Yes	Optional	Requires using a Molex-to-SATA power connector if the power supply lacks adequate SATA connectors
PCIe 6-pin	No	Yes	No	Midrange PCIe video cards
PCIe 8-pin	No	Yes	No	High-performance PCIe video cards
ATX12V	No	Yes	No	Most recent and current motherboards, except those using EPS12V
EPS12V	No	Yes	No	Split into two ATX12V-compatible sections

If your power supply does not have enough connectors, you can add Y-splitters to divide one power lead into two, but these splitters can short out and also reduce the efficiency of the power supply. You can also convert a standard Molex connector into a SATA connector with the appropriate adapter.

Standard power supply wires are color-coded thus:

**Red:** +5V

**Yellow:** +12V

**Orange:** +3.3V

**Black:** Ground (earth)

**Purple:** +5V (standby)

**Green:** PS-On

**Gray:** Power good

**White:** No connection (24-pin); -5V (20-pin)

**Blue:** –12V

## Redundant Power Supply

Redundancy in a computer system or in network design means that a duplicate device is (or devices are) in place to keep things operational in case of failure. A power supply failure for even a second or two can be a disaster for a high-end computer or server. For systems requiring highly reliable uptime, a redundant power supply is an appropriate investment. Redundant power supplies are much more likely to be found in enterprise data centers than in personal computers or workstations.

In most cases, a redundant power supply has two power supplies, including power cables, built into the case. If there are two power units, each of the units carries half the workload during normal operations. If one supply fails, however, the other power supply has enough power to take over operations and keep the system up until the failed supply can be replaced.

Replacing the failed component can happen while the machine remains online if the power supply is hot swappable. A technician can unplug and remove the failed unit and replace it with a good one, and the units then return to sharing the work. The users of the computers will be unaware of the downtime.

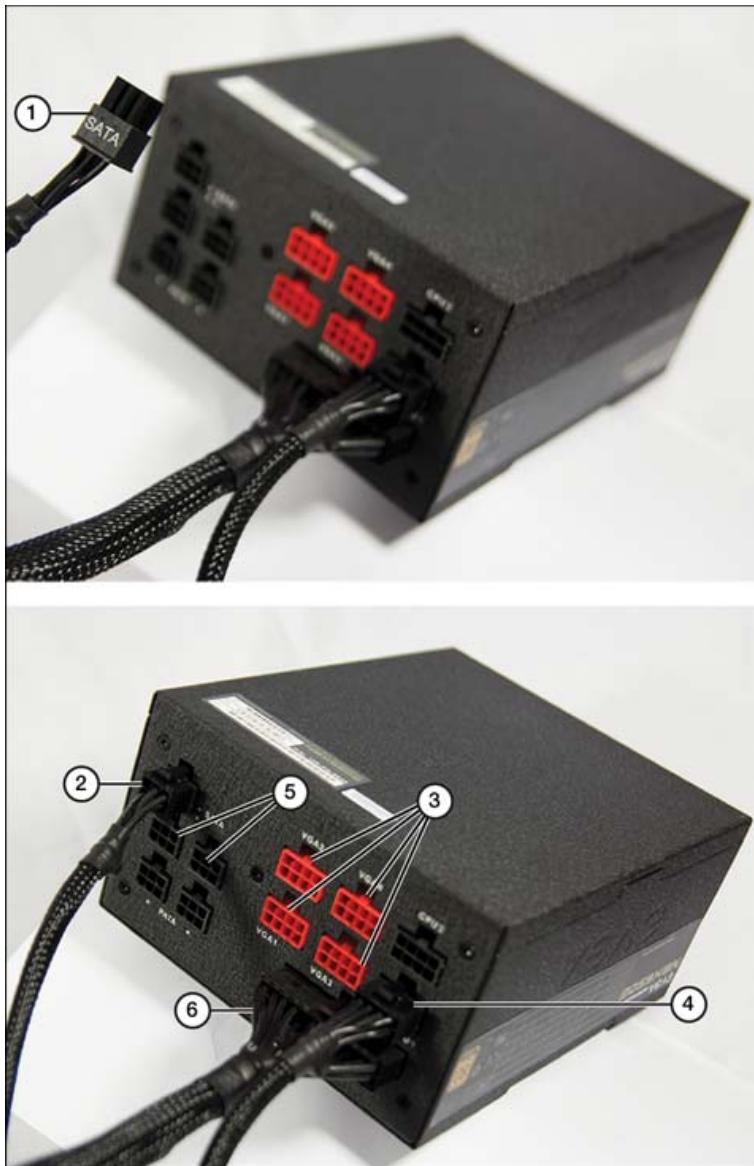
The idea of redundancy is to eliminate a single point of failure in the system. As an added precaution, some data centers even design separate electrical circuits for the redundant supplies.

### Note

A redundant power supply differs from an uninterruptible power supply (UPS), which is a separate device that sits outside the computer and provides temporary battery-powered backup if the building experiences a general power failure. [Chapter 9](#) covers UPS.

## Modular Power Supply

Some power supplies (see [Figure 3-87](#)) use modular connections so that you can customize the power supply connections needed for your hardware. An advantage of a **modular power supply** is that the cables can detach from the power supply, and cable management is much easier.



1. SATA power cable for modular power supply
2. SATA power cable after connection
3. PCIe power ports
4. EPS12V power cable
5. Additional SATA power ports
6. Motherboard main power cable

**Figure 3-87** A Modular Power Supply with Cables You Can Attach to Customize Support for Your System's Needs

If your wattage calculations or your tests agree that it is time to replace a power supply, make sure the replacement meets the following criteria:

- Has the same power supply connectors and the same pinout as the original
- Has the same form factor (shape, size, and switch location) as the original

- Has the same or higher wattage rating as the original (a higher wattage rating is highly desirable)
- Supports any special features required by your CPU, video card, and motherboard, such as SLI support (support for PCIe connectors to power two or more high-performance PCIe video cards), high levels of +12V power (ATX12V v2.2 4-pin or EPS12V 8-pin power connectors), and so on

## TIP

To ensure form factor connector compatibility, consider removing the old power supply and taking it with you if you plan to buy a replacement at retail. If you are buying a replacement online, measure the dimensions of your existing power supply to ensure that a new one will fit properly in the system. So-called EPX power supplies are longer than ATX power supplies and do not fit into smaller cases.

When replacing a power supply, make sure the new one is robust enough to handle any extra work from upgrades in the past or planned upgrades in the future. Power supplies are best in the middle of their wattage range; a PC that is underpowered can have many problems that are difficult to diagnose. The power supply is no place to scrimp on budget.

To determine the **wattage rating** needed for a replacement power supply, add up the wattage ratings for everything connected to your computer that uses the power supply, including the motherboard, processor, memory cards, drives, and bus-powered USB devices. Include any external devices that are used occasionally. If the total wattage used exceeds 70 percent of the wattage rating of your power supply, you should upgrade to a larger power supply. Check the vendor spec sheets for wattage ratings.

If you have amperage ratings instead of wattage ratings, multiply the amperage by the volts to determine the wattage, and then start adding. If a device uses two or three different voltage levels, be sure to carry out this calculation for each voltage level; then add up the figures to determine the wattage requirement for the device. Review [Figure 3-82](#) and the “Wattage vs. Amperage” sidebar, earlier in this chapter, for a reminder of the importance of +12V amperage.

[Table 3-21](#) provides calculations for typical compact desktop and high-performance desktop systems, based on the eXtreme Outer Vision online calculator at <https://outervision.com>. The components in the table were entered into the online calculator, and the recommended power supply specifications are in the last row.



**Table 3-21** Calculating Power Supply Requirements

Components	microATX System with Integrated Video	Full-Size ATX System with SLI (Dual Graphics Cards)
CPU	AMD A8-7650K (4 core, Intel Core i7-5930K (6 core, 3.3GHz with 4MB cache)	3.7GHz with 15MB cache)
RAM Size/Type	2 × 4GB DDR3	2 × 8GB DDR4
Rewritable DVD drive	Yes	Yes
Blu-ray	No	Yes
SATA hard disk	5400RPM	7200RPM
SSD	No	M.2
Case fans	2 × 120mm	2 × 140mm
Liquid cooling	No	Corsair Hydro H75
GPU	Integrated into CPU	NVIDIA GeForce GTX TITAN Z SLI
PCIe card	0	High-end sound card TV tuner (cable) card
USB 2.0 device	1	2
Estimated wattage	224 Watts	1239 Watts
Recommended power supply size (80 percent efficiency assumed)	400 Watts	1600 Watts

## Multifunction Devices/Printers and Settings

**220-1101: Objective 3.6:** Given a scenario, deploy and configure multifunction devices/printers and settings.

220-1101  
Exam

When performing technical support in a small office/home office (SOHO) environment, a technician needs to keep machines and devices up and functioning so that staff can continue to be productive. IT personnel are often called to support printing machines, many of which are multifunction devices that incorporate copy, scan, and fax features. (Although many have claimed that faxing is an outdated technology, it is still commonly used and is considered more secure than email.)

Multifunction devices output hard-copy versions of files such as documents and photos that are stored on the computer. Most office printers are laser printers, but in a SOHO setting, you will find inkjet, thermal, impact, and virtual (software) technologies for document output. Printers and multifunction devices can connect to a computer's USB via Bluetooth, Wi-Fi, cellular wireless networks, or directly to a wired Ethernet network.

## Unboxing a Device/Setup Location Considerations

The multifunction device is really several complex devices packaged into one unit. Combining these devices does not simplify things; it multiplies the opportunities for operational problems. To minimize the potential issues, consider the following decisions.

Make sure the printer is accessible to all users. Choosing a central location with access to the network is a good start. Make sure there is room to store paper and toner supplies close by, and be sure that users can find instructions for troubleshooting paper jams and the like.

## Appropriate Drivers for the Office Environment

Printers largely use one of two drivers to perform printing tasks. They differ in how they work and the machines they are designed to support. These drivers are **Printer Control Language (PCL)** and **PostScript (PS)**.

- PCL is a common driver language used by many different printer companies. It works with many different operating systems. PCL uses the printer hardware to process the print job data, comprised of print and graphics. This can take work off the computer and speed the printing process. The PCL method of printing incurs a couple potential drawbacks. One is that, because the printer does the processing work, the print job output can vary, depending on the brand of printer. Another is that PCL is not usually supported by devices running on the macOS, which could be a problem in some environments.
- PostScript is also supported by many manufacturers, including Apple computers, but not as many as PCL. Unlike PCL, PS does not depend on the printer for processing the print job, so the printing could be slower than with PCL printers. The advantage is that the print jobs will be consistent, no matter where they are printed in the network.

Choosing the correct print driver for the work environment is an essential first step. The main differences between PCL and PostScript is that PCL is better for fast printing and is widely supported by many operating systems, whereas PostScript is better for printing more detailed graphics. Windows assists with downloading drivers and many other issues by going to the Printers & Scanners page in the Settings menu.

## Configuration Settings

Typical configuration options for printers or multifunction devices include the following:

- **Duplex (double-sided) printing:** This option might be available on single-sided printers as well as true duplex (both sides of paper) printers. With a single-side printer, the duplex setting is used to determine how to position the paper for printing the second side.
- **Collate setting:** This setting is used when printing two or more copies of a document that has two or more pages. When the Collate setting is enabled, the printer prints each copy of page 1 before printing page 2, and so on. This is useful when creating print jobs for binding, stapling, or punching, but it is slower than uncollated print jobs.
- **Orientation:** Portrait (long side up) or landscape (short side up) can be selected automatically in some printer drivers, based on the orientation of the document to be printed. If the correct orientation is not selected automatically, choose it. Use Print Preview to help determine the setting needed.
- **Print quality:** Different quality settings are available, depending on the type of printer:
  - With laser printers and multifunction devices, you might be able to select the desired resolution (dots per inch [DPI]). Higher DPI levels produce smoother text output and more finely detailed graphics, but they require more printer RAM. As an alternative, some drivers have options to enable smoother text printing or to adjust page compression.
  - Instead of using specific resolutions, inkjet printers use quality settings such as High, Standard, Fast (Canon); Draft, Text, Text and Image, Photo, and Best Photo (Epson); and Draft, Normal, Best (HP). Each setting optimizes the size of the ink droplet and paper coverage for the best results with the specified paper.

## Public/Shared Devices

Printer and multifunction devices can be shared between two or more computers by using USB, Serial, Ethernet, and wireless connectivity.

Serial (RS-232) and USB sharing involve using switch boxes that can be manually switched between devices or that can automatically detect print jobs and switch to the active computer. Serial switch boxes are obsolete for most tasks, and USB switch boxes are limited by the number of computers that can share a printer (typically two or four).

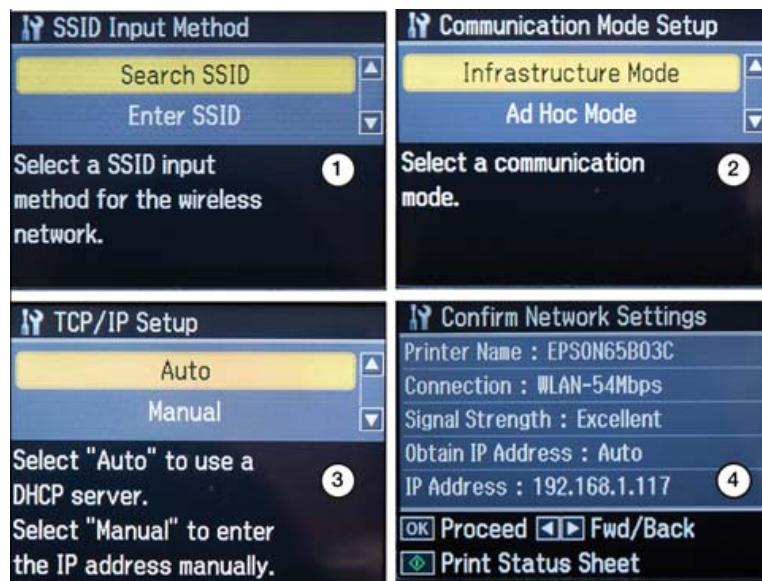
Both serial and USB printer sharing are also limited by relatively short cable runs and lack of management capabilities. Most wired printer/multifunction device sharing now uses Ethernet.

## Integrated Ethernet Print/Multifunction Device Sharing

Most recent printers and multifunction devices include software with an integrated print server that has support for Ethernet network printing. To configure them for sharing, follow these steps:

- Step 1.** Connect the printer or multifunction device to the network via an Ethernet (RJ-45) cable.
- Step 2.** Configure the printer or multifunction device to use Ethernet.
- Step 3.** Name the printer so that it can be located on the network.
- Step 4.** Specify whether the printer or device will get an IP address from a DHCP router.
- Step 5.** If you need to manually configure the IP address for the printer or device, determine which IP addresses on the network are not in use by DHCP and then manually assign the printer or device to one of those addresses.
- Step 6.** Record the configuration information for reuse. Some printers and devices print the information at the end of the setup process.

Figure 3-88 shows some print server setup dialog boxes from a typical small office printer with wireless Ethernet support.



1. Selecting how to locate the SSID for wireless print serving
2. Selecting the network mode for the wireless print server
3. Specifying where to get an IP address (wired/wireless)
4. Confirming network settings

**Figure 3-88** Configuring a Printer as an Ethernet or Wireless Ethernet Print Server

A multifunction device has an Ethernet port that takes on a network IP address. To print to a network printer or device, you might need to install a network printer driver instead of the normal printer driver on the computer that will use the printer or multifunction device. To learn more about TCP/IP and DHCP, see [Chapter 2, "Networking."](#)

## Wireless Device Sharing Options

The two major network protocols used for wireless device sharing are Bluetooth and 802.11 (Wi-Fi). Bluetooth is suitable for very short-range sharing among a few devices, whereas 802.11-based print sharing supports a much larger number of guest devices over much longer ranges.

### Bluetooth

Most printers with built-in Bluetooth support are portable or receipt printers.

Printers that lack Bluetooth support can use special Bluetooth adapters to connect with computers or mobile devices that use Bluetooth. Check with the printer device vendor for models that are compatible with a specific printer.

Before a computer or mobile device can connect to a printer or multifunction device using Bluetooth, both the computer/mobile device and the printer/multifunction device must have Bluetooth transceivers. Bluetooth support is common among laptop and mobile devices and can be added with a USB dongle to computers that lack Bluetooth support.

After enabling Bluetooth on the printer and computer, you must configure both for pairing and pair them before print jobs can be sent. For details, see [Chapter 2](#).

### 802.11(a, b, g, n, ac, ax)

Most new printers and multifunction devices include some level of 802.11 (Wi-Fi) support. The configuration process is typically similar to that used for wired Ethernet, with the added step of specifying the wireless network's SSID and encryption key (if used). When this configuration is complete, all devices on the network with the proper print driver can use the multifunction device.

### Infrastructure vs. Ad Hoc

If you want to use wireless Ethernet (Wi-Fi) printers or multifunction devices but do not use Wi-Fi networking with a wireless router, configure the printers or devices to work in

ad hoc mode. In ad hoc mode, each device is connected directly to other devices: No router is used.

Infrastructure mode supports WPA3 encryption; ad hoc mode supports only WEP encryption, making it unsuitable for secure networking.

## Ad Hoc Wireless Network Support in Windows

Ad hoc wireless networking is supported in previous versions of Windows through the Network and Sharing Center or from the command line using Netsh, but it has been removed in Windows 10/11.

## Ad Hoc Wireless Network Support in macOS

macOS supports ad hoc wireless networking through the Wi-Fi Status icon on the Finder menu. macOS refers to this feature as “computer-to-computer” networking (see [Figure 3-89](#)). When you enable this feature, your computer cannot connect to other Wi-Fi networks at the same time.



1. Select the least-used wireless channel
2. Click to create network

**Figure 3-89** Creating a Computer-to-Computer (Ad Hoc) Wireless Network with macOS

## Ad Hoc Wireless Networking Support in Linux

Ad hoc wireless networking in Linux is sometimes referred to as an *IBSS* (independent basic service set) network. Depending on the distro, this can be set up by turning on the wireless hotspot service in the network settings or by using the command-line utilities iw and ip. Network Manager can be installed on distros that lack easy network management.

## Wireless Hosted Networking

As a replacement for ad hoc mode, Windows 7 introduced wireless hosted networking, which is also available in Windows 10/11. With wireless hosted networking, you can

create a Wi-Fi network hotspot that is detectable and usable by Wi-Fi-enabled printers and other computers and devices.

To create an unsecured wireless hosted network, open a command prompt and enter this command:

**netsh wlan start hostednetwork**

Check the Network and Sharing Center, or Network & Internet in Windows 11, to ensure that your new network is available.

Set up your printer or multifunction device to use the same network name. To print, have each user connect to that network. A printer or multifunction device can use only one network at a time, but computers can connect to this network and to other networks (including wireless networks) at the same time.

## **Using Public and Shared Devices**

Sharing printers on a network previously required both the printer and the user to be on the same local network. Recent print-sharing technologies have made shared printing available beyond physical access to a printer.

Public cloud printing devices are available in some office supply stores, schools, and other business centers located in hotels and airports. The customer can submit print jobs via email, web interfacing, mobile apps, or special print drivers. Thus, public cloud printing is available to any type of computer or device that has Internet access. To receive the print job from the printer, the user must provide the credentials needed, such as a retrieval code or account code. Google Cloud Print is an example of a service that allows printing to a Web-enabled computer from anywhere on the Web, including using phones.

Thanks to public cloud printing services, users might no longer need to buy a printer they use only occasionally. For example, a person working remotely from home (or any user, for that matter) might have very little use for a printer or might not use it enough to justify the cost. When the rare print job is required, the user can instead send the document to an account at a neighborhood Office Depot or similar business and then go there and print from a professional machine by entering the code on the keypad.

## **Using Apps**

Smartphones and tablets that run Android or Apple iOS operating systems typically install apps from their respective app stores to make cloud or remote printing possible.

Connect older printers and multifunction devices that do not have built-in Google Cloud Print support to a computer running Google Chrome, and enable its Google Cloud Print feature to enable cloud printing. The Google Print Connector can be used to enable multiple printers in businesses or schools to be used with Google Cloud Print.

## Maintaining Data Privacy

When a document is sent to a printer, the print spooler creates a special print file. To prevent unauthorized users from opening the print file and extracting information from it, two methods can be used: user authentication and hard drive caching.

### Using User Authentication/Audit Logs

User authentication (which matches print jobs to the IP address of the computer or device requesting the print job) can be enabled at the printer itself or by security settings used on Active Directory–enabled networks.

When user authentication is enabled in the printer (a common feature on enterprise-level print or multifunction devices), the user must provide the appropriate identification during the print process. On a macOS system, this can be done through the Job Log portion of the printer submenu (the same menu that includes sections for layout, print settings, and so on). On a Windows system, the printer driver or the network might prompt for this information.

### Using Hard Drive Caching

On a system running Windows, print spool files are normally stored on the system hard drive at C:\Windows\system32\spool\PRINTERS. If a different location is desired, make sure the location is not shared on the network, to avoid access from unauthorized users.

The default location of the print spool files can be changed by selecting the printer or multifunction device in Devices and Printers, opening the Print Server Properties dialog box, clicking Advanced, clicking Change Advanced Settings, and specifying a different location.

## Network Scan Services

Printing is not limited to paper in network printing. Three services that can use printing are printing to an email, printing to a folder on a network using the **SMB** protocol, and printing to or from the cloud.

These are variations of printing to a file, in which the document is printed to an Adobe .pdf file to be sent or shared. Other companies have developed their own methods of sharing print files.

## Scanning to Email

Windows and other printing software allow you to scan a document with the multifunction device and have it sent to the user as a .pdf attachment. This requires a

device that is networked and can interface with the organization's email services. To scan to email, follow these steps:

**Step 1.** Select to scan to an email from the menu.

**Step 2.** Enter in or select the receiver of the mail.

**Step 3.** Press Enter to scan.

The scanner generates a .pdf file, attaches it to an email, and sends it to the destination.

## Scanning to an SMB Folder

As when scanning to an email, the printer must know the IP address of the server on the network that is hosting the destination folders for the document. When user permissions are authenticated, the user can create a shared folder on the network and then scan the document into it.

## Cloud and Remote Printing

With cloud printing, you no longer need to be at your office or home office to make a printout. With remote printing, you can print a document stored on your host using your remote printer.

Cloud and remote printing require the following:

- A printer or multifunction device that can be accessed from the cloud or remotely via the Web.
- An app that supports remote or cloud printing. The printer settings are loaded into the app, and the cloud-based document is downloaded and printed from the mobile device.

## Automatic Document Feeder/Flatbed Scanner

**Automatic Document Feeder (ADF)** is a feature found in printers, photocopiers, and scanners that automatically feeds a single sheet of paper from a stack of paper into the machine. This allows the user to print, scan, or copy without needing to manually feed the machine paper one at a time. Typically, ADFs are described by speed, pages per minute, and sheet capacity. A flatbed scanner is used to scan documents using the flatbed. Some flatbed scanners have an ADF and can scan multiple papers without human intervention.

## Print Technologies

**220-1101: Objective 3.7:** Given a scenario, install and replace printer consumables.

Printing has long been one of the most common issues confronting help desk technicians. Although in many ways print technologies have become simpler over time, the skills of knowing printer types and being able to perform printer maintenance remain in high demand.

## Laser Printers



A ***laser printer*** is a page printer that stores the entire contents of a page to be printed in its memory before printing it. By contrast, inkjet, thermal, and impact printers print a page as a series of narrow bands.

The major components of a laser printer include the following:

- ***Imaging drum:*** Applies the page image to the **transfer belt** or roller. It is frequently combined with the toner supply in a toner cartridge.
- ***Developer:*** Pulls toner from the toner supply and sends it to the imaging drum.
- ***Fuser assembly:*** Fuses the page image to the paper.
- ***Transfer belt (transfer roller):*** Transfers the page image from the drum to the page.
- ***Pickup rollers:*** Pick up paper.
- ***Paper separation pad (separate pad):*** Enables the pickup rollers to pick up only one sheet of paper at a time.
- ***Duplexing assembly (optional):*** Switches paper from the front to the back side so that the printer can print on both sides of the paper.

The following sections take a closer look at how these and other components work together to make laser printing possible.

## Toner Cartridges

Most monochrome laser printers use toner cartridges that combine the imaging drum and the developer, along with a supply of black toner. This provides you with an efficient and easy way to replace the laser printer items with the greatest potential to wear out.

Depending on the model, a new toner cartridge might also require that you change a wiper used to remove excess toner during the fusing cycle. This is normally packaged with the toner cartridge.

When installing a toner cartridge, be sure to follow the directions for cleaning areas near the toner cartridge. Depending on the make and model of the laser printer, this can involve cleaning the mirror that reflects the laser beam, cleaning up stray toner, or cleaning the charging corona wire or conditioning rollers inside the printer. If you need to clean the charging corona wire (also called the *primary corona wire* on some models), the laser printer will contain a special tool for this purpose. The printer instruction manual shows you how to clean the item.

Keep the cartridge closed; it is sensitive to light, and leaving it out of the printer in room light can damage the enclosed imaging drum's surface.

## **CAUTION**

When you change a toner cartridge, take care to avoid getting toner on your face, hands, or clothing; it can leave a messy residue that is hard to clean. For information about cleaning up toner spills and taking precautions against inhaling toner, see [Chapter 9](#).

## **Laser Imaging Process**

A laser printer is an example of a page printer. A page printer does not start printing until the entire page is received. At that point, the page is transferred to the print mechanism, which pulls the paper through the printer as the page is transferred from the printer to the paper.

## **TIP**

To master this section, keep these tips in mind:

- Memorize the seven steps involved in laser printer imaging.
- Master the details of each step and their sequence.
- Be prepared to answer troubleshooting questions based on these steps.

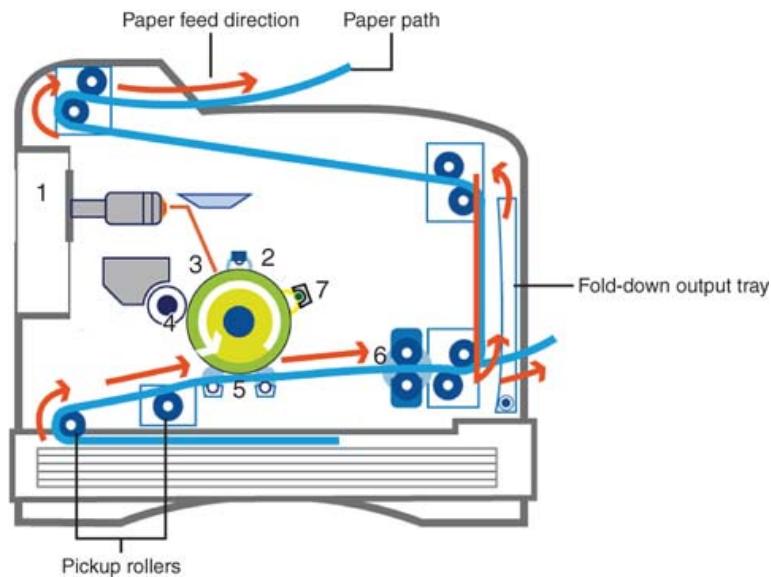
The laser printing process often is referred to as the electrophotographic (EP) process.

Before the seven-step laser printing imaging process can take place, the following events must occur:

- Because laser printers are page based, a printer must receive an entire page before it can start printing.
- After the page has been received, the printer pulls a sheet of paper into the printer with its feed rollers.

After the paper has been fed into the print mechanism, a series of seven steps takes place, resulting in a printed page: processing, charging, exposing (also known as writing), developing, transferring, fusing, and cleaning.

The following section describes this process in more detail. Steps 1–7 are identified in [Figure 3-90](#).



**Figure 3-90** A Conceptual Drawing of a Typical Laser Printing Process



## TIP

Make sure you know this exact order of the laser printer imaging process for the exam:

- Step 1.** Processing
- Step 2.** Charging
- Step 3.** Exposing
- Step 4.** Developing
- Step 5.** Transferring
- Step 6.** Fusing
- Step 7.** Cleaning

Also make sure you know the parts that make up a laser printer:

- Imaging drum
- Developer

- Fuser assembly
- Transfer belt
- Transfer roller
- Pickup rollers
- Separation pads
- Duplexing assembly

## Step 1: Processing

The printer's raster image processing engine receives the page, font, text, and graphics data from the printer driver; creates a page image; and stores it in memory. Depending on the amount of information on the page, compared to the amount of memory in the printer, the printer might need to compress the page image to store it. If not enough memory is available to store the page image, a memory error is triggered.

## Step 2: Charging

During the **charging** process, the cylinder-shaped imaging drum receives an electrostatic charge of  $-600\text{VDC}$  (DC voltage) from a conditioning roller. (Older printers used a primary corona wire.) The smooth surface of the drum retains this charge uniformly over its entire surface. The drum is photosensitive and retains this charge only while kept in darkness.

## Step 3: Exposing

During the **exposing** process, a moving mirror moves the laser beam across the surface of the drum. As it moves, the laser beam temporarily records the image of the page to be printed on the surface of the drum by reducing the voltage of the charge applied by the charger corona to  $-100\text{VDC}$ . Instead of using a laser beam, an LED printer activates its LED array to record the image on the page.

## Step 4: Developing

During the developing process, the drum has toner applied to it from the developer; because the toner is electrostatic and is also at  $-600\text{VDC}$ , the toner stays on only the portions of the drum that have been reduced in voltage to create the image. It is not attracted to the rest of the drum because the toner and the drum are at the same voltage, and like charges repel each other. This "like charges repel" phenomenon is similar to two like poles of magnets repelling each other.

## Step 5: Transferring

During the transferring process, while the sheet is being fed into the printer, it receives an electrostatic charge of +600VDC from a corona wire or roller; this enables it to attract toner from the drum, which is negatively charged (see step 3). As the drum's surface moves close to the charged paper, the toner adhering to the drum is attracted to the electrostatically charged paper to create the printed page.

As the paper continues to move through the printer, its charge is canceled by a static eliminator strip so that the paper itself isn't attracted to the drum.

## Step 6: Fusing

During the **fusing** process, the printed sheet of paper is pulled through fuser rollers, using high temperatures (approximately 350° Fahrenheit) to heat the toner and press it into the paper. The printed image is slightly raised above the surface of the paper.

The paper is ejected into the paper tray, and the drum must be prepared for another page.

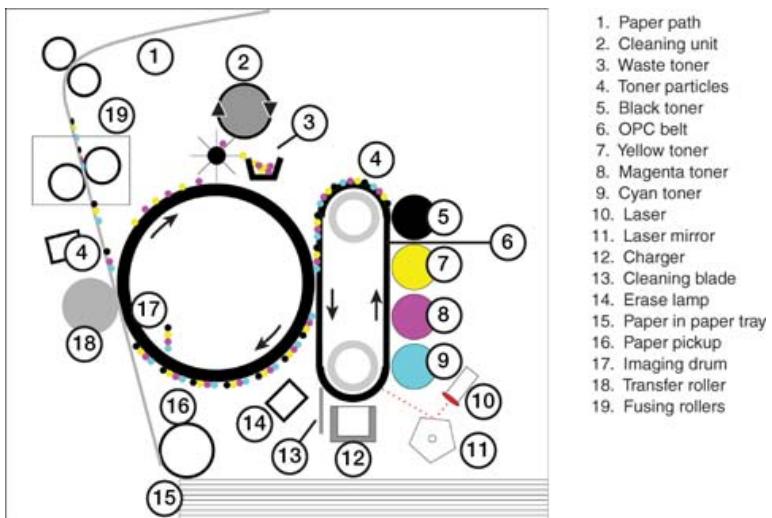
## Step 7: Cleaning

To prepare the drum for a new page, the image of the preceding page placed on the drum by the laser or LED array (see step 3) is removed by a discharge lamp. During the **cleaning** process, toner that is not adhering to the surface of the drum is scraped from the drum's surface for reuse.

## Color Laser Printing Differences

Color laser printers differ from monochrome laser printers in two important ways: They include four different colors of toner (cyan, magenta, yellow, and black), and the imaging drum is separate from the toner. Thus, instead of waste toner being reused, as in a monochrome laser printer that has a toner cartridge with an integrated imaging drum, waste toner in a color printer is sent to a separate waste toner container.

Color laser printers use the same basic process as monochrome lasers, but some use a transfer belt instead of an imaging drum. The use of a transfer belt enables all four colors (cyan, magenta, yellow, and black) to be placed on the paper at the same time, making color print speeds comparable to monochrome print speeds. When a transfer belt is used, the conditioning and transferring processes are performed on the transfer belt (see [Figure 3-91](#)).



**Figure 3-91** The Printing Process in a Typical Color Laser Printer That Uses a Transfer Belt

## Laser Media Types

Laser printers use standard smooth-finish printer or copier paper. It is important to use labels and transparency media that are especially designed for laser printers: Other types of media might jam the printer or become distorted because of the high heat used in the laser printing process.

Labels made for copiers are not suitable for laser printers because they can come off the backing and stick to the printer's internal components.

## Laser Maintenance

The major elements in laser printer maintenance include replacing toner, applying maintenance kits, performing calibration (color lasers only), and cleaning.

### Replacing Toner Cartridges

If a laser printer's toner cartridge also includes the imaging drum, replacing the toner cartridge also involves replacing the imaging drum. Because the imaging drum's surface can become damaged, leaving marks on print output, changing the toner cartridge is helpful in improving print quality.

### Applying Maintenance Kits

Many HP and other laser printers feature components that should be replaced at periodic intervals. These components often include fuser assemblies, air filters, transfer rollers, pickup rollers, other types of rollers, and separation pads (separate pads).

These components wear out over time and can usually be purchased as a maintenance kit (as well as separately).

A printer that uses a maintenance kit displays a message or an error code (such as "Perform printer maintenance" or "Perform user maintenance") when the printer reaches the recommended page count for maintenance kit replacement. Depending on the printer model and whether it is used for color or monochrome printing, the recommended page count could be as few as 50,000 pages or as much as 300,000 pages (or more).

After a fuser assembly or full maintenance kit is installed in a laser printer, the page count must be reset; otherwise, you will not know when to perform recommended maintenance again. Typically, the page count is reset by pressing a specified combination of buttons on the printer's control panel.

### **Note**

If the printer is under a service contract or is being charged on a per-page (or per-click) basis, it is not recommended to reset the paper count after servicing. However, most laser printers print the page count when you perform a self-test.

## Performing Calibration

Color laser printers should be calibrated if print quality declines. The printer calibration process on a color laser printer adjusts image density settings to make up for changes caused by environmental differences or aging print cartridges.

Some color laser printers perform automatic calibration, but you can also force the printer to perform calibration on an as-needed basis. See the instruction manual for your printer for details.

### **Note**

Print quality is affected by many factors, such as the print resolution for graphics. The higher the dpi, the sharper and better the print quality; conversely, using an economy printing mode that uses less toner reduces print quality. A damaged imaging drum or dirty rollers can leave marks on the paper that detract from print quality. If a color laser printer requires four passes to print in color and the colors are not properly lined up (a process known as color registration), print quality will be affected.

## Cleaning

Because laser printers use fine-grained powdered toner, keeping the inside of a laser printer clean is an important step in periodic maintenance. If you want to use a vacuum cleaner to pick up loose toner, be sure to use a vacuum cleaner that is *designed* to pick up toner: Toner particles are so small that they pass through conventional bags and filters. If you prefer to use a damp cloth, be sure to first turn off the laser printer and disconnect it from power.

To keep the paper path and rollers clean, use cleaning sheets made for laser printers, as follows:

**Step 1.** Insert the sheet into the manual feed tray on the laser printer.

**Step 2.** Create a short document with Notepad, WordPad, or some other text editor, and then print it on the sheet.

As the sheet passes through the printer, it cleans the rollers. If a specialized cleaning sheet is not available, you can also use transparency film designed for laser printers. Some laser printers use a special software program to print a cleaning pattern onto plain paper.

### Note

Be sure to know how to maintain a laser printer for the 220-1101 exam: replacing toner, applying a maintenance kit, performing calibration, and cleaning.

### CAUTION

Never use transparency media that is not designed for laser printers in a laser printer. Copier or inkjet media is not designed to handle the high heat of a laser printer and can melt or warp and possibly damage the printer.

## Inkjet Printers



**Inkjet printers** are the most popular type of printer in small office/home office (SOHO) use. Their print quality can rival that of laser printers, and virtually all inkjet printers in use today can print both color and black text and photographs.

From a tightly spaced group of nozzles, inkjet printers spray controlled dots of ink onto the paper to form characters and graphics. On a typical 5,760×1,440dpi (dots per inch) printer, the number of nozzles can be as high as 180 for black ink and more than 50

per color (cyan, magenta, and yellow). The tiny ink droplet size and high nozzle density enable inkjet printers to perform the seemingly impossible at resolutions as high as 1,200dpi or higher: fully formed characters from what is actually a high-resolution, nonimpact, dot-matrix technology.

Inkjet printers are character/line printers. This means that they print one line at a time of single characters or graphics, up to the limit of the print head matrix. Inkjet printers are functionally fully formed character printers because their inkjet matrix of small droplets forming the image is so carefully controlled that individual dots are not visible. Larger characters are created by printing a portion of the characters across the page, advancing the page to allow the print head to print another portion of the characters, and so on until the entire line of characters is printed. Thus, an inkjet printer is both a character printer and a line printer because it must connect lines of printing to build large characters. Some inkjet printers require realignment after each ink cartridge/print head change to make sure that vertical lines formed by multiple print head passes stay straight; this realignment could be automatic or could require the user to start the process. With other models, alignment can be performed through a utility provided as part of the printer driver when print quality declines due to misalignment.

## Inkjet Components

The essential components in the inkjet printing process include ink cartridges, print head, roller, paper feeder, duplexing assembly, carriage, and belt.

### Note

Make sure you know these inkjet components for the 220-1101 exam.

Some inkjet printers use external ink tanks for longer ink life between refills.

[Figure 3-92](#) shows how many of these components look in a typical printer.



**Figure 3-92** A Typical Inkjet Printer with Its Cover Open

## Inkjet Printing Process

Inkjet printers use ink cartridges filled with liquid ink for printing. Some older inkjet printers use a large tank of black ink and a second tank with separate compartments for each color (typically cyan, magenta, and yellow; some models feature light versions of some of these colors for better photo-printing quality). However, almost all inkjet printers produced for a number of years have used a separate cartridge for each color. This improves print economy for the user because only one color at a time needs to be replaced. With a multicolor cartridge, the entire cartridge needs to be replaced, even when only one of the colors runs out.

### Note

Inkjet printers are sometimes referred to as CMYK devices because of the four ink colors used on most models: cyan, magenta, yellow, and black.

The carriage and belt mechanism moves the print head back and forth to place ink droplets as the paper passes through the printer. Depending on the printer, the print head might be incorporated into the ink tank; it might be a separate, user-replaceable item; or it might be built into the printer.

Some inkjet printers feature an extra-wide (more nozzles) print head or a dual print head for very speedy black printing. Some models enable the user to replace either the ink cartridge only or an assembly comprising the print head and a replaceable ink cartridge.

### Note

On an inkjet printer, print quality settings are typically Good, Better, Best; or Text, Text and Image, Photo, and Best Photo. They are selected in the Printer Settings dialog box. However, clogged nozzles (leading to ink dropouts), mismatch of paper type setting to actual paper used, and dirty rollers reduce actual print quality.

An inkjet printer is only as good as its print head and ink cartridges. Clogged or damaged print heads or ink cartridges render a printer useless. If an inkjet printer fails after its warranty expires, you should carefully check service costs before repairing the unit. Failed inkjet printers are often “throwaway” models and can be replaced rather than repaired, even during the warranty period.

### CAUTION

Inkjet printers should never be turned off by using the power switch on a surge protector; doing so prevents the printer from self-capping its ink cartridges, which is a major cause of service calls and printer failures. Cleaning the print head—either with the printer's own cleaning feature, using a cleaning utility built into the printer driver, or with a moistened cleaning sheet—will restore most printers to service. Always use the printer's own power switch, which enables the printer to protect the ink cartridges and properly perform other periodic tasks (such as self-cleaning).

Inkjet printers use two major methods to create the ink dots that make up the page. Most inkjet printers heat the ink to boiling and create a tiny bubble of ink that is allowed to escape through the print head onto the paper. This is the origin of the name BubbleJet for the Canon line of inkjet printers. Printers that use this method feature either ink cartridges that include the print head or print heads with removable ink cartridge inserts. If a print head gets severely clogged, you can simply replace the ink cartridge if the ink cartridge incorporates the print head.

Another popular method uses a piezoelectric crystal to distribute the ink through the print head. This method makes achieving high resolutions easier; the Epson printers using this method were the first to achieve  $5,760 \times 1,440$  dpi resolutions. This method also provides a longer print head life because the ink is not heated and cooled. However, the print heads are built into the printer, making a severely clogged print head harder to clean. Both types of inkjet printers are sometimes referred to as *drop-on-demand printers*.

The inkjet print process works as follows:

- Step 1.** A roller mechanism pulls the paper or media in a feed tray into position.
- Step 2.** The print head is suspended on a carriage over the paper and is moved across the paper by a belt. As the print head moves across the paper, it places black and color ink droplets, as directed by the printer driver.
- Step 3.** At the end of the line, the paper or media is advanced, and the print head either reverses direction and continues to print (often referred to as Hi-Speed mode), or returns to the left margin before printing continues.
- Step 4.** When the page print is completed, the media is ejected.

## **Inkjet Media Types**

Inkjet printers can use the same types of paper and labels that laser printers can use. However, inkjet printers can also use special matte or glossy-coated paper and business card stock for presentation or photorealistic images. Transparency stock must be designed specifically for inkjet use. Because of improvements in media and print design, old inkjet photo paper should be recycled instead of used; older paper types have very slow drying times, compared to recent types.

When printing, be sure to select the correct media type in the printer driver, to avoid banding, overuse of ink, and other poor-quality results.

## Inkjet Maintenance

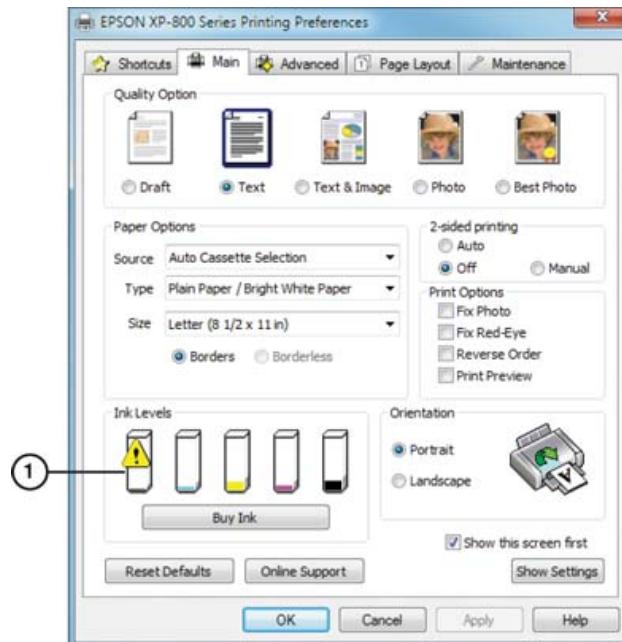
Ink cartridge replacement, calibration, nozzle check, head cleaning, and jam clearing are the major elements involved in maintaining an inkjet printer.

### Note

Make sure you know the elements of inkjet maintenance—ink cartridge replacement, calibration, nozzle check, head cleaning, and jam clearing—for the 220-1101 exam.

## Replacing Ink Cartridges

Use the Printing Preferences or Printer Properties dialog box (which varies by printer and operating system) to determine when it is time to purchase additional ink or replace the ink cartridges (see [Figure 3-93](#)).



1. Warning of critically low ink level

**Figure 3-93** A Printer with Low Ink Levels, with the ! Indicating a Cartridge That Is Nearly Empty

### Note

Most inkjet printers stop printing when one color runs out, even if that color is not being used in the current print job. Some printers offer to use a mixture of photo black and colors if the normal black ink runs low during a print job.

Some printers run automatic nozzle cleaning or calibration routines when you change ink cartridges. If the ink cartridge includes a print head, whenever you change the ink cartridge, you also change the print head. Consequently, replacing ink cartridges is the single best maintenance step you can perform on an inkjet printer.

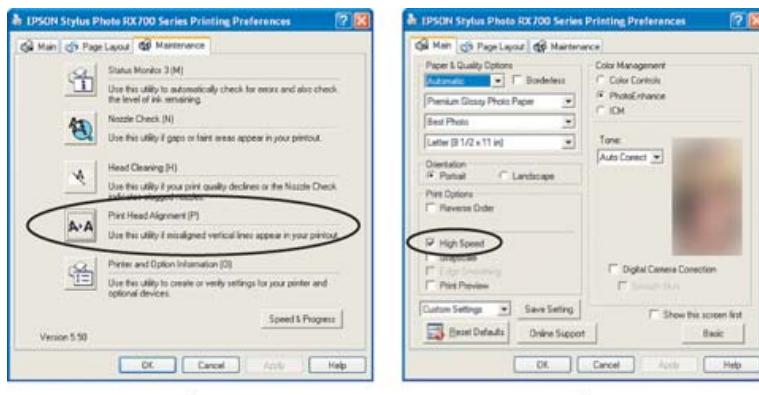
## Calibration

Inkjet printers might require or recommend some type of printer calibration—most typically, print head alignment. This process involves printing one or more sheets of paper and selecting the print setting that produces straight lines. Some printers perform this step automatically, and others require user intervention to determine the best setting.

Some inkjet printers can use two printing methods: unidirectional, in which the printer prints only when the print head is moving from left to right, and bidirectional, in which the printer prints when the print head is moving in either direction (left to right, or right to left). If the print head is misaligned, bidirectional printing (sometimes referred to as *high-speed printing*) will have much poorer print quality than unidirectional printing.

Be sure to align the print head as needed, using the calibration or alignment utility provided in the printer driver (see [Figure 3-94A](#)), to permit successful use of bidirectional printing.

To enable bidirectional printing, select the High Speed option (when it is offered) in the Print Preferences menu (see [Figure 3-94B](#)).



A

B

**Figure 3-94** Aligning the Print Head (A) Helps Produce Better-Quality High-Speed (Bidirectional) Printing (B)

## Note

With some printers, it might be necessary to realign the print head after changing ink cartridges. Some of these printers perform this task automatically; with others, it might be an optional utility that you can run on an as-needed basis.

## Nozzle Check and Head Cleaning

Periodically, especially if a printer has not been used for a while or has been used only for monochrome printing, it is a good idea to use the nozzle check routine to verify that all the print heads' nozzles are working correctly.

The nozzle check or pattern check routine prints a pattern that uses all of the nozzles in all of the print heads and displays the pattern's correct appearance. Compare the printout to the onscreen display; if you see gaps or missing colors, activate the head-cleaning routine (see [Figure 3-95](#)). Repeat these steps until the nozzle check printout matches the screen display. Keep in mind that performing a nozzle check uses ink.

### Key Topic



**Figure 3-95** The Pattern Check (Nozzle Check) Dialog Box from a Canon Inkjet Printer Driver's Maintenance Tab

Depending on the printer, these options might be located in the Printer Preferences Maintenance section, a toolbox dialog box, or someplace like the printer's onboard menu. See your printer's documentation for details.

## CAUTION

When using a Windows-provided printer driver, some printer options might not be available. Installing the latest available driver from the printer's manufacturer is a good practice.

## Thermal Printers



A **thermal printer** uses heat transfer to create text and graphics on the paper. Thermal printers are available using three different technologies:

- Dye sublimation, for high-quality printing
- Thermal wax transfer, similar to laser quality
- Direct thermal, the most common use of thermal printing, used in retail point-of-sale (POS) receipt printing

Each of these technologies has quite different processes, which are discussed in the following sections.

## Thermal Feed Assembly and Heating Element

Thermal printers can use an impact print mechanism or a dye-sublimation technology to transfer images. Direct thermal printers use heat-sensitive paper (special thermal paper), whereas thermal transfer printers use a wax, resin, or dye ribbon to create the image. Some printers can use either heat-sensitive media or a ribbon.

The feed assembly on a typical thermal receipt or point-of-sale printer pulls paper from a roll wound around a center plastic spool or spindle. The feed assembly on a typical desktop thermal barcode printer uses notched rollers and spring-loaded sprockets to advance roll paper. Larger thermal barcode printers might also use fanfold media as well as roll media.

The heating element in the print head is used to heat thermal paper or ribbons to make the image. Printers that use ribbons are thermal transfer printers, and printers that use thermal paper are known as direct thermal printers.

## Thermal Printer Ribbons

Thermal transfer printers use wax- or resin-based ribbons, which are often bundled with paper made especially for the printer. Dye-sublimation (dye-sub) printers use dye-based film ribbons technology to print continuous-tone photographs. Examples of consumer-grade dye-sublimation printers include Kodak Printer Docks and the Canon Selphy CP series; these printers print 4×6-inch photos. Many vendors also sell larger-format dye-sublimation printers for use in photo labs and professional photography studios.

[Figure 3-96](#) illustrates a typical dye-sublimation ribbon for a Canon Selphy CP printer.



**Figure 3-96** A Dye-Sublimation Ribbon for a 4-by-6-Inch Photo Printer (Canon Selphy CP)

## Thermal Print Process

Although thermal transfer, direct thermal printing, and dye sublimation all involve heating the elements in a print head to a particular temperature to transfer the image, there are some differences in operation. The basic process of thermal printing works like this:

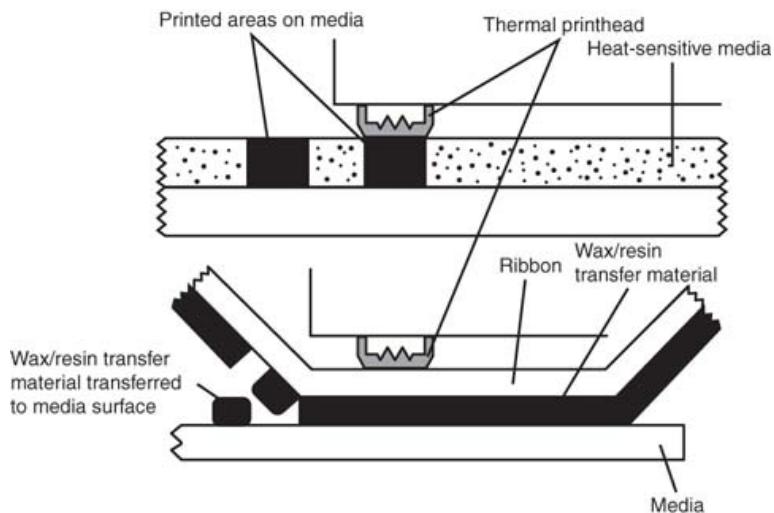
- Step 1.** The print head has a matrix of dots that can be heated in various combinations to create text and graphics.

**Step 2.** The print head transfers text and graphics directly to heat-sensitive thermal paper in direct thermal printing, or to a ribbon that melts onto the paper in thermal transfer printing.

**Step 3.** If a multicolor ribbon is used on a thermal transfer or dye-sublimation printer, each ribbon is moved past the print head to print the appropriate color. In the case of dye-sublimation printers, the paper is moved back into position to enable the next color to be printed.

**Step 4.** When all colors have been printed, the paper is ejected.

Figure 3-97 compares direct thermal and thermal transfer printing technologies.



**Figure 3-97** Direct Thermal (Top) and Thermal Transfer (Bottom) Printing Technologies

## Thermal Paper and Media

Direct thermal printers use special thermal (heat-sensitized) paper, and thermal transfer printers might use either standard copy paper or glossy photo paper, depending on their intended use.

If a printer uses direct thermal printing, heat-sensitive paper with characteristics matching the printer's design specifications must be used. For portable printers that use direct thermal printing, such as the Brother PocketJet series, the usual source for such paper is the printer vendor or its authorized resellers. If the direct thermal printer is used for barcodes or point-of-sale (POS) transactions, you can get suitable paper or label stock from barcode or POS equipment suppliers and resellers.

Thermal transfer ribbons are available in three categories: wax (for paper—smooth paper produces the best results), wax/resin (synthetics), and resin (glossy, hard films, such as polyester). Choose the appropriate ribbon type for the material you will be printing on.

Dye-sublimation photo printers in the consumer space use special media kits that include both a ribbon and suitable photo paper stocks. Larger-format dye-sublimation printers are designed to print on standard-size and special-format roll and sheet dye-sublimation paper stocks, available separately from the ink or ribbon.

## Thermal Maintenance

The elements of thermal printer maintenance include replacing the paper when it runs out, cleaning the heating element as directed, and removing debris from the heating element, rollers, or other components, as needed. For the 220-1101 exam, be sure to know the steps for thermal printer maintenance:

- Replace the paper.
- Clean the heating element.
- Remove debris.

### Cleaning Heating Elements

Because the heating element in a thermal printer is the equivalent of the print head in impact or inkjet printers, it must be kept clean to provide maximum print quality. Many vendors recommend cleaning the print head after each roll of thermal transfer ribbon.

Some thermal transfer ribbons for POS and warehouse printers include special cleaning materials at the beginning of the roll. Some thermal printer vendors also supply special cleaning film you can use to remove dust, debris, and coating residue from print heads.

You can also use isopropyl alcohol to clean print heads; it is available in wipes, pens, pads, and swabs from various vendors. The ribbon must be removed before using isopropyl alcohol. When isopropyl alcohol is used in cleaning, it is essential to wait until the printer dries out before reinstalling the ribbon.

### Removing Debris

Debris from torn paper, solid ink flakes, and label coatings can build up on rollers and other components, as well as on the print head. Use isopropyl alcohol wipes or other cleaning materials, as recommended by the printer supplier, to clean up debris for better print quality and longer print life.

## Impact Printers

An **impact printer** is so named because it uses a mechanical print head that presses against an inked ribbon to print characters and graphics. Impact printers are the oldest printer technology, and they are primarily used today in industrial and point-of-sale applications.

Dot-matrix printers, the most common form of impact printers, are so named because they create the appearance of fully formed characters from dots placed on the page.

## NOTE

For the 220-1101 exam, be sure to know the basic elements of impact printing:

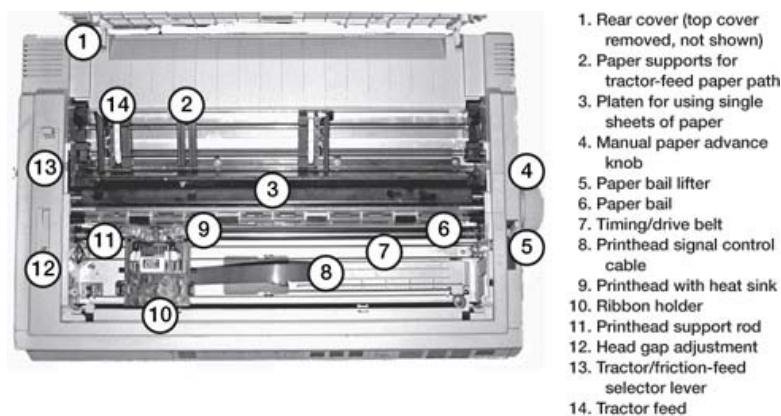
- Print head
- Ribbon
- Tractor feed
- Impact paper

## Impact Components and Print Process

Impact dot-matrix printers have a number of parts that move in coordination with each other during the printing process:

- Step 1.** The paper is moved past the print head vertically by pull or push tractors or by a platen.
- Step 2.** The print head moves across the paper horizontally, propelled along the print head carriage by a drive belt, printing as it moves from left to right.  
Bidirectional printing prints in both directions but is often disabled for high-quality printing because precisely aligning the printing is difficult.
- Step 3.** As the print head moves, the pins in the print head move in and out against an inked printer ribbon to form the text or create graphics.
- Step 4.** The ribbon is also moving, to reduce wear during the printing process.

These steps are repeated for each line until the page is printed. [Figure 3-98](#) illustrates a typical impact dot-matrix printer. The model pictured is a wide-carriage version, but its features are typical of models that use either standard or wide-carriage paper.



**Figure 3-98** Components of a Typical Impact Printer

## Impact Print Heads

The most common types of print heads include 9-pin, 18-pin (two columns of 9 pins each), and 24-pin (which produces near letter quality, or NLQ, printing when used in best quality mode).

[Figure 3-99](#) shows actual print samples from a typical 9-pin printer's draft mode, a typical 24-pin printer's draft mode, and the near letter quality (NLQ) mode of the same 24-pin printer.

```
RN_clients.html.Z -----9-pin printer draft mode  
RN_loc_cal.html.Z  
RN_loc_doc.html.Z  
RN_loc_uucp.html.Z  
  
This is a test of switching-----24-pin printer draft mode  
Congratulations!-----24-pin printer NLQ mode  
  
If you can read this inform  
Panasonic KX-P1624.  
  
The information below descr
```

**Figure 3-99** Actual Print Samples Illustrating the Differences in 24-Pin and 9-Pin Impact Printers

### Note

The print samples shown in [Figure 3-99](#) are taken from printers that use 8.5–11-inch or wider paper sizes. The print head design and print quality vary greatly on printers that use smaller paper sizes in point-of-sale applications.

## Impact Printer Ribbons

Printer ribbons for impact printers use various types of cartridge designs. Some span the entire width of the paper, and others snap over the print head. [Figure 3-100](#) shows two types of ribbons for impact printers.



**Figure 3-100** Typical Ribbons for Impact Printers

## Impact Printer Paper Types

Impact printers use plain uncoated paper or labels in various widths and sizes. Impact printers designed for point-of-sale receipt printing might use roll paper or larger sizes of paper. When larger sizes of paper are used, these printers typically use a **tractor feed** mechanism to pull or push the paper past the print head. Tractor-feed printer paper and labels have fixed or removable sprocket holes on both sides of the paper. This type of media is often called *impact*, *dot-matrix*, *continuous feed*, or *pin-feed* paper or labels. Media with standard perforations can be difficult to separate from the paper edge after printing, but that paper is less likely to separate before use than microperforated media.

Multipart forms are frequently used with impact printers used in POS systems. Be sure to adjust the head gap appropriately, to avoid print head or ribbon damage.

## Impact Printer Maintenance



The keys to successful maintenance of an impact printer include replacing the ribbon, replacing the print head, and replacing the paper.

### Note

For the 220-1101 exam, be sure to know the basic elements of impact printer maintenance:

- Replace the ribbon.
- Replace the print head.
- Replace the paper.

## Replacing the Ribbon

Keeping the ribbon fresh is important. Obviously, when the ribbon is worn, the quality of printing goes down. Furthermore, the ribbon on an impact dot-matrix printer lubricates the pins in the print head and protects the print head from impact damage. In addition to replacing the ribbon when print quality is no longer acceptable, be sure to immediately discard a ribbon that develops cuts or snags—a damaged ribbon can snag a print head pin and break or bend the pin.

## Replacing the Print Head

If you replace ribbons when needed, you minimize the chances of needing to replace the print head. However, if a print head suffers damage to one or more pins, you must replace it. Damaged pins might snag the ribbon, and if a pin breaks, it will leave a gap in the characters output by the printer.

## Replacing Paper

When you replace paper, be sure to check continuous-feed (tractor-feed) paper for problems with torn sprocket holes, separated tear-offs, and damaged sheets. Tear off any problem pages, and use only good paper from the stack in your printer.

Be sure the tractor feeders are properly adjusted, and if the printer can be run as either a push tractor (allowing zero-tear paper feed) or a pull tractor, be sure the printer is properly configured for the feed type.

Carefully check the head gap: Adjust it if you need to run multipart forms, thick labels, or envelopes. An incorrect head gap can lead to ribbon and print head damage.

## 3D Printers

*3D printing* is the common term given to what is technically known as *additive manufacturing (AM)*. Several types of 3D printing exist, and changes are constantly occurring. Two popular types of desktop 3D printing are listed here:

- **Fused deposition modeling (FDM):** This is the most popular and approachable of 3D printing in a tabletop environment.
- **Stereolithography (SLA):** This is a newer 3D tabletop process that involves photopolymer resins and lasers. 3D printing is a relatively old technology, but key patents have expired and made it available to new markets. New ideas for products are being developed at a rapid rate. Small FDM machines are common for hobbyists and small shops that need plastic components designed or manufactured onsite. SLA printers produce objects with higher detail but less strength than FDM printers, so they tend to be used for modeling and design.

work. Setting up and maintaining small 3D machines will be skills that are increasingly in demand among IT technicians.

As with other printers mentioned earlier in this section, you should know the basic process and parts of a **3D printer**. The physical process of using an FDM printer can be compared to the process of using a household glue gun: A hard material is pushed into a heating chamber, and the melted material is carefully directed through a nozzle, where it cools and becomes part of another object. Of course, FDM is much more complex because of the software for 3D design and the mechanics of moving the nozzle precisely.

In the FDM printing process, an object is created by adding layers of material to form a complete object. The most common material is a strand of *plastic filament* that is fed from a spool to a moving printer head. The printer head heats the plastic and thinly layers it onto the printing platform in cross-sections that eventually build up into the 3D object that has been designed on the computer. This process is carried out on a 3D printer using these four components:

- **Filament:** This is the material that is fed from a spool. It is usually plastic, although many different materials can be used. The two most common types of filament are polylactic acid (PLA) and acrylonitrile butadiene (ABS). The filament is the “ink” of an FDM printer and is available in various colors.
- **Extruder:** The extruder takes in the plastic filament and melts it.
- **Nozzle:** The nozzle is a small spray hole that emits the melted filament.
- **Print bed:** The bed is the platform on which the object is created. An FDM printer builds the object layer by layer, from the print bed up.

An SLA printer has a similar desktop footprint to an FDM printer and also builds objects by creating thin layers of strategically placed plastic; however, it uses a very different technology. Using a laser and mirrors below a bed of resin, SLA printers heat liquid **resins** with a laser to form thin layers of plastic. The laser light is directed to different points on the mirror and redirected to specific points of the resin for heating and fusing into a layer of plastic. When each new layer is added to the bottom, the object is pushed up. The result is an object printed in an inverted, or upside-down, position.

The SLA process delivers objects that are higher in detail and finish quality than FDM, but they are less robust and not strong enough for mechanical use.

The process of 3D printing with either printer is essentially the same:

- Step 1.** Design an object using computer-aided design (CAD) software. CAD software comes in a wide array of sophistication, and the processing demands on the computer can require enhanced GPUs.
- Step 2.** Convert the model to an STL (printing code) format.

**Step 3.** Set the print speed. (Slower speeds mean higher-quality printing. If you print too fast, melted filament will not set properly, so start at midrange settings.)

**Step 4.** Ensure that the correct temperature is chosen; different filaments (and even colors) can have variable melting points.

**Step 5.** Print.

Figure 3-101 shows a 3D printer with yellow filament being used to print a bowl.



**Figure 3-101** 3D printing

## Maintaining 3D Printers

As with all other printers, cleaning and lubrication are the essential maintenance tasks for performance. Special attention needs to be given in a few areas:

- Lubrications need to be heat resistant, or they can melt and become part of the printed object.
- Different brushes are needed to clean different parts. For example, stiff brass brushes are good for cleaning the outside of nozzles.
- Cleaning the filament between print jobs is important to ensure that the next job starts with a filament that is clean and at the correct temperature.

## Exam Preparation Tasks

As mentioned in the Introduction, you have several choices for exam preparation: the exercises here; [Chapter 10, “Final Preparation”](#); and the exam simulation questions in the Pearson Test Prep practice test software.

## Review All the Key Topics

Review the most important topics in the chapter, noted with the Key Topic icon in the outer margin of the page. [Table 3-22](#) lists these key topics and the page number on which each is found.



**Table 3-22** Key Topics for [Chapter 3](#)

<b>Key Topic Element</b>	<b>Description</b>	<b>Page Number</b>
<a href="#">Table 3-2</a>	Categories and Uses for TP Cabling	137
<a href="#">Figure 3-2</a>	T568B (Left) and T568A (Right) Wire Pairs and an Assembled T568B Cable	140
<a href="#">Figure 3-3</a>	SC, LC, and ST Fiber-Optic Cable Connectors Compared	142
<a href="#">Table 3-3</a>	Video Connector Types Overview	146
<a href="#">Figure 3-7</a>	DB15M (Cable) and DB15F (Port) Connectors Used for VGA Video Signals	147

<b>Key Topic Element</b>	<b>Description</b>	<b>Page Number</b>
<a href="#">Figure 3-8</a>	HDMI Cable Connectors Compared to DVI and DisplayPort Cable Connectors	148
<a href="#">Figure 3-9</a>	HDMI, DVI, and VGA Ports on the Rear of Two Typical PCIe Video Cards	148
<a href="#">Figure 3-11</a>	DVI-I Video Port and DVI-D Video Cable	151
<a href="#">Table 3-5</a>	USB Standards Overview	156
<a href="#">Table 3-6</a>	Network Connector Types	165
<a href="#">Figure 3-25</a>	DDR3 SODIMM Module Compared to a DDR3 DIMM Module	169
<a href="#">Table 3-8</a>	RAM Comparison	169
<a href="#">Figure 3-26</a>	DDR, DDR2, DDR3, and DDR4 DIMM Desktop Memory Modules with Different Notch Locations	171
Section	Installing Memory	175
<a href="#">Figure 3-28</a>	A DIMM Partly Inserted (Top) and Fully Inserted (Bottom)	176
Section	DVD Recordable and Rewritable Standards	180
<a href="#">Table 3-9</a>	Comparison of the Three Hard Drive Types	187
<a href="#">Figure 3-34</a>	Front (Left) and Rear (Right) Internal Optical, Desktop, and Mobile Internal Hard Disks, and Mobile Internal SSD Drives	189
Section	Flash Drives/Memory Cards	190
<a href="#">Table 3-12</a>	Comparisons of Common RAID Levels	195
<a href="#">Table 3-13</a>	ATX Motherboard Family Comparison	202
<a href="#">Figure 3-44</a>	A Typical Late-Model ATX Motherboard	203
<a href="#">Figure 3-45</a>	A Typical Late-Model microATX (mATX) Motherboard	204
<a href="#">Figure 3-46</a>	A Typical Mini-ITX (mITX) Motherboard Optimized for Home Theater Applications	205
<a href="#">Figure 3-47</a>	ATX, microATX, and Mini-ITX Motherboard Component Layouts Compared	206
<a href="#">Figure 3-48</a>	PCI Express Compared to PCI Slots	207
Section	Land Grid Array Sockets	213
Section	mPGA Sockets	215

<b>Key Topic Element</b>	<b>Description</b>	<b>Page Number</b>
<a href="#">Table 3-15</a>	Examples of Intel and AMD Desktop and Mobile Series CPUs	216
Section	BIOS/UEFI Configuration	218
Paragraph	Accessing the BIOS/UEFI setup program	219
<a href="#">Table 3-18</a>	Major CMOS/BIOS/UEFI Settings	222
<a href="#">Figure 3-57</a>	Boot Sequence and Other Boot Settings in the UEFI/BIOS Features Menu	225
<a href="#">Figure 3-58</a>	A Typical Boot Menu Configured to Permit Booting from a CD/DVD or USB Flash Drive Before the Hard Drive	226
Section	Firmware Updates	226
Section	Security Features	229
Section	CMOS Battery	234
<a href="#">Figure 3-64</a>	A Typical CMOS Battery (CR2032)	235
Section	CPU Cores: Single Core and Multicore	238
<a href="#">Figure 3-71</a>	A PCIe x16 Video Card Designed for Multi-GPU (CrossFire) Support	246
Section	Removing Drivers for an Old Video Card or Onboard Video	247
Section	Video Card Physical Installation	250
Section	Heat Sink	256
Section	Power Supply Ratings	261
Section	20-Pin-to-24-Pin Motherboard Adapter	265
<a href="#">Figure 3-86</a>	Power Supply Connectors for Peripherals and Modern Motherboards	267
<a href="#">Table 3-20</a>	Power Levels for Different Connector Types	267
<a href="#">Table 3-21</a>	Calculating Power Supply Requirements	271
Section	Laser Printers	280
Tip	Seven-step laser printing imaging process	282
Section	Inkjet Printers	288
<a href="#">Figure 3-95</a>	The Pattern Check (Nozzle Check) Dialog Box from a Canon Inkjet Printer Driver's Maintenance Tab	294

<b>Key Topic Element</b>	<b>Description</b>	<b>Page Number</b>
Section	Thermal Printers	295
Section	Impact Printer Maintenance	301

## Complete the Tables and Lists from Memory

Print a copy of [Appendix C, “Memory Tables”](#) (found online), or at least the section for this chapter, and complete the tables and lists from memory. [Appendix D, “Memory Tables Answer Key,”](#) also online, includes completed tables and lists to check your work.

## Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

Cat 5  
 Cat 5e  
 Cat 6  
 Cat 6a  
 plenum  
 unshielded twisted pair  
 shielded twisted pair  
 direct burial  
 T568B  
 T568A  
 fiber-optic cabling  
 subscriber connector (SC)  
 lucent connector (LC)  
 straight tip (ST)  
 coaxial  
 F type  
 Video Graphics Array (VGA)  
 High-Definition Multimedia Interface (HDMI)  
 DisplayPort  
 Digital Visual Interface (DVI)  
 Thunderbolt  
 USB-C  
 USB 2.0  
 USB 3.0

Serial

Serial Advanced Technology Attachment (SATA)

Integrated Drive Electronics (IDE)

Small Computer System Interface (SCSI)

expansion card

RJ-11

RJ-45

microUSB

miniUSB

DB9

lightning port

Molex

RAM

Double Data Rate 3 (DDR3)

Double Data Rate 4 (DDR4)

Double Data Rate 5 (DDR5)

Small Outline Dual Inline Memory Module (SODIMM)

virtual RAM

single-channel

dual-channel

triple-channel

quad-channel

error correction code (ECC)

optical drives

mSATA

Non-Volatile Memory Express (NVMe)

SATA

flash drives

Redundant Array of Independent (or Inexpensive) Disks (RAID)

RAID Level 0 (RAID 0)

RAID Level 1 (RAID 1)

mirroring

RAID Level 5 (RAID 5)

RAID Level 1+0 (RAID 10)

microATX (mATX)

Advanced Technology eXtended (ATX)

microATX (mATX)

Information Technology eXtended (ITX)

Peripheral Component Interconnect (PCI)

Peripheral Component Interconnect Express (PCIe)

External SATA

headers

M.2

Trusted Platform Module (TPM)

Secure Boot

hardware security module (HSM)

Advanced RISC Machine (ARM)

single-core

multicore

multithreading

capture card

network interface card (NIC)

heat sink

thermal paste

thermal pads

modular power supply

wattage rating

Printer Control Language (PCL)

PostScript

SMB

Automatic Document Feeder (ADF)

laser printer

imaging drum

fuser assembly

transfer belt

transfer belt (transfer roller)

pickup rollers

duplexing assembly

charging

exposing

fusing

cleaning

inkjet printer

thermal printer

impact printer

tractor feed

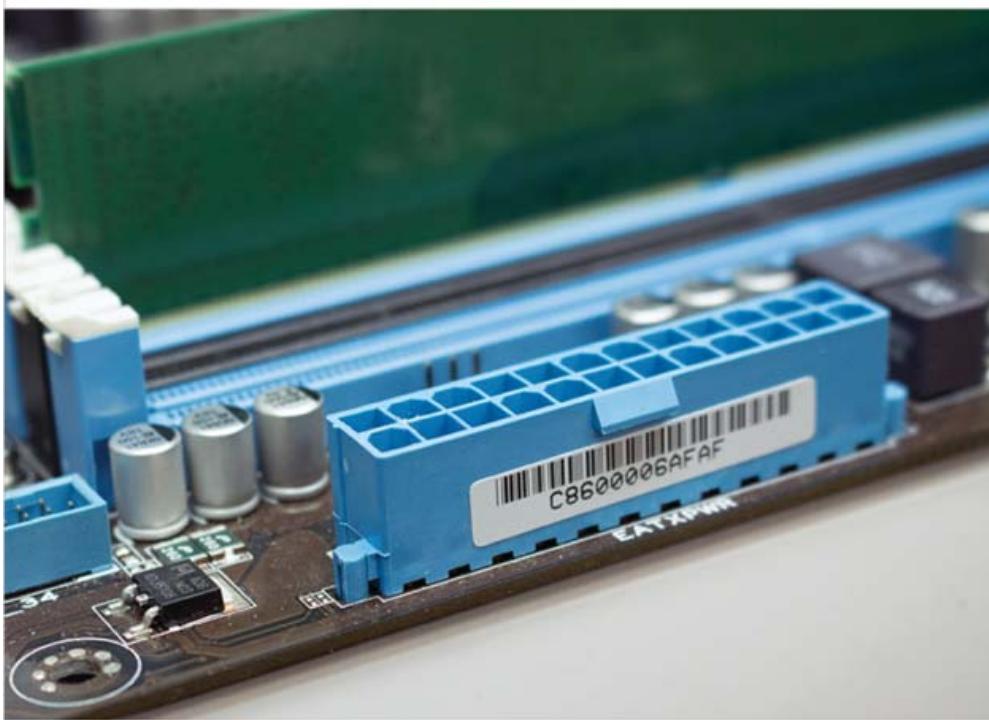
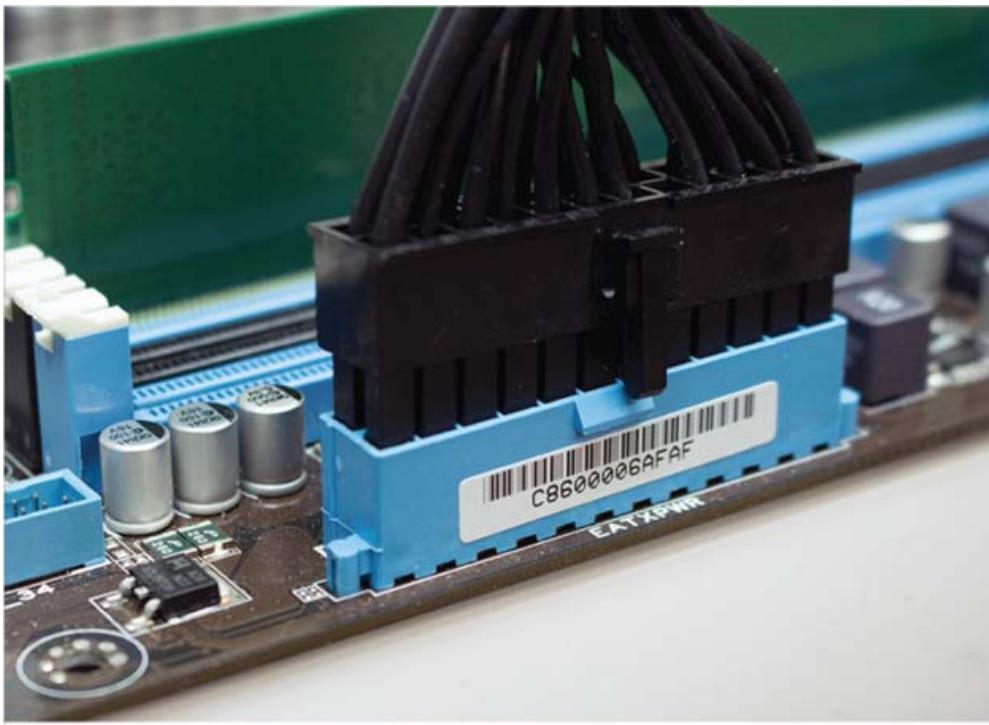
3D printer

filament

print bed  
resin

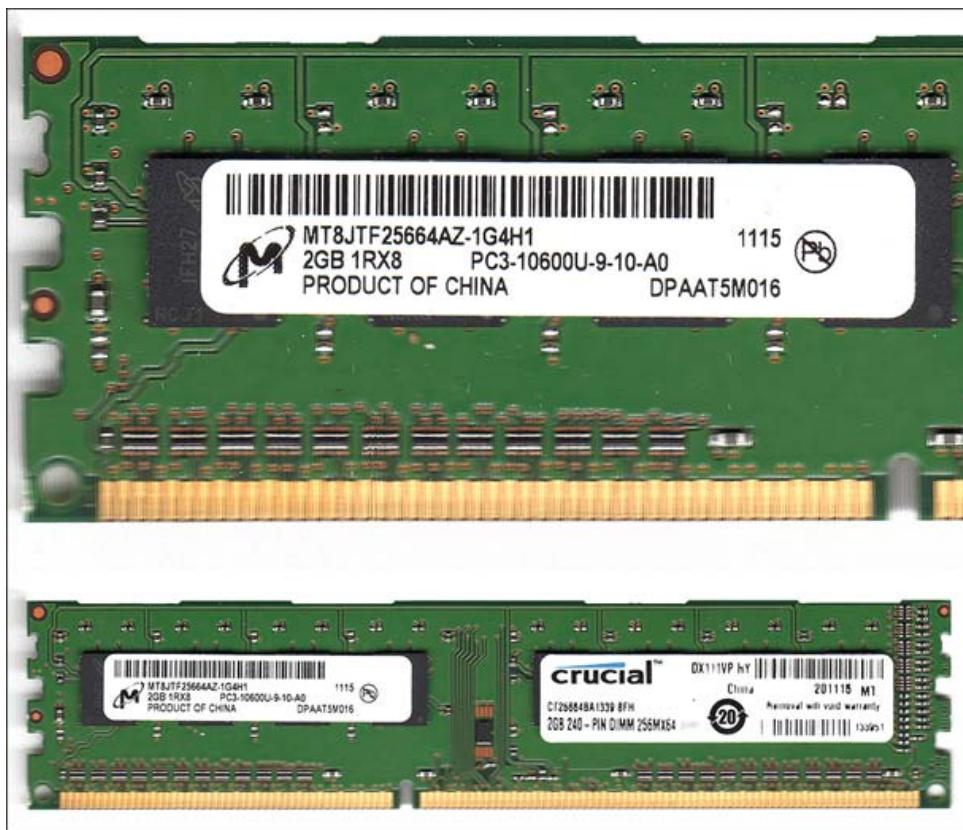
## Answer Review Questions

- 1.** Identify the port and connector shown in the following display. Choose from the following options:
  - a.** ATX 24-pin power supply cable and connector
  - b.** ATX12V power supply cable and connector
  - c.** EPS12V power supply cable and connector
  - d.** USB 3.0 cable and connector



2. Your client has just connected a computer to a receiver for better music playback, but no audio is coming from the receiver. You check the SPDIF cable connection and the output setting on the receiver, and verify that audio is not muted on the computer. Which of the following is the most likely cause?
- a. SPDIF audio is not selected as the default output.
  - b. The VGA cable is loose.

- c. The microphone is disconnected.
  - d. There is interference from the smart card reader.
3. Which of the following loses its contents when you shut down the computer?
- a. Hard disk drive
  - b. USB flash drive
  - c. RAM
  - d. ROM
4. Identify the type of RAM in the following figure.



- a. DDR
  - b. DDR2
  - c. DDR3
  - d. DDR4
5. What kind of support is provided by a system that uses matched pairs of memory modules?
- a. ECC
  - b. Dual-channel
  - c. Buffered

**d.** SDRAM

**6.** Which methods are used to protect the reliability of memory? (Choose two.)

- a.** Parity checking
- b.** System checking
- c.** ECC (error-correction code)
- d.** Smart checking

**7.** Most types of desktop memory modules use which kind of memory?

- a.** Unbuffered non-ECC memory
- b.** Virtual memory
- c.** SODIMM module
- d.** ECC memory

**8.** Critical applications and network servers use a special type of memory. What is it called?

- a.** ECC memory
- b.** Unbuffered memory
- c.** Static memory
- d.** Crucial memory

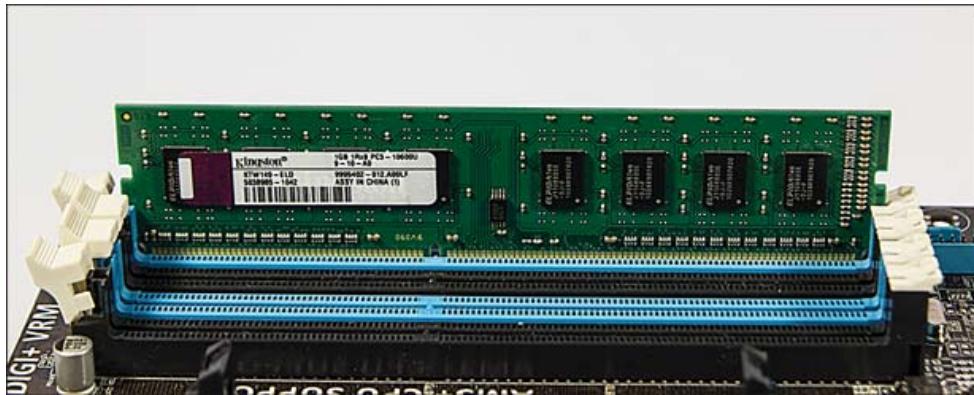
**9.** What needs to be applied to a processor before installing a heat sink?

- a.** Thermal paste
- b.** Filament
- c.** Resin
- d.** Paper separation pad

**10.** To correctly install a DIMM module, what should you do? (Choose all that apply.)

- a.** Line up the module connectors with the socket.
- b.** Verify that the locking tabs on the socket are swiveled to the outside (open) position.
- c.** Verify that the module is lined up correctly with the socket, and then push the module straight down until the locks on each end of the socket snap into place at the top corners of the module.
- d.** None of these options is correct.

**11.** You have a dual-channel motherboard. You have two identical 4GB DDR3 modules and two identical 2GB DDR3 modules. In the following diagram, one module of 4GB DDR3 is being installed in the first blue slot. Where should you install the second 4GB DDR3 module for best results?



- a. Install the second 4GB DDR3 in the second blue slot.
- b. Install the second 4GB DDR3 in the first black slot.
- c. Install the second 4GB DDR3 in the second black slot.
- d. It does not matter, as long as all the modules are DDR3.

**12.** Which of the following types of RAM is also known as PC3-10600?

- a. DDR3-800
- b. DDR3-1066
- c. DDR3-1333
- d. DDR3-1600

**13.** Write the type of storage media (optical, magnetic, or flash) that corresponds with each description.

Description	Storage Media
Records information in tracks and sectors containing 512 bytes each	
Stores data in a continuous spiral	
Used on memory cards	
Records information in a series of lands and pits	
Uses laser light to read data	
Records information in concentric circles	
Records information from the center outward	
Stores data on double-sided platters	
Records information from the outer edge inward	
Used in solid-state drives	

**14.** Your client is considering purchasing a tablet with eMMC storage. Which one of the following statements is correct?

- a.** The tablet will have faster data access than if it is used in SSD.
- b.** eMMC is supplied in microSD cards that can be removed.
- c.** The tablet cannot use USB devices.
- d.** The tablet will have slower data access than if it used an SSD.

**15.** Which printer type prints layer by layer using a filament?

- a.** Impact
- b.** Thermal
- c.** 3D
- d.** Inkjet

**16.** Your client has requested a hard disk upgrade for a laptop with the following parameters: 1TB and lowest power consumption. Which of the following factors will a matching drive have? (Choose all that apply.)

- a.** 3.5-inch form factor
- b.** 5400RPM
- c.** 7200RPM
- d.** 2.5-inch form factor

**17.** A user has requested a RAID array that balances high performance with data safety. Which of the following would you recommend?

- a.** RAID 1
- b.** RAID 10
- c.** RAID 5
- d.** RAID 0

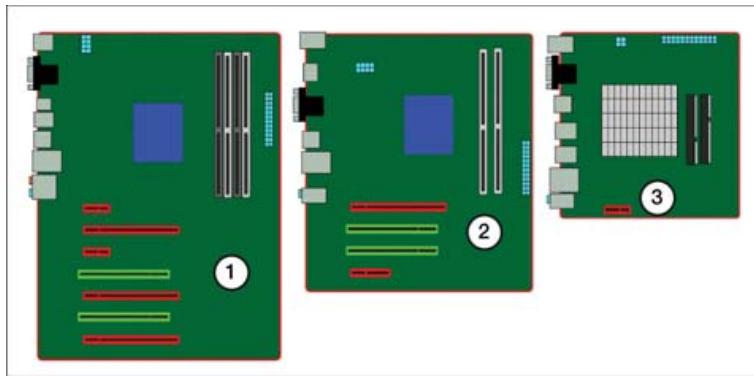
**18.** Which of the following is the most common motherboard form factor used in desktop computers today?

- a.** ATX
- b.** microATX
- c.** ITX
- d.** Mini-ITX

**19.** Which motherboard form factor is the smallest in size?

- a.** ATX
- b.** microATX
- c.** ITX
- d.** Mini-ITX

**20.** In this figure, match each motherboard diagram with the form factor that it represents.



- A. Mini-ITX
- B. ATX
- C. microATX

**21.** In the following figure, select the numbers that indicate power connectors. (Choose two.)



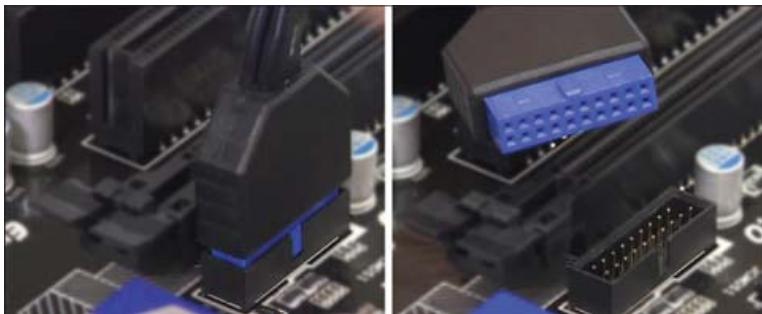
**22.** Refer to the figure from question 21, and answer the following question. Which numbers identify the RAM slots? (Choose two.)

**23.** True or false: DDR4 and DDR5 DIMMs are compatible with each other and can be used interchangeably in the same RAM slots on a motherboard.

**24.** Most motherboards have one connector for the CPU fan and one or more connectors for the system fans that circulate air inside the case. How do these fan connectors differ?

- a. The CPU fan has an extra pin for fan timing.
  - b. The system fans have an extra pin to regulate air flow direction.
  - c. The CPU fan has an extra pin to control fan speed.
  - d. The system fan has an extra pin to control fan speed.
- 25.** Which of the following statements best describes how to make changes to the bus speeds of components such as the processor, chipset interconnect, or memory?
  - a. You make changes to POST and then save those changes on the BIOS/UEFI chip.
  - b. You download the changes you want to make from the manufacturer's website and then save the changes to the BIOS/UEFI chip.
  - c. You make changes to the BIOS settings and then save those changes on the CMOS chip.
  - d. You make all desired changes and save those changes to the South Bridge chipset.

- 26.** Identify the component that uses the connector shown in the following figure.



- a.** PCIe
  - b.** PCI-X
  - c.** USB 2.0
  - d.** USB 3.0
  - e.** SATA
- 27.** The CMOS chip allows the user to save and store changes made to the BIOS configurations. Which of the following statements best describes how to clear the CMOS settings and revert to the original BIOS configurations?
- a. Place a jumper block over the CMOS jumper pins.
  - b. Write a new program for the CMOS chip.
  - c. Download a new program from the manufacturer and flash it to the CMOS chip.
  - d. Edit the South Bridge programming to change the CMOS settings.

- 28.** You have noticed that your computer's clock has begun to lose time. You have reset the clock repeatedly, but it still continues to lose time. Which component is most likely at fault?
- a. One of the PCI slots
  - b. The CMOS battery
  - c. An incorrect entry in the BIOS configurations
  - d. An incompatible RAM module
- 29.** When designing and building a new customized PC to be used for graphic design, audiovisual editing, 3D game development, or virtualization, which of the following will probably need to be upgraded?
- a. CPU
  - b. RAM
  - c. Sound and display
  - d. Cooling system
  - e. All of the above
- 30.** Which of the following statements best describes the function of a computer's power supply?
- a. To provide DC power from the wall outlet to the computer
  - b. To convert DC power to AC power
  - c. To convert AC power to DC power
  - d. To provide AC power from the wall outlet to the computer
- 31.** Refer to the following figure, which depicts two different power supplies, and complete the chart.



Total Watts (W)	Number of +12V Rails(R)	Amp Output from +12V Rails (Amp)
Power Supply A		
Power Supply B		

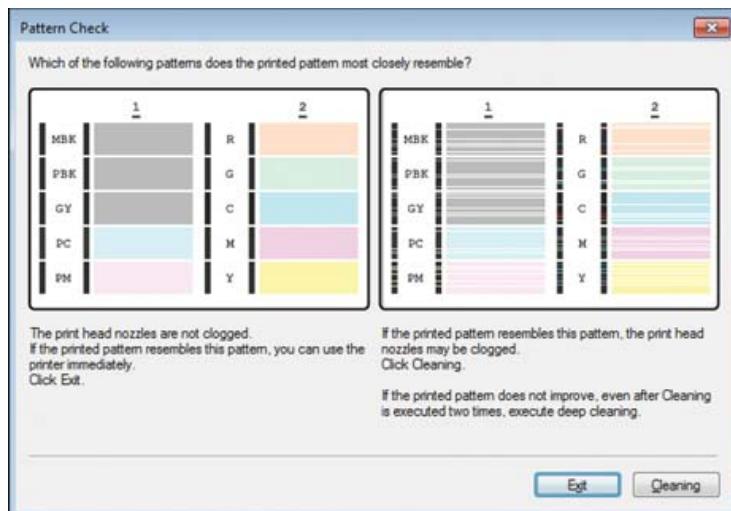
**32.** Which one of the following USB devices is most likely to need additional drivers installed to operate?

- a. Keyboard
- b. Mouse
- c. Touchpad
- d. Scanner

**33.** Place the steps in the laser printing imaging process in the correct order on the right side of the table.

Charging	1
Cleaning	2
Developing	3
Exposing	4
Fusing	5

- 34.** True or false: During the charging step in the laser printing imaging process, the drum receives an electrostatic charge of –600V. Because the drum is photosensitive, it retains its charge only if it is kept in the dark.
- 35.** A laser printer uses which of the following processes?
- a. Line-by-line printing
  - b. Impact plus heat transfer
  - c. Impact against an inked ribbon
  - d. Whole-page printing
- 36.** How do inkjet printers create characters and graphics?
- a. By spraying tiny dots of ink onto the page
  - b. By fusing fine grains of toner into the page
  - c. By using a thermal transfer ribbon
  - d. By using an ink impregnated ribbon
- 37.** Which acronym refers to the colors used by an inkjet printer?
- a. CMYB
  - b. CMYK
  - c. RBG
  - d. RBGY
- 38.** In the following figure, which kind of problem does the right half of the screen demonstrate?



a. The drum of a laser printer has old toner clinging to it and needs to be cleaned.

b. The ribbon on an impact printer is old and is wearing out.

c. The heating mechanism of a thermal printer is not getting hot enough.

d. The print heads on an inkjet printer are clogged or faulty.

**39.** Thermal printers use which of the following?

a. A nonimpact matrix of dots that can be heated and used in various combinations to create an image

b. Toner to create an image and heated rollers to fix the toner to the paper

c. Closely grouped nozzles of heated ink to produce an image

d. An ink-impregnated ribbon to create an image, followed by heated rollers to set the image

**40.** Which type of printer typically uses multipart forms?

a. Laser printer

b. Impact printer

c. Inkjet printer

d. Thermal printer

**41.** Which of the following are common print drivers?

a. PostScript

b. ECC

c. PCI

d. PCL

**42.** You have just bought a new printer and are about to install it. Which of the following statements describes the best way to be sure that your drivers are up-to-date?

a. Use the installation disc that shipped with the printer.

b. Use Windows Update to automatically select the best drivers.

c. Go to the vendor's website to select drivers.

d. Connect the printer to the computer and allow it to autoinstall.

**43.** Which of the following is not a typical print configuration setting for a printer or multifunction device?

a. Selecting duplex printing

b. Configuring collating

c. Choosing a cover page

d. Changing the orientation of the page

**44.** Which type of encryption is supported by a printer in ad hoc mode?

- a.** WEP
- b.** WPA2
- c.** WPA3
- d.** NIC

# Chapter 4

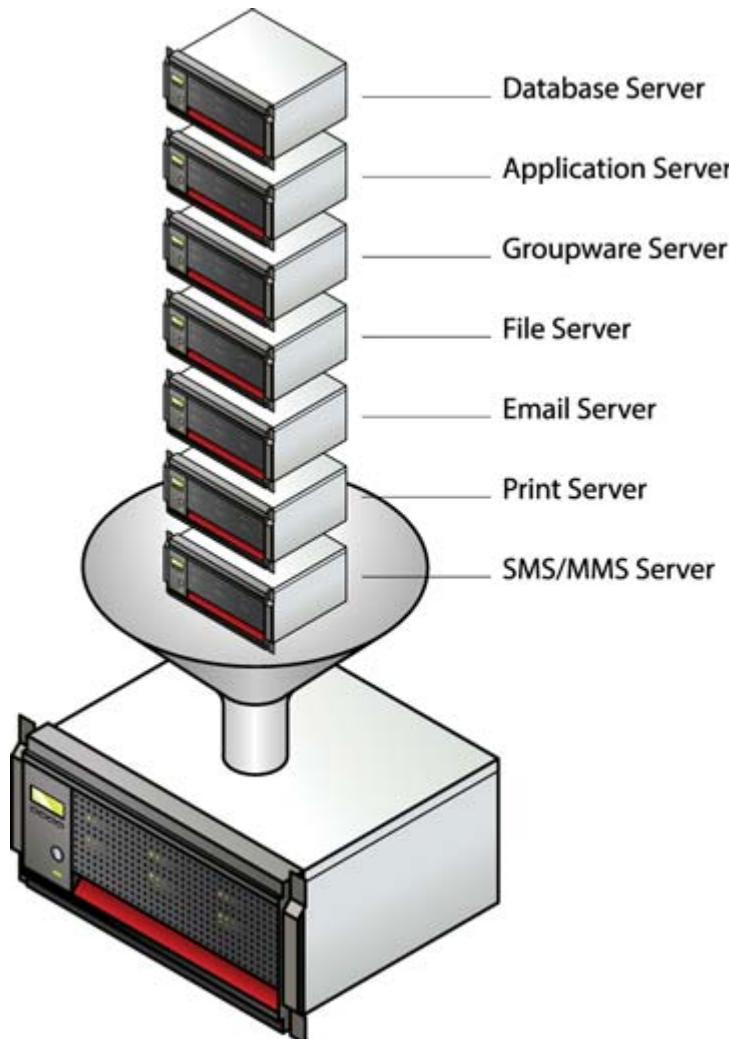
## Virtualization and Cloud Computing

**This chapter covers the two A+ 220-1101 exam objectives related to virtualization and cloud computing. These objectives may comprise 11 percent of the exam questions:**

- **Core 1 (220-1101): Objective 4.1:** Summarize cloud-computing concepts.
- **Core 1 (220-1101): Objective 4.2:** Summarize aspects of client-side virtualization.

Cloud computing involves using remote servers in the Internet “cloud” to store, manage, and process data instead of using local servers or a personal computer. Cloud servers usually reside in large server farms, where powerful servers host thousands of virtual machines.

Remember that a computer is made up of hardware components that process software instructions. Virtual computing technology creates and runs multiple instances of software operating systems—such as desktops, servers, and even networks—on a single piece of hardware. Multiple software systems sharing the resources of one hardware system is known as virtualization. A single laptop, desktop, or server commonly is used to run two or more different operating systems, such as Linux and Windows 10, at the same time. [Figure 4-1](#) depicts several different servers virtually running on one robust hardware machine.



**Figure 4-1** One Hardware Machine Running Several Virtual Servers (Image © Zern Liew, Shutterstock)

Cloud computing involves using virtual machines in commercial data centers, to relieve customers of the expense of maintaining a network center. Cloud-based systems enable customers to pay for only the services and capacity they use, which allows businesses to grow their technology capacity as they need it and avoid high up-front costs.

## **“Do I Know This Already?” Quiz**

The “Do I Know This Already?” quiz allows you to assess whether you need to read the entire chapter. [Table 4-1](#) lists both the major

headings in this chapter and the “Do I Know This Already?” quiz questions covering the material in those headings so that you can assess your knowledge of these specific areas. The answers to the “Do I Know This Already?” quiz appear in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes and Review Questions.”

**Table 4-1** “Do I Know This Already?” Section-to-Question Mapping

Foundation Topics Section	Questions
Common Cloud Models	1–5
Client-Side Virtualization Overview	6–10

## CAUTION

The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for the purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

- 1.** Which cloud computing model allows companies to access software when they need it but avoid the expense of maintaining the software when they do not need it?
  - a.** Resource pooling
  - b.** Rapid elasticity
  - c.** On-demand
  - d.** Hybrid
- 2.** You have been asked to arrange for your team to develop software in a cloud environment. Which of the following services

will you seek as a solution?

- a.** PaaS
  - b.** SaaS
  - c.** IaaS
  - d.** None of these options are correct
- 3.** A company requires high security and high reliability for its network services. What type of cloud environment is likely to meet these requirements?
- a.** Public cloud
  - b.** External cloud
  - c.** Internal cloud
  - d.** Infrastructure as a Service
- 4.** Which of the following allows users to access remote applications and use them as if they were installed on their own machine?
- a.** Application virtualization
  - b.** Sandboxing
  - c.** VMM
  - d.** File synchronization
- 5.** What term describes a cloud provider's capability to rapidly scale up and scale back computing resources as needed?
- a.** Rapid elasticity
  - b.** Flex data services
  - c.** Virtual data flexing
  - d.** Expansive data services
- 6.** Which of the following are used to create and run a VM?  
(Choose two.)
- a.** Hypervisor

- b. VMM
  - c. Emulator
  - d. Virtual sphere
- 7. Which of the following is a reproduction of an operating system?
  - a. Virtual machine
  - b. VMware Fusion
  - c. Emulator
  - d. Hyper-V
- 8. Which operating systems can be guests on a VM?
  - a. Windows
  - b. Linux
  - c. UNIX
  - d. None of these options are correct
  - e. All of these options are correct
- 9. Which of the following is true?
  - a. A 32-bit system can host a 64-bit VM.
  - b. A VMM can create only one operating system per hardware device.
  - c. A 64-bit system can host a 32-bit system.
  - d. Only one VM can run at a time on a workstation with one display.
- 10. Which of the following is true of the BIOS/UEFI when creating a VM?
  - a. Hypervisors create their own BIOS/UEFI settings.
  - b. The BIOS/UEFI firmware must support VMs.
  - c. All BIOS/UEFI firmware supports VMs.
  - d. A separate hard disk must be installed for each VM.

# Foundation Topics



## Common Cloud Models

**220-1101: Objective 4.1:** Summarize cloud-computing concepts.



The *cloud* refers to any type of computing—including program execution, storage, or services—that takes place remotely. Understanding basic cloud concepts is important for technicians, who will increasingly be asked to manage software or data in the cloud. Some of those functions are described in the following sections.

### IaaS

Infrastructure as a Service (**IaaS**) enables customers to purchase access to data center infrastructure such as storage, network, and networking services. In this model, the cloud provider covers the costs and work involved in equipment, firewall configurations, and other maintenance. Thousands of companies are realizing that they can reduce the costs of their network infrastructure by outsourcing storage and computing services to a cloud provider. These include new startup companies that lack the capital resources to buy and manage equipment as they grow and established companies that want to reduce the costs related to backup and storage of their networks.

One key feature of IaaS is the flexibility it offers to customers, who can now just use the virtual resources they need when they need them instead of having to pay for them when they don't need them.

IaaS puts users in charge of all the software used in a project, from applications and data to the operating system. IaaS vendors supply the hardware and network support tools.

Amazon first introduced cloud services in 2006, and the field of cloud providers continues to grow. At press time, the three largest cloud providers are as follows:

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud

## SaaS

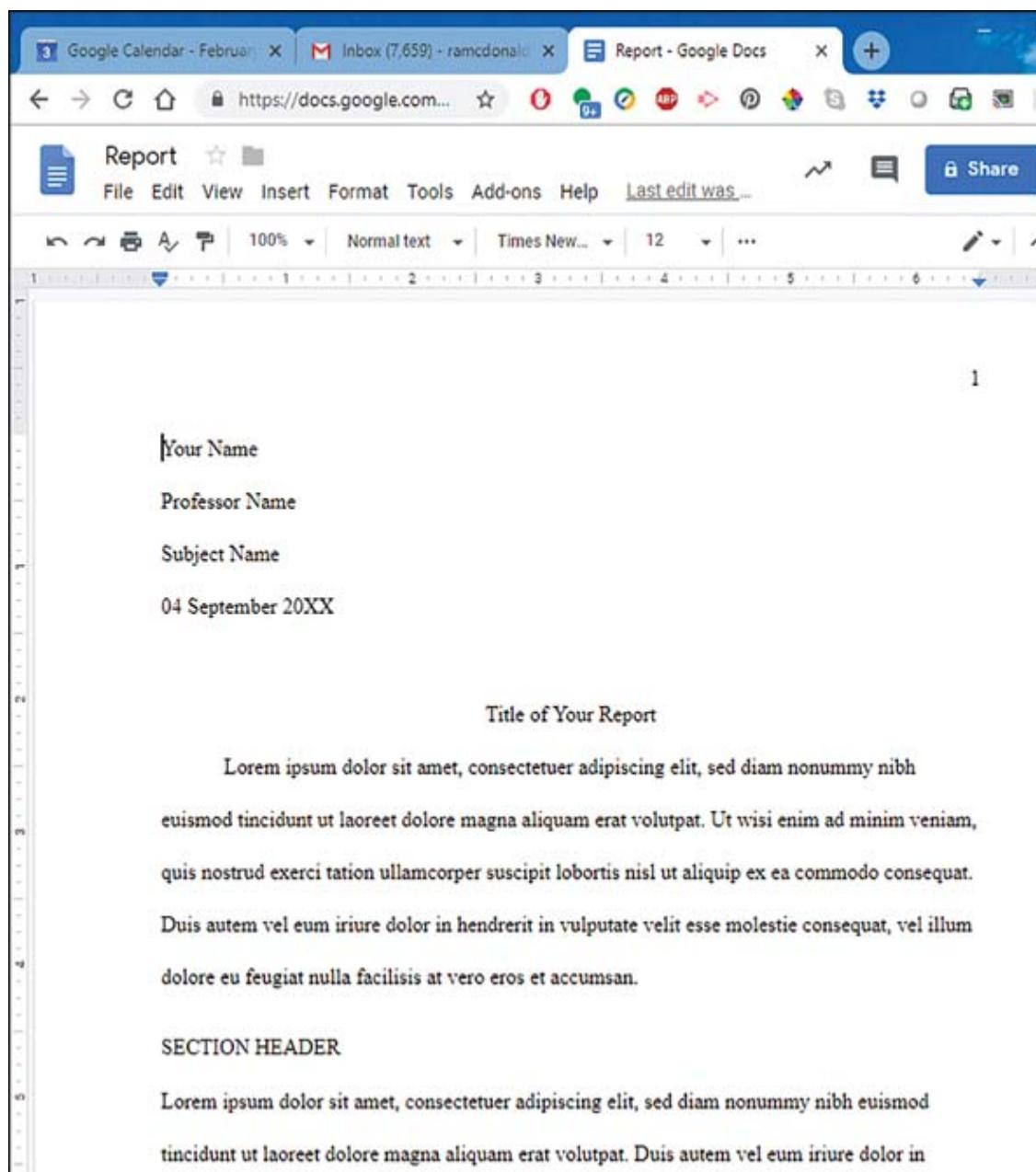
Software as a Service (**SaaS**) refers to software that is hosted on servers and accessed through a web browser. Because SaaS processing is performed at the server, a thin client, smartphone, or tablet is sufficient to run the software. A browser-based service that does not require a user to download an application code to use the service is an example of SaaS.

Perhaps the best-known SaaS is Google Mail (Gmail). Gmail servers provide the Gmail service to anyone who has a web browser. Other examples of SaaS include the following:

- **Google Docs:** Word processing, spreadsheets, presentations, and forms ([www.google.com/intl/en/docs/about/](http://www.google.com/intl/en/docs/about/))
- **Microsoft Office 365:** Word processing, spreadsheets, presentations, calendar, collaboration, and email ([www.office.com](http://www.office.com))
- **FreshBooks:** Small business accounting ([www.freshbooks.com](http://www.freshbooks.com))
- **Salesforce:** Customer relationship management ([www.salesforce.com](http://www.salesforce.com))

- **Basecamp:** Project management (<https://basecamp.com>)

SaaS is a cloud-based software licensing and delivery model that grants customers access to software on a subscription basis using the SaaS vendor's servers. SaaS is designed for organizations that need to use a service rather than develop or deploy one. [Figure 4-2](#) illustrates the word processor in Google Docs.



**Figure 4-2** Using the Google Docs Word Processor to Create a Report from a Template, with Random Text as Placeholders

## PaaS

Platform as a Service (**PaaS**) enables vendors to develop and deploy application software in a cloud environment. A developer using PaaS can concentrate on software features instead of possible issues with server hardware and operating systems.

Some of the major PaaS vendors include the following:

- **Oracle Cloud:** <https://cloud.oracle.com>
- **Google Cloud Platform:** <https://cloud.google.com>
- **Microsoft Azure:** <https://azure.microsoft.com>
- **Salesforce Platform:** [www.salesforce.com](http://www.salesforce.com)

Many vendors provide many services across multiple platforms.

### Note

Microsoft Azure is listed in both the PaaS and IaaS categories because it can be used in either role, depending on the services a user purchases.

Keep in mind the following considerations in selecting a PaaS vendor:

- **Language and server-side support:** Make sure the vendor selected supports the languages used for development and the server-side technologies the apps depend on. Most major PaaS vendors support languages such as Java, Ruby, PHP, and Python, but server-side technology support varies a great deal.

- **Integration with existing investments:** Some PaaS vendor products can integrate with existing apps and data, meaning that cloud platforms can work with existing resources instead of requiring users to replace them entirely.
- **Costs:** Most PaaS vendors use pricing by the hour, but some price by the month. Be sure your precommitment cost estimations take into account the software tools and services you need; pricing can vary according to the tools or services bundled.

## Public vs. Private vs. Hybrid vs. Community

Four general types of cloud computing are used. Each type can have variables in its implementation, depending on customer needs.



- **Public cloud computing** is available to any organization that signs up or pays for it. The connection between services and organizations is the public Internet. Public cloud computing typically includes built-in features and tools that would be too expensive to implement on their own. This allows organizations to pay for the features and options needed without buying, setting up, and maintaining the hardware themselves.
- **Private cloud computing** is available only to authorized users in divisions or departments of a single company. The company owns and manages the cloud behind its corporate firewall, and its employees maintain the equipment. Private cloud computing is considered to be more secure than public cloud computing. Private cloud computing is great for organizations that are highly regulated or need strict control over business-critical data, such as financial or health care organizations.
- **Hybrid cloud computing** combines features of public and private cloud computing. A typical hybrid installation includes

dedicated and cloud-based servers and high-speed interconnections with load balancing to move workloads between the environments as needed. Hybrid cloud computing is best for organizations that need to utilize both private and public clouds. For example, a financial institution might want to store critical and sensitive data on a private cloud while using a public cloud to store lower-risk data.

- **Community cloud computing** is a type of hybrid cloud computing used by different organizations that are working together. The organizations work as partners to build the community cloud and share its costs. This model works well for organizations that are working together temporarily on a single goal or project. When the project is finished, they can dissolve the cloud.

## Cloud Characteristics

*Cloud computing* is a generic term that can encompass several different computer network models and features that serve a customer's unique requirements. This section describes different ways a computer cloud can be designed and implemented to meet the computing and network needs of a company or institution.

## Shared Resources



**Shared resources** refers to the practice of sharing equipment or data on a network to save costs. This is the most common reason for implementing cloud computing. The way clouds are designed and implemented can vary according to the customer's needs. Devices and data can be shared over the Internet in two main ways: using an internal cloud or using an external cloud.

## Internal Cloud

Internal and external clouds are defined by the ownership of the cloud's resources. With an internal cloud, a company might need the flexibility of cloud services but also have security and guaranteed availability requirements that prevent the company from accessing cloud services outside its own network. An internal cloud is similar to a private cloud, but it is built and owned inside the organization. With an internal cloud, the company gets the virtualization services and flexibility of a commercial cloud, but with the security and reliability that comes from existing within the company's network infrastructure. The cost of an internal cloud might be higher than the cost of outsourcing to commercial services, but sharing resources internally still reduces the cost.

## External Cloud

An external cloud is a cloud solution that exists outside an organization's physical boundaries. It can be private, public, or community based, as long as it is not located on an organization's property.

## Rapid Elasticity

**Rapid elasticity** refers to the capability to rapidly scale up and scale back cloud computing resources as needed. For example, selling high-demand concert tickets in the days before cloud computing often resulted in crashing servers and disappointed customers. Thanks to the rapid elasticity of the cloud, high-demand events can quickly expand capacity for online sales without leaving customers unserved when they try to buy.

## High Availability

The cloud is always up and open for work. Providers maintain reliable service by replicating cloud servers in clusters within their data centers. This way, if one server crashes, other servers can pick up the work.

Another way providers ensure reliable **high availability** is to replicate entire data centers in different parts of a geographical region, or even across the globe. This model ensures that a customer's computing services will not be disrupted by natural disasters such as earthquakes, fires, and storms. With global availability, customers can place their services closest to their customers around the world, to reduce access time to web servers and data.

## File Synchronization

Storing, moving, backing up, and updating data can be a huge task for a company's IT department. Cloud providers have designed **file synchronization** services to make replicating on-premises data synching to multiple sites both automated and reliable. AWS DataSync and Microsoft's SQL Data Sync are two examples of this specialized service. These automated services allow companies' IT departments to focus on other tasks.

## On-Demand

**On-demand** is a shortened term for *on-demand self-services*. On-demand self-services from SaaS providers such as Salesforce.com, Gmail, and others are available to customers when they need them but do not need to be maintained by the customer when they are not needed.

## Metered Utilization

Organizations purchase cloud computing services in much the same way as utilities such as gas, water, and electricity. With ***metered utilization***, these services are measured in some way, and the price is based on the amount used. Cloud providers can base prices in different ways for different services. For example, cloud computing services are metered by the minute: The user pays only for the minutes used. Storage services are usually charged by the gigabyte. More complex cloud services, such as replication of servers to be used in different areas, charge by the instance of snapshots or other services.

Of course, cloud providers have many different pricing schedules. Three common ones follow:

- **Pay as you go:** The customer pays only for services used and pays for computing time only when needed. This can be beneficial for new businesses that are unsure of their future computing needs.
- **Bulk purchasing:** This arrangement is similar to pay-as-you-go pricing, but it involves a commitment to use a specific amount over a period of one to three years.
- **Tiered pricing:** The more services are used, the less they cost per unit. For example, the more storage service a company purchases, the less it pays per gigabyte of storage.

Metered cloud services can mean immense savings for customers whose computing needs are periodic or uncertain, and their popularity accounts for much of the growth of cloud services. To save money, many companies are outsourcing their data center tasks to the cloud.



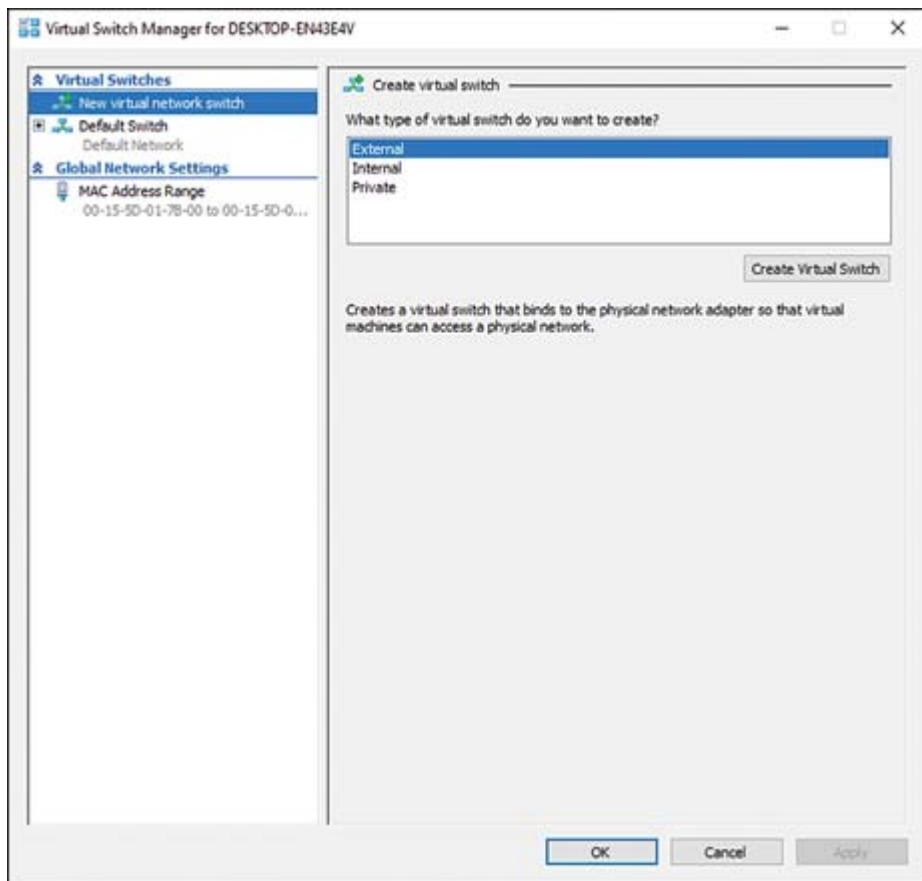
## Desktop Virtualization

**Desktop virtualization** refers to creating a user interface to a computer that is hosted on a central server on-premises or perhaps in the cloud. Either way, the user experience with the virtual desktop is the same. When a company uses a vendor's **virtual desktop infrastructure (VDI)**, users can use minimally powered devices with an Internet connection and work as if processing were happening locally. Basically, VDI allows organizations to offer users remote access to virtual desktop environments from almost any device, such as a smart phone, tablet, or laptop. They can access this through client software installed on their local device or on a web browser.

Desktop virtualization is also known as *thin client networking* because the processing is centralized. Only mouse and keyboard inputs are sent across the local network for on-premises VDI or across the Internet for VDI in the cloud.

When a VM has an operating system installed, it appears and can behave like any other computer on a network. To interact with other machines, it needs to have a virtual network interface card (NIC) installed so that it can have a physical MAC address and an IP address. The virtual NIC behaves almost exactly like a physical NIC, but the administrator can use the virtual machine manager (VMM) to assign a specific MAC address. This is different from physical NICs with MAC addresses that are burned into the hardware by the manufacturer.

If administrators want the VM to communicate with other machines, they can create a path, or bridge, between the virtual NIC and the physical NIC on the VMM hardware. This allows the VM to communicate like any other machine in the LAN. In Hyper-V, this can be done by creating a virtual switch under the Virtual Switch Manager (see [Figure 4-3](#)).



**Figure 4-3** Creating a Virtual Switch in Hyper-V

## Client-Side Virtualization Overview



**220-1101: Objective 4.2:** Summarize aspects of client-side virtualization.



Microsoft (Hyper-V) and third-party vendors, such as Oracle (VirtualBox), VMware (VMware Workstation, VMware Fusion), and Parallels (Parallels Desktop), have offered virtualization solutions for some time. Virtualization enables a single computer to run two or

more operating systems at the same time, using the same hardware resources.

To understand virtualization, make sure you understand these terms:

- **Virtual machine manager (VMM):** A VMM, also called the *hypervisor*, is software that creates and manages virtual machines. It is a specialized operating system that uses minimal hardware resources so that memory and processing are available for the VMs it creates. (Later in this section, you see the differences between a VMM and a hypervisor.)
- **Virtual machine (VM):** A VM is a machine created by a hypervisor/VMM that runs like any other computer. It usually needs an operating system installed on it to become functional. A VM uses the VMM/hypervisor for access to memory, CPU, network, video, and other resources.
- **Emulation:** Emulation involves software-based reproduction of various operating systems, but without the functionality and resource use of virtualization.

When creating a VM, a VMM/hypervisor sets aside memory space that provides access to virtualized storage, ports, video, and other hardware, as well as a hard disk image file known as a virtual hard disk (VHD and the newer VHDX). When the VM is created, the user specifies the type of operating system that will be installed.

After the VM starts, the user can install the operating system from an .iso image file or from physical media. After the operating system is installed, the VM detects and uses the virtualized hardware that the VMM set up.

The VMM/hypervisor can start and stop the VM and modify the virtual hardware that the VM has access to. For example, the VMM can adjust the amount of RAM that the VM uses, change the virtual network adapter that the VM uses, and specify what type of network

access the VM has. If a VM malfunctions, it can be stopped and restarted without affecting the host device.

A computer can run a different operating system in two ways:

- **Virtualization:** In virtualization, the physical resources (for example, RAM, disk space, and CPU cycles) are divided between VMs that can run independently of each other. An operating system is loaded into each VM.
- **Emulation:** In emulation, a full reproduction of a different operating system and different hardware is created by an emulation app, which is then used to run software made for that operating system. Some switch and router emulators have been created to provide training and testing without requiring expensive physical equipment. Other emulators have been created to enable modern PCs to run legacy video games created for systems such as the Atari 2600.

Several categories of virtualization exist: host/guest, hypervisor, server-hosted, and client-side virtualization.

## Host/Guest Virtualization

In host/guest virtualization, a PC or workstation runs a standard operating system and a VMM that runs inside the host operating system; each VM is a guest operating system. Connections to hardware (networking, display, printing, and so on) are passed from the guest operating system, to the virtualization program, to the host computer's operating system.

[Figure 4-4](#) illustrates Oracle VM VirtualBox, a popular free host virtualizer. Other examples include Windows Virtual PC from Microsoft (for Windows 7), Microsoft Hyper-V (for Windows 8 and later), and VMware Workstation Player.



**Figure 4-4** Oracle VM VirtualBox Manager Preparing to Start a VM

This type of virtualization is often used for client-side virtualization. However, client-side virtualization can also be centrally managed from the standpoint of the creation and management of VM images, although the images are being run locally.

## Purpose of Virtual Machines

Software developers use virtual machines to develop applications and operating system enhancements. Three key ways developers use VMs are for sandboxing, test development, and application virtualization.

A common use for VMs is **sandboxing**, creating an isolated machine (or network of machines) where experiments can be run or software can be securely tested without risk to machines on the production network. For example, building and testing a new web server in a sandbox can be helpful so that mistakes happen before customers experience them.

The term *sandboxing* refers to a play area where children freely play with toys and sand inside a safe environment. Sandboxing is also a great way for students to learn new networking skills and try new code in an isolated, nonproduction environment where mistakes won't result in expensive consequences.

**Test development** with virtual machines enables software developers to write and test computer applications. A key step in software development is seeing how code presents itself on a computer. This can involve trying several different scenarios, troubleshooting bugs that arise, and then tweaking the code. With virtual machines, a developer can capture different stages of development in snapshots and then try different tests and tasks to check performance. If the new code doesn't work, they can easily revert to the last snapshot and try something else. Developers can also keep a library of different operating systems in one place, to test performance in different environments.

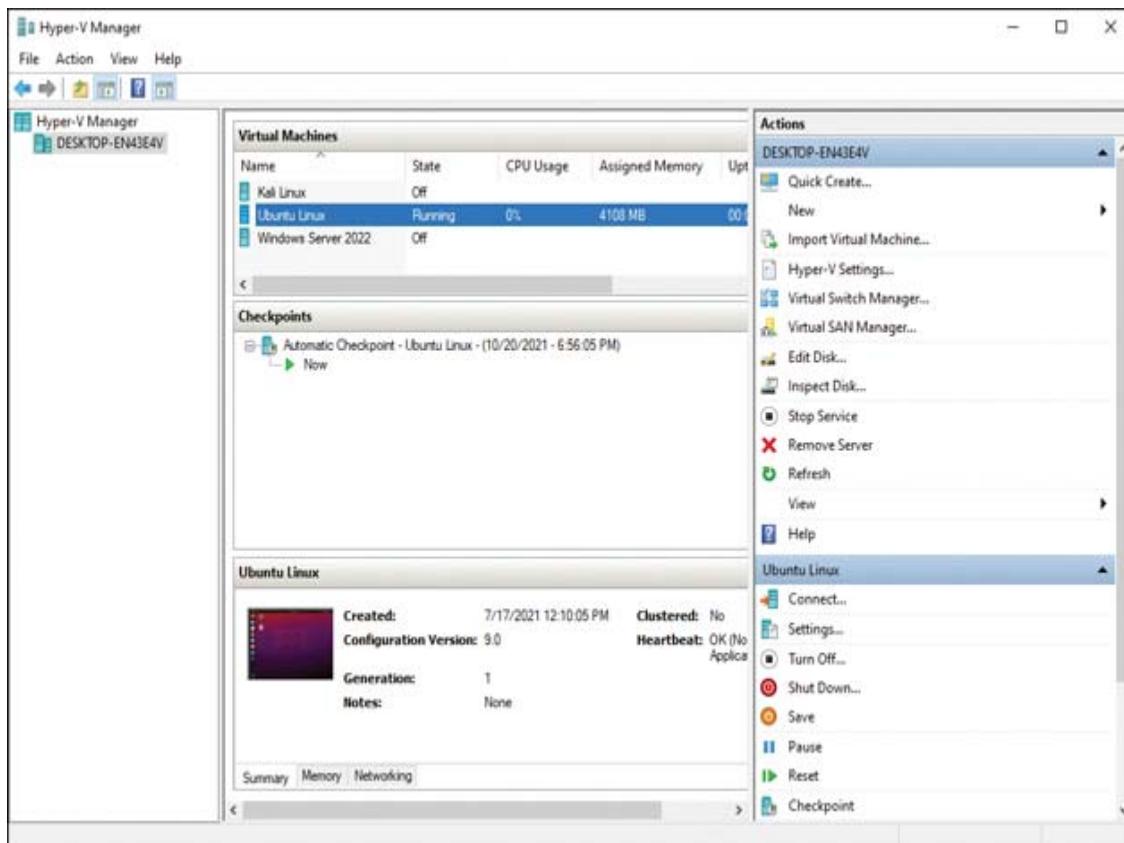
**Application virtualization** is the logical next step from hardware virtualization. Instead of installing applications on office computers, for example, users can install a desktop client that can access and manage application streaming from a company server located in a data center or in the cloud. The desktop client isolates the use of the streaming application from the user's computer and any other applications in use. Basically, application virtualization allows users to access remote applications and use them as if they were installed on their own machine. This makes it easy to manage and maintain applications across an organization and enables different kinds of devices to access the applications, regardless of the device's operating system or storage space.

**Cross-platform virtualization** is a type of application virtualization that can involve different underlying virtualization technologies. For example, the virtual software Microsoft 365 can be run across platforms as well as operating systems, so users on iPads, Linux devices, or macOS can have the same application software experience.

**Legacy software and operating systems** can be used in other types of application virtualization. Support specialists can run several legacy operating systems on one machine without rebooting their systems. These VMs are isolated, or containerized, so that they don't interfere with other machines. Virtual machines even enable a single PC to run both 32-bit and 64-bit versions of the same operating system so that applications that run better in 32-bit mode can be run without the need for a separate computer. For example, in [Figure 4-4](#), a 32-bit version of Windows 8 is virtualized but not currently running in the figure.

The virtual machines on a computer can perform different tasks at the same time, making it possible to do more work with less hardware investment.

[Figure 4-5](#) illustrates the Microsoft Hyper-V Manager after creating a VM running Ubuntu Linux.



## **Figure 4-5** Hyper-V Manager Running Ubuntu Linux

By running virtual machines on servers, fewer physical servers are required to perform the same tasks, which leads to continuing cost savings, easier scaling to suit the workload, and easier disaster recovery.

System images can be centrally created, modified, and managed for easier installation. Because the VMM acts as a translator between the VM and the actual computer hardware, fewer problems arise from differences in system hardware.

## **Resource Requirements**

A workstation that will be used for virtualization needs to be designed with fast multicore processors and as much RAM as possible, given the limitations of the motherboard and VMM (or host operating system). For this reason, the preferred approach is to use 64-bit processors and a 64-bit-compatible VMM (and host operating system, if hosted virtualization is being used instead of a hypervisor). The 64-bit operating systems or VMMs are not subject to the 4GB RAM limit imposed by 32-bit architecture.

Processors selected for a virtualization system should also feature hardware-assisted virtualization. The system BIOS/UEFI firmware must support this feature and be enabled in the system BIOS/UEFI firmware. Otherwise, VMs will run much more slowly, and some VMMs will not be supported.

If several VMs will be run at the same time on a workstation, using two or more displays is highly recommended.

Although a VM is created using an actual operating system instead of a reproduction of one, the physical hardware that will be used for the VMM must meet or exceed the minimum requirements for the VMM. Consider some examples:

- VMware Workstation Player 16 is a simplified version of VMware. It requires a 1.3GHz or faster 64-bit processor, Intel CPU with VT-x support (enabled in BIOS/UEFI firmware) or AMD CPU with AMD-V support, and 2GB minimum (with 4GB or more recommended).
- Hyper-V requires a 64-bit CPU with Data Execution Prevention (DEP) and hardware virtualization (enabled in BIOS/UEFI firmware), second-level address translation (SLAT), and a minimum of 4GB of RAM (with more recommended).

## Note

SLAT (second-level address translation), also known as *nested paging*, reduces the overhead required to map virtual addresses to physical addresses. Reducing overhead makes it possible to run more virtual machines at the same time on a server.

## Security Requirements

Virtual networks require the same attention to security details as physical networks. Because a single physical computer can house two or more VMs, knowing which computers in an organization are using VMs is a vital first step in securing a virtualized environment. The following are some issues to consider:

- **Network traffic monitoring:** When multiple VMs running on a single physical workstation or server communicate with each other, the hypervisor must monitor the traffic unless it is routed to the physical network and then back to the other VM. A feature known as extensible switch modules enables the operating system to monitor network traffic between VMs.
- **VMs backups:** Virtualized storage needs to be backed up with tools made especially for VMs. A VM backup needs to include configuration files and virtual disks to ensure that the VM can

be restored wherever needed. Most VMMs and hypervisors include a feature known as *virtual machine checkpoints* (or virtual machine snapshots). A checkpoint saves the state, data, and hardware configuration of a VM while it is running.

- **Updates and patches:** Updates and patches must be kept current. Additionally, antivirus software must be installed and updated because the host machine cannot scan the VMs for viruses.
- **Security:** A VMM that enables sandboxing (isolation) of each VM and that provides physical partitioning of resources provides better security against attacks.
- **Best security practices for VMMs and VMs:** Operating systems and apps in VMs must be kept up-to-date and need to use firewalls and anti-malware to protect the VM. VMMs also need to be kept up-to-date, and remote administration should be secured by using a VPN. Connections between the VMs, such as clipboards or file sharing, should be limited to only those that are necessary.

## Exam Preparation Tasks

As mentioned in the Introduction, you have several choices for exam preparation: the exercises here; [Chapter 10, “Final Preparation”](#); and the exam simulation questions in the Pearson Test Prep practice test software.

## Review All the Key Topics

Review the most important topics in the chapter, noted with the Key Topic icon in the outer margin of the page. [Table 4-2](#) lists these key topics and the page number on which each is found.



**Table 4-2** Key Topics for Chapter 4

<b>Key Topic Element</b>	<b>Description</b>	<b>Page Number</b>
Section	Common Cloud Models	327
List	General types of cloud computing	329
Section	Shared Resources	330
Section	Desktop Virtualization	333
Section	Client-Side Virtualization Overview	334

## Define Key Terms

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

IaaS

SaaS

PaaS

public cloud computing

private cloud computing

hybrid cloud computing

community cloud computing

shared resources

metered utilization

rapid elasticity

high availability

file synchronization

on-demand

desktop virtualization

virtual desktop infrastructure (VDI)  
sandboxing  
test development  
application virtualization  
cross-platform virtualization  
legacy software and operating systems

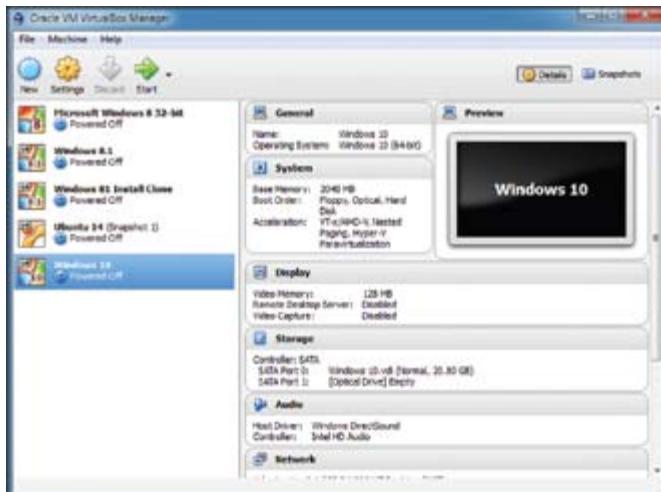
## Answer Review Questions

- 1.** Match each of the following cloud-based models to its description.

Model	Description
a. SaaS	
b. IaaS	
c. PaaS	

- 1.** Provides access to storage, network services, virtualization, and servers
- 2.** Gives application developers the opportunity to develop and deploy software in a cloud environment
- 3.** Enables software to be hosted on remote servers and accessed through web browsers
- 2.** Which of the following are characteristics of a virtual machine? (Choose all that apply.)
- a. A user can access multiple guest operating systems without rebooting.
  - b. 32-bit and 64-bit operating systems can be installed on different virtual machines on a single host machine.
  - c. Multiple virtual machines use the same hardware as the host computer.

- d. Running multiple guest operating systems is more expensive than running those same operating systems as host systems.
- 3.** Which of the following are advantages of cloud computing?  
(Choose all that apply.)
- a. Rapid elasticity
  - b. DHCP services
  - c. Resource pooling
  - d. Metered service
- 4.** What is the name of the program that acts as the translator between the host machine and its virtual machines?
- a. Virtual machine server
  - b. Virtualization machine manager
  - c. Virtual host manager
  - d. Virtualized guest server
- 5.** The Windows 10 VM is selected in the following figure.  
Assuming that the host system has 8GB (8,192MB) of RAM, can you determine how much RAM will be available to the host system when the Windows 10 VM is running?



- a. 8192MB
  - b. 2048MB
  - c. 6144MB
  - d. Impossible to determine from the image
- 6.** Which of the following best describes sandboxing as it relates to a virtual machine?
  - a. It is a type of hybrid cloud computing.
  - b. It is a type of firewall between the host server and the outside world.
  - c. It is a backup for virtual machines.
  - d. It is the isolation of VMs within the host system for better security.
- 7.** A VMM that runs directly on the hardware instead of inside the operating system is known as which of the following?
  - a. Hypervisor
  - b. Thin-client virtualization
  - c. Client-side host/guest virtualization
  - d. DEP (Data Execution Prevention)
- 8.** Which of the following refers to creating a user interface to a computer that is hosted on a central server on-premises or in the cloud?
  - a. Community cloud
  - b. File synchronization
  - c. Desktop virtualization
  - d. VM checkpoint
- 9.** The virtual software Microsoft 365 is running across platforms as well as operating systems, so users in the company on iPads, Linux devices, and macOS can have the same application software experience. What is this an example of?

- a.** Virtual machine management
  - b.** Supporting legacy software and operating systems
  - c.** On-demand self-service
  - d.** Cross-platform virtualization
- 10.** A technician is setting up a workstation that will be used for virtualization. Which of the following should the technician ensure? (Choose three.)
- a.** The system has as much RAM as possible.
  - b.** The BIOS/UEFI supports hardware-assisted virtualization.
  - c.** The VMM runs inside the guest operating system.
  - d.** Virtualization support must be enabled in the BIOS/UEFI.

# Chapter 5

## Hardware and Network Troubleshooting

This chapter covers the seven A+ 220-1101 exam objectives related to best practice troubleshooting methodology; troubleshooting common problems with motherboards, RAM, CPUs, and power; troubleshooting storage drives and RAID arrays; troubleshooting video, projector, and display issues; troubleshooting common mobile device issues; troubleshooting and resolving printer issues; and troubleshooting wired and wireless network problems. This exam domain may comprise 29 percent of the exam questions and consists of the following specific objectives:

- **Core 1 (220-1101): Objective 5.1:** Given a scenario, apply the best practice methodology to resolve problems.
- **Core 1 (220-1101): Objective 5.2:** Given a scenario, troubleshoot common problems related to motherboards, RAM, CPU, and power.
- **Core 1 (220-1101): Objective 5.3:** Given a scenario, troubleshoot and diagnose problems with storage drives and RAID arrays.
- **Core 1 (220-1101): Objective 5.4:** Given a scenario, troubleshoot video, projector, and display issues.
- **Core 1 (220-1101): Objective 5.5:** Given a scenario, troubleshoot common issues with mobile devices.

- **Core 1 (220-1101): Objective 5.6:** Given a scenario, troubleshoot and resolve printer issues.
- **Core 1 (220-1101): Objective 5.7:** Given a scenario, troubleshoot problems with wired and wireless networks.

Chapter 3, “Hardware,” introduced hardware components that make up computers, printers, networks, and mobile devices. In this chapter, you learn specific troubleshooting methods for these devices, as well as the networks they might inhabit.

## “Do I Know This Already?” Quiz

The “Do I Know This Already?” quiz allows you to assess whether you need to read the entire chapter. [Table 5-1](#) lists both the major headings in this chapter and the “Do I Know This Already?” quiz questions covering the material in those headings so that you can assess your knowledge of these specific areas. The answers to the “Do I Know This Already?” quiz appear in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes and Review Questions.”

**Table 5-1** “Do I Know This Already?” Foundation Topics Section-to-Question Mapping

Foundations Topics Section	Questions
Troubleshooting Methodology	1, 2
Troubleshooting Motherboard, RAM, CPU, and Power Issues	3–9
Troubleshooting Storage Drives and RAID Arrays	10–13
Troubleshooting Video, Projector, and Display Issues	14, 15
Mobile Device Troubleshooting	16–19
Printer Troubleshooting	20
Network Troubleshooting	21–23

## **CAUTION**

The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for the purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

- 1.** Which of the following is not one of the six steps of the CompTIA troubleshooting theory?
  - a.** Establish a theory of probable cause.
  - b.** Check all cables and link lights.
  - c.** Document findings, actions, and outcomes.
  - d.** Test the theory to determine the cause.
- 2.** At which step in the troubleshooting methodology might system logs be most helpful to a technician?
  - a.** Step 1
  - b.** Step 3
  - c.** Step 5
  - d.** Step 6
- 3.** Which is not a system error commonly identified by beep codes?
  - a.** Memory
  - b.** Processor or motherboard
  - c.** Video
  - d.** Overclocking
- 4.** When a computer boots and then displays the incorrect time or date, what are possible causes? (Choose two.)

- a. The CPU is overclocked.
  - b. The CMOS chip is bad.
  - c. The battery is depleted.
  - d. The BIOS/UEFI license has expired.
- 5. You touch the power supply inside the computer, and it is too hot to hold. Before you removed the cover at the workstation, you observed that the user's cubicle is more cluttered than most. You observed the following four issues. Which of them may be responsible for the hot power supply? (Choose two.)
  - a. Drinks and food are spread around and left open on the tower next to the desk.
  - b. A sweater is hanging down from a hook behind the tower.
  - c. Cables are pulled tight from repositioning the monitor.
  - d. Crumbs are on the floor and are mixing with dust bunnies.
- 6. Which of the following might a BSOD indicate? (Choose two.)
  - a. Network cables not properly connected during boot
  - b. Registry errors
  - c. OS license expired
  - d. Defective hardware
- 7. What can be done to isolate the cause of a BSOD? (Choose two.)
  - a. Wait 20 seconds and try again.
  - b. Remove a newly added component.
  - c. Note the error code and research it online.
  - d. Unplug the power for 1 minute.
- 8. You have a client running Microsoft Word on macOS. When he tried to print, a spinning pinwheel stopped everything. Choose a likely cause and a likely quick remedy from the following options.
  - a. Caused by printer failure; reboot the printer

- b.** Microsoft Word out-of-date; reboot and update the version
  - c.** RAM not available to process application demand; force quit the application and reopen it after closing unused applications
  - d.** System crash; unplug and remove the battery for 2 minutes, to allow data to reset
- 9.** If a device is plugged into an adapter and has no power, which is a possible step to take to alleviate the problem?
  - a.** Ensure that the adapter is set to the proper DC voltage.
  - b.** Make sure the AC outlet is working.
  - c.** Use a multimeter to test DC voltage from the adapter.
  - d.** All of these steps are correct.
- 10.** If you have determined that you need to upgrade a PC by replacing a SATA HDD with an SSD, which form factor is not a feasible replacement?
  - a.** mSATA SSD
  - b.** SATA HDD
  - c.** PCIe card
  - d.** m.2 SSD
- 11.** Which of the following is not monitored by S.M.A.R.T.?
  - a.** Slow spin-up
  - b.** Drive temperature
  - c.** Printer retry errors
  - d.** Bad sectors
- 12.** Which command can be used to find errors on a hard drive?
  - a.** dskerr
  - b.** diskpart
  - c.** chkdsk
  - d.** errdsk

**13.** You are working on a hard drive that is nearly full, and you suspect that files are stored in fragments around the hard drive. Which one of the following can help you determine whether defragmentation is a plausible solution for this client?

- a.** Use the Disk Storage Update tool.
- b.** Run defrag at the command prompt.
- c.** Run chkdsk.
- d.** Click the Analyze button in the disk optimization window.

**14.** You are asked to assist with a projector in a conference room. The presenter is having trouble getting the computer image to show on the screen. Which of the following is not a commonly known issue with projection?

- a.** The device has overheated.
- b.** The screen was set up too far from the projector.
- c.** The lens cap was not removed.
- d.** The source setting on the projector is faulty.

**15.** You have been asked to help stream a conference from a laptop to a new 55-inch television in a conference room. The laptop has an Ethernet port and a USB port. What kind of adapter and cable are most likely required to complete the task?

- a.** An Ethernet adapter and satellite cable
- b.** High-Definition Multimedia Interface and USB adapter
- c.** Splitter and DSL cable
- d.** VGA cable and USB adapter

**16.** You find your phone under a jacket placed near a heater. The phone is very warm and hard to hold. What is the first thing you should do?

- a.** Remove the phone cover and put it in ice.
- b.** Close the browser and disconnect the Wi-Fi.
- c.** Power off the phone and remove the cover.

- d. Plug in a charger so the fan will run.
- 17.** A friend can no longer connect to wireless headphones via Bluetooth. What is an appropriate step to try?
  - a. Change Wi-Fi networks.
  - b. Close the music app and restart.
  - c. Connect the charger cable.
  - d. “Forget” the device in Bluetooth.
- 18.** You located a bulge in a tablet where the screen is pulling away from the back. What steps might fix this?
  - a. With a thin screwdriver, pry off the back and reset it.
  - b. Power off the device and put it under heavy books to flatten the bulge.
  - c. Power off the device and let it cool; the bulge is likely caused by heat and will shrink when cooled.
  - d. There are no steps to fix this. Check the warranty status and make arrangements for a new device.
- 19.** Which OS is run on an iPad?
  - a. macOS
  - b. Linux
  - c. iPadOS
  - d. iOS
- 20.** You have been called to check on a printer in an office. You find a paper jam and fix it. Where do you look to resume the printing process and print jobs that were unable to print?
  - a. The sending workstation’s RAM
  - b. The print queue
  - c. The printer’s hard drive
  - d. The printer’s virtual memory

- 21.** What can be the result of EMI and/or RFI on a network segment? (Choose two.)
- a. Slow file transfer speeds
  - b. IP address conflicts
  - c. Intermittent connectivity
  - d. Slowing fiber optic transmission
- 22.** You have been called to an office where the local network and Internet do not work, but the computer is running. You notice that the office is being rearranged to accommodate people, and a desk has been moved so that another desk can be added in the future. What is a likely culprit for the problem?
- a. Adding the second user compromised the network security.
  - b. The cable was damaged in the move.
  - c. The user timed out while moving items and the user is locked out.
  - d. The Bluetooth became disconnected.
- 23.** The workstation near the break room has occasional reductions in Wi-Fi network speeds that last 2 or 3 minutes several times a day. What could be the problem?
- a. Users coming in and out of the break room bring their phones and clog the network.
  - b. The coffee pot draws too much electricity when brewing.
  - c. Complementary microwaveable popcorn bags are available on the counter.
  - d. The LED lights are motion sensitive and drain power when they are turned on.

## Foundation Topics

# Troubleshooting Methodology

220-1101  
Exam

**220-1101 Objective 5.1:** Given a scenario, apply the best practice methodology to resolve problems.

The term *methodology* often confuses people. In the IT world, it means a collection of systematic approaches to solving technical problems. Because computers and mobile devices are complex, any given problem could have multiple symptoms and several possible causes. To solve computer and mobile device problems, technicians need a proven and effective troubleshooting approach. CompTIA has traditionally defined a basic six-step theory as a best practice approach. As [Table 5-2](#) indicates, the steps help you find the source of a problem, find the solution, and prevent recurrences.

Key Topic

**Table 5-2** The Six-Step CompTIA Troubleshooting Methodology

---

## Step Description

---

Step Identify the problem.

1

- Question the user and identify user changes to the computer. If applicable, perform backups before making further changes.
- Inquire about environmental or infrastructure changes that might have occurred.
- Review system application logs for clues to possible system errors.

---

Step Establish a theory of probable cause (question the 2 obvious).

---

## **Step Description**

If necessary, conduct external or internal research based on symptoms.

---

Step Test the theory to determine the cause.

3

- When the theory is confirmed, determine the next steps to resolve the problem.
  - If the theory is not confirmed, re-establish a new theory or escalate the issue.
- 

Step Establish a plan of action to resolve the problem and

4 implement the solution.

- Refer to the vendor's instructions for guidance.
- 

Step Verify full system functionality and, if applicable,

5 implement preventive measures.

---

Step Document the findings, actions, and outcomes.

6

---

### **Note**

Always consider corporate policies, procedures, and impacts before implementing changes.

As you attempt to troubleshoot computer issues, think in terms of this six-step process. Plug the problem directly into these steps. If you test a theory in step 3 and that the theory is disproven, return to step 2 and develop another theory. Continue in this manner until you have found a theory that points to the problem. After you solve the problem and verify functionality (steps 4 and 5), be sure to document what happened (step 6) so that you or another technician can more quickly solve a similar problem in the future.

This sample scenario involves following the previously outlined steps.

You take a call from a coworker who is unable to access an Adobe application needed to edit documents. A support ticket is opened and you begin the troubleshooting process.

- 1.** You ask a few questions to clarify the problem and are able to determine that the user was able to use the application earlier in the day at home. The problem started after they returned home from a work meeting at a local coffee shop. Their access to the application was denied. Further questions help you understand that the user took their company laptop to the coffee shop and did a little work on the public network while waiting for the meeting to start.
- 2.** You are aware that the Adobe application has a limited user license on the network and that the user must be on the company network or attached via a VPN to authenticate for the license. You suspect that changing from a VPN connection, to the corporate network, to a public network at the coffee shop was part of the problem.
- 3.** You ask the user if they checked the VPN status since joining the public network at the coffee shop. They are unsure, so they check the VPN app to check the status. They are not connected.
- 4.** You have the user log back on to the VPN and try to access the licensed application.
- 5.** Success! The user can use the application and return to work.
- 6.** You advise the user that leaving their home network and then using the public network likely disconnected them from the VPN. You caution that public networks can also cause security issues and advise them that, if possible, they should keep the company laptop off public networks. You document the conversation on the help ticket, and the task is complete.

# Troubleshooting Motherboard, RAM, CPU, and Power Issues

220-1101  
Exam

**220-1101: Objective 5.2:** Given a scenario, troubleshoot common problems related to motherboards, RAM, CPUs, and power.

Many system problems are caused by bad motherboards, RAM, CPUs, and power. In the following sections, you learn about common symptoms for these problems and the most likely causes. Use this information as you track down real-life issues in your company's systems and your clients' systems.

## POST Code Beeps

The **Power-On Self-Test (POST) code beeps** are used by many BIOS versions to indicate either fatal or serious errors. Beep codes vary by the BIOS maker. Although some vendors create their own BIOS chips and firmware, most major brands of computers and virtually all "clones" use a BIOS made by one of the following vendors: American Megatrends (AMI), Phoenix Technologies, IBM, Award Software (now owned by Phoenix Technologies), or Insyde Software.

As you might expect, the beep codes and philosophies used by these companies vary a great deal. For example, AMI uses beep codes for more than 10 fatal errors. It also uses 8 beeps to indicate a defective or missing video card. Phoenix uses beep codes for both defects and normal procedures (but has no beep code for a video problem), and the Award BIOS has only a single beep code (1 long, 2 short), indicating a problem with video. Insyde BIOS uses beep codes for errors, but these codes vary widely from model to model.

### Note

Some vendors have switched from beep codes to blink codes with the advent of UEFI BIOS firmware. Check the documentation for the system or motherboard to determine whether beep, blink, or other reporting methods are used to indicate POST problems.

Because beep codes do not report all possible problems during the startup process, you cannot rely exclusively on beep codes to help you detect and solve system problems. In addition, beep codes can be heard only on systems with built-in speakers.

## TIP

To add a wired speaker to a desktop computer, plug it into the speaker jack in the front-panel header pins.

Table 5-3 lists the most common beep codes you're likely to encounter.



**Table 5-3** Common System Errors and Their Beep Codes

Problem	Phoenix BIOS	Award BIOS	AMI BIOS	IBM BIOS
Memory	Beep sequences: 1-3-4-1 1-3-4-3 1-4-1-1	Beeping (other than 2 long, 1 short)	1 or 3 or 11 beeps	(None) 1 long, 3 short beeps
Video	(None)	2 long, 1 short beep	8 beeps 1 long, short 8 short	1 long, 3

<b>Problem</b>	<b>Phoenix BIOS</b>	<b>Award BIOS</b>	<b>AMI BIOS</b>	<b>IBM BIOS</b>
			beeps	beeps, or 1 beep
Processor or motherboard	Beep sequence: 1-2-2-3	High-frequency beeps  Repeating high/low beeps	5 beeps or 9 beeps	1 long, 1 short beep

For additional beep codes and other BIOS support, see the following manufacturer resources:

- **AMI BIOS:** <https://ami.com>
- **Phoenix BIOS:** [www.phoenix.com](http://www.phoenix.com)
- **IBM, Dell, Acer, and other brands:** [www.bioscentral.com](http://www.bioscentral.com) and [www.wimsbios.com](http://www.wimsbios.com)

## Note

Don't mix up your boops and beeps! Many systems play a single short boop (usually a bit different in tone than a beep) when the system boots successfully. This is normal.

## POST Error Messages

Most BIOS versions do an excellent job of displaying POST error messages indicating the problem with the system. These messages can indicate problems with memory, keyboards, hard drives, and other components. For example, if the CMOS memory used to store system setup information is corrupt (possibly because of a battery

failure or because the CMOS memory has been cleared), systems display a message such as the following:

- **System CMOS Checksum Bad—Run Setup:** Phoenix BIOS
- **CMOS Checksum Invalid:** AMI BIOS
- **CMOS CHECKSUM INVALID—RUN SCU:** Insyde BIOS
- **CMOS Checksum Error—Defaults Loaded:** Award BIOS

Some systems document these messages in their manuals, or you can go to the BIOS vendors' websites or the third-party sites listed earlier in this chapter for more information.

## Note

Keep in mind that the system almost always stops after the first error, so if a system has more than one serious or fatal error, the first problem might stop the boot process before the video card has been initialized, to display error messages.

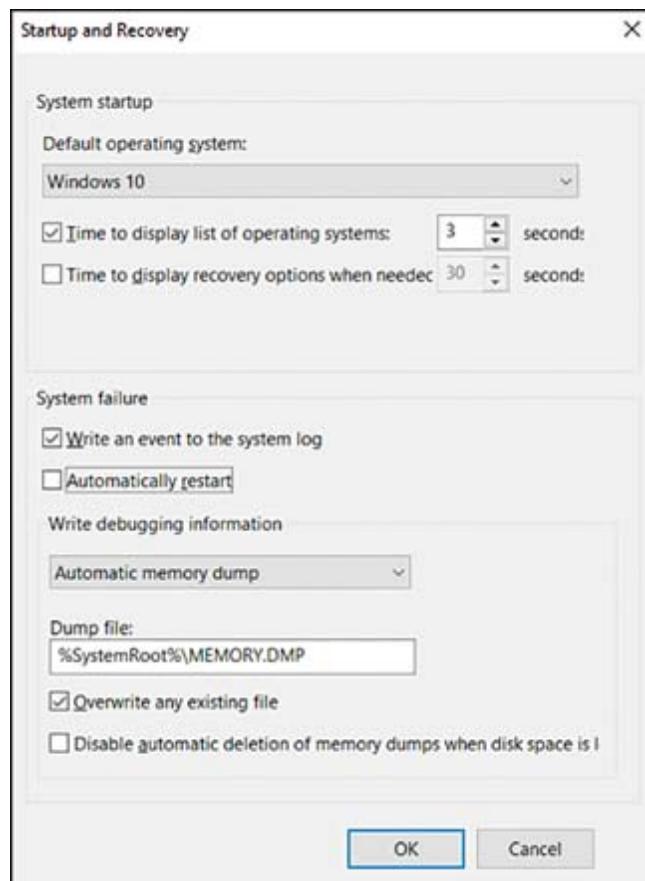
## Proprietary Crash Screens (BSOD/Pinwheel)

Proprietary crash screens such as the Windows STOP error (blue screen of death [BSOD]) or the macOS pinwheel can be caused by operating system, application, or hardware errors.

## BSOD Errors

If Windows is configured to reboot when a STOP error occurs, the system continuously reboots until the error is resolved. To leave a STOP error message onscreen until you decide to restart the system, clear the Automatically Restart check box in the System Failure setting in the Startup and Recovery section of Advanced System Properties (see [Figure 5-1](#)). This is accessed via **Control Panel >**

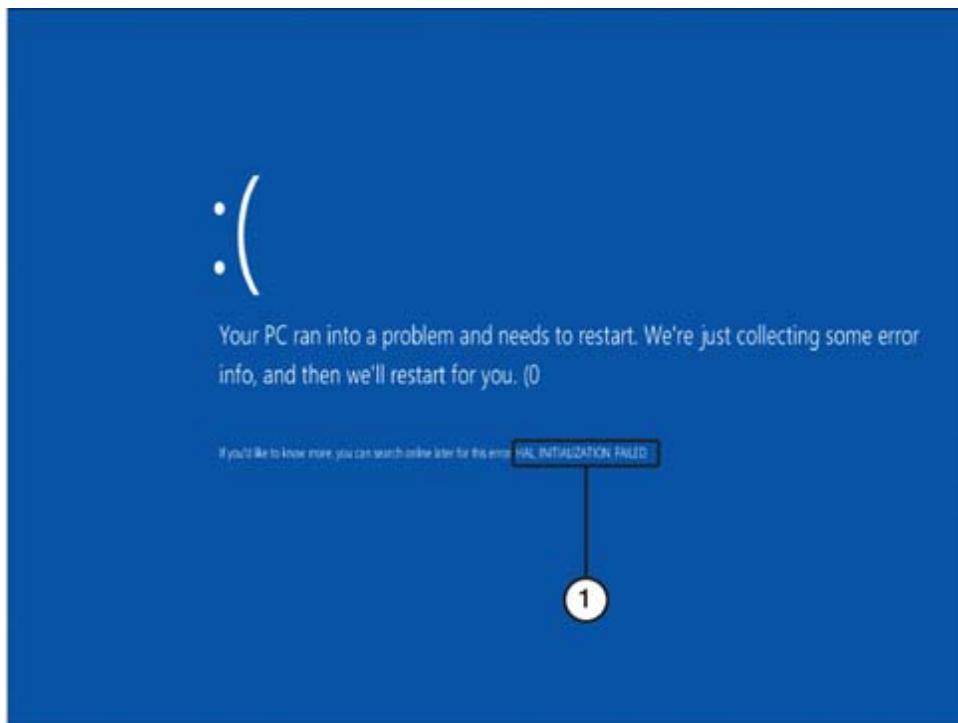
**System > Advanced System Settings.** Under Startup and Recovery, select Settings.



**Figure 5-1** Startup and Recovery Options. Note That the Option to Automatically Restart Box Under System Failure Has Been Unchecked.

## Troubleshooting Windows STOP Errors (BSOD)

STOP errors (also known as **blue screen of death**, or **BSOD**, errors) can occur either during startup or after a system is running. The BSOD nickname is used because the background is normally blue (or sometimes black), with the error message in white text. Figure 5-2 depicts the Windows 10 STOP errors.



1. STOP error message

**Figure 5-2** A Windows 10 STOP Error

## Note

Regardless of when a STOP/BSOD error occurs, the system is halted by default. If the computer does not restart on its own, you must turn off the system and turn it back on. Before you do that, however, record the error message text and other information so that you can research the problem if it reoccurs. For more information, see the next section, “Causes of BSOD Errors.”

## Causes of BSOD Errors

BSOD errors can be caused by any of the following:

Key  
Topic

- **Incompatible or defective hardware or software:** Start the system in Windows Recovery Environment (winRE) and uninstall the last hardware or software installed. Acquire updates before you reinstall the hardware or software. Exchange or test memory. Run **SFC /scannow** from Admin mode in Powershell to check for problems with system files. To enter winRE, reboot and hold the F11 key. If this doesn't work, try a hard start by rebooting the computer three times, by holding down the power button for 10 seconds. It should open in winRE.
- **Registry problems:** System Restore, found in winRE, can also be used to revert the system and Registry to an earlier state.
- **Viruses/malware:** Scan for viruses and remove any that are discovered.
- **Miscellaneous causes:** Check the Windows Event Viewer and also check the system log. Research the BSOD with the Microsoft Support website.

## Researching BSOD Causes and Solutions

To determine the exact cause of a STOP error, note the number or name of the error (for example, STOP 0x0000007B, HAL INITIALIZATION FAILED) and look it up on the Microsoft support website: <http://support.microsoft.com>. When you search for the error, be sure to specify the version of Windows in use.

### Note

STOP errors are often referred to with a shortened version of the error code or by name. For example, the shortened version of a 0x0000007B error is 0x7B.

## TIP

Unfortunately, you can't take a screen capture of a BSOD for printing because a BSOD completely shuts down Windows. In this situation, you can use a digital camera or smartphone to record the exact error message.

The solution might involve one or more of the following changes to your system:



- Changing the system Registry. Sometimes you can download an automated Registry repair tool to perform these changes for you. Whether you make the changes manually or automatically, back up the registry first.
- Removing a newly added component. For example, in the error in [Figure 5-1](#), removing a recently added memory module solved the problem.
- Replacing components such as memory.
- Upgrading an application.
- Downloading and installing a hotfix for your operating system.

On some systems, auto restart is enabled for STOP/BSOD errors, so the error messages shown in [Figures 5-1](#) and [5-2](#) appear for only a moment before the computer restarts.

## Note

Microsoft Windows 10 has a tool called Windows Troubleshooter that is available to help resolve Windows problems. Each Windows version provides slightly different access to Troubleshooter. In

Windows 10, go to **Settings > Update and Security > Troubleshoot**.

## macOS Pinwheel

The official name for the macOS **pinwheel** is the *spinning wait cursor* (see [Figure 5-3](#)).



1. macOS spinning wait cursor (pin wheel)

**Figure 5-3** The Pinwheel in macOS

The pinwheel appears most often when an application or macOS itself has become unresponsive. For this reason, it is sometimes referred to as the “pinwheel of death.” It is usually caused by an application failing, but it can also indicate that the system is locked up and needs a hard reboot. If the problem is an application failure, it can usually be resolved by force-quitting the application (see the solutions in the list that follows).

You might also hear the spinning pinwheel referred to as the “spinning rainbow” or “beachball of death.”

The following are some causes of macOS unresponsiveness:



- **Lack of system RAM:** If a macOS device frequently displays the pinwheel and the device's RAM can be upgraded, do so.
- **Less than 10 percent free space on the macOS system drive:** Free space is used as a swapfile to substitute for RAM. Remove unwanted apps and save data to external or cloud storage, to free up space. Some experts recommend keeping at least 20 percent of the macOS system drive free.
- **Damaged application:** It is generally quicker to redownload the app, making sure it is from a trusted source. If the system files are not current, they should be updated and the computer should be rebooted before the reinstall.

The following are some solutions for macOS unresponsiveness:

- Use the Force Quit command to terminate an application that will not respond. Force Quit is available from the Apple menu or by pressing Cmd+Option+Esc. Select the app and click Force Quit.
- If a particular application causes unresponsiveness, open the ~Library/Preferences folder, find the .plist file for the app, and drag it to the trash. The .plist file then is rebuilt.
- Use Activity Monitor to view CPU, memory, energy, disk, and networking performance stats. Activity Monitor is similar to the Windows Task Manager. You can use the Spotlight feature on a Mac to locate Activity Monitor in the Applications folder.
- Upgrade to the latest macOS version and keep it updated.
- A forced restart is performed by pressing and holding the Cmd+Ctrl buttons while pressing the power button. Press Cmd+Ctrl+Eject to quit all apps and restart.

## Black Screen

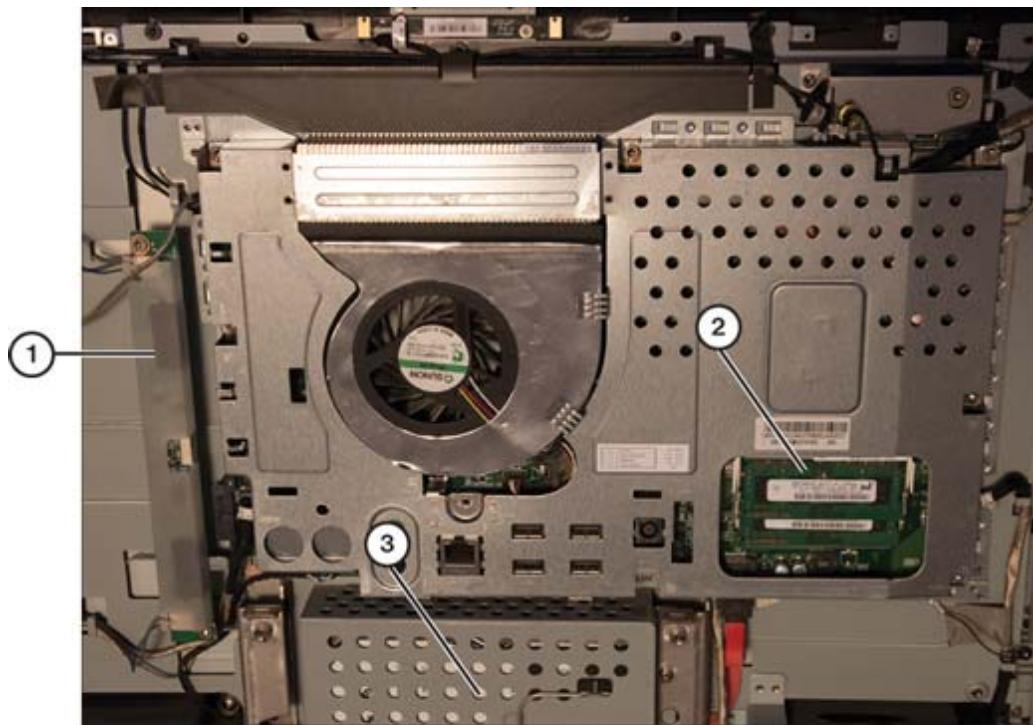
A **black screen** on bootup can be caused by a variety of video configurations or cabling problems. Some of these can be caused by motherboard issues, or the problem might involve more complex display, monitor, or graphics driver errors. Follow these steps to troubleshoot:



- If you have only one display, plugging the video cable into an inactive video port on a system causes a blank screen. For example, some systems deactivate onboard video when you install a video card. If onboard video offers DVI and HDMI ports, typically only one can be selected (usually with motherboard jumpers).
- If a display with two or more inputs (for example, DVI and HDMI or DVI and VGA) is not configured to use the correct cable, the display will be blank. Use the display's pushbutton controls to select the correct signal input.
- If a DVI or VGA cable is not tightly attached to the video port or display, the screen might be blank. Secure the cable.
- If an HDMI, miniHDMI, DisplayPort, or miniDisplayPort cable is not completely plugged into the video port or display, the screen might be blank. Completely insert the cable into the port.
- If input cables and display input settings check out, but the screen is still blank, shine a flashlight on the screen to see if any text or graphics is visible. If you can see text or graphics with the flashlight, the backlight on the display has failed. On an LCD-CCFL, check the inverter first. Inverter failures are much more common than backlight failures, and inverters are relatively easy to replace. On an LED display, check the LED driver board first. Keep in mind that LCD and LED display modules for laptops or complete displays for desktops are far

less expensive today than they used to be; it might make sense to replace the entire display assembly.

[Figure 5-4](#) shows a typical inverter for an LCD-CCFL display in an all-in-one computer.



1. LCD-CCFL inverter
2. SODIMM memory modules
3. 2.5-inch hard disk in removable drive cage

**Figure 5-4** An All-in-One Computer with the Back Open for Servicing

If the cables are okay and the issue is not resolved, removing the drivers and letting Windows 10 automatically reinstall them can fix the issue. The following steps first remove the display and monitor drivers, which Windows can easily reinstall with a restart. If that does not resolve the issue, uninstalling and replacing the graphics driver could be necessary.

This needs to be done from Safe Mode. To enter Safe Mode in Windows 10, start in the Windows Recovery Environment (winRE) and uninstall the drivers. Then follow these steps:

- Step 1.** Check the video cable on the PC.
- Step 2.** Reboot and hold the F11 key to access winRE. (If this doesn't work, try a hard start by rebooting the computer three times, by holding down the power button for 10 seconds. Then it should open in winRE.)
- Step 3.** In winRE, **select See Advanced Options.**
- Step 4.** From the Advanced Options menu, select **Troubleshoot**.
- Step 5.** From the Troubleshoot menu, select **Advanced Options** and then **Startup Settings** (you might need to select **See More Options** to see Startup settings). Then choose **Restart** and select item 4, **Enable Safe Mode**.
- Step 6.** In Safe Mode, press Windows+R to open the Run dialog box.
- Step 7.** Open the Device Manager by typing **devmgmt.msc** and click **OK**.
- Step 8.** Locate Display Adaptors in the list and display the installed adapters by selecting the drop arrow.
- Step 9.** Right-click the driver and select **Uninstall Device**. Selecting **Uninstall Windows** reinstalls fresh drivers on the next boot.
- Step 10.** Locate the monitor driver and uninstall it as in step 9.
- Step 11.** Go to the Windows menu and restart. This reboots into normal mode. If the screen works, the problem is solved. If not, repeat the process, removing and reinstalling the graphics driver.

## Note

Entering Safe Mode varies by system. Consult your systems manufacturer's documentation if the preceding procedure does not work.

## No Power

No power when you turn on the system can be caused by several issues.

- **Power supply failure:** A power supply that has stopped working prevents the system from starting. Use a multimeter or a power supply tester to determine whether a power supply has failed.
- **Incorrect front panel wiring connections to the motherboard:** The power switch is wired to the motherboard, which, in turn, signals the power supply to start. If the power lead is plugged into the wrong pins on the motherboard or has been disconnected from the motherboard, the system will not start and you will not see an error message. Check the markings on the front panel connectors, the motherboard, or the motherboard/system manual to determine the correct pinouts and installation.
- **Loose or missing power leads from the power supply:** Make sure both the ATX and ATX12V or EPS12V power leads from the power supply are connected firmly to the motherboard. The connectors lock into place.
- **Surge suppressor or UPS failure:** If the surge suppressor or uninterruptible power supply (UPS) unit connected to the computer has failed, the computer cannot start. Replace the defective surge suppressor or UPS unit, or replace the battery in the UPS unit.

## Overheating

If you touch the power supply case and it feels too hot to touch, it is overheated. Overheated power supplies can cause system failure and possible component damage. They can result from any of the following causes:



- Overloading
- Fan failure
- Inadequate airflow outside the system
- Inadequate airflow inside the system
- Dirt and dust

Use the following sections to figure out the possible effects of these problems in any given situation.

## **Overloading**

An overloaded power supply is caused by connecting devices that draw more power (in Watts) than the power supply is designed to handle. Consider upgrading the hard drive when you add more card-based devices to expansion slots, use more bus-powered USB and Thunderbolt devices, and install more internal drives in a system. This reduces the odds of having an overloaded power supply, which can cause various performance problems.

If a power supply fails or overheats, check the causes listed in the following sections before you consider replacing the power supply. If you determine that you do need to replace the power supply, purchase a unit that has a higher wattage rating and a higher +12V rating.

## **Fan Failure**

The fan or fans inside the power supply cool it and are partly responsible for cooling the rest of the computer. If fans fail, the power supply and the entire computer are at risk of damage. Fans also might stop turning as a symptom of other power problems.

A fan that stops immediately after the power comes on usually indicates incorrect input voltage or a short circuit. If you turn off the system and turn it back on again under these conditions, the fan will stop each time.

To determine whether a fan has failed, listen to the unit; it should make less noise if the fan has failed. You can also see the fan blades spinning rapidly on a power supply fan that is working correctly. If the blades are not turning or are turning very slowly, the fan has failed or is too clogged with dust to operate correctly.

To determine whether case fans have failed, look at them through the front or rear of the system—or, if they are connected to the motherboard, use the system monitoring feature in the system BIOS/UEFI to check fan speed. [Figure 5-5](#) illustrates a typical example.

PC Health Status	
Chassis Intrusion	Disabled
CPU Fan Detection	Enabled
CPU Temperature	49°C/120°F
System Temperature	35°C/95°F
CPU Fan Speed	5000 RPM
System Fan Speed	0 RPM
Vcore	1.744 V
+ 5.0V	5.030 V
+12.0V	12.288 V
-12.0V	-12.564 V
- 5.0V	-5.127 V
Battery	3.408 V
+5V SB	4.993 V

**Figure 5-5** The System Fan (Case Fan) Either Has Failed Or Was Never Connected to the Motherboard Power/Monitor Header

### Note

If a fan has failed because of a short circuit or incorrect input voltage, you will not see any picture onscreen because the system cannot operate.

If the system starts normally but the fan stops turning later, this indicates a true fan failure instead of a power problem.

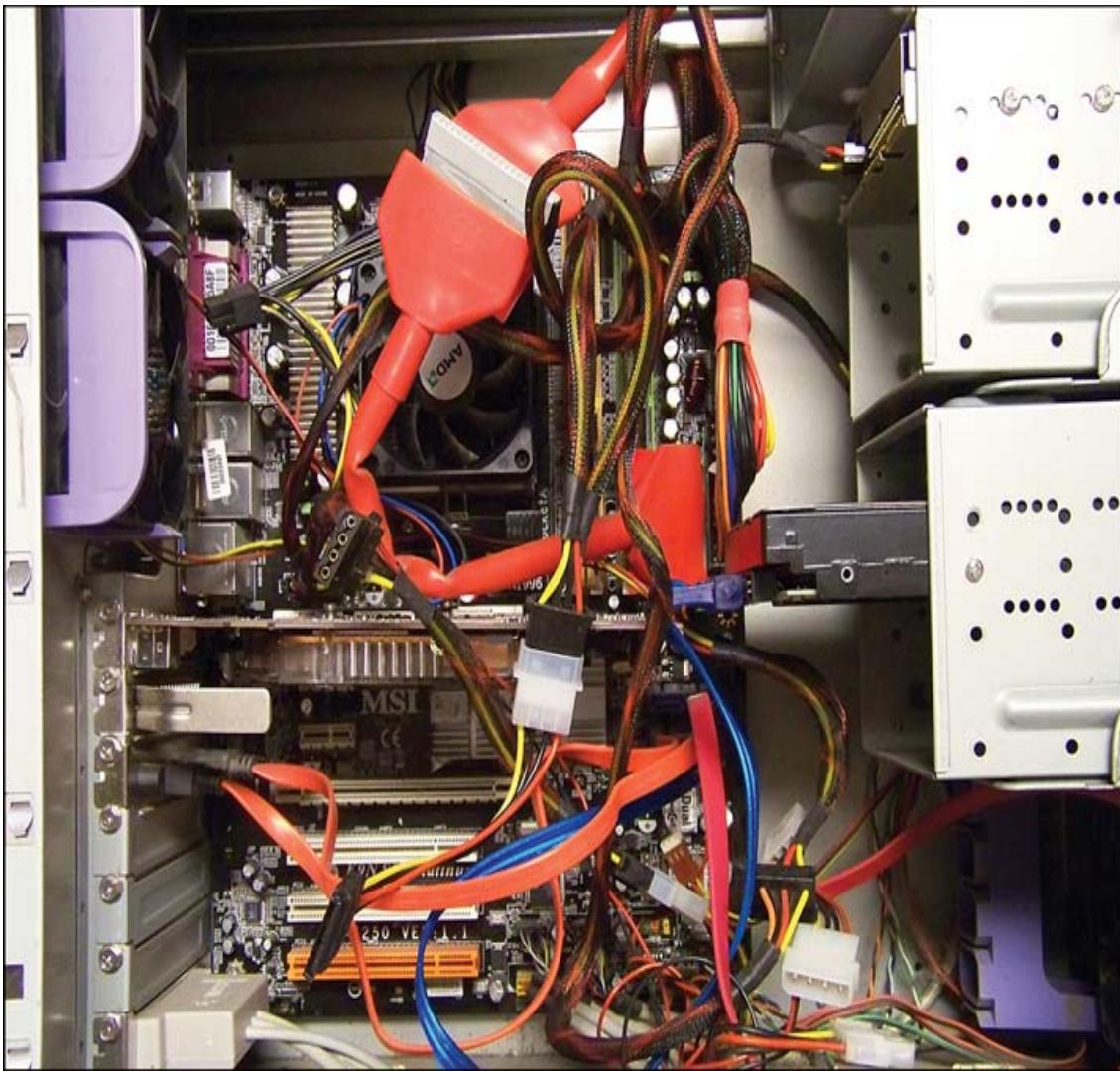
## Inadequate Airflow Outside the System

The power supply's capability to cool the system depends partly on free airflow space outside the system. If the computer is kept in a confined area (such as a closet or security cabinet) without adequate ventilation, power supply failures due to overheating are likely.

Even systems in ordinary office environments can have airflow problems; make sure that several inches of free air space exist behind the fan outputs for any computer.

## Inadequate Airflow Inside the System

As you saw in previous chapters, the interior of the typical computer is a messy place. Data cables (particularly wide ribbon cables on older systems), drive power cables, header cables, and expansion cards can create small air dams that block airflow between the heat sources—such as the motherboard, CPU, drives, and memory modules—and the fans in the power supply and the case. [Figure 5-6](#) illustrates a typical system with a lot of cable clutter, which can interfere with airflow.



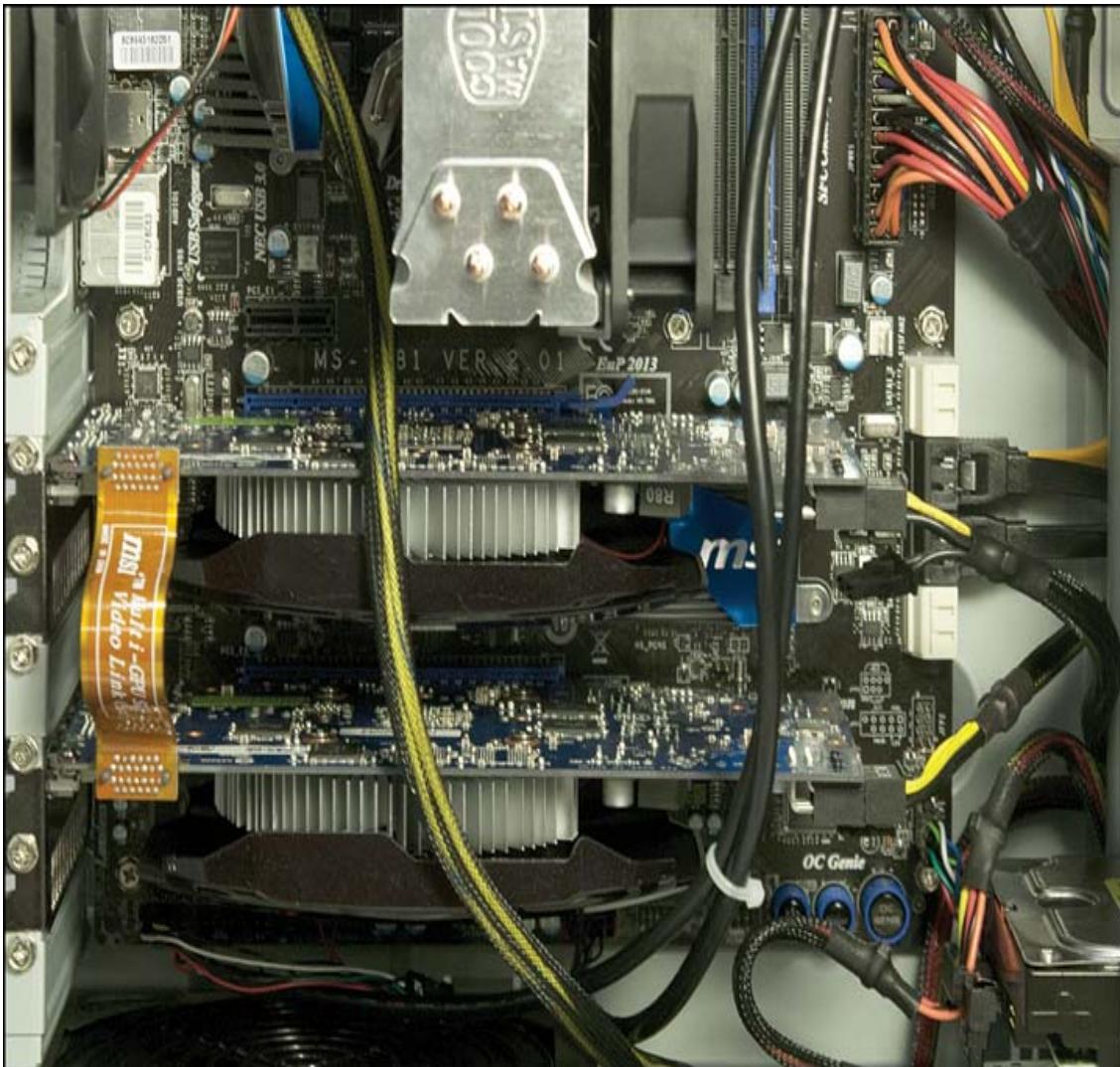
**Figure 5-6** A Cluttered System with Many Unsecured Cables Blocking Airflow

The use of **Serial Advanced Technology Attachment (SATA)** drives and the elimination of internal floppy drives means that the wide ribbon cables used on the old PATA and floppy drives are no longer used. Disorganized systems can still cause overheating, however. You can do the following to improve airflow inside a computer:

- Use cable ties to secure excess ribbon cable and power connectors out of the way of the fans and the power supply.
- Replace any missing slot covers.

- Make sure that case fans and CPU fans are working correctly.

[Figure 5-7](#) illustrates a different system that uses cable management (using cable ties, bundling cables between the drive bays and the outer case wall, and routing cables behind the motherboard) to improve airflow.



**Figure 5-7** A System with Good Airflow Due to Good Cable Management

## Dirt and Dust

Except for a few of the early ATX power supplies, most power

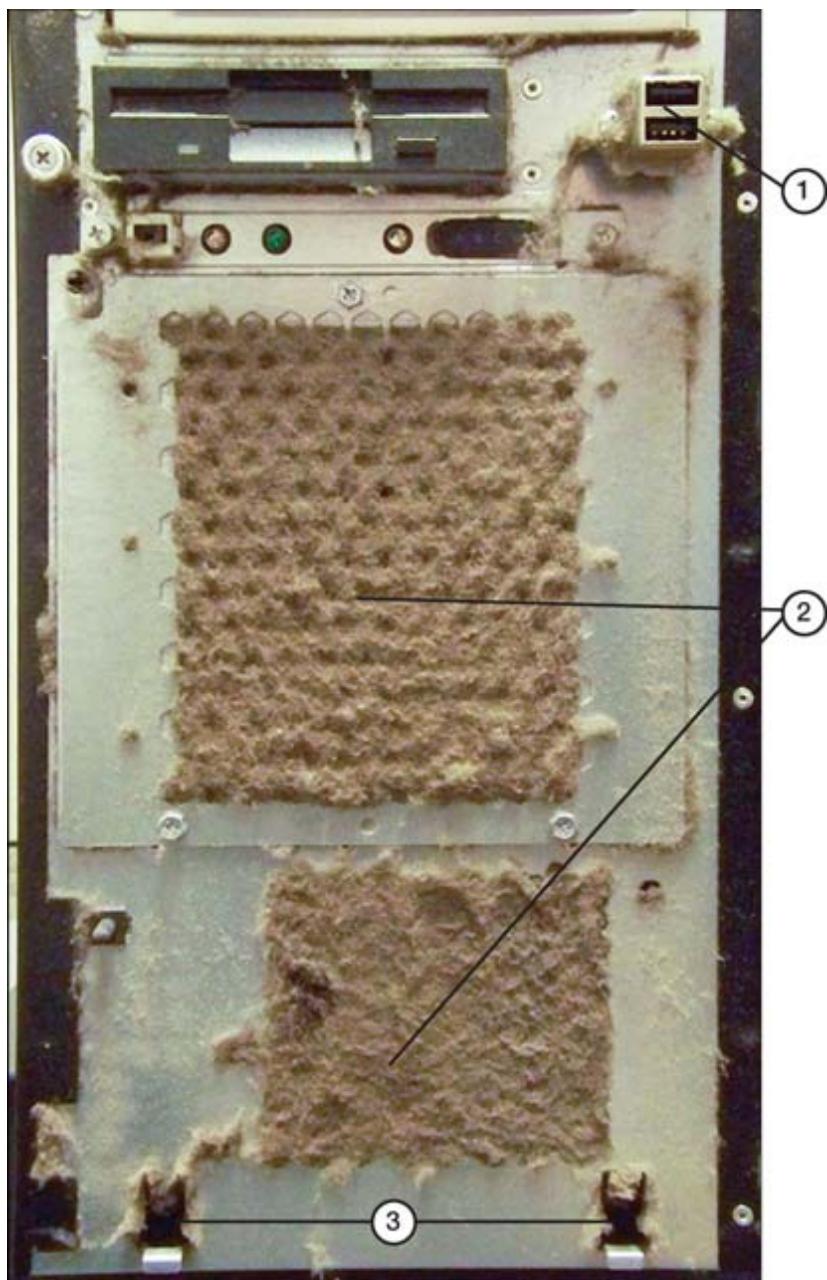
supplies use a cooling technique called ***negative pressure***. With this technique, the power supply fan works like a weak vacuum cleaner, pulling air through vents in the case, past the components, and out through the fan. Vacuum cleaners remove dust, dirt, pet hair, and so on from living rooms and offices; the power supply's weak impression of a vacuum cleaner works the same way.

When you open a system for any kind of maintenance, look for the following:



- Dirt, dust, hair, and gunk clogging the case vents
- A thin layer of dust on the motherboard and expansion slots
- Dirt and dust on the power supply vent and fans

For the most thorough check, remove the computer's front panel. You never know what you will find inside a PC that has not been cleaned out for a year or two. As you can see in [Figure 5-8](#), you might discover a system with almost completely clogged air vents. A system in this condition can fail catastrophically at almost any time.



1. Front-mounted USB ports
2. Clogged air intakes
3. Retaining clips for the front of the case

**Figure 5-8** A System with Extremely Dirty Air Vents

Use a vacuum cleaner specially designed for computer use or compressed air to remove dirt and dust from inside the system. If you are using compressed air, be sure to spread newspapers around the system to catch the dirt and dust. If possible, remove the

computer from the computer room so the dust does not spread to other equipment.

## **Installing/Replacing Case Fans**

If an overheating system has failed fans or empty fan bays, replace the failed fans or add new ones. To replace a fan, follow these steps:

- Step 1.** After removing all power to the system and opening the case, locate any failed fans.
- Step 2.** Disconnect the fan from the motherboard or the power supply.
- Step 3.** Remove the fan from the case. A fan is held in place by four screws inserted from the outside of the case.
- Step 4.** (Start here to add a new fan.) Determine the size of fan needed (typical sizes are 120mm, 140mm, and 200mm), and hold the fan inside the case as you attach screws to the fan from the outside.
- Step 5.** Connect the fan to a system fan header (use the same one as before if you are replacing a fan) on the motherboard. If no system fan header is available, use a Molex power supply connector (or a splitter if you don't have an unused Molex connector).

## **No Power**

A computer or device that is losing power while operating is usually caused by a battery being drained of its charge. The easy and obvious fix is to plug the device into a wall socket. But what if a computer does not boot even with a charged battery or while plugged in? Although this situation is less common, it can happen. Solutions can vary, depending on the device.

If a booting computer has a black screen and is emitting a series of beeps, check the manufacturer's documentation to decode this.

Sometimes it is simply a loose peripheral cable, such as a keyboard or monitor, or an unplugged fan or disk. It can also indicate complete fan failure.

- **Laptop:** Unplug the computer from the wall and remove the battery. Wait about 30 seconds, to let any extra static drain away. Then plug the computer back into the wall and boot. Because it would not boot without the battery, it might need replacing.
- **Desktop:** If the issue is not a loose peripheral cable/fan failure and the computer remains unresponsive, the problem could be a failed power supply. See how to test power supplies in the upcoming section “Burning Smells.”

Unplug your computer and plug it directly into a wall outlet that you know is working (instead of a power strip or a battery backup that could be failing). Make sure the power switch on the back of your power supply is flipped on; if the outlet is connected to a light switch, make sure that switch is turned on, too. Check/test your power supply with a tester for symptoms of failing power supply, including these:

- Random computer crashes
- Random blue screen crashes
- Extra noise coming from the PC case
- Recurring failure of PC components
- PC won’t start but your case fans spin

## Sluggish Performance

Troubleshooting sluggish performance can be tricky because the problematic behavior can vary while the computer is operating. However, several common culprits can sag a computer’s performance:

- **Maintenance:** Keeping software and antivirus/anti-malware protection up-to-date is a great first step. Operating system updates work to control security issues, so make sure the best practice of updating is in place. Malware can also eat up processing power, and outdated drivers can slow performance when using peripherals. Also consider removing rarely used programs from the startup, to free up space.
- **Hard drives:** Cleaning up storage disks is important. A disk that has to look for data can slow operation. Running disk cleaning tools can help. Upgrading an HD to an SSD also can make a big difference in performance.
- **RAM:** Few solutions fix a sluggish computer like adding RAM. Remember that the amount of RAM determines how much processing space is available for open applications. Most computers have minimum RAM standards that can meet basic needs, but if a user is simultaneously performing tasks in multiple applications, RAM space can be used up just by having applications open. If closing applications helps the sluggishness, RAM is a likely factor.
- **Video cards:** If a user is working in processor-intensive applications (for example graphics, video editing, or 3D rendering), a separate graphics card is essential. The CPU on the motherboard can process only so much at once: If regular tasks are being shared with video processing, sluggishness can result. Adding or upgrading a video card with a robust graphics processing unit (GPU) can alleviate the sluggishness issues.
- **CPU:** An older computer could be asked to do tasks it was not designed for. If it is an older motherboard with only one or two cores doing the processing, it might be time for an upgrade.

# Overheating

The most common cause for computer overheating is poor ventilation. Remember that the computer case is designed with very specific airflow patterns to best carry in cool air and then to carry away air heated by the CPU. It is common for dust to collect at the air intake vents and slow or even block the airflow. This leads to overheating in the case and can trigger a shutdown until the CPU cools down.

## Burning Smells

The following are typical causes for overheating and burning smells:



- **Dead short caused by loose screws, slot covers, or cards:** Shut down the system and secure all metal components.
- **CPU overheating:** Check the fan speed for the CPU heat sink. Clean the fan if it is dirty. Replace the fan if it has failed or is turning too slowly. Check power management settings and CPU drivers in the operating system to make sure that thermal throttling is working.
- **Power supply overheating:** Check the power supply fan and clean it, if possible. Replace the power supply with a higher wattage-rated unit if the problem persists.
- **Power supply failure:** Test the power supply to verify proper operation.

If a power supply fails any of these measurements, replace it and retest the new unit.

## Power Supply Tester

You can use a **power supply tester** to determine whether a power supply is working. The power supply does not need to be removed from the computer for testing. However, the 24-pin (or, on older systems, 20-pin) ATX power supply cable and the 4-pin ATX12V or 8-pin EPS12V connectors must be disconnected from the motherboard for testing. The power supply must also be plugged into a working AC outlet or surge suppressor.

[Figure 5-9](#) illustrates two types of power supply testers. One tester is a simple go/no-go tester. When you plug it into a power supply's 20-pin or 24-pin motherboard connector, the power supply starts if it is working, and the green LED turns on. If the power supply does not work, the green LED stays off.



1. Green LED turns on if the power supply works
2. Power supply connected to tester
3. Power supply works—green LED is on
4. Power supply plugged into Dr. Power II tester
5. The power good line has failed, so the power supply is defective
6. All other voltage levels are OK

**Figure 5-9** A Simple Power Supply Tester (Top) Compared to a Deluxe Model That Tests Voltages and Can Also Test Other Components

The second tester has its own power switch and checks the major voltage levels, including Power Good, when you turn it on. The display turns a light blue if the power supply tests okay; however, if any voltage level is out of range, the display turns red, as in [Figure 5-9](#).

## Step-by-Step Power Supply Troubleshooting

Use the procedure outlined next to find the actual cause of a dead system. If one of the test procedures in the following list corrects the problem, the item that was changed is the cause of the problem. Power supplies have a built-in safety feature that shuts down the unit immediately in case of a short circuit.

The following steps are designed to determine whether a power problem is caused by a short circuit or another problem:



**Step 1.** Smell the power supply's outside vent. If you can detect a burning odor, the power supply has failed. Replace it.

**Step 2.** Check the AC power to the system; a loose or disconnected power cord, a disconnected surge protector, a surge protector that has been turned off, or a dead AC wall socket will prevent a system from receiving power. If the wall socket has no power, reset the circuit breaker in the electrical service box for the location.

**Step 3.** Check the AC voltage switch on the power supply; it should be set to 115V for North America. If the switch is set to 230V, turn off the power, reset the switch, and restart the system. Note that many desktop computer power supplies

no longer require a switch selection because they are autoswitching.

## Note

The A+ objectives list AC voltage as 115V or 220V. AC power is supplied at slightly different voltages in different parts of the world. The normal range of voltage is 100 to 120 volts or 200 to 240 volts. Some dual-voltage power supplies can accept either; such a supply either has a selector switch on the back or can automatically recognize the appropriate setting.

## CAUTION

If your area uses 230V and the power supply is set to 115V, you need a new power supply and possibly other components because they have been damaged or destroyed by 100 percent overvoltage.

**Step 4.** Turn off the system, disconnect the power, and open the system. Verify that the power leads are properly connected to the motherboard. Connect loose power leads, reconnect the power, and restart the computer.

**Step 5.** Check for loose screws or other components, such as loose slot covers, modem speakers, or other metal items that can cause a short circuit. Correct them and retest.

**Step 6.** Remove all expansion cards and disconnect power to all drives; restart the system and use a power supply tester or a multimeter to test power to the motherboard.

**Step 7.** If the power tests within accepted limits with all peripherals disconnected, reinstall one card at a time and check the power. If the power tests within accepted limits, reattach one drive at a time and check the power.

**Step 8.** If a defective card or drive has a dead short, reattaching the defective card or drive should stop the system immediately upon powering up. Replace the card or drive and retest.

**Step 9.** Check the Power Good line at the power supply motherboard connector with a multimeter or a power supply tester.

An unreliable power supply can impact every aspect of PC performance. This is a long list of possible problems and solutions, but chances are good that you will track down the source of the problem before you reach the end of it.

## Intermittent Shutdown

**Continuous reboots** can be caused by problems with the power supply or by a Windows or other operating system configuration setting.

When the Power Good line to the motherboard carries a voltage that is too high or too low, the processor resets, shutting down the system and rebooting it. Test the power supply voltage levels; replace the power supply if Power Good tests out of specifications.

Intermittent failures of USB bus-powered devices (such as mouse devices, keyboard, USB flash drives, and portable USB hard drives) usually happen because these devices draw power from the system's power supply via the USB port. These types of failures can be an early sign of an overloaded power supply, especially for devices with low power draws, such as mouse devices and keyboards. Replace the power supply with a higher-rated unit.

Intermittent failures of other USB external devices or of internal devices can be caused by damaged data cables, power supplies or connectors, or ports.

To troubleshoot these problems, follow these steps:



**Step 1.** Shut down the device (and the computer, if the device is internal) and replace the data cable with a known-working replacement. If a USB device is plugged into a front-mounted USB port or a USB port on a card bracket, check the USB header cable connections to the motherboard.

**Step 2.** Turn on the device or computer.

**Step 3.** Test the device over time. If the device works correctly, the problem is solved.

**Step 4.** If steps 1–3 did not resolve the problem, use the original data cable and try plugging it into a different internal or external port. Repeat steps 2–3.

**Step 5.** Try steps 1–4 again, but this time use a replacement power connector or AC adapter.

**Step 6.** When you find the defective component, the problem stops. If the problem is not resolved with different data cables, connectors, or power supplies/AC adapters, the device itself needs to be replaced.

Intermittent shutdowns are often a software issue. Updating drivers is a reliable fix. Also check the settings for sleep mode in Windows 10 to make sure the computer is not simply going to sleep.



## Application Crashes

Applications can misbehave or crash for a variety of reasons.

Applications are written to work with operating system software, and well-written applications rarely have problems in that environment. However, OS software is being updated constantly for security and other reasons, and there is usually a lag between the OS and the

application revisions. During that update lag, many problems can occur.

Microsoft is constantly updating Windows 10 with code and patches that work with specific applications. These do not necessarily install automatically. You can customize the updates to your needs in the Windows Update control panel. To access the panel in Windows 10, go to **Start > Settings > Update & Security**. The Advanced Options tab is available, if needed.

When encountering application errors, also check with the application developers to see if updates are available. Software patches are small updates that can fix known problems until a full version update is available. A patch could solve the problem. If a patch is not available and the software is essential to business, you might need to roll back the OS update to improve performance. Of course, updates happen for a reason, and if security issues arise with rolling back an update, be sure to address those in some other way, if possible.

Drivers for peripheral devices and video and graphics cards can be a source of application issues. Windows Update usually has the drivers, but the manufacturer has them as well. Uninstalling a driver and replacing it can often solve the problem.

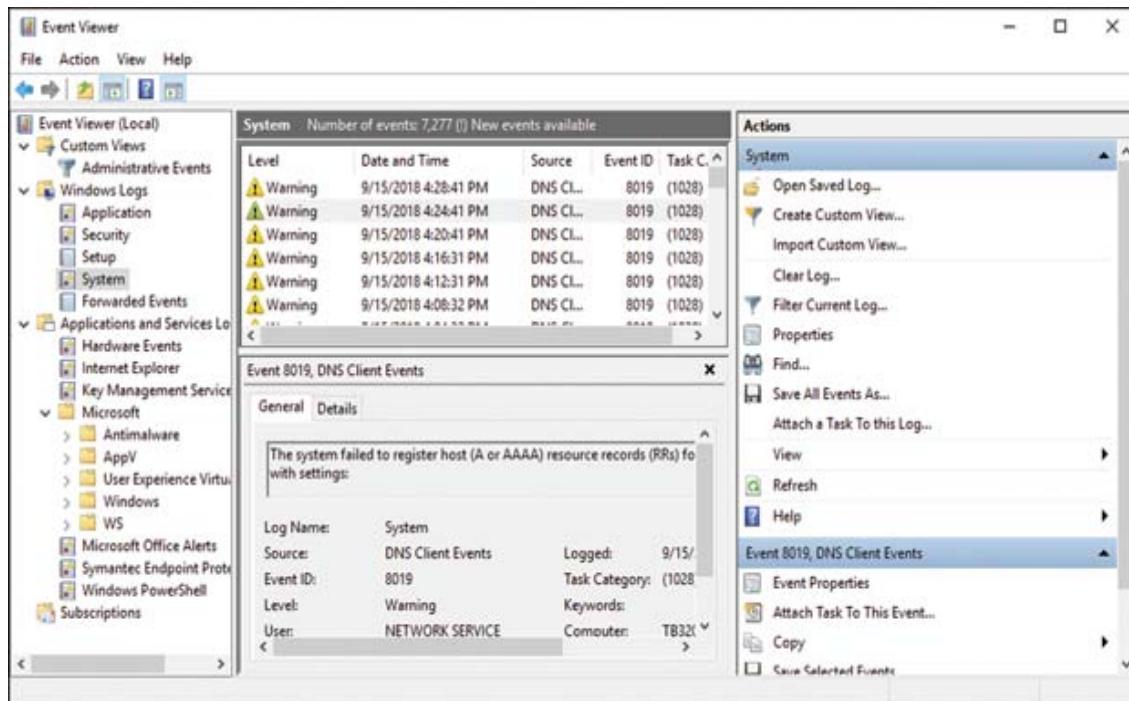
## Log Entries and Error Messages

Logs on a device are records kept to track the history of what has happened on the device. They record the tasks the computer has performed, people who have logged in or out, applications opened, and so on. Error messages tell when something went wrong (for example, a device failure or authentication rejection). These are helpful when an IT professional is trying to isolate and solve a problem on a system.

To access logs and error messages, go to **Control Panel > Administrative Tools > Event Viewer**. [Figure 5-10](#) shows the Event Viewer with the system log selected. Note the many types of

logs available in the different applications and system functions. In the System window, note the warning with a yellow triangle, indicating something that failed (in this case, DNS requests).

**Key Topic**



**Figure 5-10** Windows 10 Event Viewer

Take time to click through the different folders of events recorded on your PC, to become familiar with the vast amount of information available. This much information can be difficult to handle, and tools are available to help search and filter the information down to a manageable amount. You can explore these tools in the right pane of the Event Viewer window, shown in [Figure 5-10](#).

## Grinding Noise

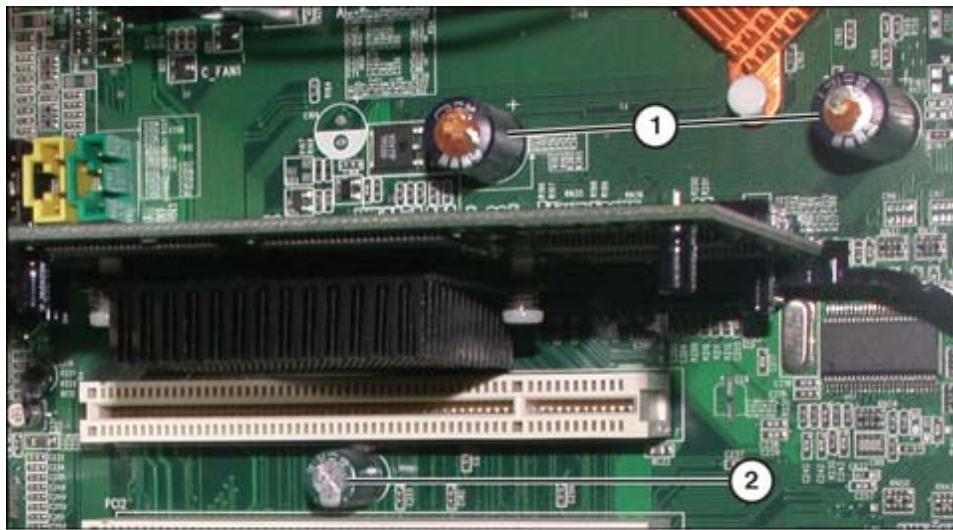
Computers usually run quietly and do not have many moving parts, so if a loud or grinding noise is coming from the computer box, pay attention—it could be serious.

If the noise is coming from the power supply, it is a sure sign of a problem. A whirring, screeching, rattling, or thumping noise while the system is on usually indicates a fan failure. If a fan built into a component such as a heat sink or power supply is failing, immediately replace the component. Any other fans in the case are usually there by design, so be sure all are working properly. If a fan is not spinning correctly, airflow could be slowed—you learned earlier that this can cause major problems, including system shutdowns.

## Capacitor Swelling

Capacitors, sometimes referred to as caps, are used as part of the voltage step-down circuits that provide power to the processor. From 2002 to 2007, many motherboards were built using faulty capacitors that became distended and leaked. This problem, known as **capacitor swelling**, causes system failure and sometimes physical damage to the motherboard.

Figure 5-11 illustrates a motherboard with **distended capacitors**.



1. Distended, leaking capacitors
2. Capacitor in good working order

## **Figure 5-11** A System with At Least Two Faulty Capacitors

Some of these systems might still be in service, and the faulty capacitors can be replaced.

### **Note**

For a detailed step-by-step tutorial on replacing bad capacitors, visit [www.itsacon.net/computers/hardware/replacing-bad-motherboard-capacitors/](http://www.itsacon.net/computers/hardware/replacing-bad-motherboard-capacitors/).

Newer systems typically use solid capacitors (see **Figure 5-12**). These capacitors are much more reliable than older capacitors.



1. Solid capacitors

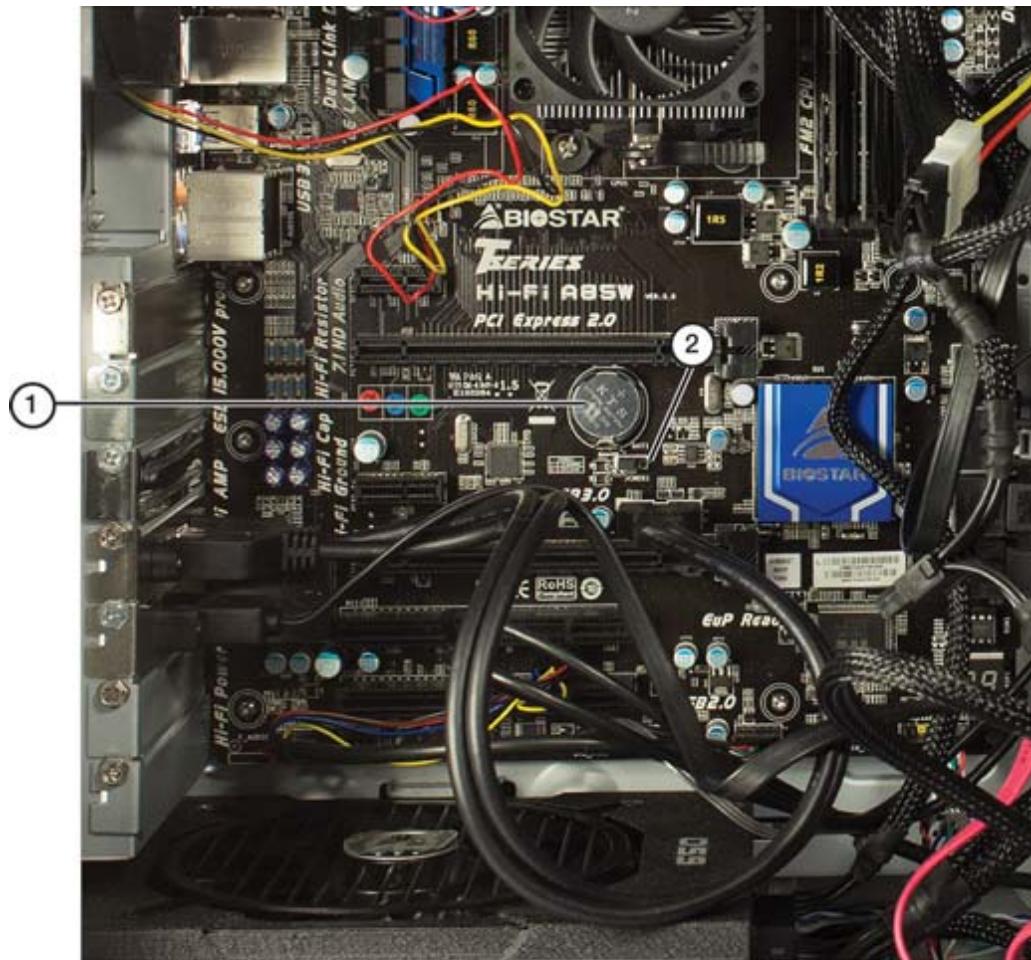
## **Figure 5-12** A Typical Recent Motherboard with Solid Capacitors

## **Inaccurate System Date/Time**

Problems with BIOS/UEFI time and settings resets are typically caused by problems with either the CMOS battery on the motherboard or the CMOS chip.

If date and time settings or other BIOS settings reset to system defaults or display CMOS corrupted errors, replace the CMOS battery and reset the BIOS settings to the correct values. A CMOS battery (usually a CR2032 on recent systems) will work properly for about 3

years before it needs to be replaced. [Figure 5-13](#) illustrates a typical CR2032 CMOS battery on a recent motherboard.



1. CR2032 battery for maintaining CMOS contents
2. JBAT jumper for clearing CMOS contents

**Figure 5-13** Removing Cards or Cables Might Be Necessary to Access the CMOS Battery on Some Systems

If replacing the battery does not solve the problem, the CMOS chip on the motherboard might be damaged. The CMOS chip is a surface-mounted chip that cannot be replaced, so if it is bad, the motherboard must be replaced.

If other settings, such as BIOS/UEFI passwords, have been lost or corrupted, the CMOS contents can be cleared by using a jumper on the motherboard. Depending on the motherboard, the jumper might

be labeled JBAT (as in [Figure 5-13](#)), CLRTC, or CLR\_CMOS. See the motherboard or system documentation for details. Turn off the system, move the jumper block, leave it in place for a few seconds, and then move it back to the normal position. The jumper is often, but not always, near the CMOS battery.

## Troubleshooting Storage Drives and RAID Arrays



**220-1101: Objective 5.3:** Given a scenario, troubleshoot and diagnose problems with storage drives and RAID arrays.

Problems with mass storage devices are among the most frightening to a business or an individual. The tips and techniques in this section can help solve problems and make data recovery possible.

The sections that follow present common symptoms a technical support specialist might encounter when summoned for help with failing hard drives.

## Light-Emitting Diode (LED) Status Indicators

Using [\*\*light-emitting diode \(LED\) status indicators\*\*](#), a technician can evaluate a computer's health at a glance. Computers, switches, routers, and other devices all use LEDs to visually communicate their activity status or any issues with communication. As with the beeps and boops of startup error codes, LEDs communicate in code as well.

Different devices also have color codes for their indicators. [Table 5-4](#) lists examples of LEDs and their meanings.

**Table 5-4** LED Status Indications

LED	Indicator Meaning	Green/Blue	Red/Off	Flashing
Hard drives	On/off; drive activity	On	Off or inactive	
Fans	Power to the fan	On	Failed or off	
Power status	Device powered on	On	No power	
Ethernet cable	Status of data	Working	Down	Data flowing

Of course, the availability of lights and the meaning of the codes varies among manufacturers, so accessing the documentation might be necessary to understand the complete situation.

Notice that, for hard drives and RAID arrays, the LED signals indicate only activity or inactivity; the technician must interpret them to understand if there is a problem. A technician should know what normal benchmark activity looks like and then troubleshoot if there is a change from the benchmark. For example, if the LEDs for a RAID array start flickering incessantly and showing activity even when there is no real load on the machine, it could indicate that the RAID is misconfigured and is working too hard to keep redundant memory updated. The same is true for a hard drive. Flickering lights could mean that background activities such as swap files are working harder than they should, and settings might need to be readjusted or upgrades need to be considered.



## Read/Write Failure

**Read/write failures** can take place for a number of reasons, including the following:

- **Physical damage to the drive:** Dropping any magnetic storage drive can cause damage to read/write heads and platters. The drive might start to make noise or might not spin up at all.
- **Damaged cables:** SATA cables are often included with new motherboards and are inexpensive to purchase. Swapping cables is an easy first step that often solves problems.
- **Damaged SATA host adapter on motherboard:** Most late-model motherboards have several SATA ports; if swapping a SATA cable does not solve a problem, use the original cable in a different SATA port on the motherboard.
- **Overheated hard disk:** The faster a hard disk turns (that is, the higher the RPM), the more likely it is that overheating will take place, especially if airflow is restricted. To prevent overheating, install a cooling fan in front of the 3.5-inch drive bays used for a hard disk(s) and make sure it pulls air into the PC. If you have two or more drives stacked on top of each other with limited airflow, move drives to other drive bays to improve airflow.
- **Overheated CPU or chipset:** Overheated CPU, chipset, or other components can cause read/write failures. Double-check case fans, the power supply fan, and the CPU and chipset heat sinks. Remove dust and dirt from air intakes and fans. Remove loose or failed heat sinks, remove old thermal grease, and reassemble them with properly applied thermal grease.

## Slow Performance

Although SATA drives can manifest slow performance, the causes and solutions for each type of drive vary widely.

To improve slow performance with SATA hard disks, look for these problems:



- **Reduced-performance configuration of 3Gbps or 6Gbps drives:** Some 3Gbps and 6Gbps SATA drives are jumpered to run at the next slower rate, to enable compatibility with older host adapters. Remove the speed-reduction jumper when it is not needed; see the drive documentation for details. [Figure 5-14](#) illustrates a jumper on a 3Gbps drive that limits its performance to 1.5Gbps.
- **Using a 3Gbps cable with a 6Gbps drive and host adapter:** SATA cables made for 6Gbps drives can also be used with slower speeds.
- **SATA host adapter configured for IDE or emulation mode:** SATA host adapters can be configured by the system BIOS (conventional or UEFI) to run in IDE (emulation) mode, RAID mode, or AHCI mode. Use AHCI mode to enable full performance because this mode supports native command queuing (NCQ) and other advanced features.
- **SATA host adapter configured to run at reduced speed:** SATA host adapters on some systems can be configured to run at different speeds, such as 6.0Gbps, 3.0Gbps, or Auto. Select 6.0Gbps when using a 6.0Gbps drive and cabling. To enable the drive and host adapter to autonegotiate the correct speed, select Auto.



1. Drive is jumpered to run at 1.5Gbps
2. Configuration pins for other settings

**Figure 5-14** To Run This Drive at Its Designed 3.0Gbps Interface Speed, Remove the Jumper

## Note

Some SATA drives use a configuration jumper to permit Power-Up in Standby (PUIS) mode. Before you remove a jumper block from a SATA hard disk, check the drive's documentation at the vendor's website. Some drives are marked with incorrect jumper block legends.

To improve slow performance with SSDs, look for the following issues:

- **The drive is connected to a slow SATA host adapter:** Early SSDs were designed for 3Gbps SATA interfaces, but most recent models support the faster 6Gbps interface. When using an SSD on a system with a mixture of 3Gbps and 6Gbps SATA ports, be sure to use the 6Gbps ports.
- **The partition might be misaligned:** Windows automatically creates the first partition on an SSD so that it is on a page boundary, to provide maximum performance. However, if you do not use the entire SSD for a single partition, additional partitions might be misaligned (starting in the middle of a page instead of on a page boundary). Misaligned partitions cause slow

read/write/reallocate performance. Instead of using Disk Management to create additional partitions, use the command-line program DISKPART and specify Align=1024 as part of the Create Partition command. See [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-vista/cc766465\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-vista/cc766465(v=ws.10)) for the complete syntax.

- **The TRIM command is not enabled for the drive:** The purpose of the TRIM command is to provide a way for Windows 10 to notify an SSD of data that is no longer needed. The SSD can delete that data and the space can be made available to the machine. The freed-up space can provide for better disk performance. If the drive does not support TRIM, you must periodically run a utility provided by the drive vendor to reallocate deleted drive sectors. If the drive supports TRIM and you are using it with Windows 10, Windows needs to be optimized for use with SSDs.
- **Not optimizing the operating system for use with SSDs:** Although Windows 10 is designed to disable SuperFetch, defragment, and other services that can slow SSD performance, Windows does not always detect an SSD as an SSD. Use the SSD Tweaker utility ([www.elpamsoft.com](http://www.elpamsoft.com)) to configure Windows for maximum performance with SSDs.

## TIP

Instead of enabling TRIM in real time, Linux users should periodically run the command **fstrim** and use the Ext4 file system. For details, see [https://wiki.archlinux.org/index.php/Solid\\_State\\_Drives](https://wiki.archlinux.org/index.php/Solid_State_Drives).

## Grinding and Clicking Noises

Magnetic hard disk drives are generally quiet. Loud noises coming from a drive can have at least two causes:

- **A loud clicking noise is typically caused by repeated rereads of defective disk surfaces by the hard disk drive heads:** This is typically a sign of a failing drive. Immediately make a backup copy and replace the hard disk.
- **Humming noises can be caused by rapid head movement on a normally functioning hard disk:** This noise can be reduced or eliminated by enabling Automatic Acoustic Management (AAM), a feature of most recent hard disks. Some vendors provide a downloadable acoustic management tool that can reduce head speed to reduce noise; it might reduce drive performance as a result.

## Note

A softer clicking noise is typical of hard disks when the system is in sleep mode. Changing the hard disk drive's power management settings, also known as Advanced Power Management (APM), can eliminate this noise. To learn more, see [www.reddit.com/r/techsupport/comments/2zmvex/while\\_in\\_sleep\\_mode\\_laptop\\_hd\\_seems\\_to\\_make\\_a/](http://www.reddit.com/r/techsupport/comments/2zmvex/while_in_sleep_mode_laptop_hd_seems_to_make_a/).

## Failure to Boot

The primary hard drive is almost always the boot drive. Failure to boot can be caused by these issues:



- **The boot sequence does not specify the system hard disk, or lists the system hard disk after other drives with nonbootable media:** Use the Boot Sequence dialog box in the system BIOS to configure the hard disk as either the first boot device or the second boot device, after the optical drive or USB. If a USB flash drive is listed as the first boot device and the

system is started with a nonbootable USB flash drive connected, the system boot process stops and displays a boot error.

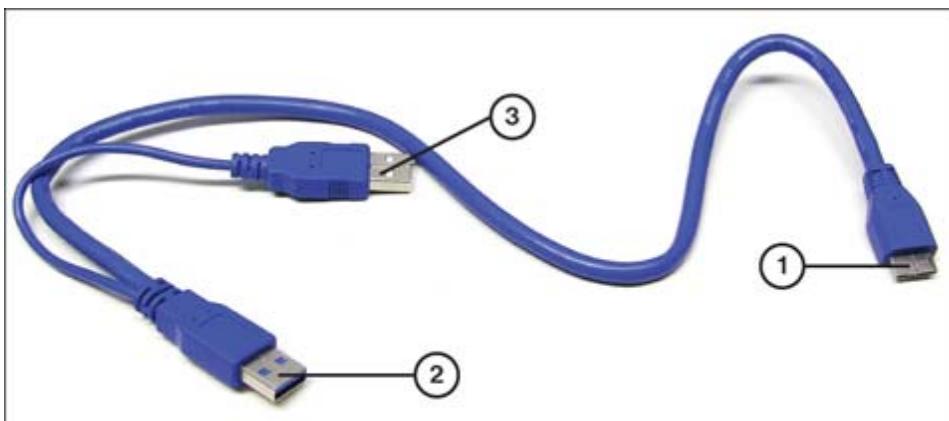
- **CMOS settings have been corrupted and the system cannot find a bootable drive:** Reconfigure the CMOS settings, specify the system drive as a boot drive, and restart the system. Replace the battery if the settings continue to be corrupted.
- **The boot configuration data (BCD) store that Windows uses to control disk booting has been corrupted:** To learn how to fix this problem, go to <https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/bcdedit-command-line-options?view=windows-11>.



## Bootable Device Not Found

A bootable device not found issue can involve problems with cabling, power, BIOS settings, or hard disk failure. If the hard disk is running (you can usually hear faint sounds from a working hard disk), check the following:

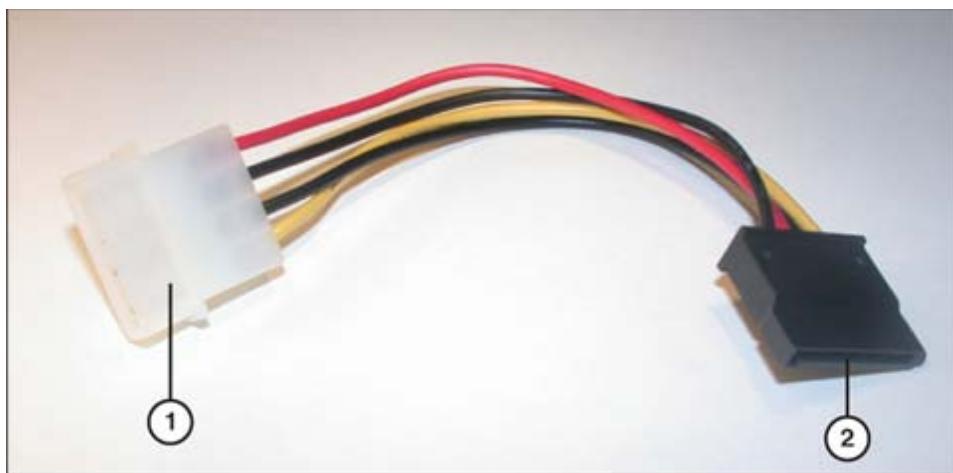
- **Bus-powered USB hard disk not recognized:** A bus-powered USB 2.0 or USB 3.0/3.1 hard disk needs 500mA of power to run (and some hard disks temporarily use more power to spin up). Some computers don't provide enough power in their root hubs (built-in USB ports) to support a bus-powered hard disk, and bus-powered hubs can provide only 100mA of power per port. Connect the drive to another port on a different root hub (each pair of USB ports is a root hub) or a self-powered USB hub, or use a Y-cable to pull power from two USB ports. [Figure 5-15](#) illustrates a USB 3.0/3.1 Y-cable.



1. mini-USB 3.0 connector to drive
2. USB 3.0 connector (data and power)
3. USB 3.0 Y-connector (power only)

**Figure 5-15** USB 3.0/3.1 Y-Cable Provides Bus Power from Two USB Ports

- **USB or Thunderbolt drive not recognized:** If the data cable between the drive and the port is loose, the drive will not be recognized. Reconnect the cable to both the drive and the port; the drive then should be recognized. If the drive is connected to a front-mounted port, make sure the port header is securely connected to the motherboard.
- **SATA hard disk or SSD drive not recognized:** Loose or missing power or data cables cause this problem. Shut down the computer, disconnect it from AC power, and reconnect the power and data cables. If you use Y-splitters or converters to provide power to some drives, keep in mind that these can fail. See [Figure 5-16](#).



1. Molex power connector  
2. SATA power connector

**Figure 5-16** A Molex-to-SATA Power Converter Cable Is a Potential Point of Failure

## Data Loss/Corruption

Users can experience data loss or corruption on their computer for many reasons. Many of them are due to hardware or software failure, and those are covered throughout this section. It is worth mentioning the many ways in which humans inflict damage to data through careless use of their computers and devices:

- Accidentally deleting data in folders
- Unintentionally formatting a hard drive (although data can often be recovered with good backup procedures in place or with recovery tools)
- Spilling liquids on laptops or, worse, dropping devices into water
- Using poor security practices and allowing malware and viruses into the network (Ransomware takes down entire networks, not just one user!)

As a technician, you will encounter these problems (and problem users). Knowing how to respond to the damage is important. Skills you can use to solve these problems are listed here:

- Know your company's backup systems and how to recover data.
- Keep food and drinks away from workspaces.
- Remind teleworkers that home environments have many more hazard areas than the standard office, and encourage them to keep children and pets away from equipment.
- Instill and enforce good security practices to keep hackers and viruses at bay.

As a support technician, controlling the users' behavior is not always easy, but advocating and modeling best practices are always important.



## RAID Failure

**RAID** failure problems can result from the following:

- **The RAID function is disabled in the system BIOS:**  
Reconfigure the BIOS to enable RAID on the SATA ports used for RAID, and restart the system.
- **Power or data cables to RAID drives are disconnected:**  
Reconnect the cables to the RAID drive(s) and restart the system.

### Note

Some motherboards offer RAID support from the chipset, as well as a separate RAID controller chip. Be sure to identify which SATA ports are controlled by the chipset versus a separate RAID controller chip, and connect the drives accordingly.

A RAID failure might be caused by the failure of one or more of the disk drives in the RAID array. Take the following steps if a single drive failure occurs:

- **RAID 0:** Determine which drive has failed. Replace it and follow the vendor's recommendations to re-create the array. Restore the latest backup. Any data that has not been backed up is lost.
- **RAID 1, RAID 10, and RAID 5:** Determine which drive has failed. Replace it. Follow the procedures provided by the RAID vendor to rebuild the array.

If both drives have failed in a RAID 0 or RAID 1 array, you must rebuild the array with new drives and restore the latest backup. Any data that has not been backed up is lost.

If two or more drives have failed in a RAID 10 or RAID 5 array, your recovery options might vary according to the exact configuration of the array. See the RAID vendor's procedures for details and recovery options.

## S.M.A.R.T. Failure

Both Serial ATA (SATA) hard disks and older Parallel ATA (PATA or ATA/IDE) hard disks support a detect-warning feature known as

***Self-Monitoring, Analysis, and Reporting Technology (S.M.A.R.T.)***—also referred to as SMART). S.M.A.R.T. monitors internal hard disks and warns of impending failure. Typical items monitored include the following:



- Drive temperature
- Read retries
- Slow spinup
- Too many bad sectors

Typical S.M.A.R.T. warnings include these:

- Hard disk failure is imminent
- A hard drive in your system reports that it may fail
- Smart failure imminent, back up your data

When S.M.A.R.T. errors appear, back up the system immediately. To determine whether the drive is actually bad or whether the message was a false positive, download and run the disk testing software provided by your system or drive vendor. The long or complete tests detect surface problems and might also swap defective sectors for good sectors.

Under normal operating conditions, you should test your hard disks every month by using a program such as chkdsk (included in Windows) or a vendor-supplied hard disk utility, and review the S.M.A.R.T. attributes for errors. On a portable or laptop hard disk, I recommend checking twice a month because these drives are in greater danger of being physically damaged or overheating.

Although third-party S.M.A.R.T. attribute testing apps are available from many sources, drive manufacturers recommend using their own apps because they are more reliable in interpreting test results and warning of immediate problems.

## **Extended Read/Write Times**

Hard drives should perform at about the same speed throughout their lifetime. If status LEDs indicate longer read/write times, consider checking for a few common culprits:

- Run a virus scan.
- Check the Task Manager to see which programs are using the most resources. Close unused programs.

- Check the Task Manager's Startup tab and uncheck any unnecessary startup programs to reduce the load running in the background.
- Check for drive errors. In Windows 10, open **File Explorer** and right-click the drive that is slow. Then select Properties and open the Tools tab. Use the Check and Optimize utilities to free up space.
- The problem could be with the SATA cable or its connection to the port. Reconnecting (or changing) the SATA cable or using a different SATA port might be all it takes to fix the issue.

## **Input/Output Operations per Second (IOPS)**

[Input/output operations per second \(IOPS\)](#) is the standard way to measure the performance of hard disk drives (HDDs) and solid-state drives (SSDs) in a computer. The IOPS number is a measure of the speed at which data can be read and written from the drive to the CPU.

Remember that HDDs are mechanical and the rotating platters limit the speeds of various HDDs. HDD IOPS run at a relatively slow speed, in the range of 150 to 250 IOPS; current SSDs are delivering around 620,000 IOPS. The performance difference between the types of storage drives explains why migrating to an SSD can greatly enhance the user's experience.

It is possible to collect and monitor the IOPS performance in Windows 10 using the Performance Monitor by typing **perfmon** in the Windows 10 search area, opening the Resource Monitor, and selecting Disk. These new tools allow a deep dive into the drive's performance.

# Missing Drives in OS



An “***OS not found***” (or “operating system not found”) error during boot can be caused by these drive errors:

- **Nonbootable disk in the USB drive:** If a USB drive is listed before the hard disk in the boot sequence and it contains a nonbootable disk, the computer displays an error message that it cannot find the operating system. Remove the USB flash drive and restart.
- **Boot sequence not listing the hard disk:** Restart the computer, start the BIOS/UEFI setup procedure, and make sure that the hard disk is both listed as a bootable drive and listed before options (such as network boot).
- **Incorrect installation of another operating system:** Windows automatically sets up its own boot manager for access to more than one Windows version if you install the older version of Windows first, followed by the later version. However, if you install a newer version first and then later install either an older version or a non-Windows OS, you cannot access the newer Windows version unless you install a custom boot manager.

## Note

For more information about solving boot problems that involve operating system issues, see [Chapter 6, “Operating Systems.”](#)

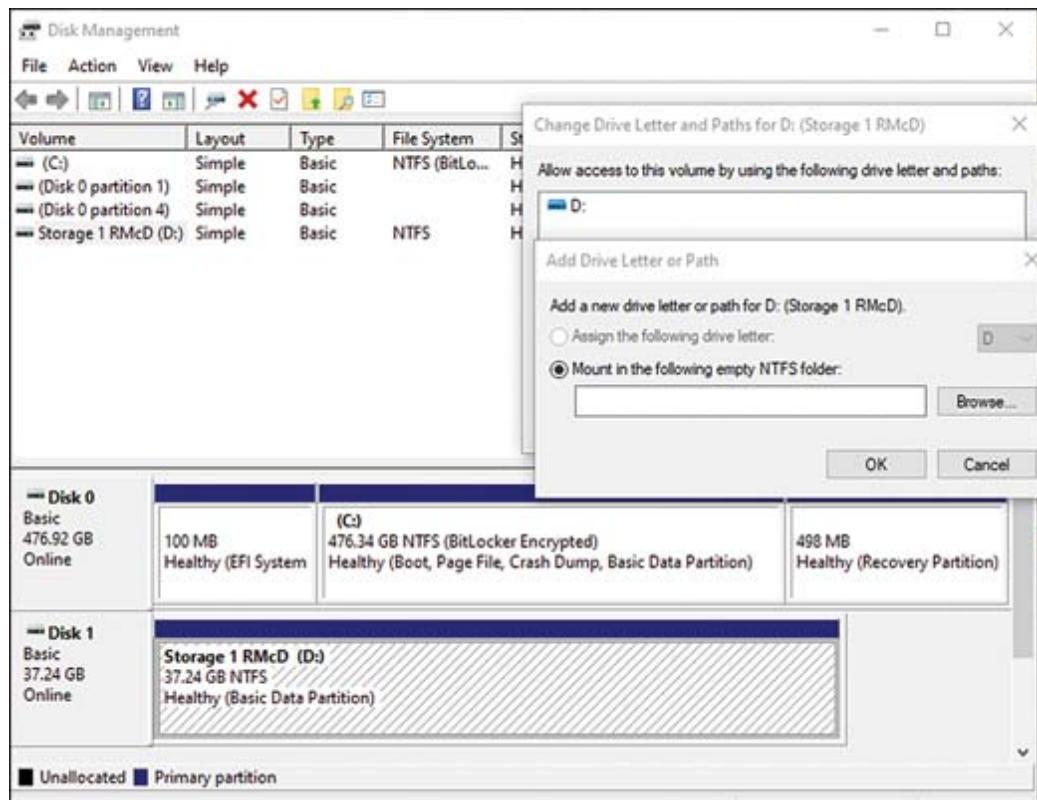
Occasionally, a Windows 10 update or reconfiguration resets the presentation of the disk drives in the OS File Explorer and other areas. The drive might be there one minute, and then after an event (a reboot, an update configuration, or some other event), a drive

letter disappears. Fortunately, in many cases, the drive is still present; it is just not scanned as a drive and presented as a drive icon.

First, check the physical connections. The cables might appear to be connected properly, but reseating them (or changing the cable) is always a good first step. Try to eliminate easy physical problems before diving into more complex troubleshooting.

The easy way to ensure that the drive is still there is to right-click the Start button and select Disk Management from the menu. If the drive is there but is missing a name, the following steps should repair it.

[Figure 5-17](#) captures this moment when the D drive was “missing.” The problem was resolved in the Disk Management window by right-clicking Disk 1, selecting Change Drive Letter and Path, then selecting Change, and finally simply assigning a letter from the drop-down menu.



## **Figure 5-17 Steps for Assigning a Missing Drive Letter**

The problem also can be repaired by simply rescanning the drive from Disk Management.

## **Troubleshooting Video, Projector, and Display Issues**

220-1101  
Exam

**220-1101: Objective 5.4:** Given a scenario, troubleshoot video, projector, and display issues.

Desktop, laptop, and mobile devices each have screens that can vary significantly, and projectors can add another layer of complexity. Setting up a meeting, training, or conference space is a common assignment for a technician. It is important for the technician to arrive early and test all the equipment before the start of the event. If possible, have the presenter come even before the attendees arrive; every technician wants to avoid the pressure of an audience while trying to troubleshoot a projection issue. This section lists some common issues that arise when setting up a projector, as well as how to diagnose and fix them.

### **Incorrect Data Source**

Projectors come in a variety of sizes, and each has its own way of accessing data to project on a screen. They can project from laptops, gaming consoles, phones, tablets, and almost any device that can be shared. If the screen is lit up but the device is not being replicated on the projection screen, the likely problem is that the projector is looking elsewhere for input. From the menu options, look for the source submenu. The inputs are likely looking for a cable interface for incoming data, but if the cable from the device is plugged into HDMI port 1 and the projector is set to look at HDMI port2, nothing

will happen. This sounds easy to fix, but it is a common problem because many projectors are wall mounted and the HDMI and other inputs can be hard to access, let alone read their labels. If everything else looks like it should be working, try scrolling through the source menu to see if the projection shows up on an interface other than the one expected.

## Physical Cabling Issues

Physical cabling issues are the first problems to troubleshoot. Any networking professional can tell a story about troubleshooting for a complex problem, only to find that the physical cable was the problem.

Always start the troubleshooting at the physical cables before you troubleshoot more complex configurations and software. When machines are moved during setup, cables come loose in their sockets or become disconnected altogether. If a projector will not light up, check the indicator lights or listen for a fan; if you cannot find a problem there, physically check the power connectors—sometimes, they appear to be connected but have come loose and are not conducting power. This is also true for HDMI, coax, Ethernet, or any cable the projector can use.

If the physical cable is plugged in, make sure it is in the right interface, as stated previously with data source selection. These fixes sound easy because they are—however, it is very common to encounter problems that have simple solutions. Think basic first.

### TIP

HDMI cables are preferable to other types because they carry high-definition video and also audio. HDMI cables are also compatible with most devices. The fewer cables are needed, the less likely physical cable issues will occur.

## Burned-Out Bulb

Light bulbs in projectors can burn out for several reasons. Eventually, they will all burn out. Always have the right replacement bulb on hand. If more than one model of projector is in inventory, be sure to have bulbs that match and make them easy to access.

It is always best to replace a bulb before it burns out, but bulbs can be expensive and it is hard to know how much longer they will last. Some projectors have LED indicator lights that warn of a potential bulb failure from excessive hours in use. The following are other possible indications:

- A bulb might dim, noticeably affecting the image being projected.
- If images are not crisp and bright or colors are faded, the bulb might no longer be at full strength.
- The image might flicker, indicating that the bulb is about to fail.
- The bulb might simply go dark, but the fan keeps running. Sometimes a loud pop is heard as the internal workings of the bulb fail.

## Intermittent Projector Shutdown

Projectors shut down when they overheat. To avoid overheat shutdown, check the following:



- Clean or replace filters when recommended. Projectors with filters usually display a message onscreen when it is time to clean or replace the filter.
- Make sure the projector has adequate ventilation.

- Check air intakes and exhaust ports for dust and dirt, and clean as necessary.
- Use a lower brightness setting on projectors, to reduce heat.
- Be sure to allow the projector to cool down completely before removing it from power.

A video card (GPU) that overheats usually displays screen artifacts before shutting down.

## Dead Pixels

Dead pixels (black pixels) typically result from manufacturing defects in an LCD screen. Check with the manufacturer of the display panel or laptop to determine the number of dead pixels that are needed to qualify for screen replacement.

Some “dead” pixels are actually stuck on (bright) or off (dark). This problem can be solved in a variety of ways, including the following:

- Navigate to the JScreenFix website ([www.jscreenfix.com](http://www.jscreenfix.com)) and start the pixel fixer app. Drag the app window to the area of your screen with the pixel problem and leave it over the area for up to 10 minutes. JScreenFix uses HTML5 and JavaScript controls in the web browser. It works with any LCD or OLED device, including mobile devices.
- Gently massage the stuck pixel with a stylus or another object with a blunt, narrow end. See [www.wikihow.com/Fix-a-Stuck-Pixel-on-an-LCD-Monitor](http://www.wikihow.com/Fix-a-Stuck-Pixel-on-an-LCD-Monitor) for illustrations.
- For Windows systems, download and run the UDPixel utility (<https://softradar.com/udpixel/>). It requires .NET Framework 2.0, which can be added to Windows 7/8/8.1/10 through Add/Remove Windows Features (in the Control Panel).

## Incorrect Color Display

Incorrect color display on a projector can have several causes, so try the following:



- Check the signal type in the projector menu, and change it if it is incorrect.
- If one LCD panel (red, green, or blue) is failing in an LCD projector, replace the panel. Panels often fail because of the impact of ultraviolet light causing excessive heat and breaking down organic compounds used in the process.
- On a DLP projector, check the LED light sources (red, green, or blue) or dichroic mirrors.
- Clean the projector LCD panels if odd-colored specks are visible.
- If a laptop has been serviced or upgraded, the LCD ribbon connector to the motherboard might have been damaged. If an external display works correctly, check the LCD ribbon cable inside the laptop.
- Check a VGA cable for bent or broken pins. (However, some pins are not present, by default.) Check all video cables for cracked outer casings and loose or damaged connectors.

## Dim Image

A dim image can be caused by settings issues or by equipment failure. Check the following:



- Check the screen brightness control on a display or projector. As mentioned earlier, it could mean a bulb is close to failure.

- If a display management program is being run (which is common on Intel, NVIDIA, and AMD 3D GPU drivers), check its settings.
- On a laptop, tablet, or mobile device, check the built-in screen brightness setting.
- On a projector, check the projector bulb. A bulb can become milky, which reduces light output, near the end of its service life.
- On a device that uses a CCFL backlight, check the inverter. A failing inverter can cause a dim display before the inverter fails. The inverter can be replaced separately from the LCD panel or backlight.

## Flashing Screen

A flashing screen can have many causes:



- Before you look at hardware replacements, try updating the GPU (video card) or chipset drivers.
- On displays that use an LCD-CCFL backlight, flickering can be caused by a failing inverter or a failing backlight. Inverters are relatively inexpensive and can sometimes be replaced without a complete teardown. Backlights cost more, and it could make more sense to buy a replacement LCD screen or retire a computer or display.
- On any type of LCD display (CCFL or LED backlight), loose internal cables can cause flickering. A two-in-one convertible device (tablet/laptop) could have a hinge problem that can lead to flicker.
- On desktop computers, check the power connector to the PCIe card (if it uses a separate power cable) and the power supply

itself. If the problem happens after the computer has been running for a while, it could indicate a heat-related problem.

## Fuzzy or Distorted Image

A fuzzy or distorted image can have several causes and solutions, including the following:

- If image tearing or distortion occurs in 3D games only, change video drivers. In most cases, the newest video driver is recommended; in a few cases with certain games, the best short-term fix might be to install an older driver. Check driver versions with Device Manager's properties sheet or the proprietary app installed by your GPU or video card maker.
- Distortion with DisplayPort connections can be caused by problems with the way some DisplayPort cables and connectors are manufactured. If you can use a different connection (DVI or HDMI) between a system and a display, and the problem is no longer present, replace the DisplayPort cable.

## Display Burn-in



Burn-in, the persistent display of a “ghost” image onscreen that was displayed previously, even after the current screen contents have changed, can affect both LCD and plasma displays.

## LCD Displays

With LCD displays, stuck pixels are the usual cause of burn-in. Programs that run constantly changing patterns across the area, such as the previously mentioned JScreenFix or UDPixel, can be used to fix this problem.

Another solution is to create an all-white image using a graphics program, set it as the screen saver, and turn down the display brightness. Leave the screen saver running about as long as the original image was onscreen.

To avoid image persistence with IPS displays (the most common type of LCD display in use, offering wide viewing angles), Apple recommends using display sleep to turn off the display when idle. To eliminate a persistent image, enable the screen saver to come on before display sleep, and run it as long as the persistent image was originally onscreen. For more information, see <https://support.apple.com/en-us/HT202580>.

## Plasma Displays

Plasma displays use phosphors, which can wear unevenly over time. This is also the cause of burn-in on CRT displays. To avoid either temporary or permanent image persistence, try the following:

- For customers who watch mainly 4:3 ratio TV or movie content, advise periodically switching to full-screen (zoomed) mode, to avoid black bar persistence on the sides of the image.
- Use the screen clean (screen washing) option available on some plasma HDTVs. This puts a constantly changing display across the entire screen.

### TIP

For plasma and LCD display/HDTV users, many YouTube videos can be played to help fix image retention. To play these on an HDTV, go to the YouTube app and search for “image retention fix.”

## **Audio Issues**

If audio issues arise with a device that is plugged into a projector, first make sure that the audio is working on the computer. Sound cards in mobile devices are usually mounted on motherboards in smaller devices and rarely fail. However, simply unplugging the device from the projector and trying the sound ensures that the computer's audio is not the issue. If you do find a problem, removing and replacing sound drivers is a good place to start.

Audio issues on projectors are similar for any audio output device. The first area to check is cable connections. If the connections are fine, look to the source's output settings to see if the output is set to HDMI/USB (if that is being used). If it still fails, try swapping the cable for a known-good cable to make sure it is not a physical issue.

If the audio is buzzing, it could be caused by electrical interference in the room. Make sure the projector and the source device are plugged into the same outlet bar, to eliminate this issue.

If the volume is too low or too high, remember that there might be multiple volume controls—one on the source device, one on the projector, and maybe even one on the software being presented.

No sound from speakers can result from several causes:

- With wired speakers, keep in mind that the case might prevent a 3.5mm mini-jack connector from making a good connection. You might need to remove the case to make a good connection.
- With Bluetooth speakers, make sure Bluetooth is turned on. Check device pairing.
- Check the volume or mute controls on the mobile device. Apple iPhones have a sliding switch to mute them, as well as software controls. The side button on an iPad can be configured to lock the screen or mute speaker output. Check the volume control on the keyboard or OS on macOS and Windows devices.

# Mobile Device Troubleshooting

220-1101  
Exam

**220-1101: Objective 5.5:** Given a scenario, troubleshoot common issues with mobile devices.

With more organizations than ever using laptops, tablets, and smartphones, it is important to know how to troubleshoot devices on the go. You need to understand the concepts covered in the following sections for the 220-1101 exam and to improve your technical skills.

## Poor Battery Health and Improper Charging

To fix a battery that is not charging on a tablet or smartphone, do the following:

Key Topic

- Make sure the charger is rated for the tablet or smartphone. Chargers are rated in amperage ( $1A = 1000mA$ ). A minimum of 500mA is needed to charge a smartphone (but 1A is much faster), and a minimum of 2.1A is needed to charge a tablet.
- Check the charging port on the device. Pocket lint can make for a faulty connection on a phone. Laptop charging ports are also susceptible to dust and debris.
- If the charger has a toggle for iOS and non-iOS devices, choose the correct setting for your device.
- If you use a USB port on a laptop or desktop computer, enable USB fast charging if it is available on the computer, and be sure to use that port.
- You cannot charge a smartphone from an unpowered USB hub; it has only 100mA available per port.

- Ordinary USB ports cannot charge a device when the computer is asleep.

If you have checked these issues with no success, replace the cable. If a known-working cable does not help, replace the battery or have the unit serviced.

On a laptop, if the system works when plugged into AC power but not on battery power, check the following:

- Make sure the battery is installed properly.
- Wipe off any corrosion or dirt on the battery and laptop battery contacts.
- Determine whether the battery can hold a charge. Make sure that the battery is properly installed and that the AC adapter has proper DC voltage output levels. Leave the system plugged in for the recommended amount of time needed to charge the battery; then try to run the system on battery power. If the battery cannot run the system, or if the system runs out of battery power in less than an hour, replace the battery. If replacing the battery does not solve the problem, the laptop needs to be serviced or replaced.
- If the battery is hot after being charged or has a warped exterior, replace it.

Various factors can still cause extremely short battery life. Check the following:

- Do not overcharge a device's battery.
- For best results, do not wait until a device is almost out of power to charge it.
- Adjust the screen brightness to the lowest level that is comfortable to use.
- On iOS devices, turn off background app refresh.

- Upgrade to the latest OS or OS updates available for your device.
- Use a phone battery helper app to manage charging, but do not run other apps while the device is charging.
- Close apps from the iOS App Switcher.
- Shut down an iOS device weekly with the slider switch.
- On devices that use AMOLED displays, switch to black wallpaper (theme), to save power.
- Extreme cold can quickly sap a device's battery, so be sure that the user takes in climate considerations and keeps the device as warm as possible in cold climate use.

## **Swollen Battery**

A swollen battery is most likely the result of overcharging. In addition to replacing the battery, check the AC adapter to make sure it is putting out the correct voltage. If the case is bulged (from the battery or for any other reason), the device is likely unusable. Check for warranty information and arrange for replacement.

## **Broken Screen**

A broken screen on a phone or tablet takes some specialty repair tools and skills, but the problem is common enough that toolkits and screen repair services are available in most areas.

A broken screen cannot be fixed, but it can get worse, so replacing the screen as soon as possible is important. An unrepairs screen can get worse with use, allowing dust and moisture into the device.

If immediate repair is not possible, at least cover the screen with a plastic screen protector, to keep it together until repairs can be made.

Screen repair kits are available online, and they have accompanying YouTube tutorials. Still, sending the device out for repair might be more economically prudent.

Some carrier contracts have insurance available. If the device is insured, contact the carrier or vendor to get a replacement or upgrade, whichever is appropriate.

After the device has been replaced or repaired, consider the likelihood that it will be dropped and broken again. If the device is often exposed to hazardous use, buy a plastic cover for the screen to prevent or minimize the cracks before the next incident.



## Poor/No Connectivity

Most laptops have a pushbutton, pressure-sensitive touch button or an Fn key combination to use to enable or disable Wi-Fi networking. If there is no wireless connectivity, press the button or use the Fn key combination to enable the connection. Most laptops display an indicator light when the connection is enabled.

Late-model laptops, tablets, and smartphones have an airplane mode that disables all onboard radios (Wi-Fi, Bluetooth, and cellular) when enabled. Turn off airplane mode and try the connection again. Wi-Fi can also be disabled separately from airplane mode. Check the Settings menu and enable Wi-Fi, if necessary.

On Windows devices, if the connection fails, check the Wi-Fi connection in the notification area. You might need to reconnect manually. If no Wi-Fi connection indication appears, open the Device Manager and check the Network Adapters category. If the Wi-Fi adapter is not listed, rescan for hardware changes.

If Device Manager cannot locate the Wi-Fi adapter, shut down the system, disconnect it from all power sources, and open the access

panel to the Wi-Fi card. If the card is loose, reconnect it and retry the connection after restoring power and restarting the computer. If the Wi-Fi antenna wires are loose, tighten them.

Some tablets and smartphones have intermittent wireless if the Wi-Fi signal is very weak. Switch to a cellular data connection (if available) until a stronger Wi-Fi signal is available.

Change the angle of your laptop or two-in-one device screen, or turn the entire unit to help improve Wi-Fi reception; these units have their antennas in the screen.

Use the signal strength indicator to find the strongest wireless signal that can be used. In a public setting, two or more open networks might be available.

## Liquid Damage

The problem with device mobility is that devices get taken places they should not—specifically, near water. Dropping a phone into a stream, lake, or hot tub while taking vacation pictures, or dropping it into a toilet or sink while in a bathroom exposes the phone to potentially terminal liquid exposure. If a device takes an unintentional bath, these steps could save the device if the exposure was minimal:

**Step 1.** Be quick in getting the phone out of the water. Every second counts, and any delay greatly reduces the chance of recovery. If the device was plugged into anything, remove it from the power source and then unplug the device. Power off the device, if necessary. Any other attachments, such as battery packs and memory cards, should come out as well.

**Step 2.** Dry off the device with a towel, and shake any water you can out of the ports.

**Step 3.** Do what you can to dry it out. A few different ways accomplish this, and because time is of the essence, using

what is available is the best choice. A common method is adding cat litter or rice to a container large enough to hold the device, to hopefully draw moisture out of the phone. Some argue that rice might do some damage, but it is usually the most available option. Put the device into the container, cover it with the ports facing down so they can drain, and seal the container to increase effectiveness.

A day or two in the container will get the water out, but only then can the device be tested to see if it survived the soaking. If it will not power up, you might need to seek out a pro who can disassemble it and check inside.

## **Overheating**

Overheating is a dangerous symptom that should be addressed as soon as it is discovered. Heat comes from the processor, but unlike with desktop computers, there is no fan to move the air away. Room-temperature air flow around a device should keep it in a normal range, but if a device is running hot, do not ignore it. Consider these causes:

- Is it stored in an enclosed space, such as a warm pocket or under a blanket? Air needs to be able to flow around it to keep it cool.
- Sometimes the CPU is working too hard and needs a rest. This can result from too many apps open and running, or maybe from an app that needs updating. Wi-Fi and Internet use also place heavy demands on a device's CPU.
- Some phone and tablet cases restrict air flow and can cause heat to be retained. If the phone is warm, remove the case and let it breathe.
- Left in the sun, especially under glass (such as in a car), the air can get too hot to allow the device to cool.

- The battery could be failing and causing excess heat. If battery swelling occurs, shut off the device and replace the battery. With any luck, the battery compartment will not be damaged. Sometimes heat is an early warning for a bad cable or charger. If so, replace the charger and/or cable.

The best treatment for an overheated phone is to shut it down, remove the cover, and give it a rest in a cool place. Some people put the device in a refrigerator, but that is not necessary—in fact, depending on the cleanliness of the fridge, it can cause its own problems. Room temperature is fine if the device is powered down and the cover is removed. If the problem continues, review the items in the preceding list and troubleshoot.

## Digitizer Issues

A touchscreen display differs from a standard laptop display because it has a digitizer layer on top of the display panel. The **digitizer** detects and transmits touches to the laptop processor. Digitizers are also used on touchscreen smartphones, tablets, fitness monitors, smart watches, phablets, e-readers, and smart cameras.

If the digitizer layer is damaged but the display panel is intact, the digitizer layer can be replaced separately.

### Note

For examples of pricing and availability of digitizers, see <https://touchscreendigitizer.net>.

## Nonresponsive Touchscreen



The most common reason for a nonresponsive touchscreen is dust, dirt, and grease on the surface. To clean it, use an antistatic wipe or spray designed for touchscreens.

Dry hands might not work well with touchscreens. Gloves without special fingertips also cannot use a touchscreen.

To determine whether the touchscreen has failed, try a stylus made for the touchscreen. Reset the device and retry. If the touchscreen is still not responsive, have the unit serviced.

## **Physically Damaged Ports**

Mobile devices have few ports, compared to a laptop or PC, but because of the harsh environment for mobile phones and tablets, problems can still occur.

One typical harsh environment for a mobile device is the user's pocket. Pocket storage of a phone invites pocket lint to invade the ports. If charging becomes difficult, the first place to look is in the charging port to see if the contacts are visible. Clean the port with a wooden toothpick—take care to lightly scrape and remove dust until the contacts are clean. Do not use a metal pick from a PC toolkit for this because it can easily damage the contacts.

USB ports on some phones (Android, for example) can come out of alignment. If this happens, remove the battery and use a soft wooden toothpick to carefully realign USB ports.

Humidity is another concern for some phone users. Liquids and phones do not mix, so users who live in rainy or humid climates can have corrosion issues over time. Use in steam rooms or around hot tubs can expose phones to excessive humidity as well. If these uses are expected, a waterproof phone or case is a good idea.

Users can prevent corrosion, but only a professional can cure it. Fixing this problem with proficiency takes practice.

## Malware

Just as malware can infect users on a network, mobile devices are subject to malicious software designed specifically to disrupt mobile operating systems. Examples are similar to the security issues facing PC users, but customized for the mobile device. They include phishing, Trojans, spyware, and adware (called madware on mobile phones).

Steps to protect against mobile malware are similar to any security steps:



- Install security software.
- Keep the OS and applications current, to enable the latest security updates.
- Use apps vetted by app stores that your provider recommends.
- Protect against loss and theft by enabling Find My Phone settings and screen-locking settings.

For a more detailed discussion on security, see [Chapter 7, "Security."](#)

## Cursor Drift/Touch Calibration

**Cursor drift** can be caused by accidentally swiping or pressing on the device's touchpad, or by encountering a problem with the device's integrated pointing stick. If you are using a mouse, disable the touchpad or change its sensitivity settings to ignore accidental touches.

## Printer Troubleshooting



**220-1101: Objective 5.6:** Given a scenario, troubleshoot and resolve printer issues.

For the 220-1101 exam, be sure you understand how to resolve printer symptom issues and how to use the tools listed in the following sections. You might want to review the section “Multifunction Devices/Printers and Settings,” in [Chapter 3](#), to brush up on the deployment and handling of printers.

## Lines Down the Printed Pages



Smudges and lines that streak down the printed pages can have many causes, depending on the type of printer in use.

### Laser Printer

Randomized streaks in printed output, such as uneven printing or blank spots, are usually caused by low toner. As a temporary workaround, remove the toner cartridge and gently shake it to redistribute the toner. Install a new toner cartridge as quickly as possible.

Long vertical streaks that repeat on each page are usually caused by damage to the imaging drum. Replace the drum or toner cartridge if it includes the drum.

### Inkjet Printer

Smudged print output from an inkjet printer can be caused by dirty printheads or paper rollers, incorrect head gap settings, and incorrect resolution and media settings.

If you see smudges only when printing on heavy paper stock, card stock, labels, or envelopes, check the head gap setting. Use the

default setting for paper up to 24-pound rating, and use the wider gap for labels, card stock, and envelopes.

Clean the printhead. If the cleaning process doesn't result in acceptable results, remove the printhead (if possible) and clean it. If the printhead is built into the printer, or if the paper-feed rollers or the platen have ink smudges, use a cleaning sheet to clean the paper-feed rollers, the platen, and the printhead.

Check the Printer Properties setting in the operating system to ensure that the correct resolution and paper options are set for the paper in use. Horizontal streaks in inkjet output are usually caused by trying to print on glossy photo paper using the plain paper setting.

Unlike laser output—which can be handled as soon as the page is ejected—inkjet output often requires time to dry. For best results, use paper specially designed for inkjet printers. Paper should be stored in a cool, dry environment; damp paper also will result in smudged printing.

## **Thermal Printers**

Streaky output in thermal transfer printers can have several causes, including media and print head problems.

If the coating on the media is poor quality, replace the media. If preprinted ink on the media is sticking to the printhead, replace the media with media printed using heat-resistant ink.

If the heating element is dirty, clean the heating element.

Smeared output (primarily when printing bar codes) can be caused by incorrect print head energy settings, a print speed that is too high, and a 90-degree or 270-degree orientation.

With direct thermal printers, check for improperly stored paper or an incorrect setting in the printer driver. If the printer can be used in

either direct or thermal transfer modes, an incorrect driver setting can cause print quality problems of various types.

## **Impact Printers**

Streaky output in dot-matrix impact printers is usually caused by a dried-out ribbon. If the ribbon has an auxiliary ink reservoir, activate it; otherwise, replace the ribbon.

## **Faded Prints**



Faded prints also have many possible causes, depending on the printer.

## **Laser Printers**

If the printing is even, the printer might be set for an economy mode or a similar mode that uses less toner. Adjust the printer properties to use normal print modes for final drafts.

For a color laser printer, also check the toner levels or the operation of the toner belt.

## **Inkjet Printers**

The print nozzles might be clogged, or some colors could be out of ink. This is a common problem for inkjet printers that have not been used in a few weeks. It is a good idea to print something using all the inks every week or so. Clean the nozzles and use the nozzle check utility to verify proper operation. Replace any cartridges that are out of ink.

## **Thermal Printers**

A faded image can result from installing a thermal transfer ribbon backward. Remove the ribbon, verify proper loading, and reinstall.

If the ribbon is installed correctly but there is still a problem, the ribbon might not be compatible with the media. Check the media settings in the printer configuration to verify.

## **Impact Printers**

If the print is evenly faded, the ribbon is dried out. Replace the ribbon, to achieve better print quality and protect the printhead. If the print appears more faded on the top of each line than on the bottom, the head gap is set too wide for the paper type in use. Adjust the head gap to the correct width, to improve printing and protect the printhead from damage.

## **Double/Echo Images on the Print**

Laser printers that display double or echo images of part or all of the previous page on a new printout might have problems with the toner cartridge, imaging drum wiper blade, or fusing unit. To determine the cause of the ghosting, measure the distance between the top of the page and the ghost image, and consult the service manual for the printer. Clean or replace the defective component.

## **Toner Not Fusing to the Paper**

The fuser in a laser printer is supposed to heat the paper to fuse the toner to the paper. Fuser failure results in **toner** that is not fused to the paper. If the printed output from a laser printer can be wiped or blown off the paper after the printout emerges from the laser printer, the fuser needs to be repaired or replaced.

## **Incorrect Paper Size**

Incorrect paper size in the paper tray can cause creases in the paper. This is usually caused by an incorrect adjustment of the paper guides for feeding pages. If the paper guide is not set to the actual paper width, the paper might move horizontally during the feed process and become creased. Adjust the paper guides to the correct width for the paper or media in use.

## **Paper Not Feeding**

The causes of paper not feeding can vary by printer type:

- With an inkjet, laser, or impact printer running single-sheet paper, check the paper's positioning in the paper tray. Remove the paper, fan it, and replace it. If the problem continues, check for paper jams. If there are no paper jams, the pickup rollers might be worn out.
- With a printer that uses continuous-feed paper (impact or thermal), check the tension of the feeder rollers or the position and operation of the tractor-feed mechanism.

## **Paper Jams**

A paper jam can have a variety of causes, depending on the printer type. Use the following sections to solve paper jams.

## **Paper Path Issues**

The more turns the paper must pass through during the printing process, the greater the chance of paper jams. Curved paper paths are typical of some inkjet printers and many laser printers, as well as dot-matrix printers that use push tractors: The paper is pulled from the front of the printer, pulled through and around a series of rollers inside the printer during the print process, and then ejected through the front or top of the printer onto a paper tray. Because the cross-

section of this paper path resembles a *C*, this is sometimes referred to as a C-shape paper path.

Some printers, especially those with bottom-mounted paper trays, have more complex paper paths that resemble an *S*.

A straight-through paper path is a typical option on laser printers with a curved paper path. Printers with this feature have a rear paper output tray that can be lowered for use to override the normal top paper output tray. Some printers also have a front paper tray. Use both front and rear trays for a true straight-through path; this is recommended for printing on envelopes, labels, or card stock. Inkjet printers with input paper trays at the rear of the printer and an output tray at the front also use this method, or a variation in which the paper path resembles a flattened V.

## **Paper Loading, Paper Type, and Media Thickness Issues**

Paper jams can be caused by incorrect paper-loading procedures, an overloaded input tray, or use of paper or card stock that is thicker than the recommended type for the printer. If the printer jams, open the exit cover or front cover and remove the paper tray(s) as needed to clear the jam.

## **Media Caught Inside the Printer**

If paper, labels, envelopes, or transparencies come apart or tear inside a printer, you must remove all the debris, to avoid additional paper jams. Do not try to use creased media because it increases the likelihood of a paper jam. However, if paper jams continue to happen, check the paper feed or paper tray operation.

Avoid using paper with damaged edges or damp paper, which can cause paper jams and lead to poor-quality printing.

## **TIP**

When you insert a stack of sheet paper into any type of printer, be sure to fan the pages before you insert the paper into the tray, to prevent sticking.

## **Multipage Misfeed**

When a printer grabs more than one page at a time to feed into the printer, the fix could be as simple as removing the paper and reloading it. While doing so, check that the paper width guides are correct and are not causing the paper to stack too tightly.

If the printer has had a lot of use, the print rollers might have worn smooth and are not engaging the paper correctly. If this is the case, replacing the rollers is the solution.

## **Garbled Print**

Garbled print on paper (that is, gibberish printing) can occur for several reasons. First check the printer driver: If the printer driver files are corrupted or the incorrect printer driver has been selected for a printer, gibberish printing is a likely result.

If you can use a printer in an emulation mode or change it to use a different printer language with a personality module or DIMM (for example, a special Postscript DIMM can be used in some PCL-language laser printers), be sure that you have correctly configured the printer and the printer driver or installed a new printer driver.

A parallel printer cable that fails can also cause this type of problem.

## **Vertical Lines on Page**

Vertical lines on pages printed with a laser printer can be caused by debris stuck to the imaging drum, surface damage to the imaging

drum, or dirty components in the printer (fuser, paper rollers, charging rollers, and so on). To determine which component is the cause, compare the distance between marks on the paper with the circumference of each component. The printer's manual provides this information. Replace the imaging drum (which is part of the toner cartridge on many printer models) if the drum is at fault. Clean other components if they are at fault, and retest.

Vertical lines on a page printed with an inkjet printer are usually caused by ink on a feed roller. Clean the feed rollers; if the problem persists, you might have a problem with a leaky ink cartridge.

Vertical lines in thermal printer output can be caused by a dirty heating element or by the failure of part of the heating element. Angled streaks can be caused by a creased ribbon. To solve this problem, adjust the ribbon feed mechanism.

Vertical lines on impact printer output usually indicate dirt on the paper. Replace the paper.

## Multiple Prints Pending in a Queue



The Windows print spooler manages and maintains print jobs. It switches to offline mode if the printer goes offline, is turned off, or has stopped for some other reason (such as a paper jam or loss of connection to the network). Print jobs are sent to the print queue, but a backed-up print queue fills up until the print jobs are dealt with. After the printer goes online, you can release the print jobs. You can also kill all print jobs or kill only selected print jobs.

To access the print queue, open the Printer icon in the notification area, or go to Printers or Devices and Printers and open the printer icon.

## **Releasing a Print Queue**

To release print jobs stored in the queue in offline mode after the printer is available, use one of these methods:

**Step 1.** Open the print queue.

**Step 2.** Open the **Printer** menu.

**Step 3.** Click the **Use Printer Offline** toggle. The print jobs then go to the printer.

## **Clearing Select Print Jobs or All Print Jobs in a Queue**

You might need to clear a print queue for a variety of reasons:

- The wrong options are selected for the installed paper.
- Gibberish printing occurs because of a problem with the printer driver, cable, or port.
- You decide not to print the queued documents.

You can clear selected print jobs or all print jobs in a queue. To discard a print job in the print queue, follow these steps:

**Step 1.** Open the print queue.

**Step 2.** Right-click the print job you want to discard.

**Step 3.** Select **Cancel Print**. The print job is discarded.

To discard all print jobs in the queue, follow these steps:

**Step 1.** Open the print queue.

**Step 2.** Right-click **Printer**.

**Step 3.** Click **Cancel All Documents** (or a similar option, depending on the Windows version) to discard all print jobs.

## Speckling on Printed Pages



When printed pages have dots, spots, or speckles on them, some dirt or other residue likely is sticking to the drum and collecting toner dust in error. To see if this is the case, try cleaning the dust from the drum by running a dozen blank copies. If the last few copies are, literally, spotless, the problem might be solved. If the output is better but not completely clean, try another few sheets to see if it improves.

Another possibility is a problem in the cartridge. If a pattern of spots is repeated every inch or two on the page, the bar in the cartridge might need cleaning. You might be able to do this, but the process requires a specialized toner vacuum for the fine particles of toner, along with gloves, a mask, and isopropyl alcohol. Check the manufacturer's support page to see if the cartridge can be returned for replacement or for instructions on how to clean. Do not try to clean the cartridge with a regular vacuum or with regular rubbing alcohol because these approaches will not work safely.

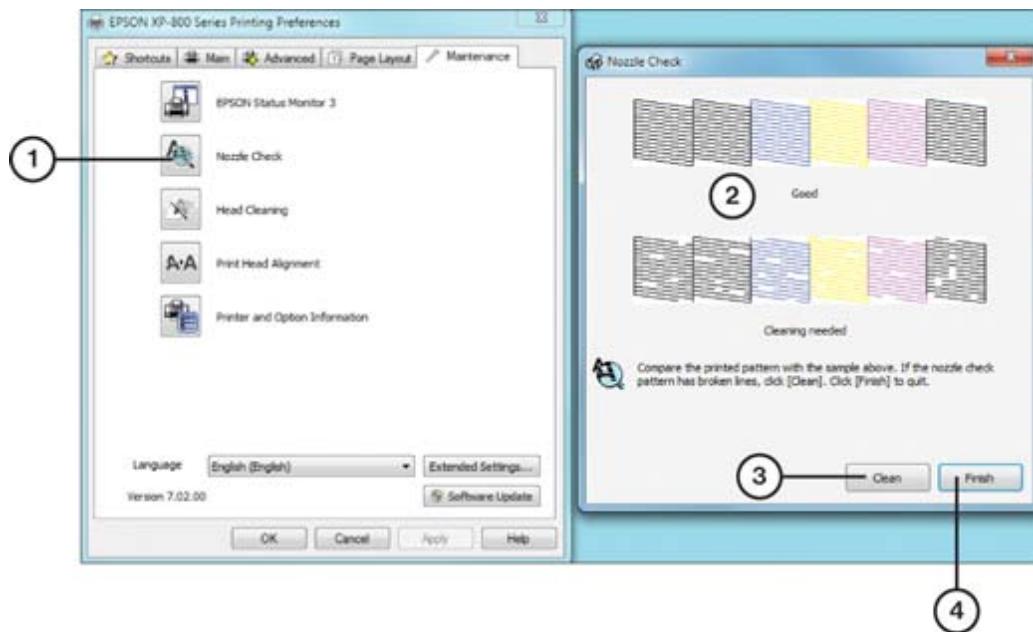
## Incorrect Chroma Display



*Chroma* refers to the amount and intensity of color in prints. A clogged printhead can impact chroma quality in print jobs on a color inkjet printer. On a color laser, check for low color toner or an empty color toner cartridge.

Inkjet manufacturers such as Epson and Cannon have a Windows interface for managing many printer functions. For Epson inkjet printers on Windows systems, use the Maintenance tab of the

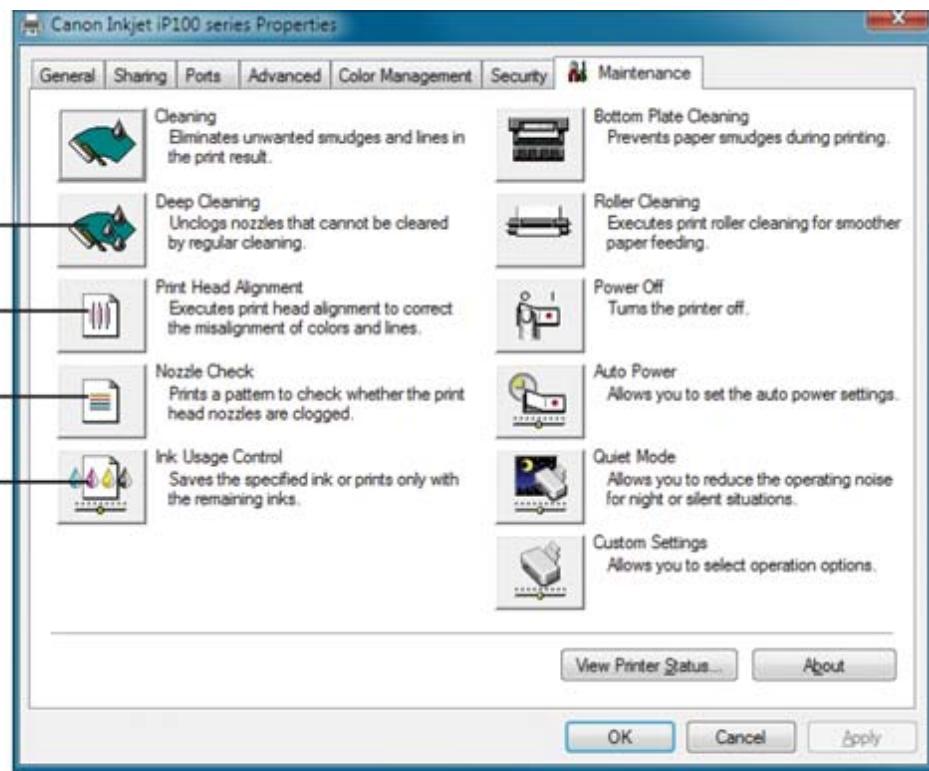
printing preferences sheet (see [Figure 5-18](#)) to check ink levels, clean and align print heads, and check nozzles for clogs.



1. Click to start Nozzle Check
2. Compare printout with these examples
3. Click to clean printheads
4. Click when Nozzle Check results are satisfactory

**Figure 5-18** Using the Nozzle Check Option on an Epson Inkjet Printer

For Canon inkjet printers on Windows systems, use the Maintenance tab of the printing preferences sheet (see [Figure 5-19](#)) to clean and align print heads, check nozzles for clogs, clean the bottom plate and rollers, and configure ink usage.



1. Click to clean print heads
2. Click to deep clean print heads
3. Click to align printheads
4. Click to run Nozzle Check

**Figure 5-19** The Maintenance Tab for a Canon Inkjet Printer Driver

If the print colors are close but not exactly what is wanted on a color photograph or a document with colored graphics or text, you need to set up color management on the printer and the display(s) used to edit the document.

## Grinding Noise

Printers vary in their complexity and the number of moving parts. The reasons for grinding noises can vary greatly, from physical issues to firmware problems. The more likely culprit is something changes after an event, such as paper loading or a cartridge change, and that during that process, something loosens or otherwise comes out of adjustment.

If the grinding noise is accompanied by error codes, the troubleshooting should be easier. Paper jams and ink or toner cartridge problems usually have codes to point directly to the problem. Each printer brand has its own codes, so access to documentation is necessary; this is generally available online.

## Finishing Issues

More expensive printers in larger offices have collating, stapling, and hole-punching capabilities. These features increase the complexity in both the mechanics and the drivers of the printer. However, the most common problems in stapling and hole punching in advanced printers are about the same as the problems that arise when doing these tasks by hand—namely, staple jams and incomplete hole punches.

Stapling issues can occur if there are problems earlier in the printing process, such as creased paper or curled ends of paper that can cause staples to jam. The whole process stops until the staples are taken out, reloaded, and replaced. Making sure that an ample staple supply is in the cartridges is important as well.

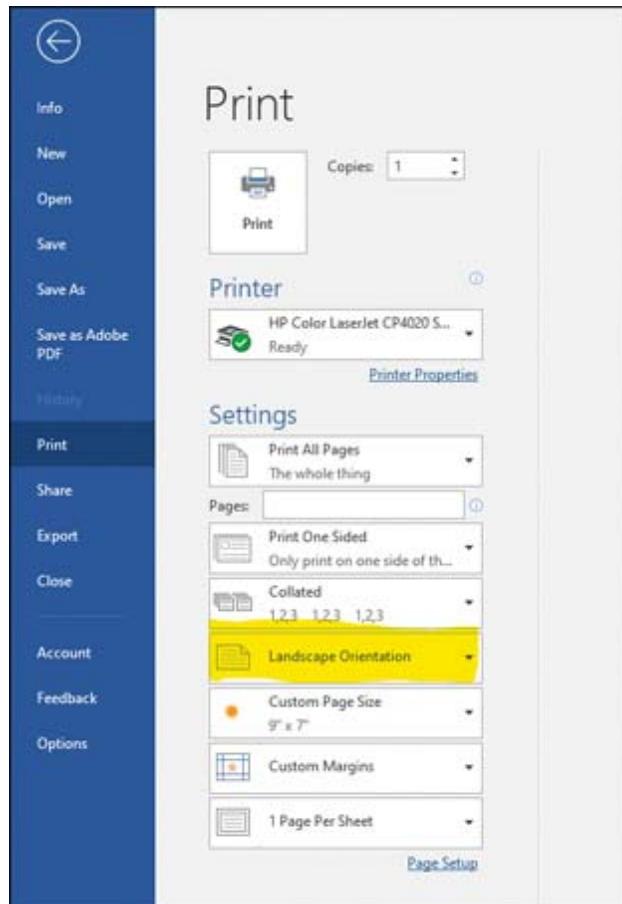
Hole punching requires manual upkeep too. The main reason for poor hole punching is that the trays for the punched holes overfill and restrict the punches from completing the job. Constant maintenance for these added features is necessary.

## Incorrect Page Orientation



When print output is turned sideways from what is expected, it is likely because the wrong orientation was selected in the software. The common choices are portrait (vertically taller) and landscape (horizontally wider), with the taller option common for printed pages and the wider option used for spreadsheets.

If the orientation is wrong, find the print settings menu for the job and change it. Each application's settings vary somewhat, but the setting is in the Print menu where the printer is selected. [Figure 5-20](#) depicts the orientation selection in the Word Print menu.



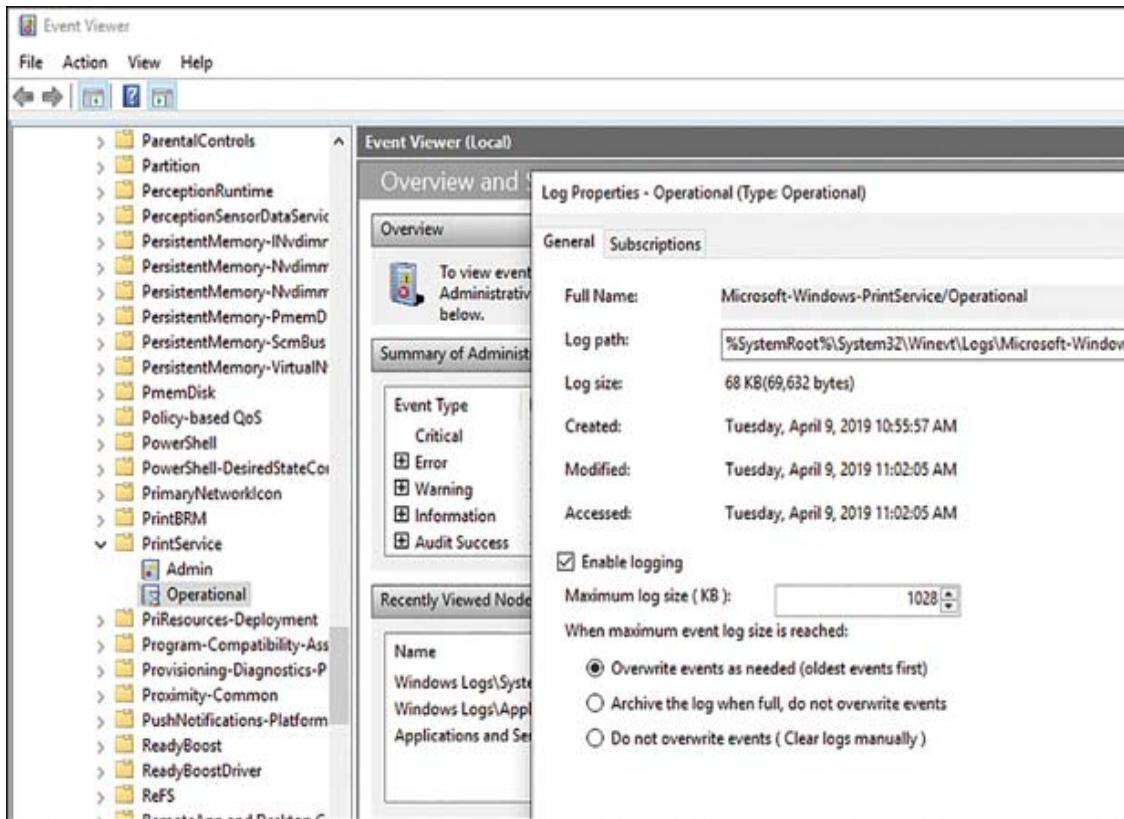
**Figure 5-20** The Orientation Setting in a Word Print Menu

## Print Logs

Print jobs on a network can be tracked by enabling print logs in Windows 10. With this feature enabled, a print job on a network can be tracked in the Print Services section of the Event Viewer.

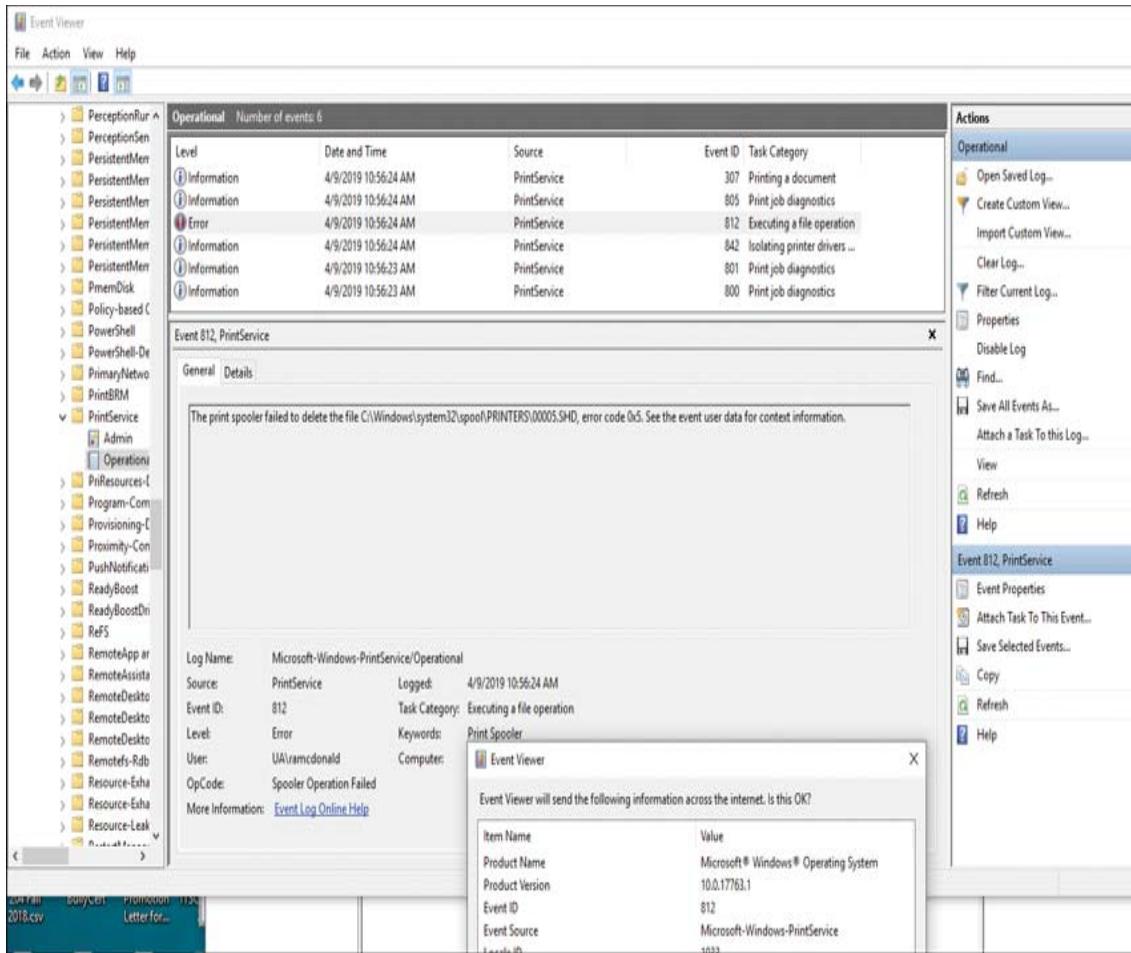
To enable the logging service, search for the Event Viewer and open it. In the left pane, expand **Application and Services Logs > Microsoft > Windows > PrintService**. To enable print logs, right-

click Operational and, from the context menu, select Properties. Then check the Enable Logging box. [Figure 5-21](#) depicts the process.



**Figure 5-21** Enabling Printer Logs in Windows 10

When they are operational, the logs can be used to evaluate errors. [Figure 5-22](#) shows an example of an error in a print log. The highlighted error indicates a problem with the print spooler.



**Figure 5-22** Print Log Error

Third-party print server software usually has a print logging feature that can assist with troubleshooting. Check with the developers' instructions for the best way to track jobs in the application.

## Network Troubleshooting



**220-1101: Objective 5.7:** Given a scenario, troubleshoot problems with wired and wireless networks.

Most computing devices that an IT professional encounters are connected to a network. The common network issues discussed in

the following sections are essential knowledge for an IT professional. Understanding the problems and solutions is important for the 220-1101 exam and to aid in your ongoing work.

## No Connectivity

For no connectivity errors, do the following:



- Check the power supply going to the hub, switch, wireless access point, or router. Reset the device.
- Isolate the problem. If only the users connected to a new switch that is connected to an existing switch lose their network connection, check the connection between the existing switch and the new one to make sure they are plugged into similar ports. Most switches have an uplink port that is used to connect an additional switch, and this is the best way to establish a reliable connection.
- If the uplink port appears to be connected properly, check the cable. Uplink ports perform the crossover for the user, enabling you to use an ordinary network cable to add a hub or switch.

### TIP

If you use a crossover cable, you must connect the new hub or switch through a regular port, not through the uplink port.

## External Interference and Intermittent Wireless Connectivity

Intermittent connectivity can be caused by the following:



- **Dead spots (poor signal) on a wireless network:** Relocate the wireless router.
- **Too many networks using the same channel:** Use a wireless network scanning device or app to see local wireless networks and their channels. Reconfigure the network to use a channel with less traffic.
- **EMI or RFI interference with the wired network:** Alarm systems, elevators, fluorescent lights, and motors can interfere with networks running UTP. Switch to STP cable or relocate cables away from interference.
- **A defective network cable, such as a cracked outer jacket or a broken locking tab:** Replace the cable.
- **Problems with the ISP's Internet service:** If the problem persists after you troubleshoot the local network, contact the ISP.

## Slow Network Speeds

Significant drops in network performance and slow transfer speeds can be traced to a variety of causes:



- **Damage to cables, connectors, hubs, switches, and routers:** Check the cables for damage.
- **Connecting high-speed NICs to low-speed switches:** When using Gigabit Ethernet switches and routers, confirm that all devices on the network (switches, router, cables, and NICs) meet Gigabit Ethernet standards (CAT 5e, 6, 6a, or 7 cable) and are configured to use Gigabit Ethernet.

- **High Internet Demand:** Fast local connections but sluggish Internet connections can be caused by too much demand for the Internet connection (perhaps due to multiple downloads or streaming services) or Internet congestion outside the home or office.
- **RFI/EMI interference with wireless networks:** Check wireless phones and microwave ovens to see if their use interferes with the network. Move the router away from interference sources. Switch to a wireless 802.11ac router and NICs, and use the 5GHz band to avoid most of this type of interference. 802.11ax, which is known as Wi-Fi 6, will broadcast at 2.4GHz or 5GHz and, when authorized by governments, in the 6GHz range. It is in beta testing and will become the standard over the next few years.

## Limited Connectivity

A low signal on a wireless network can be caused by the following:



- **Interference from other wireless networks:** Use a wireless network analyzer to determine the least-used channels for the network, and switch to one of those channels.
- **Concrete or masonry walls in the building:** If relocating the router is not possible, add another wireless access point (WAP) in places that can broadcast around obstacles.
- **Repeaters:** In residential construction, consider using powerline repeaters.
- **Improper antenna positioning on the router or NICs with adjustable antennas:** Follow manufacturer recommendations.

- **A router or NICs that do not support MU-MIMO**

**antennas:** Multiuser Multiple Input Multiple Output (MU-MIMO) enables a router to make MIMO connections to multiple users at the same time. MU-MIMO requires routers and client device support, but it can be implemented on client devices that have only a single antenna each. These devices are increasingly common, and prices are falling. With so many wireless devices in homes and businesses competing for wireless bandwidth, a MU-MIMO solution could inexpensively double the speed of downstream traffic on a network.

## Latency and Jitter



All networks experience a certain amount of data delay, called latency, which is the time it takes to get a packet of data through the devices between the sender and the receiver. Latency is normal, and networks are designed to accept a certain amount of it on a consistent level. **High latency** can be caused by router overloads or high demand on a key bottleneck of a network. Network designers know that a certain amount of latency will always exist on a network, but they try to keep it as small as their network devices will allow. Network latency problems can usually be traced to a networking device, such as a router or a switch.

Network **jitter** is the presence of variations of a network's latency. Jitter can cause problems for end users on a network. Slow web page loading in browsers and faulty speech in conversations are some of the most noticeable problems.

Jitter is usually caused by too much demand for bandwidth. This can be caused by too many users on a small network, such as in a crowded coffee shop or event space with many devices accessing the network), or by even a few people demanding too much data (say, an uncrowded coffee shop with all patrons trying to stream videos).

Either way, the network cannot process all the data. Ways to mitigate jitter can be built into the network in these ways:

- Limiting the number of connections on a Wi-Fi channel
- Limiting the number of users on the Wi-Fi network, to keep the access point from being overworked
- Limiting devices that require large data flows to wired connections (not on the wireless network)
- Blocking gaming and movies, if appropriate
- Putting voice traffic on a different network segment

## Poor Voice over Internet Protocol (VoIP) Quality

Voice over Internet Protocol (VoIP) traffic is different from most other network traffic because it must be received in the exact order it was sent to make sense. VoIP is greatly affected by excessive latency and jitter. Poor network quality means that some parts of the conversation arrive out of sequence, causing confusion and frustration, so the quality of the connection must be without jitter. Advanced network configuration allows for VoIP to be prioritized over other traffic.

The best way to ensure that VoIP is stable and high quality is to keep it on a separate local network from regular data. By configuring the router to prioritize VoIP, traffic voice conversations remain reliable and clear.

## Port Flapping

**Port flapping** occurs when the physical port on a device turns on and off intermittently, usually very rapidly. Several network configuration issues cause this and are beyond the scope of the A+

exam. However, sometimes flapping can be a very simple problem, such as a worn or loose cable.

The obvious symptom of flapping is slowed network response as several packets of information get dropped and need to be re-sent. This causes even more congestion, and sometimes the link simply appears to go down because it cannot keep up with traffic. If this is the case, change to a different switch port, if possible. Check the cable, too; sometimes a connection fails because a cable was pulled or twisted and no longer connects properly.

## Exam Preparation Tasks

As mentioned in the Introduction, you have several choices for exam preparation: the exercises here; [Chapter 10, “Final Preparation”](#); and the exam simulation questions in the Pearson Test Prep practice test software.

## Review All the Key Topics

Review the most important topics in the chapter, noted with the Key Topic icon in the outer margin of the page. [Table 5-5](#) lists these key topics and the page number on which each is found.



**Table 5-5** Key Topics for [Chapter 5](#)

Key Topic Element	Description	Page Number
<a href="#">Table 5-2</a>	The Six-Step CompTIA Troubleshooting Methodology	353
<a href="#">Table 5-3</a>	Common System Errors and Their Beep Codes	356

<b>Key Topic Element</b>	<b>Description</b>	<b>Page Number</b>
List	Causes of BSOD errors	358
List	Resolving BSOD errors	359
List	Causes of macOS unresponsiveness	361
List	Black screen	361
List	Overheating issues	364
List	Dirt and Dust	368
List	Sluggish performance	371
List	Investigating smoke or burning smells	372
Steps	Step-by-step power supply troubleshooting	374
Steps	Resolving intermittent shutdown	376
Section	Application Crashes	376
<b>Figure 5-10</b>	Windows 10 Event Viewer	377
Section	Read/Write Failure	382
List	Improving performance with SATA hard disks	382
List	Causes for failure to boot	385
Section	Bootable Device Not Found	385
Section	RAID Failure	388
List	Items monitored by S.M.A.R.T.	389
Section	Missing Drives in OS	390
List	Projector overheat shutdown	394
List	Resolving incorrect color display issues	395

<b>Key Topic Element</b>	<b>Description</b>	<b>Page Number</b>
List	Resolving dim image issues	395
List	Resolving flashing screen issues	396
Section	Display Burn-in	397
List	Resolving the issue of a battery not charging on tablets/smartphones	399
Section	Poor/No Connectivity	401
Section	Nonresponsive Touchscreen	403
List	Steps to enable protection from mobile malware	404
Section	Lines Down the Printed Pages	405
Section	Faded Prints	406
Section	Multiple Prints Pending in a Queue	410
Section	Speckling on Printed Pages	411
Section	Incorrect Chroma Display	412
Section	Incorrect Page Orientation	414
List	Resolving network connectivity issues	417
List	Causes of intermittent connectivity in wireless networks	417
List	Investigating slow transfer speeds in networks	418
List	Causes of limited connectivity in wireless networks	418
Section	Latency and Jitter	419

**Complete the Tables and Lists from Memory**

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

## Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

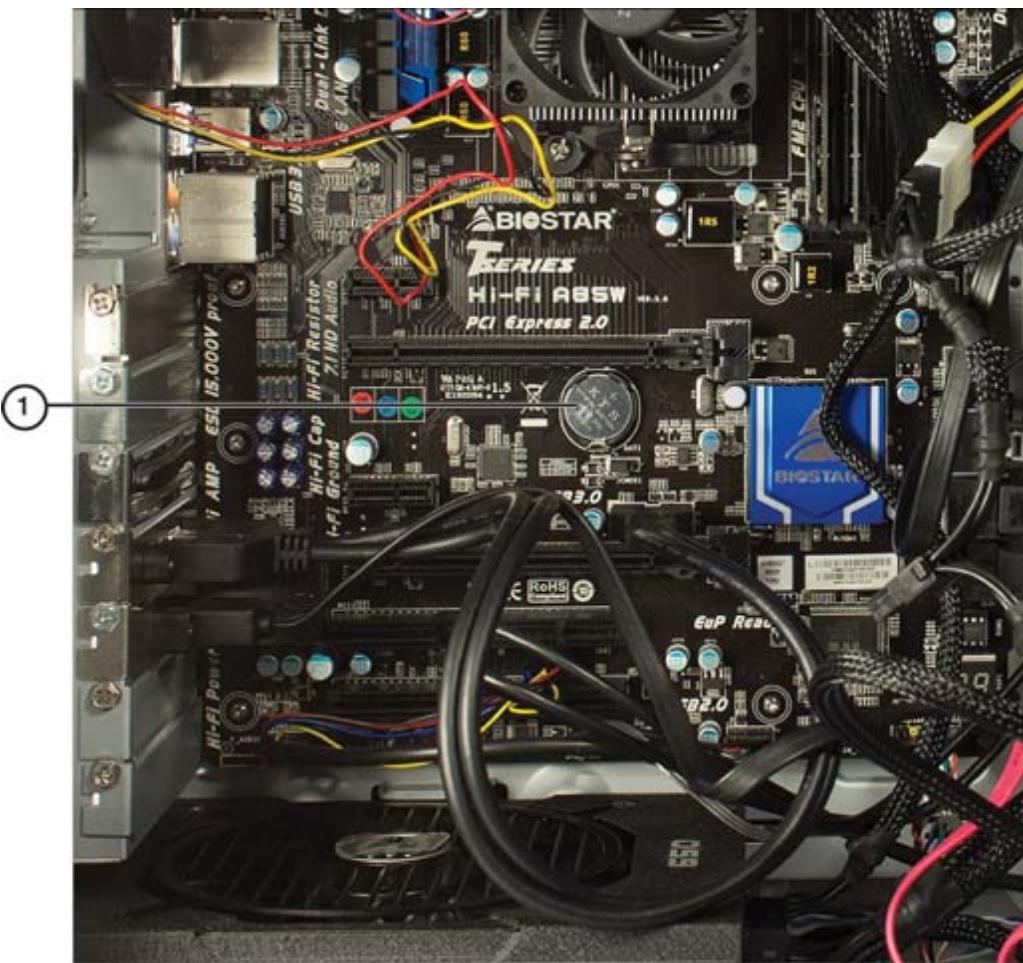
power-on self-test (POST) code beeps  
STOP errors  
blue screen of death (BSOD)  
pinwheel  
black screen  
negative pressure  
power supply tester  
continuous reboot  
distended capacitors  
capacitor swelling  
light-emitting diode (LED) status indicators  
read/write failure  
SATA  
RAID  
Self-Monitoring, Analysis, and Reporting Technology (S.M.A.R.T.)  
input/output operations per second (IOPS)  
digitizer  
cursor drift  
toner  
high latency  
jitter  
port flapping

## **Answer Review Questions**

- 1.** Your system has begun shutting down suddenly and unexpectedly. Which of the following best describes how to determine whether the cause of these shutdowns is due to the CPU overheating?
  - a.** Check the CPU temperature in the Device Manager.
  - b.** Check the CPU temperature in the System Properties.
  - c.** Check the CPU temperature in Computer Management.
  - d.** Check the CPU temperature in the system BIOS/UEFI firmware.
- 2.** Which of the following best describes the usual cause of a checksum error?
  - a.** A failing CMOS battery
  - b.** A corrupt BIOS or UEFI
  - c.** An error within the system's arithmetic calculator
  - d.** Overheating due to overclocking
- 3.** Which of the following is usually checked by POST? (Choose all that apply.)
  - a.** Memory
  - b.** Keyboard
  - c.** Mouse
  - d.** Hard drives
- 4.** When the date and time on your computer are running slowly and losing time, which of the following statements best describes the most likely cause and the most effective course of action?
  - a.** There is a fault in the BIOS settings. You should flash the BIOS.

- b.** The CPU is running slowly. You should check the CPU and its fan to see if dust is clogging it and slowing it down.
- c.** At least one of the memory modules could be faulty. You should check the memory information in the BIOS and replace any failing modules.
- d.** The CMOS battery is failing. You should replace the battery.

**5.** Which component is indicated in the following figure?



- a.** CPU
- b.** CMOS battery
- c.** Capacitor
- d.** BIOS chip

- 6.** If your system is experiencing frequent STOP errors and is automatically rebooting each time, where do you go to change the configuration setting to stop the automatic reboot process?
- a. System Properties, Advanced tab, Startup and Recovery
  - b. Drive Properties, Tools tab
  - c. Administrative Tools, Disk Management
  - d. BIOS, Boot tab, Automatic Reboot
- 7.** Which voltage is used by most personal computers in North America?
- a. 115V
  - b. 190V
  - c. 230V
  - d. 400V
- 8.** Identify the motherboard components indicated in the following figure.
- 
- a. CMOS batteries
  - b. Resistors
  - c. Jumpers
  - d. Capacitors
- 9.** You are called to an employee workstation, where it is reported that the network connectivity has failed. At some point in the process, you decide to replace the workstation Ethernet cable with one in your bag that you know to be good. Which step does

this demonstrate in the best practice methodology to resolve problems?

- a. Identify the problem.
  - b. Establish a theory of probable cause.
  - c. Test the theory to determine the cause.
  - d. Establish a plan of action.
- 10.** You have received a support call from an employee whose mouse does not work upon booting. When you ask the user whether the monitor is on and whether the keyboard is also disabled, which step does this demonstrate in the best practice methodology to resolve problems?
- a. Identify the problem.
  - b. Establish a theory of probable cause.
  - c. Test the theory to determine the cause.
  - d. Establish a plan of action.
- 11.** What is the purpose of the jumper shown in the following figure?



- a. It protects the prongs inside the connector.
- b. It moves the SATA drive to the first position in the boot sequence.
- c. It is used by RAID to configure a mirrored array.
- d. It slows SATA drive performance.

- 12.** Which of the following statements best describes how to change the boot sequence?
- a. Edit the BIOS and save the changes in CMOS.
  - b. Change the jumper settings on the SATA drive to make it the bootable drive.
  - c. Reconfigure settings for the RAID array to make a RAID drive the bootable drive.
  - d. Use the Disk Management utility in Administrative Tools.
- 13.** S.M.A.R.T. detects and reports errors for which of the following?
- a. CPUs
  - b. DDR memory
  - c. SATA and PATA hard drives
  - d. Expansion cards
- 14.** You have been asked to replace a switch in a wiring closet with an upgraded switch. Unexpectedly, it takes you about 2 hours using a tone generator to determine where the cables map to in the old switch before you can uninstall it. Which step in the best practice methodology to resolve problems is missing from this scenario and could have saved 2 hours?
- a. The first
  - b. The third
  - c. The fifth
  - d. The last
- 15.** A flickering image on an LCD display might be caused by the failure of which components? (Choose two.)
- a. Backlight
  - b. Cathode ray tube
  - c. Reflector
  - d. Inverter

- 16.** Burn-in refers to which of the following?
- a. The process of recording a CD or DVD
  - b. The process of preparing a hard drive for formatting for a clean installation
  - c. A persistent ghost image on the display screen
  - d. The damaged areas in a plasma display
- 17.** Your client reports that computers on the network cannot connect to the Internet but can connect to each other. You determine that each of the computers affected has been assigned an APIPA address. At step 2 of the best practice methodology to resolve problems, where do you look next to solve the problem?
- a. DNS
  - b. DHCP
  - c. Proxy
  - d. Router
- 18.** Which step of the best practice methodology to resolve problems is out of order?
- a. Establish a theory of probable cause.
  - b. Establish a plan of action to resolve the problem and implement a solution.
  - c. Test the theory to determine the cause.
  - d. Verify full system functionality.
- 19.** Which of the following does not apply to the first step of the best practice methodology to resolve problems?
- a. Inquiring regarding environmental changes
  - b. Inquiring regarding infrastructure changes
  - c. Performing backups
  - d. Documenting outcomes

- 20.** When your tablet or smartphone does not get a clear cellular signal, which of the following steps could improve the signal? (Choose two.)
- a. Turn off Wi-Fi.
  - b. Change the angle of your screen.
  - c. Reset your cellular settings to a faster 802.11 specification.
  - d. Use the slider switch on an iOS device to fine-tune reception.
- 21.** Which of the following steps could help increase the battery life on your mobile devices? (Choose two.)
- a. Do not overcharge.
  - b. On iOS, turn on the background app refresh.
  - c. Use the iOS slider switch to shut down weekly.
  - d. Wait until the device is almost out of power before recharging it.
- 22.** Vertical streaks extending down each page printed by a laser printer usually indicate which of the following problems?
- a. Low toner
  - b. A dirty print ribbon
  - c. Damaged ink nozzles
  - d. Damage to the imaging drum
- 23.** Smudged print from an inkjet printer could be caused by which of the following?
- a. Dirty printheads or rollers
  - b. Failure of the fuser to reach a high enough temperature
  - c. Photosensitive drum not being properly charged
  - d. Toner cartridge needing to be replaced
- 24.** If toner can be brushed off the page after printing, which component of a laser printer is malfunctioning?

- a. Print drum
  - b. Fuser
  - c. Paper-feed rollers
  - d. Corona
- 25. If a document requires the maximum amount of memory that is available to a laser printer, the printer might attempt to compress the document. Which of the following statements best describes the result of this compression on the final print page?
  - a. Some text could be lost.
  - b. The printed text might be cloudy.
  - c. The print process will be slower.
  - d. Some pictures could be deleted.
- 26. Which of the following print tools is used to manage and maintain print jobs?
  - a. Print spooler
  - b. Fuser
  - c. Printheads
  - d. XPS Document Writer

## **Part II: Core 2**

# Chapter 6

## Operating Systems

**This chapter covers the 11 A+ 220-1102 exam objectives related to operating systems, with a focus on the features, tools, versions, command-line tools, and configuration and installation of Microsoft Windows, as well as macOS and Linux operating systems. These objectives may comprise 31 percent of the exam questions:**

- **Core 2 (220-1102): Objective 1.1:** Identify basic features of Microsoft Windows editions.
- **Core 2 (220-1102): Objective 1.2:** Given a scenario, use the appropriate Microsoft command-line tool.
- **Core 2 (220-1102): Objective 1.3:** Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS).
- **Core 2 (220-1102): Objective 1.4:** Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility.
- **Core 2 (220-1102): Objective 1.5:** Given a scenario, use the appropriate Windows settings.
- **Core 2 (220-1102): Objective 1.6:** Given a scenario, configure Microsoft Windows networking features on a client/desktop.
- **Core 2 (220-1102): Objective 1.7:** Given a scenario, apply application installation and configuration concepts.
- **Core 2 (220-1102): Objective 1.8:** Explain common OS types and their purposes.
- **Core 2 (220-1102): Objective 1.9:** Given a scenario, perform OS installations and upgrades in a diverse OS environment.
- **Core 2 (220-1102): Objective 1.10:** Identify common features and tools of the macOS/desktop OS.

- **Core 2 (220-1102): Objective 1.11:** Identify common features and tools of the Linux client/desktop OS.

Many Windows versions have been used over the years, each bringing changes to features and appearances, but all the versions have used similar installation methods. For the 220-1102 A+ exam, the focus is on Windows 10, with previous versions being deprecated to legacy status. Windows 11 is not specifically mentioned in the objectives, although future editions of exam questions may refer to it. As noted in the A+ exam objectives:

Versions of Microsoft Windows that are not end of Mainstream Support (as determined by Microsoft), up to and including Windows 11, are intended content areas of the certification. As such, objectives in which a specific version of Microsoft Windows is not indicated in the main objective title can include content related to Windows 10 and Windows 11, as it relates to the job role.

Nonetheless, a description of key differences between Windows 10 and 11 is warranted and is included in this chapter.

In this chapter, you are introduced to the features and many options available both for installing Windows 10 on individual systems and for deployment to multiple computers. The chapter also covers some of the important macOS and Linux features and tools.

## “Do I Know This Already?” Quiz

The “Do I Know This Already?” quiz allows you to assess whether you need to read the entire chapter. [Table 6-1](#) lists both the major headings in this chapter and the “Do I Know This Already?” quiz questions covering the material in those headings so that you can assess your knowledge of these specific areas. The answers to the “Do I Know This Already?” quiz appear in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes and Review Questions.”

**Table 6-1** “Do I Know This Already?” Section-to-Question Mapping

Foundation Topics Section	Questions
Basic Features of Microsoft Windows Editions	1
Microsoft Command-Line Tools	2, 4

<b>Foundation Topics Section</b>	<b>Questions</b>
Microsoft Windows 10 Operating System (OS) Features and Tools	3
Windows 10 Control Panel Utilities	5, 6
Windows Settings	5
Windows Networking Features on a Client/Desktop	7
Installation and Configuration Concepts	8
Understanding Common OS Types	1
OS Installations and Upgrades in a Diverse OS Environment	9
Common Features and Tools of the macOS/Desktop OS	9, 10
Common Features and Tools of the Linux Client/Desktop OS	9

## CAUTION

The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for the purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

**1.** Which is true of FAT32?

- a.** It uses file permissions.
- b.** It has a max file size of 8GB.
- c.** Corrupt files can be repaired.
- d.** It works in macOS computers.

**2.** Which of the following are command-line tools in Windows 10?  
(Choose all that apply.)

- a.** Pages
- b.** Command Prompt App

- c. PowerShell
  - d. Winscript Manager
- 3. Which operation requires the help of a utility such as Microsoft Deployment Toolkit?
  - a. Network installation
  - b. Multiboot installation
  - c. Unattended installation
  - d. Clean installation
- 4. What is the name of the mode you enter when you run the command prompt as an administrator?
  - a. Supervisor mode
  - b. Elevated mode
  - c. Power mode
  - d. Action mode
- 5. Which of the following is not a Microsoft administrative tool?
  - a. Performance Monitor
  - b. RAM Optimizer
  - c. Task Scheduler
  - d. Print Management
- 6. Which of the following are Control Panel utilities? (Choose all that apply.)
  - a. System
  - b. Internet Options
  - c. Devices and Printers
  - d. User Accounts
- 7. What is the name of the process that involves making a shared folder accessible by selecting a drive letter on a client computer?
  - a. Tunneling
  - b. Share pointing
  - c. Mapping
  - d. Navigating

- 8.** Which two tasks are configured in the network card properties settings? (Choose two.)
- a. Half-duplex or full duplex
  - b. Wake-on-LAN
  - c. Firewall exceptions
  - d. VPN access
- 9.** When an app is not working and cannot be closed properly, what commands can you use to end the app in macOS and in Linux? (Choose one for each operating system.)
- a. terminate
  - b. Force Quit
  - c. kill
  - d. expire
- 10.** What is Time Machine?
- a. A clocking utility that is new to Windows 10
  - b. A backup utility in Linux
  - c. A macOS backup utility
  - d. A backup utility that is new to Windows 10

## Foundation Topics

### Basic Features of Microsoft Windows Editions



**220-1102: Objective 1.1:** Identify basic features of Microsoft Windows Editions.

Windows 11 was launched in the second half of 2021 as a way for Windows users to access Microsoft services and products with a higher level of general performance. Although the user experience is visually different and the network experience is more seamless, most of the core functions

settings are similar, if not the same. Knowing the Windows 10 OS is key to understanding the foundations of Windows 11.

## Windows 10 Editions

Windows 10 and 11 are the **current standard** for Microsoft operating systems. Four versions of Windows 10 are described in this section:

- **Windows 10 Home:** This is the most basic desktop version, with features that most home users need. It is capable of joining a small home workgroup and sharing resources such as printers, but it is not able to join large workplace-managed domains. Windows 10 Home is most commonly found preinstalled through an Original Equipment Manufacturer (OEM), such as Dell or HP.
- **Windows 10 Pro:** Pro is the most different version of the many Windows versions. Pro has all the features of Home, along with added security and management features found on institutional networks. These include Active Directory for network management, BitLocker, and Remote Desktop. As with Home, Windows 10 Pro can be shipped through OEMs.
- **Windows 10 Pro for Workstations:** The key differences between Pro and Pro for Workstations lie in robustness and licensing. Pro for Workstations is designed to work with high-powered computers with advanced chipsets that can handle heavy processing loads. Instead of using an OEM install, licensing must be purchased from Microsoft.
- **Windows 10 Enterprise:** This version of Windows 10 has all the features of the other versions, along with added network management and security tools designed for IT professionals managing enterprise class networks.

Table 6-2 depicts the different versions and the availability of features from the CompTIA A+ Core 2 exam.



**Table 6-2** Windows 10 Editions and Features

<b>Windows 10 Edition:</b>	<b>Home</b>	<b>Pro</b>	<b>Pro for Workstations</b>	<b>Enterprise</b>
<b>Features ↓</b>				
<b>Domain Access vs. Workgroup</b>	Workgroup	Workgroup or domain	Domain	Domain
<b>Desktop Styles/Control</b>	No	No	Yes	Yes
<b>RDP</b>	Client only	Host and client	Host and client	Host and client
<b>Minimum RAM</b>	1GB	2GB	2GB	2GB
<b>BitLocker</b>	No	Yes	Yes	Yes
<b>gpedit.msc</b>	No	Yes	Yes	Yes

## Feature Differences

### Domain Access vs. Workgroup

The key difference between **domain access** and **workgroup** computers is how they are managed. In Windows 10, all computers default to a workgroup until they join a domain. Domain computers are usually workplace computers managed by a network administrator. Workgroup computers are usually home computers that are peers to other computers on a small home network that can share files and printers.

### Desktop Styles/User Interface

Windows 10 versions come with similar interface features, including the Task View option (Windows+Tab, or selecting it from the taskbar). Desktops and wallpaper can be enhanced with Bing Wallpaper, and disability access features are found in both. When the computer comes under the control of a domain, the experience might differ because an administrator can use policies to limit desktops and other features.

## Remote Desktop Connection and Remote Assistance

To facilitate connections to remote computers and allow full remote control, Microsoft uses the Remote Desktop Connection program, which is based on the ***Remote Desktop Protocol (RDP)***.

Remote Desktop also includes Remote Assistance, which allows users to invite a technician to view their desktop, in the hopes that the technician can fix any encountered problems.

## Random Access Memory (RAM)

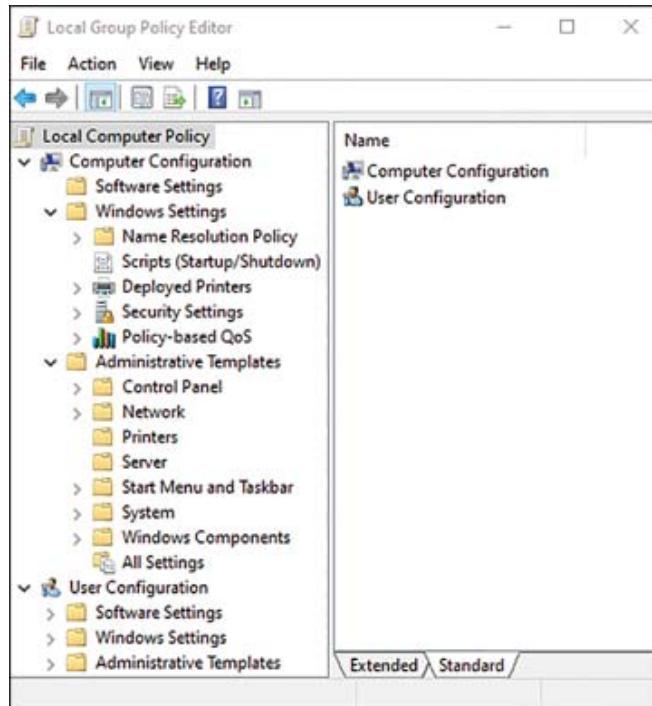
Windows 10 requires 1GB of RAM for a 32-bit installation and 2GB for a 64-bit install. These are minimums; depending on the software installed and the purpose of the computer, more RAM is recommended.

## BitLocker

**BitLocker** is a data encryption utility that encrypts hard drives for added security. It encrypts all data, including personal and system files. A companion program, BitLocker To Go, encrypts removable disks and USB drives. [Chapter 7, “Security,”](#) covers BitLocker and BitLocker To Go.

## Group Policy Editor

Group Policy is a tool for controlling the settings on a standalone computer or a group of networked computers. A network administrator can set and control almost all settings in a network using Active Directory. [Figure 6-1](#) depicts the output from the ***gpedit.msc*** command, showing the Local **Group Policy Editor** on a networked computer. Group Policy Editor is not normally available to the Windows 10 Home user; the command normally returns a “gpedit.msc not found” response. However, users can download unofficial products from non-Microsoft sources and then configure settings management.



**Figure 6-1** Local Group Policy Editor

## Upgrade Paths

**In-place upgrades** involve upgrading Windows editions while keeping user data, applications, and preferences intact. [Table 6-3](#) shows Windows 10 editions and upgrade methods. The older version of Windows 10 OS remains in place, and its installer is used to replace all the OS files for the new edition, leaving applications and other settings.

**Table 6-3** Windows 10 Editions and Supported Upgrade Methods

<b>Windows 10 Edition: - Upgrade Path for:</b>	<b>Command- Line tools</b>	<b>Product Key</b>	<b>Purchase License from Microsoft Store</b>
<b>Home to Pro</b>	no	Yes	Yes
<b>Pro to Pro for Workstations</b>	Yes—no reboot	Yes—no reboot	Yes—no reboot
<b>Pro to Enterprise</b>	Yes—no reboot	Yes—no reboot	No



## Microsoft Command-Line Tools



**220-1102: Objective 1.2:** Given a scenario, use the appropriate Microsoft command-line tool.

Windows has a number of command-line tools for system operation and management. Although it also has many administrative tools that offer graphical interfaces for managing performance and troubleshooting, mastering these commands makes the common tasks much more efficient.

In the last few years, Microsoft had gently nudged the command prompt (cmd.exe) into maintenance mode and replaced it with the more powerful Windows PowerShell command-line environment. CMD.exe is not gone, but it is no longer the default. All the commands in this section work the same in either environment, so if you want to experiment with the CMD prompt, you can simply enter **CMD** into the search bar and it will appear.

### Starting a Command Prompt Session with Windows PowerShell

Most computer users don't use a command-line prompt often. However, technicians use it to do the following:

- Recover data from systems that cannot boot normally
- Reinstall lost or corrupted system files
- Print file listings (which cannot be done in File Explorer or This PC)
- Copy, move, and delete data
- Display or configure certain operating system settings

You can start a command prompt session in Windows by clicking the Windows PowerShell option in the Start menu; however, other methods can be faster. Here are a few easy ones to get started:

- In Windows 10, press Windows+X and then click or tap Windows PowerShell to run in standard mode. An option to run as an administrator is also available.
- Type **PowerShell** in the search bar. The app will appear before you are finished typing.
- Hold the Shift key while right-clicking on the desktop. The PowerShell option appears.

## Commands Available with Standard Privileges vs. Administrative Privileges

Most of the commands in [Table 6-4](#) can be run with *standard privileges* (by any user). However, some commands can be run only with *administrative privileges* in what is known as *elevated mode* or *administrative mode*. Elevated commands can make more operational changes to the PC than basic commands.



**Table 6-4** Windows Command Prompt Commands

Navigation Commands	
<b>cd (chdir)</b>	Changes the working directory (folder).
<b>dir</b>	Displays a list of the current directory and subdirectories.
<b>md (mkdir)</b>	Creates a directory on the drive.
<b>rmdir</b>	Removes an empty directory.
<b>cd ..</b>	Navigates to the previous directory.
C:\ or D:\ or X:\	Takes you to the command prompt of the drive letter.
Command-Line Tools	
<b>ipconfig</b>	C:\Users> <b>ipconfig</b> Displays TCP/IP network configuration information for each network adapter (both physical and virtual) on the device.

---

## Navigation Commands

---

**ping** Sends IP packets to check network connectivity:  
C:\Users>**ping cisco.com**  
(reply follows)  
Pinging cisco.com [2001:420:1101:1::185] with 32 bytes of data:  
Reply from 2001:420:1101:1::185: time=64ms  
Reply from 2001:420:1101:1::185: time=65ms  
Reply from 2001:420:1101:1::185: time=65ms  
Reply from 2001:420:1101:1::185: time=69ms  
  
Ping statistics for 2001:420:1101:1::185:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli seconds:  
Minimum = 64ms, Maximum = 69ms, Average = 65ms

---

**hostname** Returns the computer name of the local device.  
C:\Users>**hostname**  
PC of RMcD

---

**netstat** Displays a list of active TCP connections on a local network.  
C:\Users>**netstat**  
  
Active Connections  
Protocol Local Address      Foreign Address      State  
TCP 10.0.0.34:49554 12.64.180.116:https ESTABLISHED  
(example output; Several lines omitted here)

---

**nslookup** Gathers the network's Domain Name System (DNS) information.  
C:\Users>**nslookup**  
Default Server: cdns01.ISPprovider.net  
Address: 2101:568:feed::1

---

**chkdsk\*** Scans the specified drive for errors and repairs them.  
C:\Windows>**chkdsk** (*Note: Run as Administrator*)

The type of the file system is NTFS.

---

## Navigation Commands

---

WARNING! /F parameter not specified.

Running CHKDSK in read-only mode.

Stage 1: Examining basic file system structure ...

895232 file records processed.

File verification completed.

---

**net user** Manages user accounts (add, remove, change).

C:\Users>**net user**

User accounts for \\PC-RMcD

admin        Administrator        ctctechs

DefaultAccount

The command completed successfully.

---

**net use** Connects to shared folders, similar to mapping a network drive.

C:\Users>**net use**

New connections will be remembered.

There are no entries in the list.

---

**tracert** Similar to ping, but returns path information to an IP address destination. Similar to the traceroute command in macOS and Linux. Can be used for troubleshooting connectivity across the Web.

C:\Users>**tracert Cisco.com**

Tracing route to cisco.com [2001:420:1101:1::185]

over a maximum of 30 hops:

1 5 ms 2601:602:cc01:16e0:623d:26ff:feb9:8830

2 13 ms 12 ms 12 ms 2001:558:4082:c6::1

3 12 ms 13 ms 13 ms 2001:558:a2:601b::1

(20 hops in *output omitted*)

---

**format** (*Note: Do not practice this command on an operational computer!*)

---

## Navigation Commands

---

Creates or re-creates the specified file system on recordable or rewritable storage (magnetic, flash, or optical media) and overwrites the contents and file table of the drive.

---

**xcopy** Copies one or more files and folders to another folder or drive.

C:\Users>**XCOPY source [destination] [/A |**

For format and function table, type:

C:\Users>**help xcopy**

---

**copy** Copies one or more files to another folder or drive.

**robocopy** Robust File Copy for Windows. Copies or moves files/folders; can be configured with various optional GUIs.

Usage :: **ROBOCOPY** source destination [file [file]...]  
[options]

source :: Source Directory (drive:\path or  
\server\share\path).

destination :: Destination Dir (drive:\path or  
\server\share\path).

file :: File(s) to copy (names/wildcards: default is “\*.\*”).

For options table, use : C:\Users>**help robocopy**

---

**gpupdate** Refreshes Group Policy on local or Active Directory systems.

C:\Users>**gpupdate**

Updating policy...

---

**gpresult** Displays the resultant set of policy for the specified computer and user. For the usage guide, type: C:\Users>**gpresult /?**.

---

**shutdown** (*Note: Do not practice this command on an operational computer!*)

Shuts down the computer. For usage, enter:

C:\Users>**shutdown /?**.

---

**sfc\*** Scans system files and replaces damaged or missing files.

C:\Windows>**sfc /scannow** (*run as administrator*)

Beginning system scan. This process will take some time.

Beginning verification phase of system scan.

Verification 4% complete.

---

---

## Navigation Commands

---

**[command name]/?** Displays help for the specified command name—for example, **xcopy /?**.

---

**diskpart\*** (*Note: Do not practice this command on an operational computer!*)  
Creates, removes, and manages disk partitions.

---

**pathping** Similar to **traceroute** but provides information on network latency along the path to the destination. **pathping** traces and tests network connections to an IP address.  
C:\Users>**pathping cisco.com**

---

**taskkill** Stops specified task(s) on a local or remote computer.  
C:\Users>**TASKKILL /IM notepad.exe**

---

**winver** Returns version information of the current Windows OS.  
C:\Users>**winver**

---

To run in Administrator mode, select Windows PowerShell (Admin) from the Windows+X menu. The Administrator Command Prompt window opens. [Figure 6-2](#) shows an example of both.

```

Windows PowerShell
PS C:\Users\ramcdonald> ping 192.168.108.1

Pinging 192.168.108.1 with 32 bytes of data:
Reply from 192.168.108.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.108.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\ramcdonald>
PS C:\Users\ramcdonald> chkdsk
Access Denied as you do not have sufficient privileges or
the disk may be locked by another process.
You have to invoke this utility running in elevated mode
and make sure the disk is unlocked.
PS C:\Users\ramcdonald>

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> chkdsk
The type of the file system is NTFS.

WARNING! /F parameter not specified.
Running CHKD SK in read-only mode.

Stage 1: Examining basic file system structure ...
      592384 file records processed.
File verification completed.
Phase duration (File record verification): 3.29 seconds.
      10415 large file records processed.
Phase duration (Orphan file record recovery): 0.00 milliseconds.
      0 bad file records processed.
Phase duration (Bad file record checking): 0.51 milliseconds.

Stage 2: Examining file name linkage ...
      431 reparse records processed.
PS C:\Windows\system32> 92 done; Stage: 71%; Total: 56%; ETA: 0:00:06 ...

```

**Figure 6-2** Windows PowerShell in Normal (Top) and Administrator Mode (Bottom)—Note that the **ping** Command Was Successful in Normal Mode, but the **chkdsk** Command Runs Only in Administrator Mode

## Windows Command-Line Commands

Table 6-4 lists the basic commands and their uses. Commands are listed here in all caps, but Windows allows you to enter them in lower case, upper case, or mixed case. Open a command prompt and try out these commands in preparation for the exam. Further command details are provided after the table.

The first set of commands refers to navigation commands that take the user to different directories in the drive. They are followed by the command-line tools that provide information or perform tasks for the user. Commands listed with an asterisk (\*) must be run in Administrator mode. Try these

commands on your PC to become familiar with the input and output information.

## format



In Windows, the **format** command is used primarily to create or re-create the specified file system on recordable or rewritable storage (magnetic, flash, or optical media). In the process, the contents of the drive are overwritten.

**format** appears to “destroy” the previous contents of magnetic storage (such as a hard disk), but if **format** is used on a hard disk by mistake, third-party data recovery programs can be used to retrieve data from the drive. This is possible because most of the disk surface is not changed by **format** when a quick format option is selected.

Windows overwrites the entire surface of a disk with zeros if the Quick Format option is not selected. If the Quick Format or Safe Format option is used, the contents of the disk are marked for deletion but can be retrieved with third-party data recovery software.

### Note

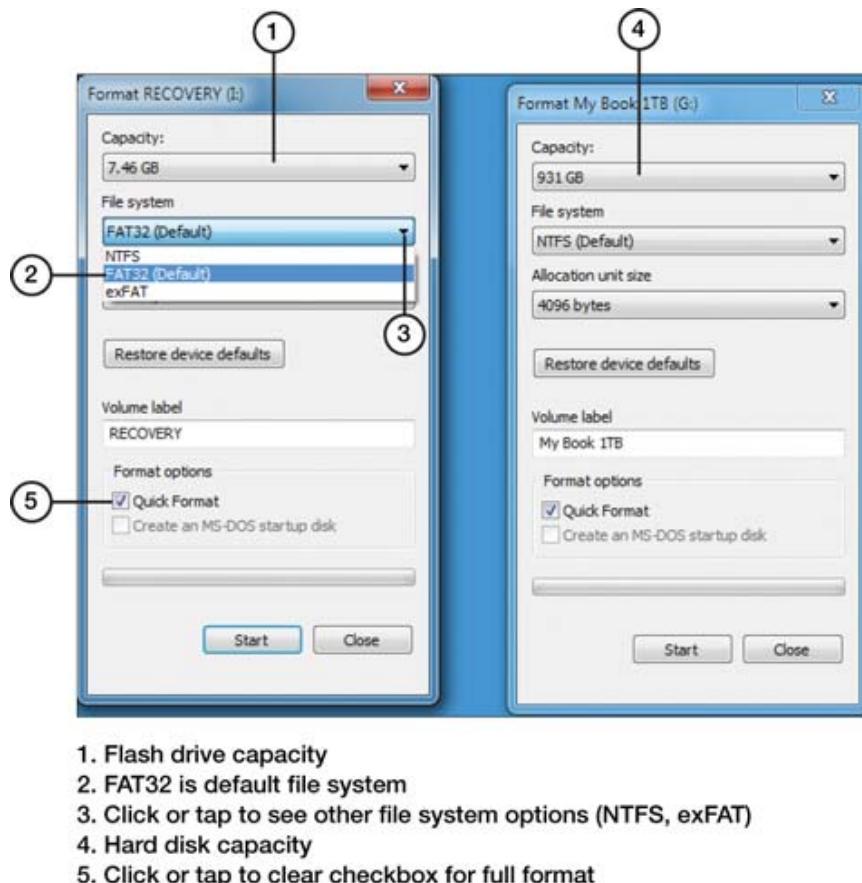
The hard-disk format process that the **format** command performs (which creates the file system) is sometimes referred to as a standard format, to distinguish it from the low-level format that hard drive manufacturers use to set up magnetic structures on the hard drive.

## Using format with USB Flash and Removable-Media Drives

Although USB flash memory drives and removable-media drives are preformatted at the factory, **format** is still useful to quickly erase the contents of a disk, especially if it contains many files or folders. It also places new sector markings across the disk.

## Formatting Drives with File Explorer

Use Windows File Explorer/This PC to format all types of drives. Right-click the drive you want to format, and select Format. The Format options for Windows appear (see [Figure 6-3](#)). The Format tool is also available in Disk Management; for most users, this is the preferred method of formatting disks.



**Figure 6-3** The Format Menu for a Flash Drive (Left) and for a Hard Disk (Right)

## Using format from the Command Prompt

The **format** command overwrites the current contents of the target drive unless the **/Q** (Quick Format) option is used. When **/Q** is used, only the file allocation table and root folder are overwritten. To retrieve data from a drive that has been formatted, you must use third-party data recovery software.

The **format** command includes a variety of options for use with hard disks, removable media and optical drives, and USB flash memory drives. The most useful examples follow:

**format F: /FS:exFAT** formats drive F: using the exFAT file system.

**format F: /Q** performs a quick format on drive F:.

To see the additional options for **format**, use **format /?**.

Note that the FAT and FAT32 file systems impose the following restrictions on the number of clusters on a volume:

**FAT:** Number of clusters ≤ 65,526

**FAT32:** 65,526 < Number of clusters < 4,177,918

**format** immediately stops processing if it decides that the preceding requirements cannot be met using the specified cluster size. NTFS compression is not supported for allocation unit sizes above 4,096.



## copy

The **copy** command copies files from one drive and folder to another folder and drive. The folder specified by **copy** must already exist on the target drive. **copy** does not work with files that have the system or hidden file attributes; to copy these files, use **xcopy** or **robocopy** instead.

The syntax for **copy** in Windows follows:

```
copy [/D] [/V] [/N] [/Y | /-Y] [/Z] [/L] [/A | /B] source [/A |  
/B]  
[+ source [/A | /B] [+ ...]] [destination [/A | /B]]
```

The following are some examples:

**copy\*.\* F:** copies all files in the current folder to the current folder on the F: drive.

**copy\*.TXT C:\Users\Username** copies all .txt files in the current folder to the *Username* folder on the C: drive.

**copyC:\WINDOWS\TEMP\\*.BAK** copies all \*.bak files in the \Windows\Temp folder on drive C: to the current folder.

**copyC:\WINDOWS\\*.BMP D:** copies all .bmp files in the \Windows folder on drive C: to the current folder on drive D:.

To see a list of all the options for **copy**, use **copy/?**.



## **xcopy**

In most cases, the **xcopy** command can be used in place of **copy**. It has the following advantages:

- **Provides faster operation on a group of files:** **xcopy** reads the specified files into conventional RAM before copying them to their destination.
- **Creates folders as needed:** If you specify the destination folder name in the **xcopy** command line, the destination folder will be created if needed.
- **Operates as a backup utility:** **xcopy** can be used to change the archive bit on files from on to off, to allow it to be used in place of commercial backup programs.
- **Copies files changed or created on or after a specified date:** This is useful when using **xcopy** as a substitute for commercial backup programs.

**xcopy** can be used to “clone” an entire drive’s contents to another drive. For example, the following command copies the entire contents of the D: drive to the H: drive:

**xcopyD:\ H:\ /H /S /E /K /C /R**

This command copies all files from the root folder (root directory) and subfolders in drive D: to the root folder and subfolder in drive H:, including system and hidden files, empty folders and subfolders, and file attributes. This process continues even if errors are detected, and it overwrites read-only files.

To see a list of all the options for **xcopy**, use **xcopy/?**, as shown previously in [Table 6-4](#).



## robocopy

**robocopy** is a robust file-copying Windows utility that can be used in place of **xcopy**. **robocopy** offers several advantages over **xcopy**, including the capability to tolerate pauses in network connections, to mirror the contents of the source and destination folders by removing files as well as copying files, to perform multithreaded copies for faster copying on multicore PCs, to log copy processes, and to list or copy files that match specified criteria (including minimum file size).

The syntax for **robocopy** for Windows is available from <https://technet.microsoft.com/en-us/library/cc733145.aspx>. Let's look at two examples of what you can do with **robocopy**.

To copy files in *sourcefolder* that are at least 16MB (16,777,216 bytes) in size to a *targetfolder*, use

**robocopy C:\SOURCEFOLDER D:\TARGETFOLDER /MIN:16777216**

Add the **/L** option to the end of this command to list the files to be copied.

To mirror a local folder to a network folder with tweaks for more reliable operation and omit hidden files (**/XA:H**), use:

**robocopy \\SOURCESERVER\SHARE  
\\DESTINATIONSERVER\SHARE /MIR /FFT /Z /XA:H /W:5**

**/FFT** uses the 2-second rule for comparing files, which can prevent the recopying of files that are unchanged but that have a time stamp that is off by a second or two from the destination's version. **/W:5** changes the wait time between retries from the default of 30 seconds to 5 seconds.

These examples were adapted from the excellent TechNet Wiki posting "Robocopy and a Few Examples," available at <https://social.technet.microsoft.com/wiki/contents/articles/1073.robocopy-and-a-few-examples.aspx>.

As you can see from these examples, **robocopy** uses much different syntax than **xcopy**. If you used **robocopy** in Windows XP or older versions, keep in mind that **robocopy** has had syntax changes over its different versions. For these reasons, you might prefer to run it by means of a GUI, such as the **robocopy** GUI available at [https://docs.microsoft.com/en-us/previous-versions/technet-magazine/cc160891\(v=msdn.10\)](https://docs.microsoft.com/en-us/previous-versions/technet-magazine/cc160891(v=msdn.10)) or third-party GUIs available online.



## diskpart

diskpart is a disk-management program included in Windows. It can be used to perform disk partitioning and management commands that are not included in Computer Management's Disk Management module.

When you run diskpart, a new window opens with a diskpart> prompt. Only diskpart commands can be entered in this window. For a full list of diskpart commands, use **diskpart/?**.

Figure 6-4 demonstrates two **diskpart** commands: **select disk X** and **detail disk**. In this example, diskpart shows that the selected disk drive is the boot drive, contains the pagefile, and is used to store crashdump information.

The screenshot shows a command-line window titled 'C:\Windows\system32\diskpart.exe'. The user has entered the command 'select disk 1' followed by 'detail disk'. The output displays detailed information about Disk 1, which is identified as the ATA Device with ID 823B0499F. It is an online disk with path 0, target 0, and LUN ID 0. The location path is PCIROOT\0\PCI\1200\ATA\CC00T00L00. The disk is not read-only and is the boot disk. It contains a pagefile and is used for crashdump storage. The disk is also clustered. A table at the bottom lists volumes: Volume 4 (Label: System Reserved, Type: Partition, Size: 100 MB, Status: Healthy, Info: System Boot) and Volume 5 (Label: C, Type: Partition, Size: 465 GB, Status: Healthy, Info: Boot).

Volume #	Ltr	Label	Fs	Type	Size	Status	Info
Volume 4		System Reserved	NTFS	Partition	100 MB	Healthy	System Boot
Volume 5	C		NTFS	Partition	465 GB	Healthy	

**Figure 6-4** Using **diskpart** to Determine Details About the Selected Disk

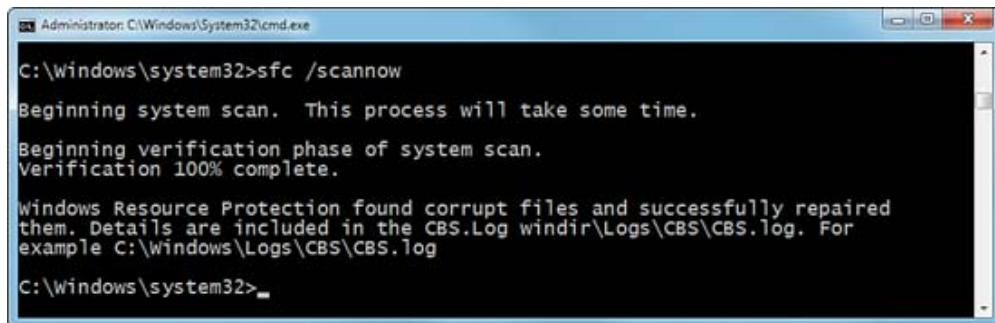


## sfc

System File Checker (**sfc**) is a Windows utility that checks protected system files (such as .dll, .sys, .ocx, and .exe files, as well as some font files used by the Windows desktop) and replaces incorrect versions or missing files with the correct files.

Use **sfc** to fix problems with built-in Windows programs caused by the installation of obsolete Windows system files, user error, deliberate erasure, virus or Trojan horse infections, and similar problems.

To run **sfc**, open the command prompt in elevated mode (that is, run as administrator), and type **sfc** with the appropriate switch. A typical option is **sfc/scannow**, which immediately scans all protected files (see [Figure 6-5](#)).

A screenshot of a Windows Command Prompt window titled "Administrator: C:\Windows\System32\cmd.exe". The window shows the command "c:\Windows\system32>sfc /scannow" being run. The output text is:

```
c:\Windows\system32>sfc /scannow
Beginning system scan. This process will take some time.
Beginning verification phase of system scan.
Verification 100% complete.

Windows Resource Protection found corrupt files and successfully repaired them. Details are included in the CBS.Log windir\Logs\CMS\CBS.log. For example C:\Windows\Logs\CMS\CMS.log
C:\Windows\system32>_
```

The window has a blue title bar and a black background for the text area.

**Figure 6-5** sfc /scannow Reports That Corrupt Files Were Repaired

Another option is **sfc /scanonce**, which scans all protected files at the next boot. If SFC finds that some files are missing and replacement files are not available on your system, you are prompted to reinsert your Windows distribution disc so that the files can be copied to the DLL cache. Other options include **/scanboot**, which scans all protected files every time the system starts; **/revert**, which returns the scan setting to the default; and **/purgecache** and **/cachesize=x**, which enable a user to delete the file cache and modify its size.

If errors are detected, they are logged in the CBS.log file, found in %WinDir%\Logs\CMS\.

To read the contents of CBS.log, you can use the **findstr** command, which sends the details to a separate file called sfcdetails.txt.

For more information about using **sfc** and **findstr**, and to learn how to replace corrupted system files manually if **sfc** cannot do it, see

<https://support.microsoft.com/en-us/kb/929833>.



## chkdsk

**chkdsk** is a command-line tool for checking disk drives for errors and, optionally, repairing those errors. It must be run in elevated/administrator mode. Note that some commands differ, depending on the file system (FAT/FAT32 or NTFS) of the target drive. The syntax of the **chkdsk** command follows:

```
chkdsk [volume[[path]filename]]] [/F] [/V] [/R] [/X] [/I] [/C]
[/L[:size]] [/B]
```

Consider these examples:

**chkdsk/F** scans for and fixes errors on the current drive.

**chkdskF: /F** scans for and fixes errors on drive F:.

If **chkdsk/F** is run on the system drive, the following message appears:

[Click here to view code image](#)

```
The type of the file system is NTFS.  
Cannot lock current drive.  
Chkdsk cannot run because the volume is in use by another  
process. Would you like to schedule this volume to be  
checked the next time the system restarts? (Y/N)
```

If you answer Y, chkdsk runs before the Windows desktop appears and displays a message in the notification area about the condition of the drive. If **chkdsk/F** is run on a nonsystem drive, it runs immediately.

For a complete list of chkdsk options, use **chkdsk/?**.



## **gpupdate**

**gpupdate** is used to update the Group Policy on a local or remote computer. Its syntax follows:

```
gpupdate [/Target:{Computer | User}] [/Force] [/Wait:<value>]  
[/Logoff] [/Boot] [/Sync]
```

For example, you can use this command to refresh the Group Policy on a specified computer called **AccountingPC** and then reboot that computer after processing is complete:

```
gpupdate/target:accountingpc /boot
```

For a complete list of options for the **gpupdate** command, use **gpupdate/?**.

## **gresult**

Use **gresult** to display the current policy for a specified user and computer. Its syntax follows:

```
gresult [/S system [/U username [/P [password]]]] [/SCOPE  
scope]  
[/USER targetusername] [/R | /V | /Z] [(/X | /H) <filename>  
[/F]]
```

For a complete list of options for the **gresult** command, use **gresult/?**.

Consider these examples:

**gresult/R** displays summary data.

**gresult/H GPReport.xhtml** saves a report as GPReport.xhtml.

**gresult/USER targetusername /V** provides verbose information for the specified username.

## **pathping**

**pathping** is a PowerShell command for gathering information on routes and latency (or delay) in communications across a network or the Internet.

The **ping** command simply tests an address's availability, whereas **pathping** gathers statistics about the journey of the IP packets.

## Microsoft Windows 10 Operating System (OS) Features and Tools

220-1102  
Exam

**220-1102: Objective 1.3:** Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS).

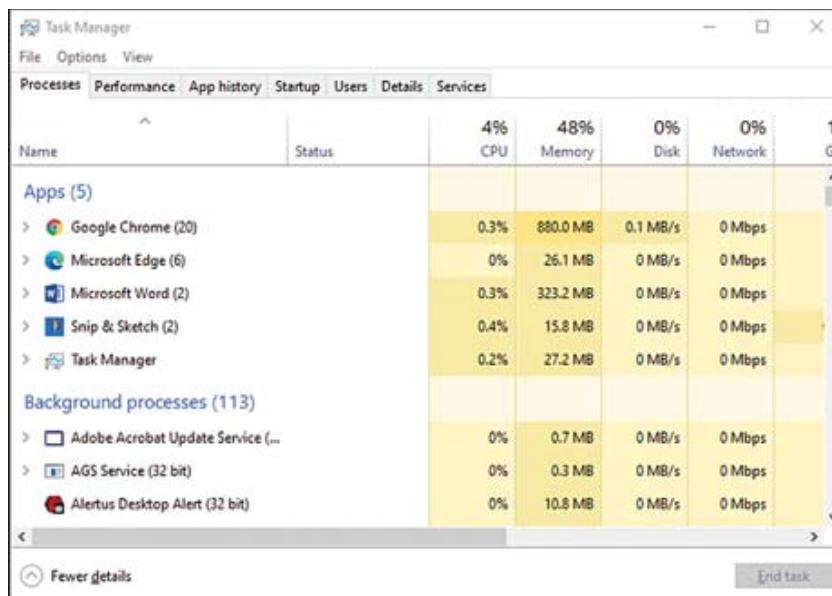
Many administrative Windows tools provide graphical interfaces for managing performance and troubleshooting. Mastering these tools makes common tasks much more efficient.

### Task Manager

The **Task Manager** utility provides a useful real-time look into the inner workings of Windows and the programs that are running. Task Manager is displayed in several ways:

- Right-click the taskbar and select Task Manager.
- Press Ctrl+Shift+Esc.
- Type **Task Manager** in the search box.
- Press Ctrl+Alt+Del and select Task Manager from the Windows Security dialog.

Any of the preceding approaches opens Task Manager, shown in [Figure 6-6](#).



**Figure 6-6** The Windows Task Manager’s Process Tab in Windows 10

The Windows 10 Task Manager includes the following tabs:

- **Processes:** Displays apps and background processes in memory
- **Performance:** Displays CPU, memory, disk drives, Bluetooth, Ethernet, and Wi-Fi stats
- **App history:** Displays app resource usage in the current system session
- **Startup:** Displays startup programs and their impact on system performance
- **Users:** Lists current users
- **Details:** Displays PID, status, username, CPU, and memory usage by app or service
- **Services:** Lists services and their status

One of the most common uses of Task Manager is to end programs (processes) that are malfunctioning. To end a program, click the Processes tab, right-click the process of the nonresponsive program, and select End Task. It is also possible to right-click a process and choose additional details about the status.

## **Microsoft Management Console (MMC) Snap-in**

Instead of hunting for different utilities in different places in Windows, it's simpler to use the Computer Management console window. It has most of the tools you need in one organized window system. How you open Computer Management depends on the Windows version.

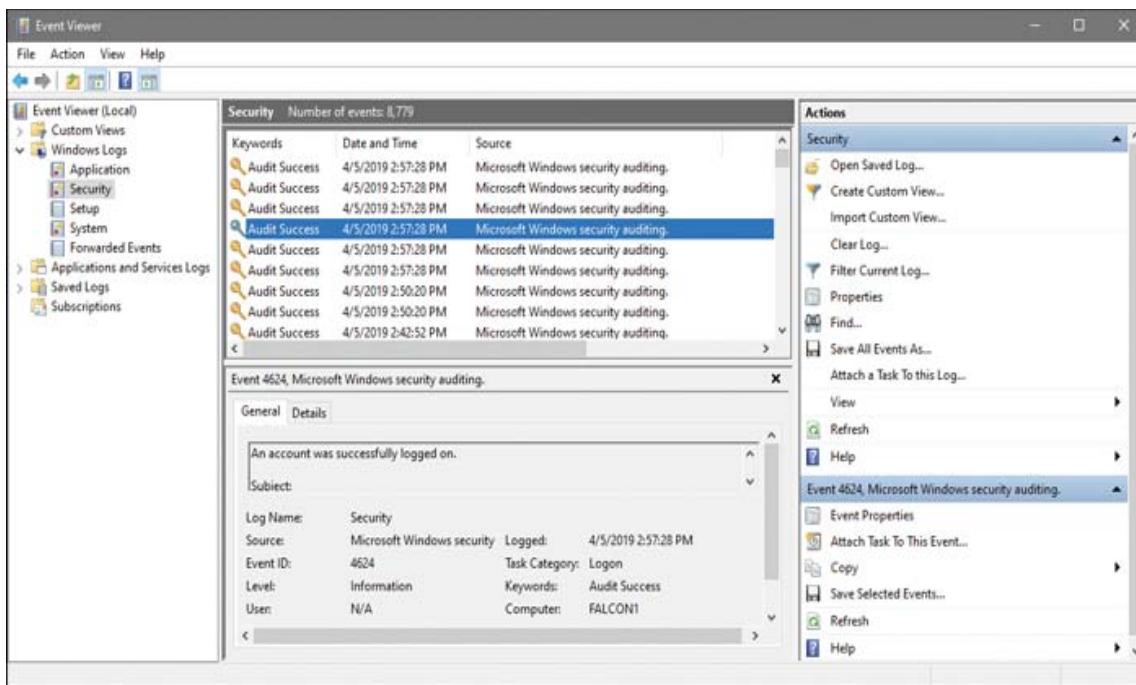
Computer Management is an example of the **Microsoft Management Console (MMC)**, which is a blank console that uses various snap-in console windows. MMC saves the consoles that you snap in and remembers the last place you were working, which makes it a valuable and time-saving tool.

To open the MMC, enter **MMC** in the Run box. A new blank MMC appears. To add the console windows, go to **File > Add/Remove Snap-in** (or press Ctrl+M). From there, click the Add button to select the desired console, such as Computer Management, Performance Logs and Alerts, or ActiveX Controls.

When you are finished using it, save the MMC and consider adding it as a shortcut within the desktop or in the Quick Launch area, and maybe add a keyboard shortcut to open it. The MMC remembers all the console windows added and starts you at the location used when the program was closed. MMC version 3.0 is used with Windows 10.

## **Event Viewer**

The **Event Viewer (eventvwr.msc)** enables an administrator to track and log event logins, security actions, crashes, and other events that have happened in the computer. **Figure 6-7** shows an example of the events tracked in the Event Viewer for Windows 10.



**Figure 6-7** Event Viewer

## Disk Management

The **Disk Management (diskmgmt.msc)** snap-in of the MMC is a GUI-based application for analyzing and configuring hard drives. Try some of the configurations listed in the following sections on a test computer with one or two drives of unpartitioned space. Disk Management is also accessible by right-clicking the Windows icon (start) and selecting Disk Management from the menu that appears.

### CAUTION

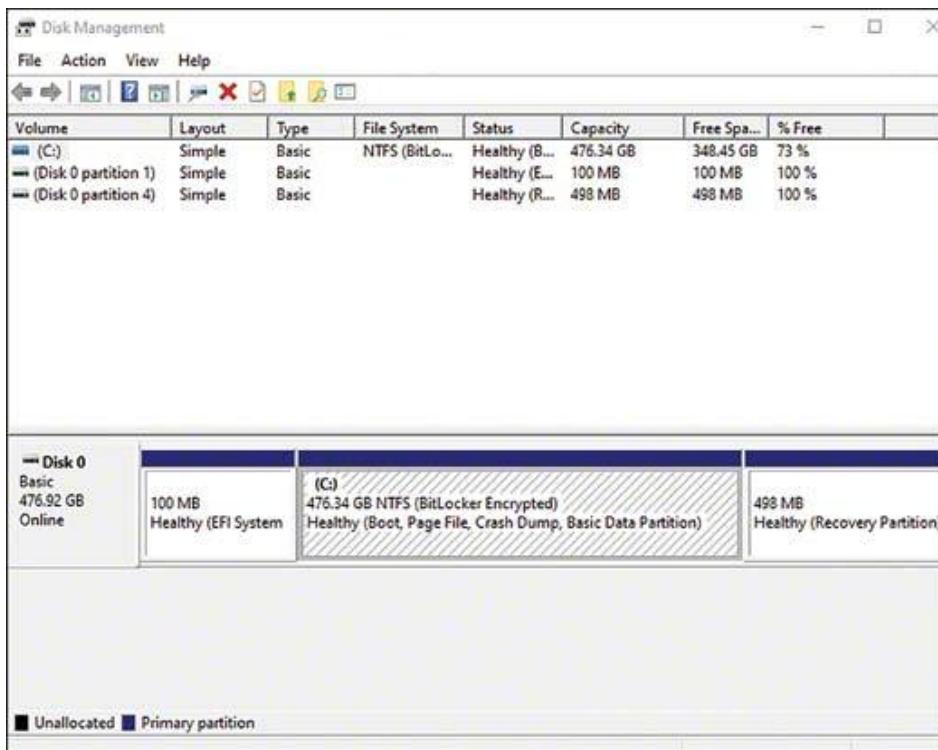
Some operations wipe out all drive contents. Make sure you back up any data that you want to keep before you try any of these tasks.

## Drive Status

Disk Management displays the status of connected drives with Drive Status.

**Figure 6-8** displays the disks and their status at the top of the window. For example, the C: partition is healthy. This window also shows the percentage

of the disk used and other information, such as whether the disk is currently being formatted, whether it is basic or dynamic, and whether it has failed.



**Figure 6-8** Using Disk Management

In some cases, you might see a “foreign” status. This means that a dynamic disk has been moved from another computer (with another Windows operating system) to the local computer, and it cannot be accessed properly. To fix this and enable access to the disk, add the disk to your computer’s system configuration.

To add a disk to your computer’s system configuration, right-click the disk and then click Import Foreign Disks. Any existing volumes on the foreign disk become visible and accessible when you import the disk.

## Task Scheduler

Windows uses **Task Scheduler (taskschd.msc)** to run a task on a specified schedule.

To create a basic task in Windows, follow this procedure:

**Step 1.** Type **Task Scheduler** (or **taskschd.msc**) in the search bar or Run box.

**Step 2.** Click **Create Basic Task** in the Actions menu.

**Step 3.** Enter a name and a description for the task, and click **Next**.

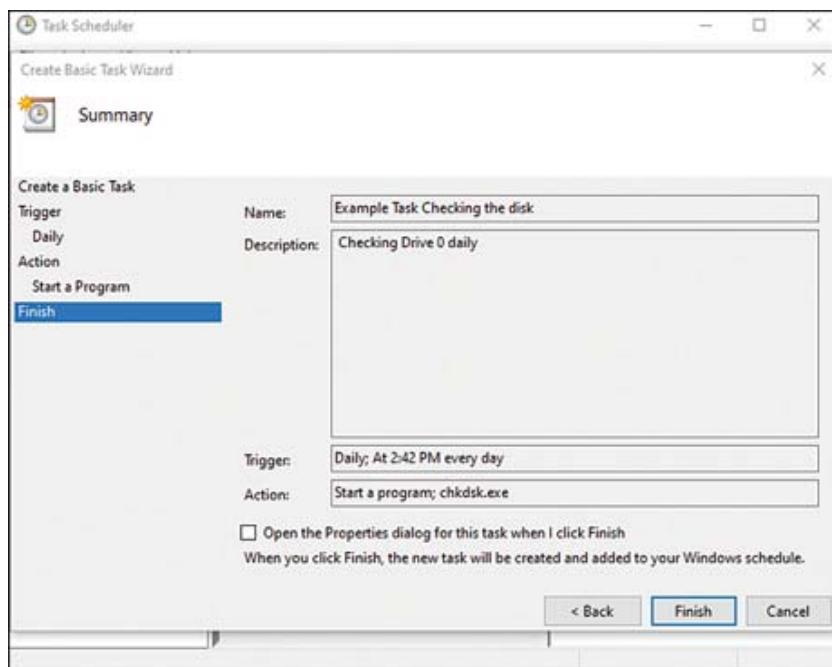
**Step 4.** Select an interval (for example, Daily, Weekly, Monthly, One-Time Only, When My Computer Starts, When I Log On, or When a Specific Event Is Logged), and click **Next**.

**Step 5.** Specify when to start the task and the recurrence, and whether to synchronize across time zones; then click **Next**.

**Step 6.** Specify to start a program (or send an email or display a message), and click **Next**.

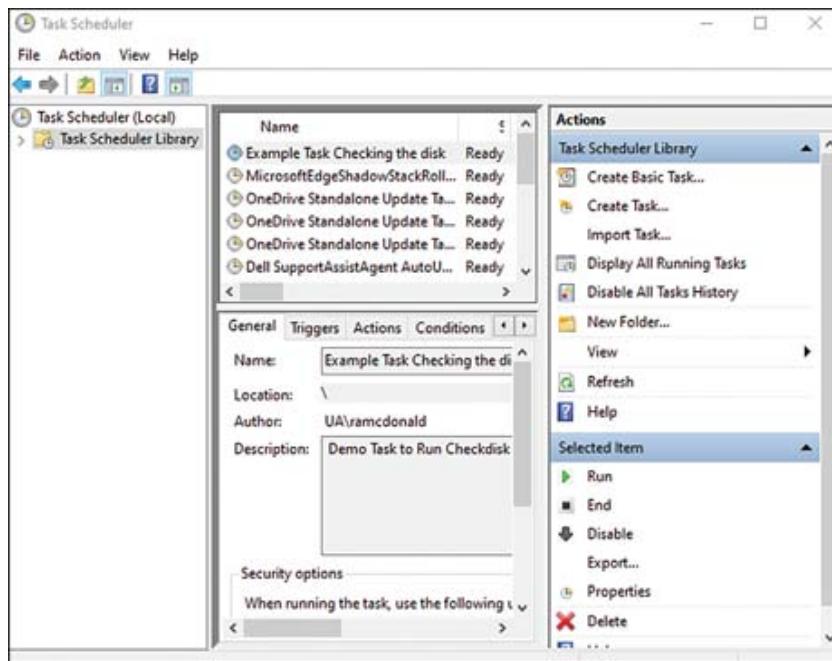
**Step 7.** Select a program or script to run, add options (arguments), and specify where to start the program or script. Click **Next**.

**Step 8.** Review the settings for the task (see [Figure 6-9](#)) and click **Finish**.



**Figure 6-9** Reviewing a Disk Check Task Created with the Task Scheduler

The task is saved in the Task Scheduler library (see [Figure 6-10](#)). Tasks can be edited or deleted in this folder as needed.



**Figure 6-10** The Task Scheduler Library After a New Task Is Added (the New Task Is Listed First, in This Example)

## Device Manager



Windows **Device Manager** (`devmgmt.msc`) is used to display installed device categories and specific installed devices, as well as to troubleshoot problems with devices.

To start Device Manager in Windows 10, follow these steps:

**Step 1.** In the search bar, type **Device Manager**, or enter `devmgmt.msc` in the Run box.

**Step 2.** Open the Device Manager.

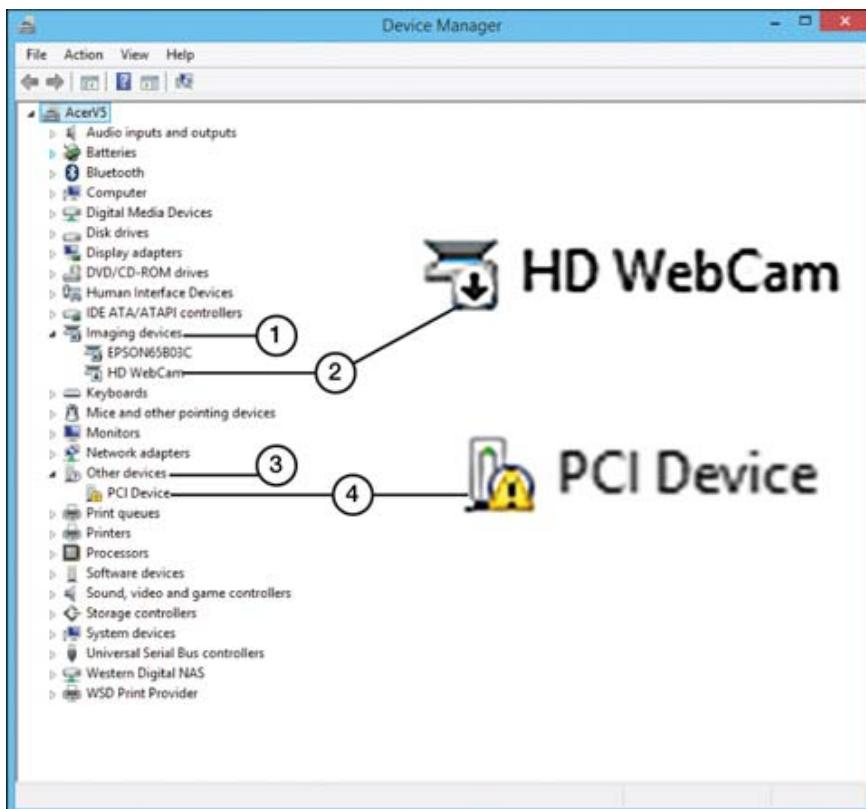
**Step 3.** Click or tap the **Device Manager** link.

Alternatively:

**Step 1.** Press Windows+X.

**Step 2.** Select **Device Manager**.

To view the devices in a specific category, click the plus (+) sign next to the category name, as shown in [Figure 6-11](#). If a particular category contains a device with problems, the category automatically opens when you start Device Manager.



1. Imaging devices category has a device with a problem
2. The HD webcam has been disabled
3. Other devices category is used for unidentified devices
4. An unidentified device

**Figure 6-11** Device Manager with Selected Categories Expanded

## Note

Different systems have different categories listed in Device Manager because Device Manager lists only categories for installed hardware. For example, the system shown in [Figure 6-11](#) is a laptop, so it has a Batteries category.

If a computer has devices that are malfunctioning in a way that Device Manager can detect, or if it has devices that are disabled, they are displayed

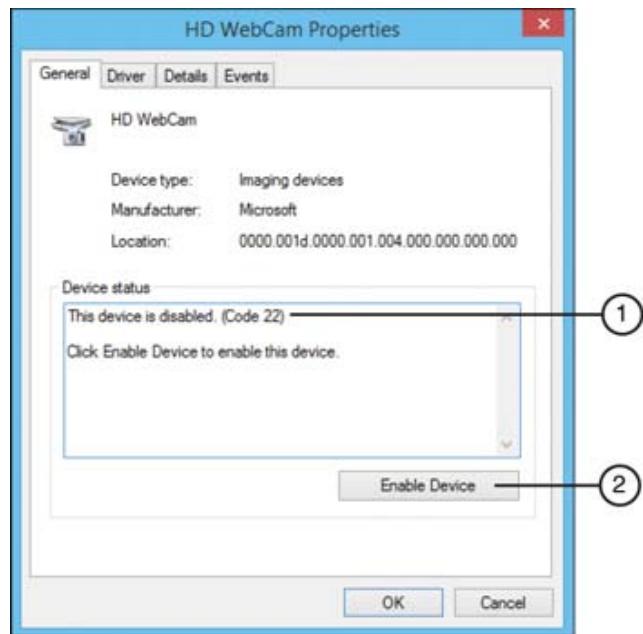
as soon as you open Device Manager. For example, in [Figure 6-11](#), the Imaging Devices category lists a disabled device, indicated by a down-arrow icon. The Other Devices category lists a device that cannot run, indicated by an exclamation point (!) in a yellow triangle.

If a malfunctioning or disabled device is an I/O port, such as a serial, parallel, or USB port, any device attached to that port cannot work until the device is working properly.

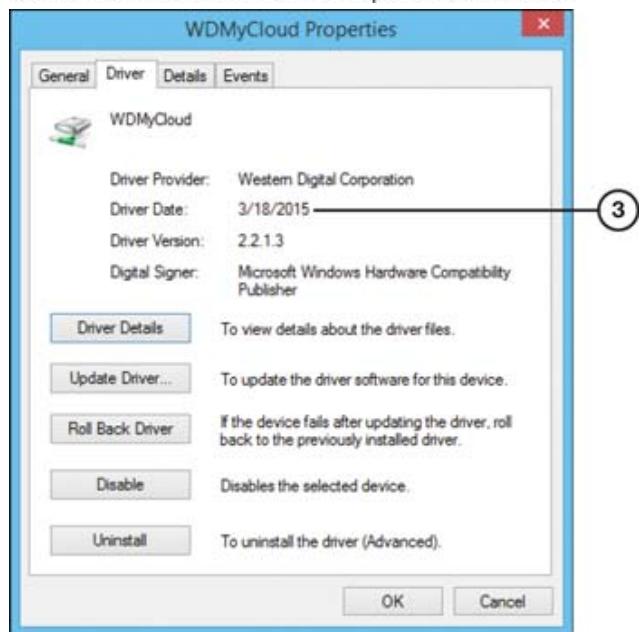
To see more information about a specific device, double-click the device to open its properties sheet. Device properties sheets have a General tab and some combination of other tabs, including the following:

- **General:** Displays device type, manufacturer, location, status, a troubleshooting button, and usage. Applies to all devices.
- **Properties:** Displays device-specific settings. Applies to multimedia devices.
- **Driver:** Displays driver details and version information. Applies to all devices.
- **Details:** Displays technical details about the device. Applies to all devices.
- **Policies:** Optimizes external drives for quick removal or performance. Applies to USB, FireWire (IEEE 1394), and eSATA drives.
- **Resources:** Displays hardware resources such as IRQ, DMA, memory, and I/O port address. Applies to I/O devices.
- **Volumes:** Displays drive information such as status, type, and capacity. Click Populate to retrieve information. Applies to hard disk drives.
- **Power:** Displays the power available per port. Applies to USB root hubs and generic hubs.
- **Power Management:** Specifies device-specific power management settings. Applies to USB, network, keyboard, and mouse devices.

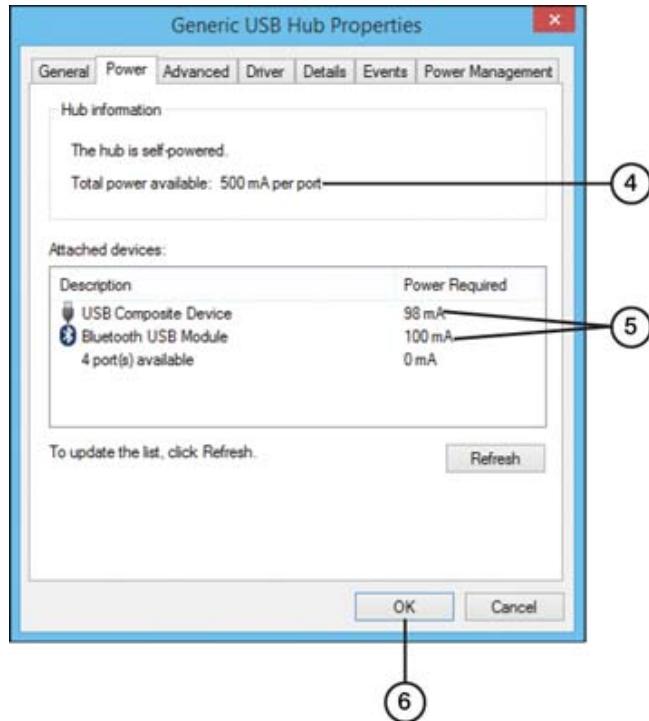
[Figure 6-12](#) illustrates some of these tabs.



1. Device status—disabled device (Code 22)
2. Troubleshoot button—click or tap to enable device



3. Driver overview



4. Available power per USB port on this hub
5. Power required for connected devices
6. Click or tap to close properties sheet

**Figure 6-12** Selected Device Manager Tabs: the General Tab for a Disabled Device (A), the Driver Tab for a Network Storage Device (B), and the Power Tab for a USB Hub (C)

To troubleshoot problems with a device in Device Manager, open its properties sheet by double-clicking the device. Use the General tab (shown in [Figure 6-12](#)) to display the device's status and to troubleshoot the disabled or malfunctioning device.

When you have a malfunctioning device such as the one shown on the left in [Figure 6-12](#), you have several options for resolving the problem:

- Look up the Device Manager code to determine the problem and its solution. (See [Table 6-5](#) for a few examples of device manager codes and solutions.)
- Click the troubleshooting button (if any) shown on the device's General Properties tab; the button's name and usage depend on the problem. [Table 6-5](#) lists a few examples, their meanings, and the solution button (if any).

- Manually change resources (primarily in older systems that do not use ACPI power management). If the nature of the problem is a resource conflict, you can click the Resources tab, change the settings, and try to eliminate the conflict.
- Manually update drivers. If the problem is a driver issue, but an Update Driver button isn't available, open the Driver tab and install a new driver for the device.

**Table 6-5** Examples of Some Device Manager Codes and Solutions

Code Number	Problem	Recommended Solution
1	This device is not configured correctly.	Update the driver.
3	The driver for this device might be corrupted, or your system might be running low on memory or other resources.	Close some open applications. Uninstall and reinstall the driver. Install additional RAM.
10	The device cannot start.	Update the driver. View Microsoft Help and Support article 943104 for more information.
12	This device cannot find enough free resources that it can use. If you want to use this device, you need to disable one of the other devices on this system.	You can use the Troubleshooting wizard in Device Manager to determine where the conflict is and then disable the conflicting device. Disable the device.
22	The device is disabled.	Enable the device.

You can also use Device Manager to disable a device that is conflicting with another device. To disable a device, follow these steps:

**Step 1.** Click the plus (+) sign next to the device category containing the device.

**Step 2.** Double-click the device, click the **Driver** tab, and select **Disable**.

Depending on the device, you might need to physically remove it from the system to resolve a conflict. To use Device Manager to remove a device, follow these steps:

**Step 1.** Click the plus (+) sign next to the device category containing the device.

**Step 2.** Double-click the device and select **Uninstall**.

**Step 3.** Shut down the system and remove the physical device.

Or:

**Step 1.** Double-click the device and select **Properties**.

**Step 2.** Click the **Driver** tab and click the **Uninstall** button.

**Step 3.** Shut down the system and remove the physical device.

If a device malfunctions after a driver update, roll back the driver. Click the Roll Back Driver button on the Driver tab to return to the preceding driver version.

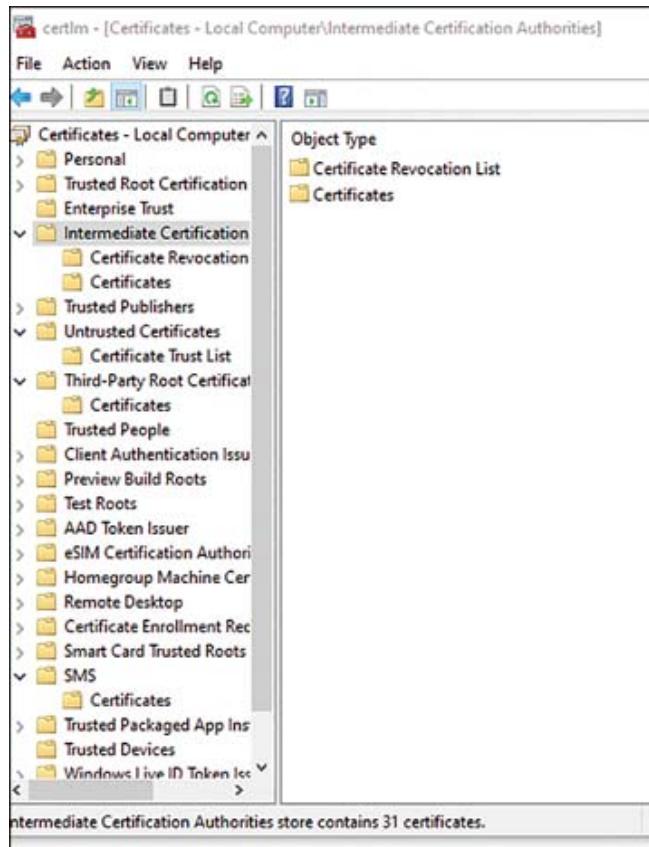
## Certificate Manager

The **Certificate Manager (certmgr.msc)** enables the import, export, modification, or deletion of root certificates. These digital certificates are how Windows manages authentication when sending and receiving information. This includes personal user authentication, as well as trusted certificates for an enterprise.

The information for each certificate issued includes the following:

- Issued to
- Issued by
- Expiration date
- Intended purpose (for example, server authentication)
- Friendly name
- Status

You can view your security certificates by accessing the tool and typing **Certificate** (or **certmgr.msc**) in the search bar. Figure 6-13 shows an example of the different types of securities.



**Figure 6-13** Certificate Manager

## Local Users and Groups

**Local Users and Groups** (**lusrmgr.msc**) is a snap-in console for managing local users and groups. The local user or group settings enable the administrator to assign permissions that regulate access and activities on the local machine.

You can access Local Users and Groups in several ways. Try these on a local machine:

- Press Windows+R to access the Run app; then enter **lusrmgr.msc**.
- Open the Computer Management App and select Users and Groups.

This tool enables you to see all the accounts, visible and hidden, on the computer, as well as to create and manage new users and groups. By default, Windows uses some built-in accounts, such as Administrator, DefaultAccount, and Guest. The Windows Defender antivirus uses the WDAGUtility account.

## Performance Monitor

The Windows **Performance Monitor (perfmon.msc)** can be used for real-time performance monitoring or to record performance over time.

To access Performance Monitor, open the Run prompt and search for Performance Monitor (or just type **perfmon**) in the search box, and then click the Performance Monitor node.

Many different types of performance factors can be measured. You can measure objects, including physical devices such as the processor and memory, and software, such as protocols and services. These objects are measured with counters. For example, a common counter for the processor is % Processor Time.

To see whether additional RAM is needed in a system, for example, select the object called Paging File; then select the counters % Usage and Pages/Sec, as described in the following steps:

**Step 1.** Click the + sign or right-click in the table beneath the graph, and select **Add Counters**.

**Step 2.** Select **Paging File** as the performance object and then choose **% Usage**.

**Step 3.** Click **Add**.

**Step 4.** Select **Memory** as the performance object and then choose **Pages/Sec** from the drop-down menu.

**Step 5.** Click **Add**.

**Step 6.** Click **OK** and then run normal applications for this computer.

If Performance Monitor indicates that the Paging File % Usage counter is consistently near 100 percent or the Memory Pages/Sec counter is consistently higher than 5, add RAM to improve performance.

## Additional Tools

A technician needs to know information about a machine and then perform routine tasks such as disk maintenance and other adjustments. The following tools can quickly provide information and maintenance options. Simply typing the name of the tool into the Windows search bar provides quick access to the apps.

### System Information (msinfo32)

The **System Information (msinfo32.exe)** tool displays a great deal of information about the computer hardware and Windows installation in a system. To access the tool, type **msinfo32** in the search bar or run **msinfo.exe**.

The System Summary (see [Figure 6-14](#)) provides basic information about the Windows installation and hardware configuration. Simply click a subnode (left pane) for more detailed information about system hardware, components, or software environment. To dig deeper, open the nodes in the left pane. [Figure 6-15](#) shows the loaded program modules listed.



System Summary		
	Item	Value
Hardware Resources	OS Name	Microsoft Windows 7 Home Premium
Components	Version	6.1.7601 Service Pack 1 Build 7601
Software Environment	Other OS Description	Not Available
	OS Manufacturer	Microsoft Corporation
	System Name	HP-PC7
	System Manufacturer	Hewlett-Packard
	System Model	HP Pavilion dv4 Notebook PC
	System Type	x64-based PC
	Processor	AMD Turion(tm) II Dual-Core Mobile M500, 2200 Mhz, 2 Core(s), 2 Logical Pr...
	BIOS Version/Date	Insyde F.17, 12/10/2009
	SMBIOS Version	2.6
	Windows Directory	C:\Windows
	System Directory	C:\Windows\system32
	Boot Device	\Device\HarddiskVolume1
	Locale	United States
	Hardware Abstraction Layer	Version = "6.1.7601.17514"
	User Name	HP-PC7\Marcus_Lap
	Time Zone	Central Daylight Time
	Installed Physical Memory (RAM)	8.00 GB
	Total Physical Memory	7.75 GB
	Available Physical Memory	4.76 GB
	Total Virtual Memory	15.5 GB
	Available Virtual Memory	12.0 GB
	Page File Space	7.75 GB
	Page File	C:\pagefile.sys

Find what:

Search selected category only  Search category names only

**Figure 6-14** msinfo32 System Summary

System Information					
	Name	Version	Size	File Date	Manufacturer
Adapter	adclui	6.1.7600.16385	150.50 KB	7/13/2009 6:57 P...	Microsoft Co...
Protocol	actioncenter	6.1.7601.17514	762.50 KB	4/14/2011 5:30 P...	Microsoft Co...
WinSock	actpxnry	6.1.7601.17514	936.00 KB	4/14/2011 5:31 P...	Microsoft Co...
Ports	advapi32	6.1.7600.16385	856.50 KB	7/13/2009 7:41 P...	Microsoft Co...
Serial	altab	6.1.7600.16385	52.00 KB	7/13/2009 6:55 P...	Microsoft Co...
Parallel	apphelp	6.1.7601.17514	334.00 KB	4/14/2011 5:31 P...	Microsoft Co...
Storage	atichx64	8.17.10.1077	777.00 KB	4/20/2011 4:07 A...	ATI Technolo...
Drives	atiupnp64	8.14.16.6210	38.00 KB	4/20/2011 3:21 A...	Advanced Mi...
Disks	atiumd64	7.14.10.833	5.19 MB (3...)	4/20/2011 3:40 A...	ATI Technolo...
SCSI	atiumd6a	8.14.10.308	3.69 MB (3...)	4/20/2011 3:40 A...	Advanced Mi...
IDE	atiupxp64	8.14.16.6210	40.00 KB	8/4/2010 3:15 AM	Advanced Mi...
Printing	ati	3.5.2284.0	88.50 KB	7/13/2009 7:34 P...	Microsoft Co...
Problem Devices	ati90	9.0.30729.6161	172.32 KB	10/20/2011 4:34 ...	Microsoft Co...
USB	audioses	6.1.7601.17514	289.50 KB	4/14/2011 5:31 P...	Microsoft Co...
Software Environment	authui	6.1.7601.17514	1.84 MB (1...)	4/14/2011 5:31 P...	Microsoft Co...
System Drivers	authz	6.1.7600.16385	173.50 KB	7/13/2009 6:50 P...	Microsoft Co...
Environment Variables	avrt	6.1.7600.16385	18.00 KB	7/13/2009 7:22 P...	Microsoft Co...
Print Jobs	batmeter	6.1.7601.17514	732.00 KB	4/14/2011 5:30 P...	Microsoft Co...
Network Connections	bcrypt	6.1.7600.16385	121.00 KB	7/13/2009 6:49 P...	Microsoft Co...
Running Tasks	bcryptprimitives	6.1.7601.17514	291.12 KB	4/14/2011 5:31 P...	Microsoft Co...
Loaded Modules	browcli	6.1.7601.17514	57.50 KB	4/14/2011 5:30 P...	Microsoft Co...
Services	bthprops	6.1.7601.17514	704.50 KB	4/14/2011 5:30 P...	Microsoft Co...
Program Groups	cabinet	6.1.7601.17514	92.50 KB	4/14/2011 5:30 P...	Microsoft Co...
Startup Programs					
OLE Registration					
Windows Error Reporting					

Find what:

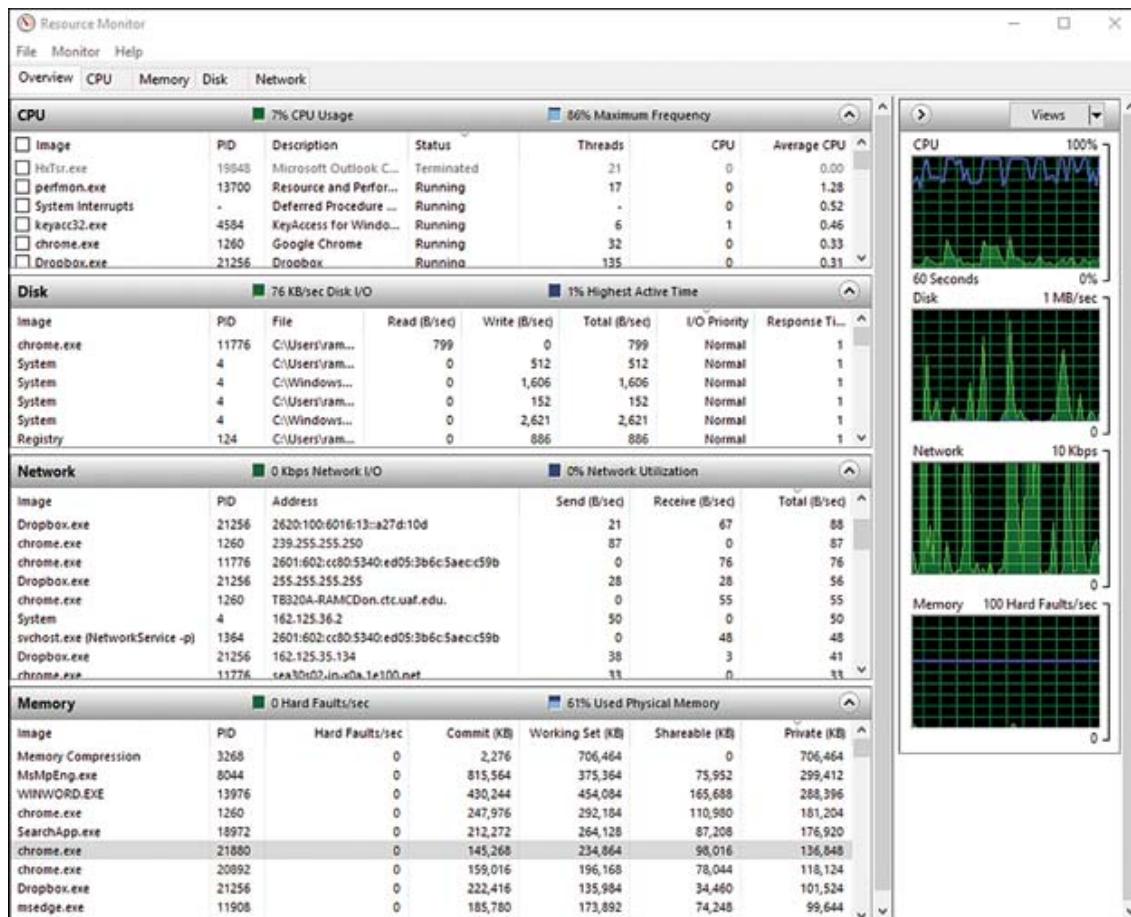
Search selected category only  Search category names only

**Figure 6-15** msinfo32 Loaded Program Modules Display (Right Pane)

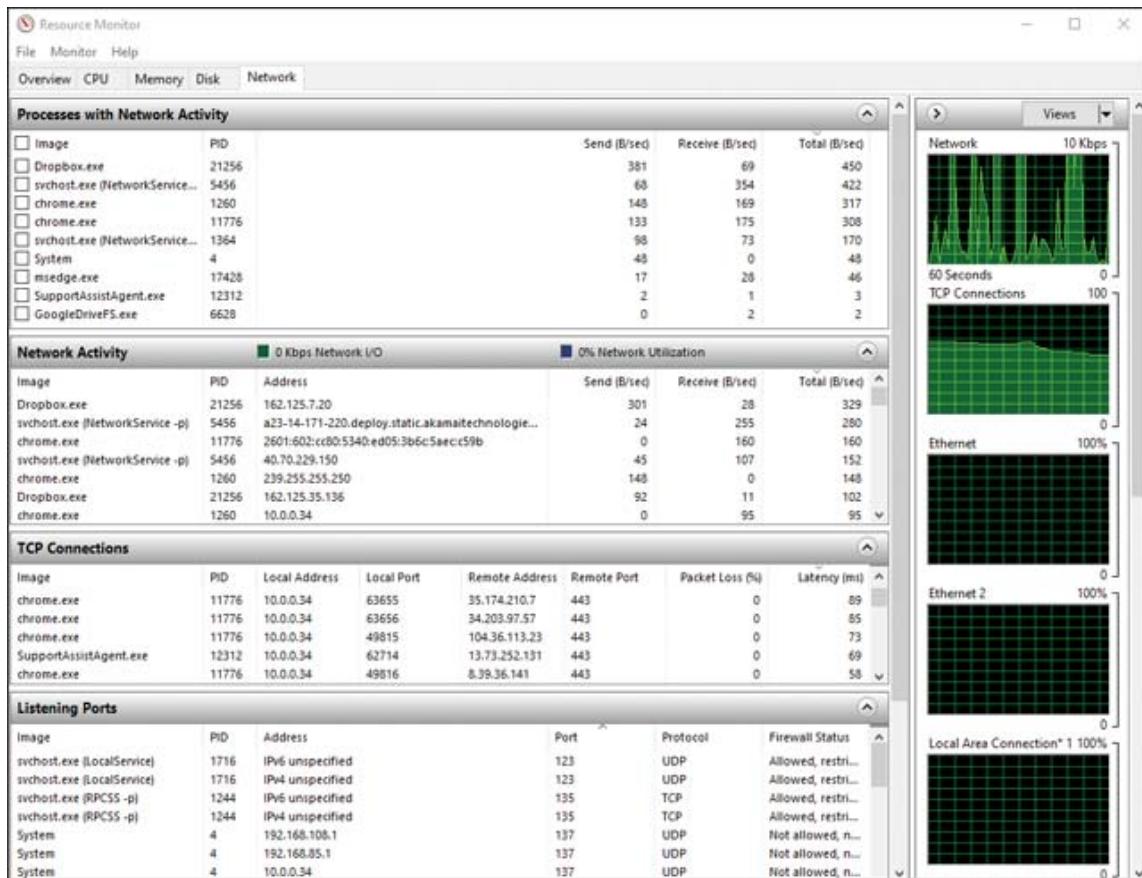
Use the Find What window to locate specific information. Use the File menu to save a report or to export it as a text file.

## Resource Monitor

The **Resource Monitor (resmon.exe)** is similar to the Performance Monitor, mentioned earlier in this section. Both track the performance of the CPU, memory, and so on. For most users, the Performance Monitor is enough to find most problems and disable processes, but sometimes a deeper understanding of resources is needed: That is where the Resource Monitor comes in. The Resource Monitor allows for more detailed tracking of resources. The following figures show the deeper detail offered in the Resource Monitor. [Figure 6-16](#) depicts the overview provided when the monitor is opened; [Figure 6-17](#) details the network information, with additional information on activity, connections, and ports. The graphs on the right provide a visual context for the data on the left.



**Figure 6-16** Resource Monitor Window (resmon.exe)



**Figure 6-17** Resource Monitor with the Network Tab Selected



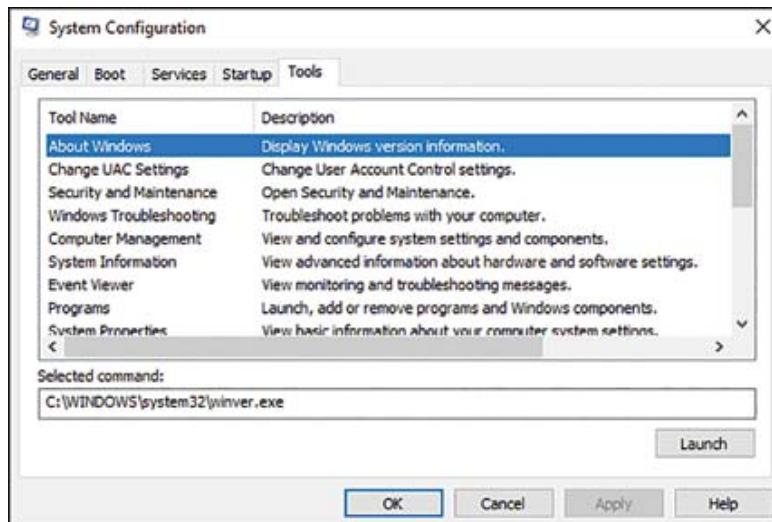
## System Configuration Utility

Use the **System Configuration (msconfig.exe)** utility to configure how Windows starts, to choose startup programs and services, and to change the boot procedure.

The Microsoft System Configuration utility (msconfig.exe) enables the selective disabling of programs and services that run at startup. If a computer is unstable, runs more slowly than usual, or has problems starting up or shutting down, using msconfig can help you determine whether a program or service running when the system starts is at fault.

To start msconfig.exe, press Windows+R, type **msconfig**, and press Enter.

msconfig has a multitabbed interface used to control startup options. The General tab (see [Figure 6-18](#)) offers Normal, Diagnostic (clean boot), or Selective Startup. (You choose which items and services to load.) Use the Boot tab to specify how to boot a Windows system.



**Figure 6-18** System Configuration Utility (msconfig) Tools Tab in Windows 10

Use the Services tab to disable or reenable system services. Use the Tools tab to launch System Restore, Computer Management, and other management tasks. When trying this, note that the Startup tab, once used to manage startup programs, now links to the Task Manager for those changes.

[Figure 6-18](#) shows the System Configuration dialog's Tools tab in Windows 10. Note that many of the tools listed in this section are accessible from this utility.

### TIP

When you select a tool from the Tools tab, msconfig displays the command line needed to run it. Add any options desired before you start the tool.

## Disk Cleanup

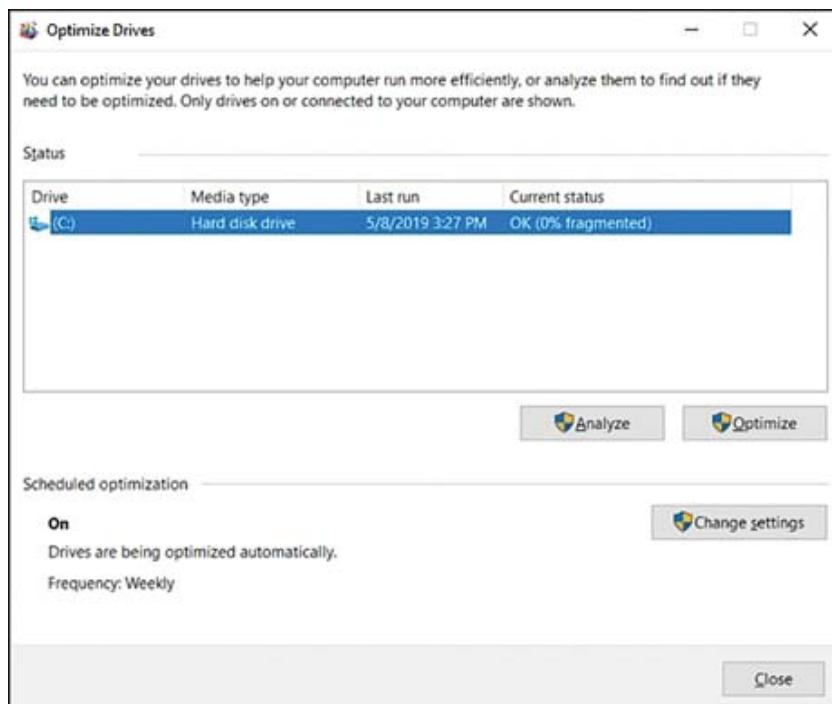
**Disk Cleanup (cleanmgr.exe)** is a utility for optimizing drives by removing unnecessary files and freeing space for better disk performance. Running **cleanmgr.exe** brings up a window to choose a disk to clean. When a disk is selected, another window opens and presents check boxes to select file types that can be removed. These files include temporary Internet files, the Recycle Bin, and other temporary files. If still more space is needed, select Clean Up System Files in Disk Cleanup and choose the file types you no longer need.

Storage Sense is a convenient tool on Windows 10 and 11 that facilitates automatically maintaining storage use on a PC. Access Storage Sense by opening **Settings > System > Storage**. From here, you can enable or disable Storage Sense. If it is enabled, further settings determine how to handle temporary files and preferences for running the utility.

## Disk Defragment/Optimize Drives

Defragging a hard disk drive can help improve system performance, especially if the drive is frequently changed. With heavy use, the data on a disk can be spread around the drive, which slows access. Defragmentation is the process of reorganizing the data into contiguous blocks.

Defragmenting SSD storage is not as necessary as on HDDs, but Windows can still defrag SSDs on a schedule with the Optimize Drives (dfrgui.exe) app in Windows 10. Defragmentation is set by default and can also be scheduled. [Figure 6-19](#) shows the Optimize Drives app in Windows 10.



**Figure 6-19** The Optimize Drives App in Windows 10

## Registry Editor



The Windows Registry is a hierarchical database that contains all the configurations and settings Windows uses. The Registry Editor is the application you use to view or edit settings and configurations. Advanced users can modify and create configurations in the Registry database.

Under most normal circumstances, the Registry does not need to be edited or even viewed. However, Registry editing might be necessary under the following circumstances:

- To view a system setting that cannot be viewed through other interfaces.
- To add, modify (by changing values or data), or remove a Registry key that cannot be changed through normal Windows menus or application settings. This might be necessary, for example, to remove traces of a program or hardware device that was not uninstalled properly or to allow a new device or program to be installed.

- To back up the Registry to a file.

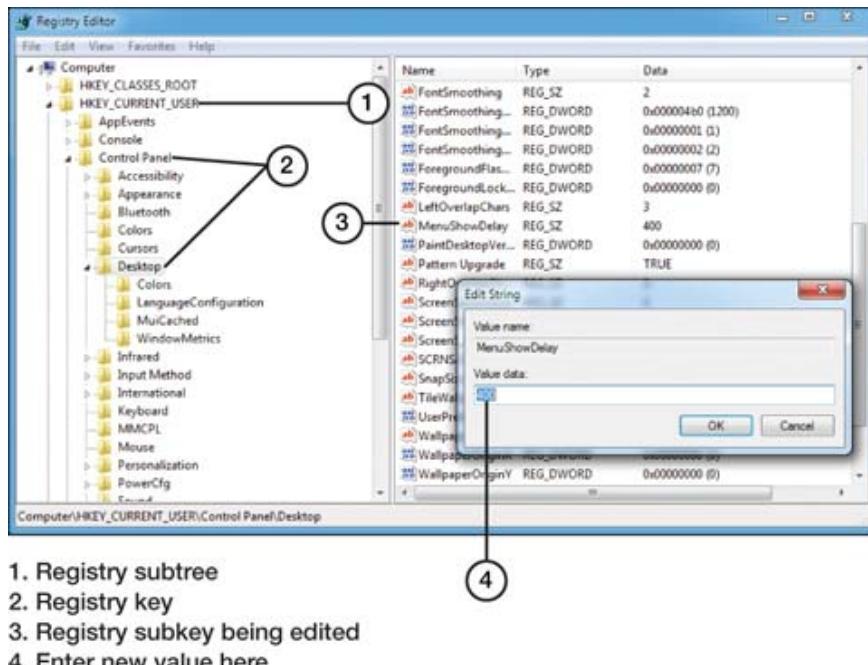
To access the **Registry Editor (regedit.exe)**, either press Windows+R, enter the command **regedit**, and press Enter; or use the search bar and type **regedit**. Changes made using regedit are automatically saved upon exit. However, you might need to log off and then log back on or restart the system for changes to take effect.

## CAUTION

The Registry should never be edited unless a backup copy has been made first. No Undo option exists for individual edits, and there is no way to discard all changes when exiting regedit.

Editing the Windows Registry can be difficult because Registry keys can be expressed in decimal, hexadecimal, or text. When editing the Registry, be sure to carefully follow the vendor instructions.

**Figure 6-20** shows the Registry with a modification being made to the MenuShowDelay Registry key, which is not accessible within normal Windows display menus.



## **Figure 6-20** Using regedit

Always back up the Registry before editing it. Follow these steps to back up part or all of the Registry to a text file:

**Step 1.** Start **regedit**.

**Step 2.** To make a partial backup, highlight the section of the Registry to be backed up.

**Step 3.** Click **File** and select **Export**.

**Step 4.** Select a location to store the Registry backup.

**Step 5.** Enter a name for the backup.

**Step 6.** Click **All** to back up the entire Registry. Click **Selected Branch** to back up only the Registry branch you selected in step 2.

**Step 7.** Click **Save**.

## **Windows 10 Control Panel Utilities**



**220-1102: Objective 1.4:** Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility.

The Control Panel is the major starting point for adjusting the hardware and user interface settings in Windows. Although Windows 10 includes Settings, many configurations in Windows are performed through the Control Panel.

### **Note**

Just as there are often different ways to access information in the Windows OS, this section repeats some content from other chapters, but in the context of the Control Panel. This repetition is done to help readers who are tracking the CompTIA A+ Core 2 objectives, which themselves have elements of redundancy.

## Starting Control Panel

To start Control Panel in Windows 10, type **Control Panel** in the search box and then select the Control Panel link. Another option is to press Windows+R, type **control**, and press Enter.

## Internet Options

Access the Internet Options menu via the Control Panel. [Figure 6-21](#) shows the Internet Properties dialog that appears, with the Security tab selected. Note that these choices differ from the options available in the Network and Sharing Center.



**Figure 6-21** Internet Options in the Control Panel

The Internet Properties dialog accessed from the Control Panel has seven tabs, which [Table 6-6](#) describes.



**Table 6-6** Internet Properties Dialog Tabs

Tab	Function
General	Set the home page; set tab settings; delete browsing history, cookies, temporary files, and saved passwords; change appearance; and configure accessibility settings
Security	Configure security zones
Privacy	Select privacy settings for the current zone, location settings, pop-up blocker, and InPrivate browsing settings
Content	Set options for family safety, SSL certificate management, AutoComplete, and feeds
Connections	Set options for VPNs, dial-up, LAN connections, and proxy servers
Programs	Select the default web browser, manage add-ons, select the default HTML editor, and set the default apps for email and other Internet services
Advanced	Enable and disable accelerated graphics; configure accessibility settings, browsing settings, HTTP settings, international settings, multimedia settings, and security settings; and reset Internet Explorer to the default settings

Many of the Control Panel utilities in the A+ objectives are discussed in other chapters. [Table 6-7](#) briefly summarizes them.

**Table 6-7** Control Panel Utilities and Their Settings

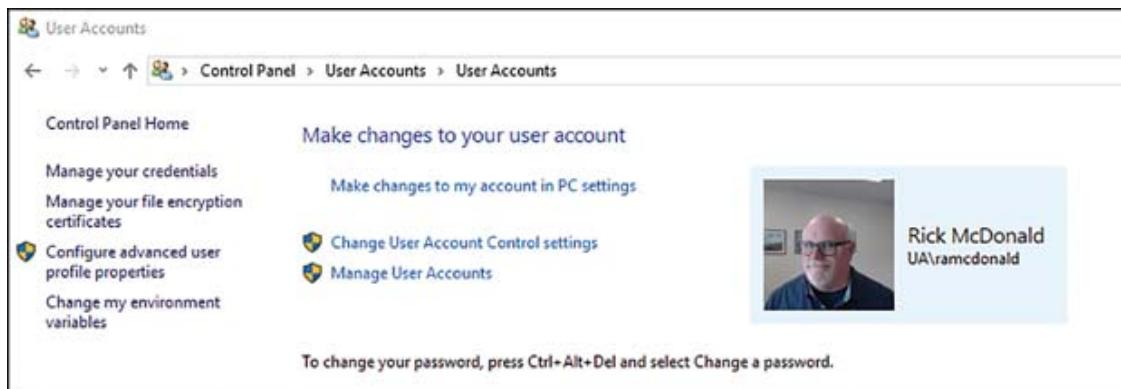
Control Panel Utility	Function	Chapter
Devices and Printers	Adding displays, cameras, scanners, and so on.	3
Programs and Features	Uninstalling and changing programs.	6
Network and Sharing	Viewing and managing network connections.	2

Control Panel Utility	Function	Chapter
Center		
System	Contains many of the other settings in the control panel. Most settings that users will want to change reside here, including Windows Defender, sound, and displays.	Various
Windows Defender Firewall	Configuring security.	7
Mail	Adjusting mail settings for Microsoft Outlook email users.	3
Sound	Setting up speakers, headphones, and microphones; managing event sounds and themes.	1

The following sections discuss some less intuitive Control Panel utilities.

## User Accounts

From the Control Panel, if you select Accounts, you can manage the user account and access to other users. [Figure 6-22](#) shows the Windows 10 account options from the Control Panel.



## **Figure 6-22 User Accounts in the Control Panel**

## **Device Manager**

The Device Manager accessed in the Control Panel is the same one discussed under the MMC, in the earlier section, “Microsoft Windows 10 Operating System (OS).” It is a good place to start for adding and removing devices and troubleshooting device problems.

## **Indexing Options**

The Indexing Options page in the Control Panel manages the indexing of data on a computer. Using these options can help increase the ease and speed for finding information. Just as the index in the back of this book helps you locate a specific topic, indexing the computer makes it easy for the search tool and selected apps to find useful information.

Files and their text content are indexed by default. If a user is searching for a specific document and remembers key words but not the name of the document, typing in the words returns documents that use those words.

Indexing can be administered. If enabled, it automatically indexes new documents and files as they are created.

## **Administrative Tools**

The Administrative Tools page in the Control Panel is an easy way to access tools to manage the computer. Some of these tools are familiar from the previous section, such as the System Information, Resource Monitor, System Configuration, Disk Cleanup, Disk Defragment, Registry Editor, and Event Viewer utilities. Several of the tools in this panel are discussed in other sections.

## **File Explorer Options**

The File Explorer Options properties sheet affects how Explorer does the following:

- Displays file and folder information (View tab)
- Selects folders to index for searching (Search tab)

- Opens folders (General options tab)

By default, File Explorer hides the following file information:

- File extensions for registered file types. For example, a file called letter.docx displays as letter because Microsoft Word is associated with .docx files.
- The full path to the current folder.
- Files or folders with hidden or system attributes, such as the AppData folder.
- The Windows folder.

Concealing this information is intended to make it harder for users to “break” Windows, but having this information hidden also makes management and troubleshooting more difficult.

The default hidden settings can be changed using the File Explorer Options applet in Control Panel. To change defaults, follow these steps:

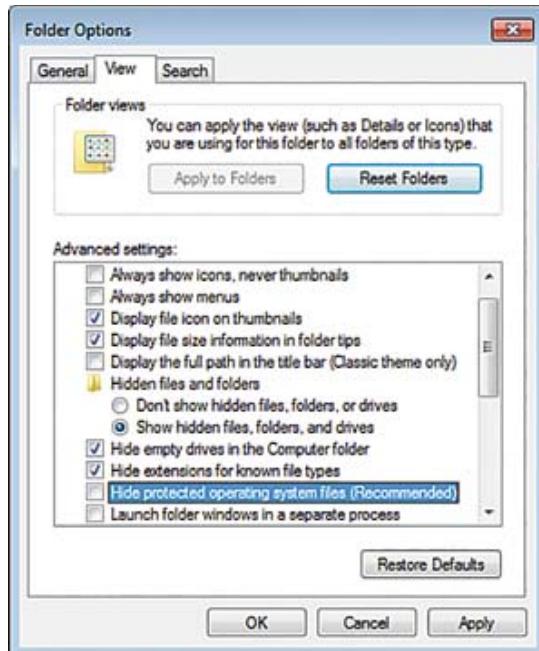
**Step 1.** Open **File Explorer**.

**Step 2.** Click or tap the **View** tab. Select the **Options** drop-down and then choose **Change Folder and Search Options**.

**Step 3.** Select the options you want (see [Figure 6-23](#)). The following changes are recommended for experienced end users:

- Enable the Display the Full Path in the Title Bar option
- To see all file extensions, disable the Hide Extensions for Known File Types option.
- If you are maintaining or troubleshooting a system, change the following:
  - To view hidden files, enable the Show Hidden Files, Folders, and Drives setting.
  - Disable the Hide Protected Operating System Files setting.

**Step 4.** Click **OK** to close the Folder Options window.



**Figure 6-23** The View Tab of the Folder Options Dialog in Windows with Recommended Options Set

## Power Options

You can manage power options from the Control Panel Power Options applet. If a Power Options icon is available in the notification area of the Windows taskbar, use it to view the current power option setting and, if desired, select a different one.

## Hibernate

The Hibernate option, which was originally available in Windows 7, creates a special disk file (hiberfil.sys) that records open apps, memory contents, and the apps' positions onscreen. In effect, it "pauses" the system so that you can return to right where you left off.

In Windows 10, Hibernate is not a listed option for the shutdown menu; however, it can be added by modifying a power plan: Select the Choose What the Power Buttons Do link under **Power & Sleep Settings >**

**Additional Power Settings.** Hibernate is an available option when you are choosing what happens when you press the power button, press the sleep button, or close the lid. To awaken a system from hibernation, press

the power button on the computer. If the system has a password set for access, you are prompted to enter the password to restart the system.

## Note

The options of sleep and hibernate are available. They are similar power-saving options but differ in where they store active programs. Sleep mode stores running programs in RAM and uses little power. Hibernate stores them in the hard drive and allows the power to turn off.

## Power Plans

Standard Windows versions offer three standard power plans (with a fourth power plan available only in Windows Pro):

- **Balanced:** Default plan. Balances performance with energy consumption.
- **Power Saver:** Reduces CPU performance and screen brightness more than the Balanced plan, for longest battery life.
- **High Performance:** Offers the fastest CPU performance, brightest screen, and shortest battery life.
- **Ultimate Performance:** Limited to Windows 10 Pro Workstation edition for high-end computers.

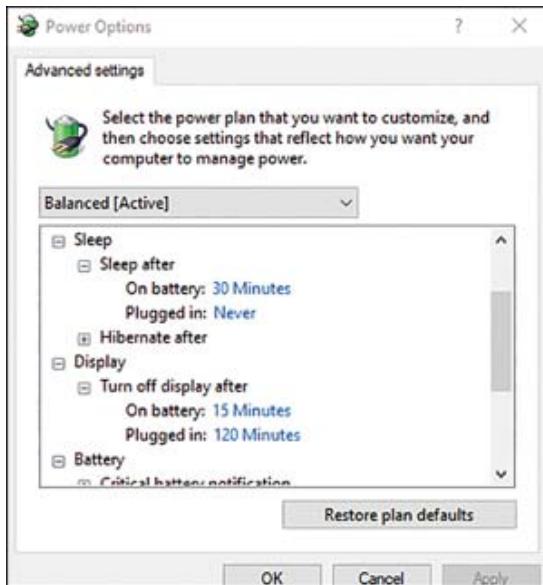
## Note

If your computer supports Modern Standby, a power management plan in Windows, it may be that the only option available is Balanced. However, you can still create a custom plan. Desktop computers hide Power Saver by default; laptop computers hide High Performance by default.

## Note

Some portable device vendors offer additional plans in systems with Windows preinstalled. Tablets offer only the Balanced power plan.

To change a plan, click or tap Change Plan Settings. You can change the sleep or hibernate settings for sleep times, display times, and battery levels. Figure 6-24 shows the **Power Options > Advanced Settings** menu.



**Figure 6-24** Advanced Power Options

To create a new power plan, click Create a Power Plan in the Power Options dialog. Then in the Create a Power Plan dialog, follow these steps:

- Step 1.** Select a plan to use as the basis for your plan.
- Step 2.** Enter a plan name and click **Next**.
- Step 3.** Specify timings for the display and sleep, and then click **Create**.

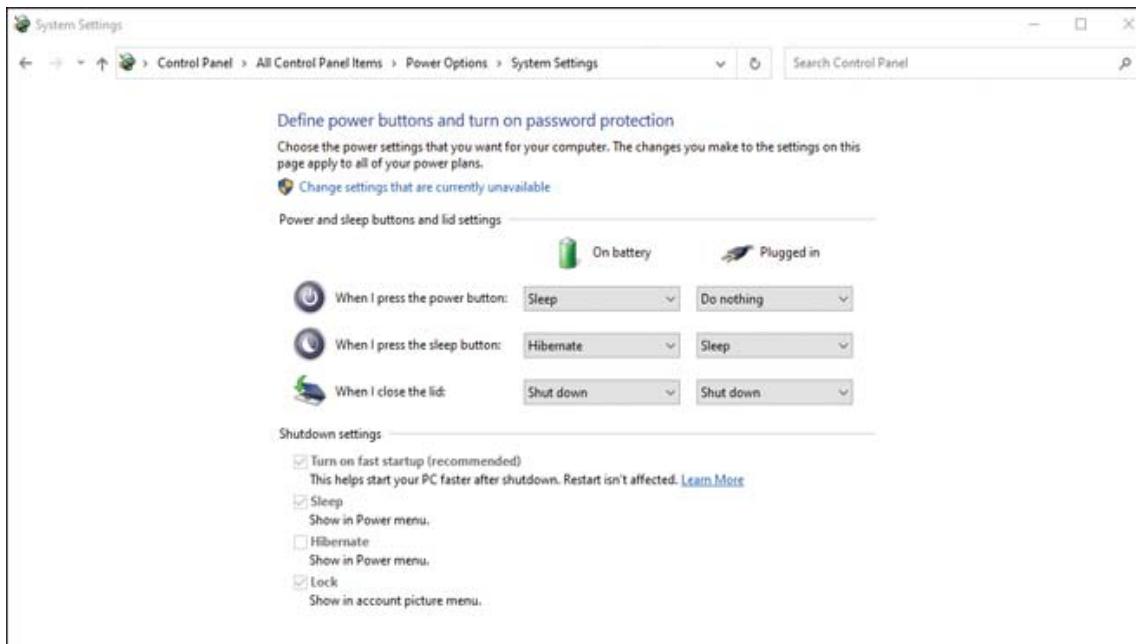
## Sleep/Suspend

Sleep/Suspend mode is supported in Windows 10. If the system does not correctly enter Sleep/Standby mode, startup programs might be interfering with this mode. Use **msconfig** to selectively disable startup programs until you discover the offending app.

With most laptops and many desktops, you can put the computer into sleep mode by pressing a special sleep key or by pressing the power key and releasing it right away. To change how the sleep or power key works, modify your power plan.

## Standby, Lid, and Fast Startup Options

Settings for power, sleep, and lid closure are managed in the Power Options by choosing the link What Closing the Lid Does. This brings up System Settings for power options. Note that options are set with both check box and drop-down menus, as shown in [Figure 6-25](#). This figure shows options for doing nothing, sleeping, hibernating, and shutting down.



**Figure 6-25** Advanced Power Options

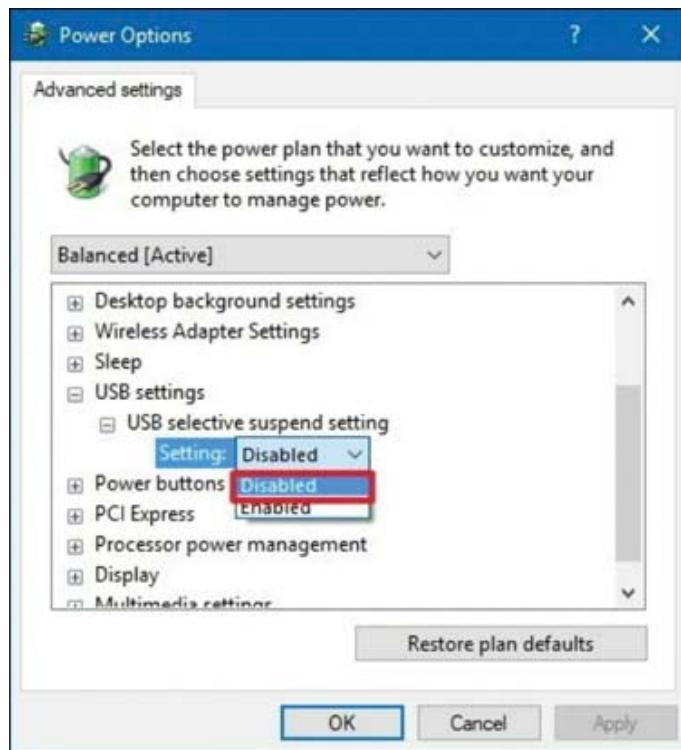
## Universal Serial Bus (USB) Selective Suspend

USB selective suspend is a power management setting that allows a computer to awaken from sleep with a signal via the USB port, such as a USB mouse. The setting is necessary because if all USB ports went to sleep, wiggling a mouse would not wake the computer; selective USB ports are set to respond to a signal from an attached device.

Occasionally, this feature, which is enabled by default, can cause problems with USB devices. Disabling the setting can help because sleep mode no longer powers off USB devices.

To disable USB selective suspend from the Power Options menu, click the link to Change Plan settings then click the link for Change Advanced Power

Settings. This brings up the menu in [Figure 6-26](#). Open the USB settings and select Disable, and then select OK to save the change.



**Figure 6-26** Advanced USB Selective Suspend Settings

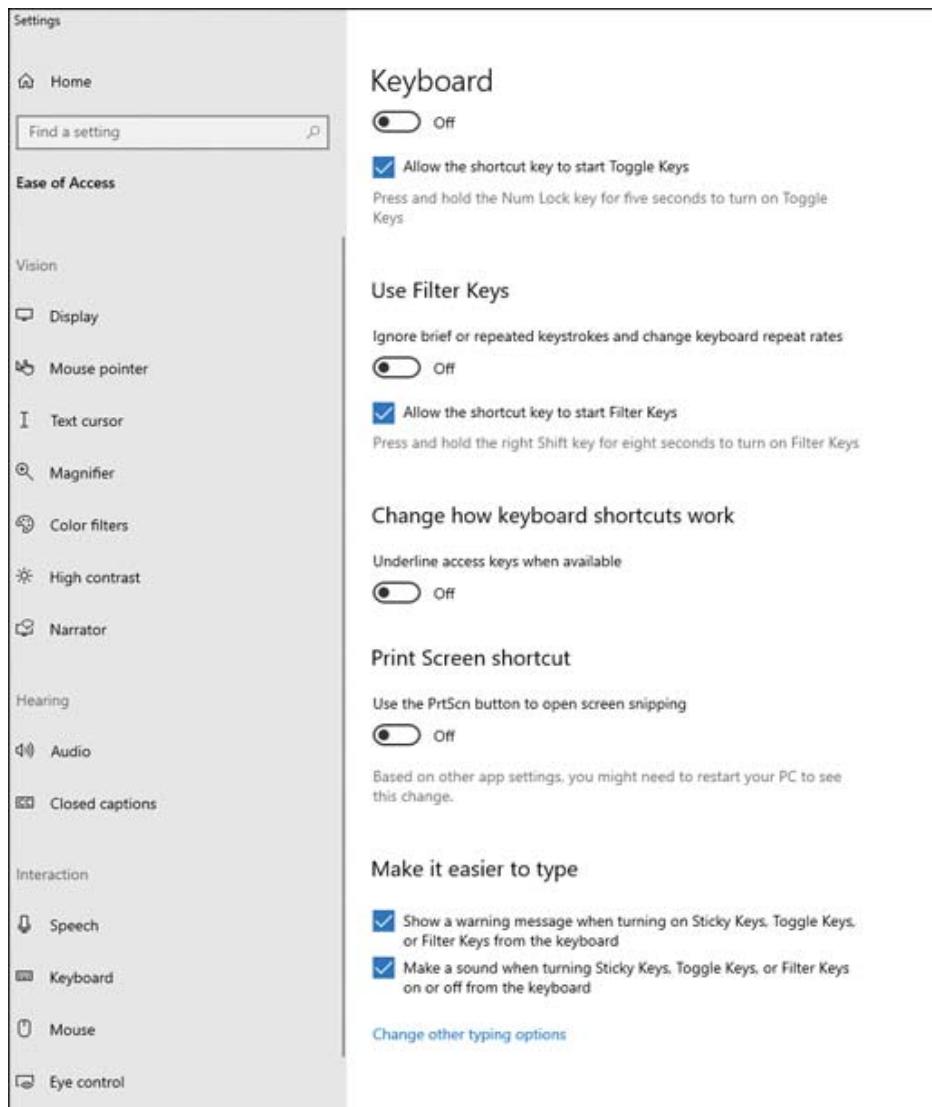
## Note

For Sleep/Standby mode to work correctly, the system needs to support the S3 power setting in the system BIOS/UEFI.

## Ease of Access

[\*\*Ease of access\*\*](#) settings are used to customize settings to the user's needs and tastes. Search for Ease of Access and select the app. Note that the column on the left has groups of settings for Vision, Hearing, and Interaction. These settings help users of varying abilities more easily interact with the computer.

[Figure 6-27](#) shows settings available from the keyboard section of the Interaction group. Explore all the settings to become familiar with all the options available.



**Figure 6-27** Keyboard Settings in the Ease of Access Settings Menu

## Windows Settings

220-1102  
Exam

**220-1102: Objective 1.5:** Given a scenario, use the appropriate Windows Settings.

A thorough understanding of the Settings menu is essential for an IT support technician. This section provides a basic overview of key Windows settings. It is recommended that you explore all the options in the Settings menu as sections are highlighted and described.

Access the Settings menu by using the Windows+X shortcut and then selecting Settings by entering **n**. With a mouse, select the Windows icon and click the Settings gear from the menu. The settings options have their own search bar, which is the easiest way to find unfamiliar settings. The previous section looked at the Ease of Access settings, but there are many more to explore.

## Note

Some settings are from view if a computer is on a managed network.

## Time and Language

The menu for Time and Language includes the following settings:

- **Date and Time:** Setting time and date formats and automatic time settings
- **Region:** Setting the country or region and the local format of date and time
- **Language:** Adding languages and changing keyboard language options
- **Speech:** Enabling voice recognition and choosing the computer's voice

## Update and Security

[Chapter 7](#) covers security, but you should be familiar with the security settings here. Be sure to visit and familiarize yourself with the links listed on the left under Windows Update and Security in the Settings menu.

## Personalization

The menu for Personalization includes settings for the following:

- **Background:** Choosing a background color, picture, or slideshow
- **Colors:** Light and dark colors for menus (such as the Windows menu)
- **Lock Screen:** Settings for locking an idle computer and the locked display

- **Themes:** Choices for background sounds, colors, or images
- **Fonts:** Font choices for Windows text and tools for importing fonts
- **Start (Windows key) Menu:** The Windows key hints at which keyboard key is being configured
- **Taskbar:** Preference settings for badge display, showing or hiding the taskbar, and setting the command prompt/PowerShell default when right-clicking the taskbar

## Apps

The menu for Apps includes the following settings:

- **Apps & Features:** Installing new apps or removing old ones
- **Default Apps:** Determining the apps chosen for music, pictures, mail, browser, and so on
- **Offline Maps:** Downloading maps to use when offline
- **Apps for Websites:** Setting opening sites with an app or the browser
- **Video Playback:** Setting video resolution and battery power settings
- **Startup:** Managing which apps will start when logging in

## Privacy

Privacy settings are generally about sharing your usage information and data history with Microsoft for research purposes. These settings determine what is shared and what is not:

- **General:** Sharing web activity and app launches, managing web advertising settings
- **Speech:** Collecting speech patterns
- **Inking & Typing Personalization:** Collecting user handwriting and typing patterns
- **Diagnostic and Feedback:** Sharing software problems and crashes with Microsoft

- **Activity History:** Managing settings for local storage and external sharing of activity
- **App Permissions:** Managing privacy settings for each app or device

## System

This is likely the most important app to study. System settings are used throughout the A+ content in this book, and many will be familiar by now. Many of the settings impact the performance of the computer.

## Devices

The menu for Devices includes the following settings:

- **Bluetooth & Other Devices:** Managing settings for keyboard, mouse, audio, and so on
- **Printers and Scanners:** Adding and removing printers and scanners
- **Mouse:** Managing mouse settings such as the primary button, scrolling, and pointer options
- **Touchpad:** Managing settings for sensitivity, scrolling, zoom, and so on
- **Typing:** Managing settings for spell checking, text suggestions, and spacebar options
- **Pen and Window Ink:** Handling settings for the handwriting font
- **AutoPlay:** Determining default settings for playing videos or music from apps
- **USB:** Issuing charging notifications and managing battery settings

## Network and Internet

The menu for Network and Internet includes the following settings:

- **Status:** Managing general information on current network settings and activity

- **Wi-Fi:** Setting specific Wi-Fi settings, handling IP and hardware information
- **Ethernet:** Granting access to physical and virtual Ethernet interface settings
- **Dial-up:** Granting access to dial-up settings if phone line and modem are available
- **VPN:** Allowing and adding virtual private network access
- **Airplane Mode:** Enabling and disabling wireless, Bluetooth, and cellular data
- **Mobile Hotspot:** Sharing and Internet connection over Bluetooth or Wi-Fi
- **Proxy:** Managing settings for using a proxy server (not applicable to VPNs)

## Gaming

The menu for Gaming includes the following settings:

- **Xbox Game Bar:** Setting shortcuts on an Xbox game bar
- **Captures:** Managing settings to capture game play audio and video
- **Game Mode:** Optimizing the PC for gaming
- **Xbox Networking:** Monitoring status and performance, handling Xbox Live connectivity

## Accounts

The menu for Accounts includes the following settings:

- **Your Info:** Managing profile settings for the user
- **Email & Accounts:** Adding accounts used by other apps for easier sign-in
- **Sign-in Options:** Setting sign-in procedures with security settings and requirements

- **Access Work or School:** Handling connection settings for managed computers on a domain
- **Other Users:** Adding other accounts to the computer
- **Sync Your Settings:** Allowing settings to sync across devices on a Microsoft account

## Microsoft Windows Networking Features on a Client/Desktop

220-1102  
Exam

**220-1102: Objective 1.6:** Given a scenario, configure Microsoft Windows networking features on a client/desktop.

Windows networking includes three different types of networks, remote control and assistance options, a built-in firewall, and much more. The following sections can help you master networking concepts.

Key  
Topic

### Workgroup vs. Domain Setup

Windows 10 supports both two different types of networks: **workgroups** and **domains**. The following sections describe how they differ from each other.

### Workgroup Networking

Windows 10 supports workgroup networks. In a workgroup network, the following applies:

- All computers can share folders and devices with other computers in a peer-to-peer arrangement. File and printer sharing (which is configured by default) is required for any computer that will share resources.
- All computers must be part of the same local network or subnet. For example, computers in the IP address range 192.168.1.100–192.168.1.120 with the subnet 255.255.255.0 can share resources with

each other but not with computers in the IP address range 192.168.2.100–192.168.2.120.

- The workgroup does not have a password; however, each computer must have a user account for each user who will access that computer (unless password-protected sharing is disabled). For example, a computer can have an account for Mark and an account for Mary, and another computer could have an account for Mark and an account for Jerry. Mark might be able to connect to both computers, but Mary and Jerry might be able to connect to only one computer. In this situation, Mark could use one of the computers and log in via the network to another computer.

The workgroup is identified in the Device Specification section of the System About sheet. Go to Settings, select System, and select About from the links menu on the left.

The easiest way to view your computer's name is to type the name in the search box; the option to view your device name links to the About page above.

## Creating a Workgroup

To create a workgroup in Windows, follow these steps:



**Step 1.** Configure all devices in the workgroup to use the same range of IP addresses and the same subnet. If the devices obtain their IP addresses from a router, this step has already been done for you.

**Step 2.** Confirm that each device has a unique computer name. The name is generated automatically when Windows is installed on a device. To verify the name, press Windows+R, type the command **sysdm.cpl** in the Run dialog box, and press Enter. Alternatively, simply right-click **Start > Settings** and select **System** to bring up the Setting About screen. An easy way to access System Properties is to open File Explorer, right-click **This PC**, and select **Properties**.

**Step 3.** Confirm that each device is in the same workgroup. (The default workgroup name is WORKGROUP.)

## Domain Setup

Larger networks, including networks with users in multiple locations, use domain networking. Some of the special features of domain networking include the following:

- **Shared resources** (files, folders, printers, and devices) and user accounts are stored on servers. An Active Directory server is used to authenticate users, and other servers can be used for print, file, email, and other services.
- User accounts are not tied to a particular computer. A user on a domain can use any computer or computers on the domain and have access to their files and shared resources.
- Group Policy can limit resources available to a particular user. For example, Group Policy settings can prevent a user from connecting a USB flash drive.
- Group Policy can also limit configuration settings that are available to a user. For example, Group Policy can be used to turn off AutoPlay for removable-media devices.
- Different local networks with hundreds to thousands of users can be part of a single domain.

The domain setup for a computer is performed from the Computer Name section of the System properties sheet. To join a domain, follow these steps:

**Step 1.** Open the System Properties sheet.

**Step 2.** Click or tap **Change Settings**.

**Step 3.** On the Computer Name tab, click or tap **Network ID**.

**Step 4.** Confirm that This Computer Is Part of a Business Network is selected. Click or tap **Next**.

**Step 5.** Confirm that My Company Uses a Network with a Domain is selected. Click or tap **Next**.

**Step 6.** Review the information needed to connect to a domain, and click **Next**.

**Step 7.** Enter the username, password, and domain name, and click **Next**.

**Step 8.** Click **OK** on the “Welcome to the Domain” message.



## Network Shares

A shared folder or drive can be accessed by other computers on the network. Shares can be provided in three ways:

- On a client/server-based network or on a peer-to-peer network with peer servers that support user/group permissions, shares are protected by lists of authorized users or groups. Windows 10 supports user/group access control.
- A workgroup network can offer unlimited sharing (full control or read-only) for any user who connects to a system if password-protected sharing is disabled. (This is not recommended.)
- A network share can be accessed by either its mapped drive letters or its folder names in File Explorer.

When user/group-based permissions are used, only members who belong to a specific group or who are listed separately on the access list for a particular share can access that share. After users log on to the network, they have access to all shares they have been authorized to use, without needing to provide additional passwords. Access levels include full and read-only; on NTFS drives, other access levels include write, create, and delete.

## Administrative Shares

Administrative shares are hidden shares that can be identified by a \$ at the end of the share name. Standard users who are browsing to the computer over the network cannot see these shares; they are meant for administrative use. All the shared folders that include administrative shares can be found by navigating to **Computer Management > System Tools > Shared Folders > Shares**. Note that every volume within the hard drive (C: or D:, for example) has an administrative share; for example, C\$ is the administrative share for the C: drive. Although it is possible to remove these by editing the Registry, this is not recommended because it can cause other networking issues. Only administrators should have access to these shares.

## Sharing a Folder

To share a folder with Windows 10, follow these steps:

**Step 1.** Ensure that file sharing is enabled by opening the Control Panel and double-clicking the **Network and Sharing Center** icon.

**Step 2.** Open Windows File Explorer on the taskbar and click **This PC**.

**Step 3.** In the This PC window, navigate to a folder that you want to share.

**Step 4.** Right-click the folder that you want to share and choose **Share With**.

**Step 5.** If password-protected sharing is enabled, click **Selected People**; select which users will have access to the shared folder and select their permission levels. To allow all users, select the **Everyone** group within the list of users.

**Step 6.** When you have finished configuring permissions, click **Share** and then click **Done**.

## Mapped Drives

Windows enables shared folders and shared drives to be mapped to drive letters on clients. In File Explorer/This PC, these mapped drive letters show up in the list along with the local drive letters. A shared resource can be accessed either through Network (using the share name) or through a mapped drive letter.

Drive mapping offers the following benefits:

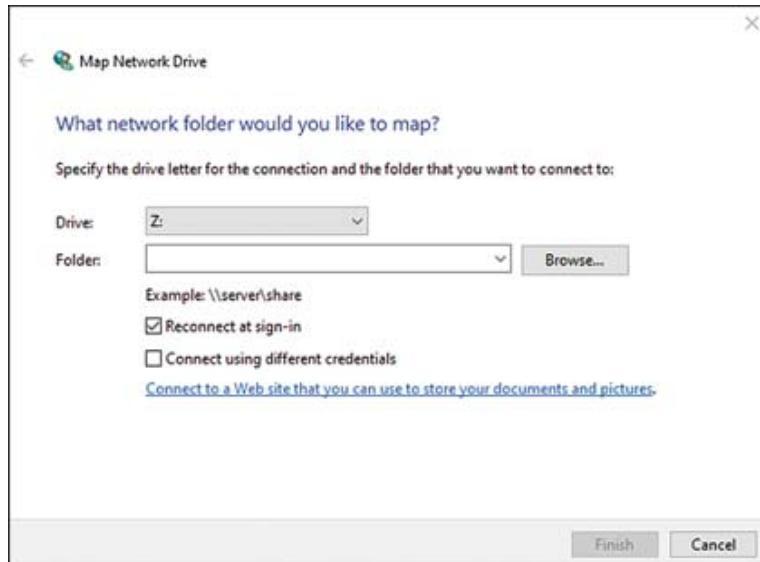
- A shared folder mapped as a drive can be referred to by the drive name instead of by using a long Universal Naming Convention (UNC) path.
- When using MS-DOS programs, keep in mind that using mapped drives is the only way for those programs to access shared folders.

Mapping drives and folders is a rather straightforward procedure:



**Step 1.** Launch the File Explorer from the taskbar and right-click **This PC**.

**Step 2.** Select **Map Network Drive** from the right-click drop menu to display the window in [Figure 6-28](#).



**Figure 6-28** The Map Network Drive Dialog for Creating a Temporary or Permanent Drive Mapping

**Step 3.** Select a drive letter from the list of available drive letters; only drive letters not used by local drives are listed. Drive letters already in use for other shared folders display the UNC name of the shared folder.

**Step 4.** Click the **Reconnect at Login** box if you want to use the mapped drive every time you connect to the network. This option should be used only if the server will be available at all times; otherwise, the client will receive error messages when it tries to access the shared resource.

**Step 5.** Click the **Connect Using Different Credentials** box if you want to use a different username/password to connect to the shared resource.

**Step 6.** Click **Finish**.

## Printer Sharing vs. Network Printer Mapping

Printers connected to network computers can be shared or printers can be connected directly to a network with Ethernet or wireless Ethernet (Wi-Fi) connections.

To perform printer sharing, follow these steps:

**Step 1.** In the Settings menu, open Devices and click **Printers & Scanners** on the left.

**Step 2.** Click the printer to be shared.

**Step 3.** Click the **Manage** button.

**Step 4.** Click the **Printer Properties** option.

**Step 5.** Click the **Sharing** tab.

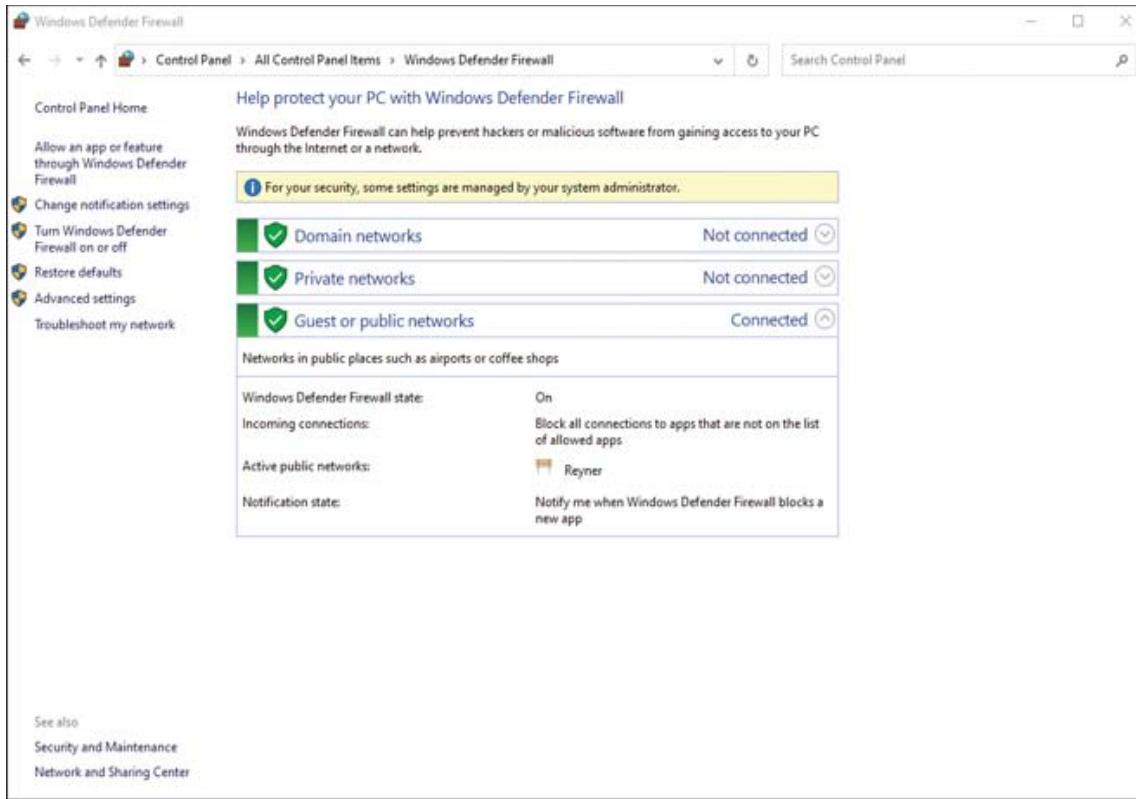
**Step 6.** Check the **Share This Printer** option.

## Local OS Firewall Settings

**Windows Defender Firewall** provides protection against unwanted inbound connections and can also be configured to filter outbound connections. Use one of the following methods to open Windows Defender Firewall:

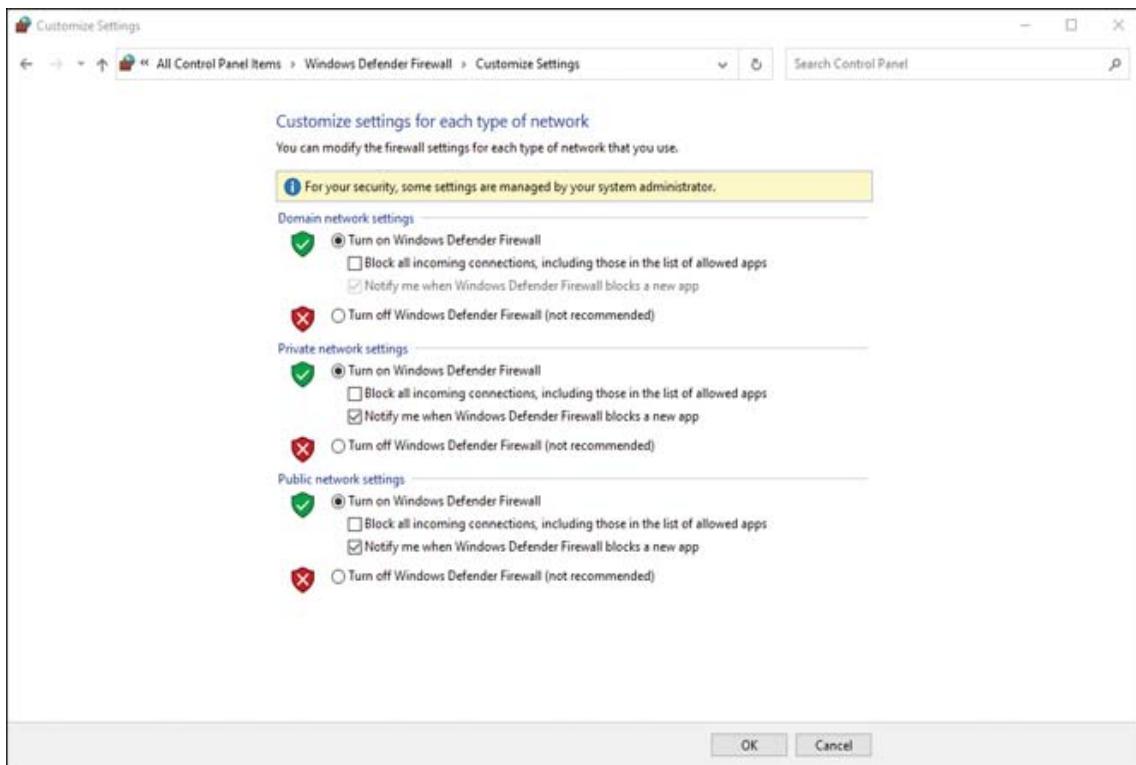
- Click or tap the Windows Defender Firewall link in the Control Panel.
- Search for Windows Defender Firewall and start it.

When Windows Defender Firewall starts, it displays Firewall settings for the current connection (see [Figure 6-29](#)).



**Figure 6-29** Viewing the Firewall Settings for the Current Connection

To change notification settings or turn the firewall on or off, click or tap the Change Notification Settings link or the Turn Windows Firewall On or Off link in the left pane (see [Figure 6-29](#)), to open the Customize dialog box (see [Figure 6-30](#)). Either selection opens the Customize dialog box for settings in a private and public network.



**Figure 6-30** Viewing the Customize Settings Dialog Box

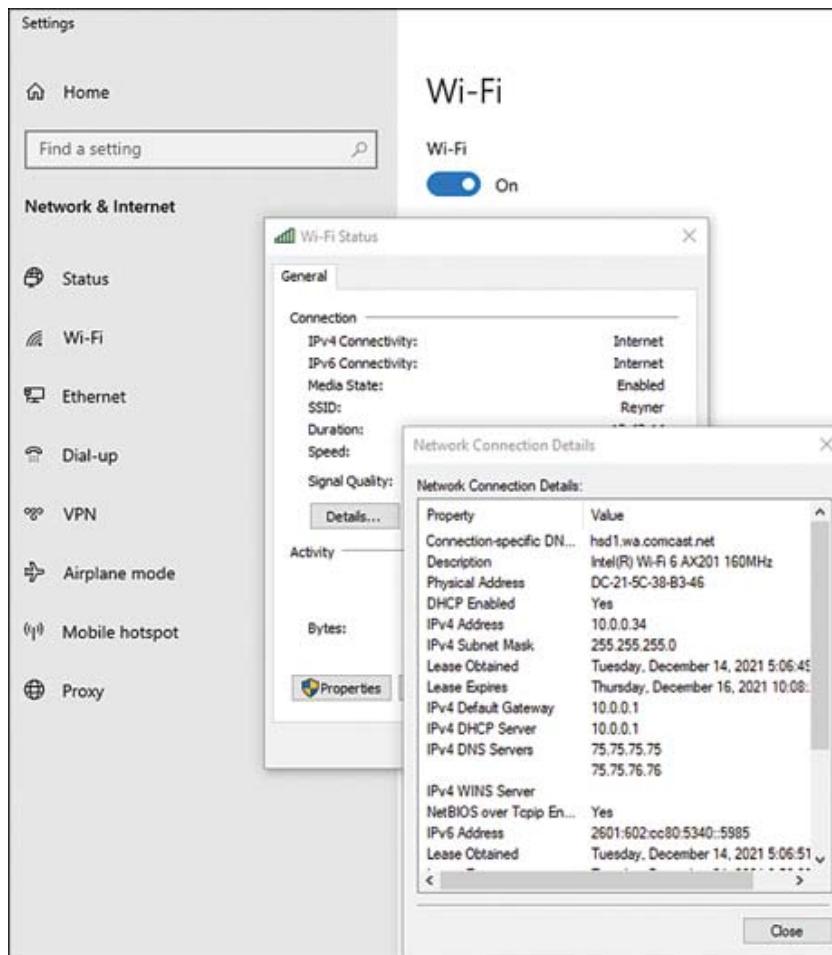
In this dialog box, the default settings are the same:

- Windows Defender Firewall is turned on.
- The user is notified when Windows Defender Firewall blocks a new app.
- To block all incoming connections on a public network, click or tap the first check box in the Public Network Settings section.
- If malware or user error has turned off Windows Defender Firewall and no other firewall is present, click or tap Turn On Windows Defender Firewall in both sections.
- If the computer uses a third-party firewall, click or tap Turn Off Windows Defender Firewall in both sections.
- If an app's installer recommends or requires that firewalls be turned off, turn off Windows Defender Firewall and then turn it on again when the app installation process is complete.

For more information on firewalls, see [Chapter 7](#).

# Client Network Configuration

Computers that are members of a local network must be configured so that they can communicate with each other. This is most often done with an **Internet Protocol (IP) addressing scheme**. Figure 6-31 shows the settings that are necessary to attach a device to a network. You configure these address settings by accessing the active network interface in the Network and Sharing Center. Current network address settings can be viewed by accessing the active network interface in Settings. Some of the key settings are described next. (Most of these can be quickly accessed by clicking the network connection icon on the taskbar and selecting Properties.)



**Figure 6-31** Local IP Settings

Networking is a broad topic worthy of its own certification, and many books have been written on the topic. An IT support technician will encounter the

basic settings described here, so knowing what those settings involve is important. This section discusses the basic inputs to have a device join an IPv4 network.

Computers on a network have two types of addresses. The MAC address is permanent and does not change; it identifies devices physically on their own network. Administrators also can assign an IP address, which helps them communicate with devices on other networks beyond their local network and out to the Internet. Routers are the devices that keep track of network addresses and forward communication between networks. This is done using IP addressing. This section describes both IPv4 and IPv6 addresses within the scope of the A+ exam objectives.

As you read the following sections, refer to [Figure 6-31](#) to locate the settings in the Network Connection Details output.

## Internet Protocol (IP) Addressing Scheme

An IPv4 address is input using a decimal notation scheme with four 8-bit parts to an address. These parts are called octets because the number represents 8 bits. For example, many home routers and devices have an IPv4 network address similar to 192.168.1.0. In this case, the first three octets describe the network; the last octet, when assigned to a device, has a nonzero number to identify it on the network. A device on a network can be assigned any number from 1 to 254, which is the highest allowed number in this 8-bit addressing scheme.

## Subnet Mask

The number of bits representing networks and the number representing the host can change. Just looking at an address, there is no way to tell which bits or part of a bit describes the network address and which describes the host address. This is where the **subnet mask** comes in.

The purpose of a subnet mask is to help routers and devices distinguish network bits from host bits. The subnet mask is also 32 bits long and noted in groups of 8 bits. When a subnet mask bit is “on,” or a binary 1, the router does some calculating with the address to determine which is the network and which is the host. An IPv4 address is meaningless to a router (and to humans, for that matter) unless a subnet mask is configured.

For example, an IPv4 address of 192.168.1.1 with a subnet mask of 255.255.255.0 has the first three octets as the network and the last octet as the host. For a subnet mask of 255.255.0.0, the first three octets define the network and the last two define the hosts. The number here is 255 because it represents all 8 bits of the octet being set to 1.

Remember that the router is also a device on the network, and the interface connecting the router needs an IP address on the network. It is common practice to reserve the first host address, -x.x.x.1, for the router. This is not required, but it can make network management troubleshooting easier.

## Domain Name System (DNS) Settings

A domain name server usually belongs to an Internet service provider (ISP). **Domain Name System (DNS)** servers are special computers that keep track of the IP addresses of domain names, such as Microsoft.com, IRS.gov, and NYT.com. People use domain names in their browsers because they are much easier to remember than IP addresses (but you can type IP addresses into browsers, too). Each domain name has a specific IP address for locating the server on the Internet. The job of a DNS server is to match the domain name with the correct IP address so that packets can be delivered.

For the network in [Figure 6-31](#), DNS information can be found in the Network Connection Details window. In this example, the local router sends the domain name to the DNS server, whose IPv4 address is 75.75.75.75. The server responds to the router with an IP address for Microsoft.com and uses it to forward the information across the Web. This is a very fast process that lasts milliseconds, so a user will not notice the DNS conversation taking place.

## Gateway

Devices on a local network know about only other devices on the local network. They rely on a more sophisticated device (the router) for any communication outside. Setting a **gateway** address, also known as a default gateway, ensures that when a computer is sending communication out of the local network, it goes to the router. The default gateway is most likely the local router's local interface. In [Figure 6-31](#), the router interface is 10.0.0.1.

## Static vs. Dynamic

An IP address is assigned to a device on the network in two ways. Static IP addresses are configured by a network administrator and do not change over time. Dynamic addresses are assigned, or *leased*, temporarily and need to be renewed after a period of time. The network administrator can adjust how much time applies for the lease.

The vast majority of user IP addresses are assigned dynamically using the Dynamic Host Configuration Protocol (DHCP). A pool of network addresses is made available to the DHCP server; whenever a new device joins the network, it can be assigned a temporary, or leased, address.

Not all addresses should be dynamic, however. A network administrator can reserve some network addresses and not allow DHCP to use them. Those addresses can be statically assigned to servers, printers, and other important resources that need IP addresses that never change in the network.

Note that in [Figure 6-31](#), the default gateway (which is the router) is also assigned to be the DHCP server. Most routers can be configured to run the DHCP protocol.

## Establish Networking Connections

The Network and Internet page in the Control Panel is where options and wizards are found for the following connection types:

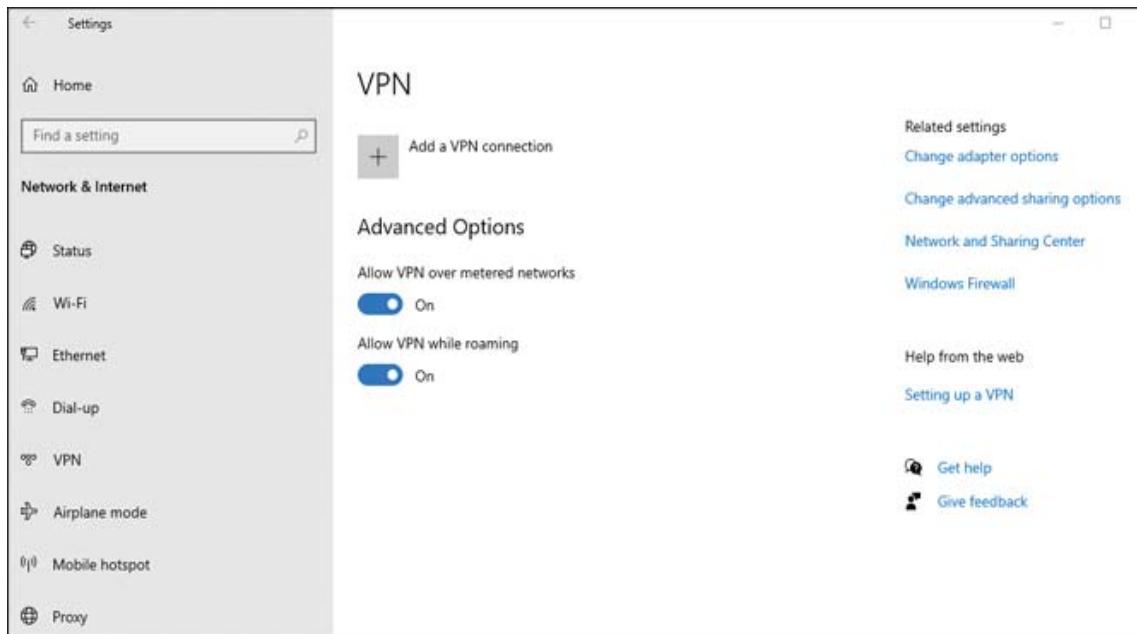
- Wi-Fi
- Ethernet (for wired connections)
- Virtual private networking
- Dial-up networking
- Hotspot
- Proxy

# VPN Connections

A **virtual private network (VPN)** connection creates a secure tunnel over a public network, such as the Internet, between two computers. Most domain VPNs have separate client software available for VPN access, but this can also be set up from Windows in the Control Panel or Settings. A VPN can be configured in both the Control Panel and in Windows Settings. To configure a new VPN connection in Windows Settings, follow these steps:



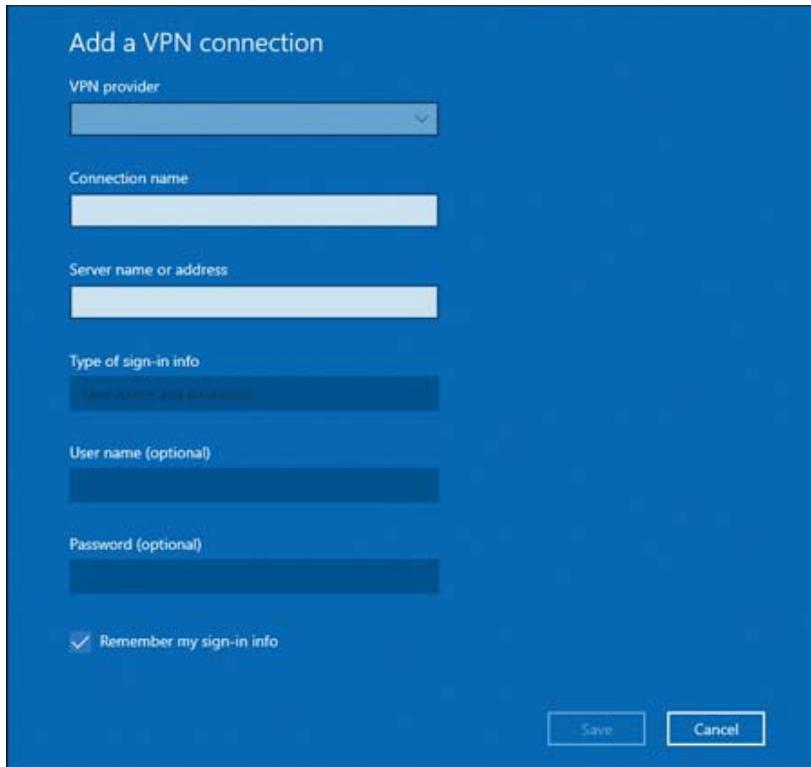
**Step 1.** On the **Settings > Network and Internet** page, select **VPN** from the left. This opens the dialog box in [Figure 6-32](#).



**Figure 6-32** Starting the VPN Connection Creation Process in Windows 10

**Step 2.** Click **Add VPN** Connection.

**Step 3.** Complete the VPN connection in [Figure 6-33](#).



**Figure 6-33** Setting Up a VPN Connection

## Wireless Connections

A wireless connection can be configured when the user clicks on the SSID from the taskbar or Settings menu. However, if you use the Wireless Connection option in the Network and Sharing Center in the Control Panel window, you can specify more options, including security types:



- Step 1.** In the Set Up a Connection or Network dialog box, click or tap **Connect to a Wireless Network** and click or tap **Next**.
- Step 2.** Enter the network name. Select the security type and enter the security key. To start the connection automatically, check the **Start This Connection Automatically** box. Click or tap **Next**.
- Step 3.** Click or tap **Close**. The connection is added to the list of connections.

## Wired Connections

Use the option to configure a wired connection if you are setting up a Point-to-Point Protocol over Ethernet (PPPoE) connection. This type of connection is used by cable or DSL ISPs that require the user to log in to the connection:



**Step 1.** In the Set Up a Connection or Network dialog box, click or tap **Connect to the Internet** and click or tap **Next**.

**Step 2.** Click or tap **Broadband (PPPoE)** and click or tap **Next**.

**Step 3.** Enter the username and password. Enter the domain. Check the **Remember This Password** box if the user does not want to enter the password again. Click or tap **Connect**.

The connection is stored along with other network connections.

## WWAN (Cellular) Connections

A **wireless wide area network (WWAN)** (cellular) connection shows up in the list of network connections after a SIM card is installed and activated by a mobile provider. To use this type of connection, select it from the list of network connections displayed when selecting the network icon in the taskbar or Settings.

If the access point name (APN), username, password, or other information has not yet been stored for the WWAN, the user must provide this information during the first use of the connection.

## Proxy Settings

A corporate network can use a proxy server as an intermediary between a network client and the destination of the request (such as a web page) from the network client.

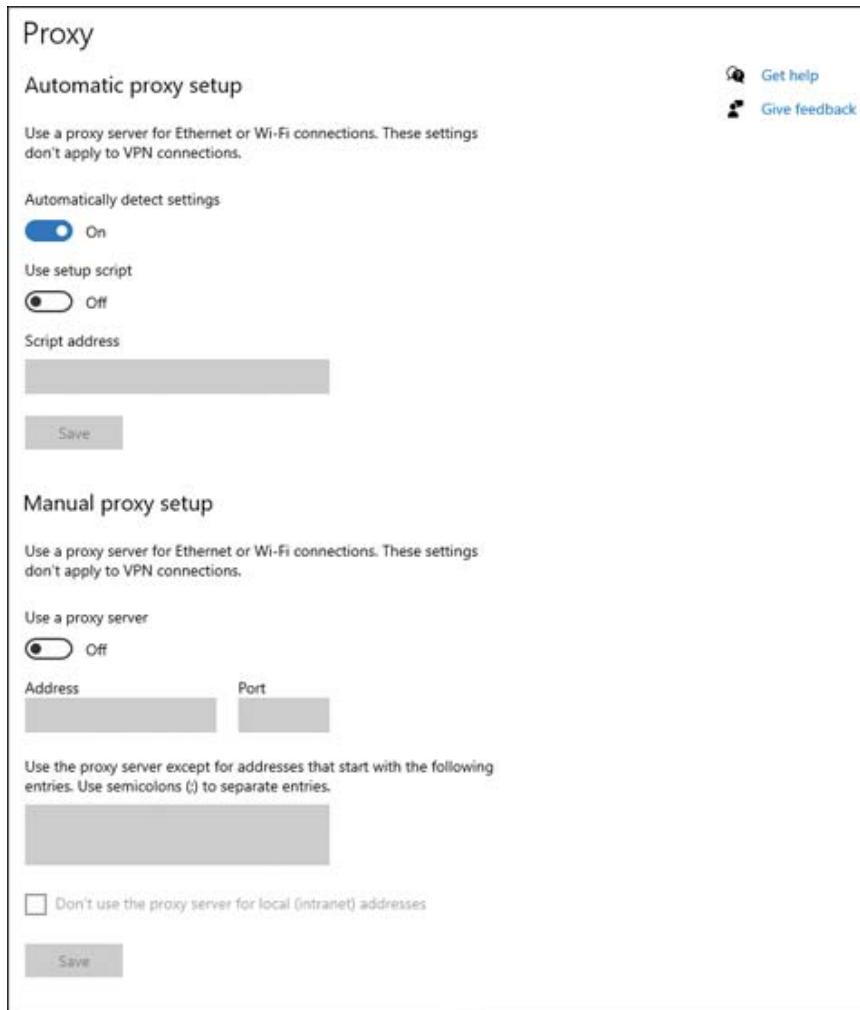
If a proxy server is used for Internet access and a configuration script or automatic detection are not available, the proxy server must be specified by server name and port number. To configure manual **proxy settings** for a LAN connection in Windows:

**Key Topic**

**Step 1.** Open the Network and Internet settings from the Control Panel.

**Step 2.** Click **Proxy**.

**Step 3.** If a script is provided, turn on the **Use Setup Script** option and enter the address. If configuring manually, turn on the **Use Proxy Server** option and add the address and port (see [Figure 6-34](#)).



**Figure 6-34** Setting Up Proxy Servers

**Step 4.** Click **Save** to save changes in each dialog box until you return to the browser display.

## **Public Network vs. Private Network**

When joining a Wi-Fi network, it is possible to choose whether to be seen by other users or to be undiscoverable by them.

For security reasons, it might be wise to remain undiscoverable on a public network, such as a coffee shop or other public venue, to avoid unwanted attention from unknown users.

If the computer is being used in a known, private network environment, it could be desirable to be discovered by others for the purposes of sharing files and printing resources. In that case, selecting a private network option is preferred.

It is possible to toggle the status of the network privacy setting by going to the wireless icon on the taskbar and clicking the Properties button. From there, simply choose Public or Private (see [Figure 6-35](#)).



**Figure 6-35** Public/Private Network and Metered Connections Settings

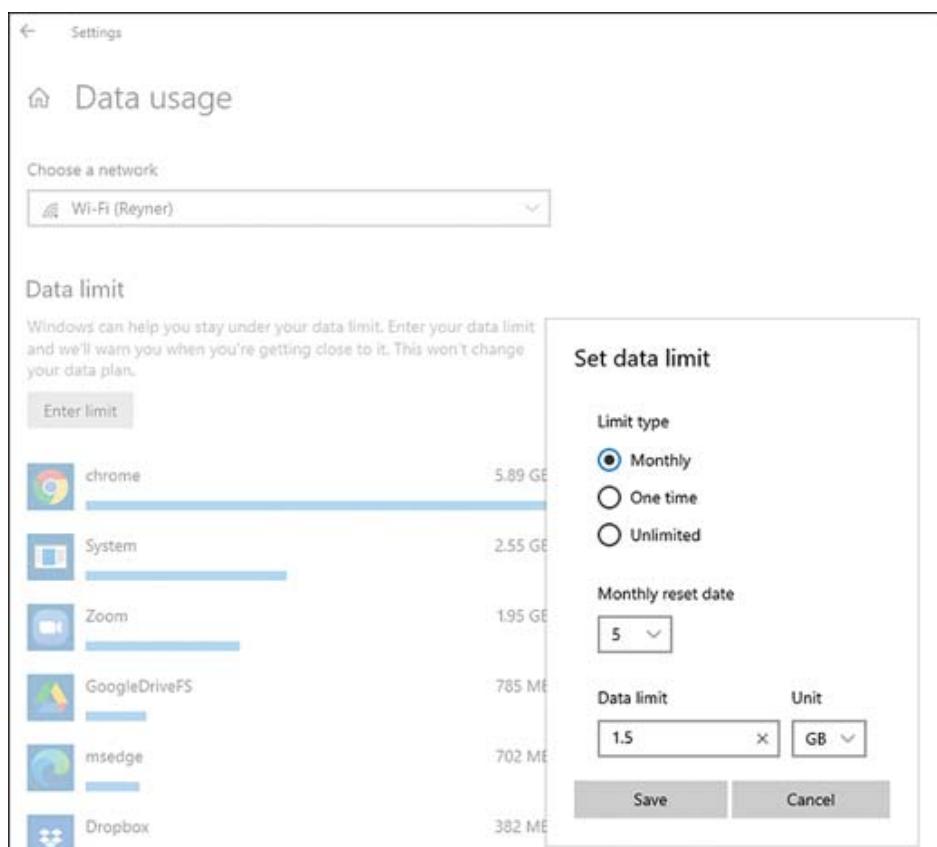
## File Explorer Navigation: Network Paths

Earlier in this chapter, the File Explorer (the folder icon on the taskbar) was used to map a network drive. Similarly, network information can be mapped using File Explorer by selecting the Network icon from the menu on the left. To trace a path to a network, and for other information, click the Network tab in the top left to see the ribbon of network options. From here, you can view network paths and add devices to the network.

## Metered Connections and Limitations

Many ISPs and mobile companies have data plans with usage thresholds that, when passed, can lead to increased costs and unpleasant surprises in a billing statement. One way to avoid accidental overages is to manage usage in the **Metered Connection** settings (see the bottom of Figure 6-35).

When the Metered Connection setting is turned on, details can be managed by clicking the Set a Data Limit to Help Control Data Usage on This Network link below the setting. Figure 6-36 shows the result. In this example, Windows enforces a monthly use of 1.5GB of data on the Reyner network, refreshing on the 5th of each month.



**Figure 6-36** Setting Data Limits for a Metered Connection

## Installation and Configuration Concepts

**220-1102: Objective 1.7:** Given a scenario, apply application installation and configuration concepts.



## System Requirements for Applications

Before you make any changes to a computer by installing hardware or software, it is essential to understand what hardware will work on the computer and what software will work with the hardware in place. This section is a basic review of considerations when upgrading hardware or installing software.



## 32-Bit vs. 64-Bit File Systems

A key purpose of operating systems is to keep track of all the files that are used on a computer. A file system describes how data and drives are organized. In Windows, the file system you choose for a hard drive affects the following:

- The rules for how large a logical drive (drive letter) can be and whether the hard drive can be used as one big drive letter or several smaller drive letters, or whether it must be multiple drive letters
- The efficiency of data storage (the less wasted space, the better)
- The security of a system against tampering
- Whether a drive can be accessed by more than one operating system

The term *file system* is a general term for how an operating system stores various types of files. Windows supports three different file systems for hard drives and USB flash drives: FAT32, NTFS, and exFAT. For CD storage, it uses CDFS.

### FAT32

FAT32 was introduced in 1995 and has the following characteristics:

- It has a 32-bit file allocation table, which allows for 268,435,456 entries ( $2^{32}$ ) per drive. An entry can be a folder or an allocation unit used by a file.
- The root directory can be located anywhere on the drive and can have an unlimited number of entries, which is a big improvement over FAT.
- FAT32 uses an 8KB allocation unit size for drives as large as 16GB.

The maximum logical partition size allowed is 2TB (that is, more than 2 trillion bytes).

## Note

Windows cannot create a FAT32 partition larger than 32GB. However, if a larger partition already exists, Windows can use it.

FAT32 does have some limitations: It can support individual files only up to 4GB in size, it cannot use file permissions, and it does not support journaling systems that can fix file corruption issues. These three limitations moved the industry beyond FAT32, although it is still possible to use FAT32 to format hard drives.

Because the limitations do not apply to most USB flash and SD cards, FAT32 is still used to format flash memory cards and USB flash drives for use in not only workstations, but also media players, smart TVs, printers, cameras, and anything else that has a USB port. FAT32 is still compatible with macOS and Linux as well, so FAT32 is far from legacy. Even as the capacity of USB flash drives is increasing and 4GB files will need to be supported, FAT32 will likely stay around to support other devices.

## Note

In a 32-bit machine, the maximum amount of memory that can be used is around 4GB. On a 64-bit machine, the maximum amount of memory is  $2^{64}$  bytes.

## exFAT (FAT64)

exFAT (also known as FAT64) is a file system designed to enable mobile personal storage media to be used seamlessly on mobile and desktop computers. exFAT is designed to be as simple as FAT32, but with many improvements in capacity and scalability.

exFAT is also called FAT64 because it supports 64-bit addressing. The main features of exFAT include the following:

- It supports volumes (drive letters) larger than 32GB. 512TB is the recommended maximum volume size, but the theoretical volume size is 64ZB (zettabytes; 1ZB = 1 billion terabytes).
- The recommended and maximum file sizes increase to 512TB and 64ZB, respectively.
- Improvements in file system structure enable better performance with flash media and for movie recording.
- It supports Universal Time Coordinate (UTC) date stamps.

[Figure 6-37](#) illustrates exFAT as a formatting option for a USB thumb drive in Windows.

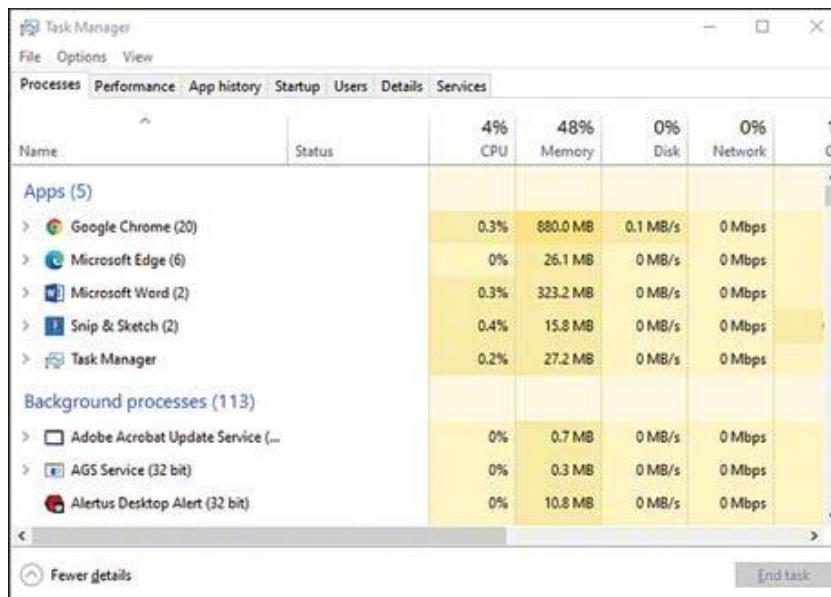


**Figure 6-37** File System Formatting Options for a 16GB USB Thumb Drive in Windows, Including FAT32, NTFS, and exFAT

## 32-Bit vs. 64-Bit Dependent Application Requirements

Remember that 32-bit apps date back to the X-86 days of processors (see [Chapter 3, “Hardware”](#)) and, by current standards, were inefficient to run. 64-bit apps can take advantage of more computing resources in the CPU and RAM. Windows 10 running on a 64-bit machine can support 32-bit programs, but 32-bit processors on smaller mobile devices cannot support 64-bit apps. Be sure of what the computer is running and what the software requires before you install an app.

Most software running on desktops today is 64 bit, but plenty of 32-bit applications are still in use. To see what kind of software is running in Windows, open the Task Manager (Ctrl+Alt+Esc); the list of running 32-bit programs is identified (see [Figure 6-38](#)). In this example, note that the AGS Service and the Bing Wallpaper are 32 bit.



**Figure 6-38** Task Manager Showing 32-Bit Software

## Dedicated Graphics Card vs. Integrated Graphics

## **Card**

An integrated graphics card refers to the graphics chip embedded into the motherboard. It is smaller and more energy efficient, and current integrated cards provide sufficient quality for the average user. Integrated cards count on system RAM for their processing, so they take a toll on overall system performance.

However, the integrated graphics card does not match the quality of a dedicated card. Dedicated cards are designed for different purposes, such as gaming or crypto currency mining, but they all have a graphics processing unit (GPU), onboard RAM, and a cooling fan for the processor. Most new dedicated cards can work with the embedded graphics for better efficiency.

## **Video Random Access Memory (VRAM) Requirements**

**Video random access memory (VRAM)** is RAM dedicated to processing graphics displays. VRAM can be an assigned part of the system RAM, for an integrated graphics card. For example, a computer might have 4GB of RAM, with 1GB dedicated to the onboard graphics chip.

VRAM also refers to the RAM mounted on a dedicated card to support the GPU. This RAM is next to the GPU and does not draw on system resources for high-quality display.

For most users, the integrated VRAM is sufficient. For software and applications that need powerful processing, extra VRAM for a dedicated card is a good solution.

## **RAM Requirements**

Before installing software on a computer, make sure that the current amount of RAM will support the application. Use the Task Manager (refer to [Figure 6-38](#)) to see how the computer is currently using available RAM resources. It is wise to assume that machines and devices run best up to the middle of their range of capability, so if RAM is above 50 percent, consult the software developer's RAM requirements to make sure the computer can handle it.

When RAM is installed and running, return to the Task Manager with the software running (along with other normal applications) and check the memory performance. If it is above 60 percent, consider installing more RAM, if possible. Fewer improvements aid a computer's performance more than adding RAM. See [Chapter 3](#) for a more detailed discussion of RAM.

## Central Processing Unit (CPU) Requirements

Choosing the CPU should happen while shopping for a computer or other device. Upgrading CPUs is fairly uncommon because they are designed to work with the motherboard they are installed on. Knowing the expected purpose and demands of the user can guide the CPU selection. For a more detailed discussion of CPUs, see [Chapter 3](#).

## External Hardware Tokens

Multifactor authentication is in much higher use now than in years past, but the need for high levels of computer security has been around for decades. One early method for authenticating into a network was using an external hardware token to access a code or password to enter into a computer or network for access. The token (also known as a *dongle*—see [Figure 6-39](#)), along with the authentication server, generated a random code every minute or so to validate a user who had entered a password. The two factors working together to protect the network were knowing the password and providing a physically present code.



**Figure 6-39** Hardware Token

The prevalence of smartphones that have their own security allows for tokens to be pushed out to users in an authentication app. Users can now

log into their phones or other devices to approve multifactor authentication.

## Storage Requirements

When installing software, it is important to consider what resources besides RAM and CPU will be required for use. For example, video editing software might require added resources for graphics and VRAM, but editing can generate massive files that need to be readily accessible. Make sure sufficient storage is available in the local disks and external drives, or on network attached storage (NAS). See [Chapter 3](#) for a detailed discussion of these storage options.

## OS Requirements for Applications

Not every application will run on every OS. Applications need to be specifically adapted to work on Windows, Apple, or Linux Platforms. Compatibility within the platform is a concern as well; whenever an OS is updated, the application might also need updating.

## Application-to-OS Compatibility

It seems pretty fundamental to say that it is important to ensure that the software version selected will run with the operating system. However, that task can get complicated. Operating system updates happen regularly, and software manufacturers do not always keep up. When installing software, be sure to check for the latest updates at the vendor's website.

## 32-Bit vs 64-Bit OS

As mentioned earlier in this section, Windows 32-bit software can run on a 64-bit machine, but a 64-bit machine cannot run on a 32-bit machine. The difference might not be noticeable to the user, but a 64-bit machine provides a much more powerful environment to work in. Any current machine designed to run Windows 10 or 11 is a 64-bit machine. Many 32-bit machines are still in use, but as of 2020, new machines running Windows 10 have 64-bit processors. Microsoft will continue to offer 32-bit support, but security and other features will not be as robust as with the 64-bit versions.

macOS, starting with the Catalina version 10.15 of the macOS in 2019, dropped support for 32-bit apps. Running legacy apps on macOS can be tricky, so be sure that legacy apps are updated if you are migrating an older macOS to a newer version. The older macOS versions list whether an app is 64-bit compatible. To find the list, go to **Finder > Apple icon > Overview > System Report > Software > Applications**. The upper window lists all applications and denotes whether they are 64 bit.

## Distribution Methods

### Physical Media vs. Downloadable

The days of getting physical media versions of software are nearly over. Creating physical media to install Windows now involves downloading an image file (.iso) to a USB/eSATA boot (booting from USB thumb drive) or optical disc (CD-ROM/DVD/Blu-ray). Use this method to install Windows to an individual PC and to create a master PC from which disk images can be created. The Windows USB/DVD Download Tool available from [www.microsoft.com/en-us/download/windows-usb-dvd-download-tool](http://www.microsoft.com/en-us/download/windows-usb-dvd-download-tool) can create a bootable USB drive from a Windows ISO (.iso) image that you have downloaded. If necessary, change the boot order in the system BIOS/UEFI firmware to permit booting from USB.

#### Note

These methods are discussed in detail later in this chapter in the section “OS Installations and Upgrades in a Diverse OS Environment.”

## Other Considerations for New Applications

A good rule in managing computer networks is that every benefit to a network has a cost. Some costs are money, but other costs can be a sacrifice of performance or capability. Sometimes the costs are unknown until it is too late and come in the form of unintended consequences—these can be the most expensive and can even lead to system failures.

Determining the cost or impact of a technical change is an important skill to develop. Making changes should be done not in a vacuum, but rather

through an established change control process agreed upon by the users of the machines and the network. These change control processes let all users review any changes or upgrades to assess any negative impact they might have on their work environment. The following are just a few examples of considerations the committee should have when determining the impact of a change to a computer network environment. Feel free to brainstorm and add your own questions to the examples.

- **Impact to device:**

- Will adding hardware or software for one user degrade the user experience for another user?
- Will updating the OS cause legacy software to stop working?

- **Impact to network:**

- Will adding new users and devices degrade the current network performance?
- How will adding network storage improve or degrade network capabilities?

- **Impact to operation:**

- Will new software updates take down the network for significant periods?
- Will moving to the cloud impact the processing time of sales transactions?

- **Impact to business:**

- Will adding security software lock out business partners?
- Can the business financially afford upgrades, and do they make economic sense in the long run?

## **Understanding Common OS Types**

220-1102  
Exam

**220-1102: Objective 1.8:** Explain common OS types and their purposes.

Different types of computers require different functionality from their operating systems. This section discusses differences between workstation and mobile operating systems and the file types they support.



## Workstation OSs

Operating systems can be classified as open source, which refers to software that is effectively free to download and modify, and closed source, which refers to software that cannot be modified without express permission and licensing. Other terms used to describe closed source software are *vendor specific*, which means that only one company has access to the source code, and *proprietary*, which means that the software is owned and patented and can be used only with permission (and usually by paying a licensing fee).

## Windows

Microsoft **Windows** is a closed source product and is the most widely used OS in the world. In the 1980s, when businesses transitioned into the digital age using IBM-compatible PCs, Microsoft usually provided the OS, which was known as the Disk Operating System (DOS). DOS is a command-line OS, which means that commands are entered as strings of text. DOS has since been replaced with Windows, which uses a graphical user interface (GUI) to allow commands to be entered with the click of a mouse. But the DOS legacy lives on with many of the same commands used in the PowerShell.

Windows has had many iterations over the years, but Windows 10 and perhaps 11 are the versions covered in the 220-1102 A+ exam.

### Note

The following note in the CompTIA A+ exam objectives sets out guidelines for that content of Windows 11 when the 220-1101 and 220-1102 exams were released. Although Windows 11 is not specifically detailed in separate objectives, the following applies:

"Versions of Microsoft Windows that are not end of Mainstream Support (as determined by Microsoft), up to and including Windows 11, are intended content areas of the certification. As such, objectives in which a specific version of Microsoft Windows is not indicated in the main objective title can include content related to Windows 10 and Windows 11, as it relates to the job role."

## Apple Macintosh OS

**macOS** is the OS for Apple desktop products. As with Windows, macOS is closed source, and only some components are open to developers. macOS was released in 2016 and designed to integrate with devices using the iOS operating system, such as the iPhone, Apple TV, and Apple Watch. As of this printing, the latest version of macOS is Monterey, which is version 12.

[Figure 6-40](#) shows the Monterey desktop.





**Figure 6-40** macOS Monterey

Linux

**Linux** was derived from the UNIX operating system (used on mainframe computers predating PCs). It is named for Linus Torvalds, who developed Linux in 1991. Linux is an open source OS, which means that the source code is free. Many companies, such as Red Hat, modify Linux source code and then charge individuals and organizations to support the modifications.

Because Linux is open source, it is available free on the Web in the form of distros (distributions). Linux is available as command-line distros; and others are GUI distros. Popular distros of Linux are Ubuntu, Mint, Kali, and Red Hat.

Figure 6-41 shows a Linux Mint desktop environment.



**Figure 6-41** Mint Desktop

## Chrome OS

**Chrome OS** is a relatively new OS developed by Google. It is an open-source OS, based on an open-source Gentoo Linux OS. The functionality is unique, in that the OS runs off the Google Chrome web browser. Chrome OS can be installed off a USB drive and can run on a PC or Mac.

Chrome can run applications from Android, Linux, and Windows. When first released, Chrome OS ran Chromebook laptops that were inexpensive but also limited. Newer versions of Chromebooks and the Chrome OS offer better performance, but inexpensive versions are still available.



## Cellphone/Tablet Operating Systems

Smartphones use typically either Android or iOS operating systems.

Some differences between Android and iOS smartphones include the following:

- Operating system updates are provided by the wireless carrier for Android phones.
- Wireless carriers provide network-specific updates for iPhones (iOS), but Apple provides the OS updates.

## Android

**Android**, which is an operating system based on the Linux kernel, is an example of open source software. Used mostly on smartphones and tablet computers, Android is developed by the Open Handset Alliance, a group directed by Google. Google releases the Android OS code as open source, allowing developers to modify it and freely create applications for it. Google also commissioned the Android Open Source Project (AOSP), whose mission is to maintain and further develop Android.

Newer versions of Android are in constant development.

To determine the current version in use on a device, start at the Home screen (that is, the main screen that boots up by default). Tap the Menu button and then tap Settings. Scroll to the bottom and tap the About Phone (or About) option. Then tap Software Information or a similar option. Versions 1-10 were famously named after desserts, such as Lollipop (version 5) and Pie (version 9), but starting with version 10, the code names were dropped. As of this writing, the latest version is 12.

Unlike other mobile operating systems, Android licensing agreements allow for a great deal of customization of the finished product. Thus, Android smartphones and tablets from different vendors are likely to have different user interfaces and features.

## iOS

The Apple **iOS** is an example of closed source software.

Known as the iPhone Operating System, this is now simply referred to as iOS because it is used on the iPod Touch, and iPhone. iOS is based on macOS (used on Mac desktops and laptops) and, therefore, has its roots in

UNIX. [Figure 6-42](#) shows the Home screen of an iPad Mini 2 running iOS version 9.0.1.



1. iOS OS update available
2. App updates available
3. Battery charge level

**Figure 6-42** iPad Mini 2 Home Screen

The iPad once ran on iOS, but with version 13 (2019), it was powerful enough to have its own **iPadOS**, which is more robust than iOS and supports using a keyboard and multitasking.

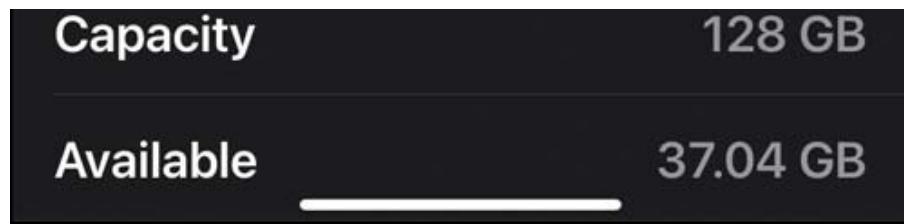
To determine the version of iOS a device is running, go to the Home screen and tap **Settings > General > About**. For example, [Figure 6-43](#) shows an iPhone running version 15.1. iPad 15 was released in fall 2021 for iPad Pro, iPad (fifth generation onward), iPad Mini (fourth generation onward), and iPad Air (second generation onward).

A screenshot of an iPhone's "About" screen. The top status bar shows the time as 3:36 and battery level. Below the status bar, there are navigation buttons: a back arrow pointing left labeled "General" and a title "About". The main content area displays the following device information:

Name	iPhone Example >
Software Version	15.1
Model Name	iPhone 11
Model Number	MWLE2LL/A
Serial Number	DNPZMJ9YN72Q

Below this section is a header "AppleCare Services >". The bottom half of the screen displays media statistics:

Songs	395
Videos	52
Photos	2,547
Applications	148



**Figure 6-43** iPhone Using Version 15.1 of iOS

Unlike Android, iOS is not open source. Only Apple hardware uses this operating system.

## Various File System Types

What exactly is a file system? A file system determines how data and drives are organized, but it is also a general term for how an operating system stores various types of files. As discussed earlier in this chapter, Windows supports three different file systems for hard drives and USB flash drives: FAT32, NTFS, and exFAT.

The **New Technology File System (NTFS)** is the native file system of Windows 10. NTFS has many differences from FAT32, including the following:



- **Access control:** Different levels of access control, by group or user, can be configured for both folders and individual files.
- **Built-in compression:** Individual files, folders, or an entire drive can be compressed without the use of third-party software.
- **Individual Recycle Bins:** Unlike FAT32, NTFS includes a separate Recycle Bin for each user.
- **Support for the Encrypting File System (EFS):** The Encrypting File System (EFS) enables data to be stored in an encrypted form. It requires no password and no access to files.
- **Support for mounting a drive:** Drive mounting enables you to address a removable-media drive's contents, possibly as if its contents are stored on your hard drive. The hard drive's drive letter is used to access data on both the hard drive and the removable media drive.

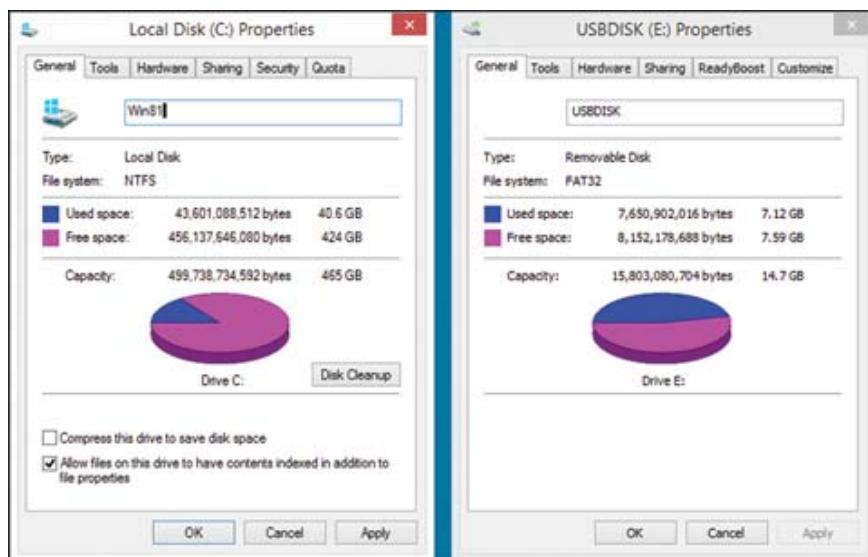
- **Disk quota support:** The administrator of a system can enforce rules about how much disk space each user is allowed to use for storage.
- **Hot-swapping:** Removable-media drives that have been formatted with NTFS (such as USB) can be connected or removed while the operating system is running.
- **Indexing:** The indexing service helps users locate information more quickly when the Search tool is used.

Follow these steps to determine what file system was used to prepare a Windows hard drive:

**Step 1.** Open Windows File Explorer.

**Step 2.** Right-click the drive letter in the Explorer window and select **Properties**.

The properties sheet for the drive lists NTFS for a drive prepared with NTFS and FAT32 for a drive prepared with FAT32 (see [Figure 6-44](#)).



**Figure 6-44** A Hard Drive Formatted with NTFS Version 5 (Left) and a Flash Memory Drive Formatted with FAT32 (Right)

During installation, Windows 10 automatically formats the partitions created by the partition process with NTFS.

exFAT, FAT32, and NTFS are common Windows files systems. [Table 6-8](#) briefly describes these and other file systems that perform the same tasks but on different operating systems.

**Table 6-8** File System Format Comparison

System Type	Full Name	Details
<b>exFAT</b>	<b>Extended File Allocation Table</b>	Microsoft file system used for flash drives larger than 32GB and files larger than 4GB.
<b>FAT32</b>	<b>File Allocation Table</b>	Format for USB flash drives that hold files smaller than 4GB, game consoles, and so on. Works with all operating systems.
<b>NTFS</b>	<b>New Technology File System</b>	Windows default formatting for hard drives. Supports sharing and journaling.
<b>APFS</b>	<b>Apple File System</b>	Apple file system of macOS that is designed to enhance performance with solid state drives (SSD) and flash storage. It is available on macOS 10.13 and higher.
NFS	Network File System	Open source system that works independently of the operating system, allowing network user access. It appears local but is a common network drive.
<b>ext3</b>	<b>Third Extended File System</b>	Linux version of NTFS. Allows journaling of changes, to minimize damage if a crash occurs. Supports a maximum of 32,000 subdirectories.
<b>ext4</b>	<b>Fourth Extended File System</b>	Linux system. Supports larger file sizes than ext3. Can disable journaling. Supports a maximum of 64,000 subdirectories.

## Vendor Life-Cycle Limitations

The economic concept of planned obsolescence applies to computers and OSs even more so than in other commercial products. When a CPU, computer model, or OS update is rolled out, chances are very good that its replacement model is well into the development stage. Two concepts discussed in this section are end of life (EOL) and **product life cycle**.

## **End of Life (EOL)**

Most customers demand that computer manufacturers stay on the leading edge of technology in their products. Quality of experience and security concerns are central to keeping customers loyal. But the market has only so much capacity; with each new version of a product or OS, an old one is usually assigned “deprecated” or “legacy” status. When a new product is released, such as a CPU rollout or GPU card, the EOL is already planned because the next generation is usually well into development. This is true of both hardware and OS updates. For example, Windows 7 is already EOL, and the Windows 8 EOL is scheduled for January 2023. Windows 10 EOL is currently scheduled for October 2025.

## **Update Limitations**

Not all OS updates are feasible on all products. For example, iOS 15 cannot run on most phone models earlier than iPhone 6s or SE. This is because the software advancements went further than the physical capabilities of the chipset—this can be processing power, video power, or another factor. Be sure to check vendor websites before updating, to make sure the device is compatible with the update.

Updating can have hidden costs as well. If users have accessories to go with their devices—video cable, USB adapters, and writing pens, those might also need to be replaced. As devices migrate to USB-C interfaces, many of the old accessories are rendered useless when the new device arrives.

## **Vendor-Specific Limitations/Compatibility Concerns Between OSs**

Nearly all smartphones in the United States use either Android or iOS. Each OS has loyal users, and the debate over which is better has proponents on both sides. Both are good systems, but several considerations are involved when choosing between the vendor-specific, closed source Apple iOS and the open source Android OS.

One can argue that because Apple has control of iOS, it can better control the quality and safety of Apple products. In addition, Apple can develop better applications, such as iMessage, Find My Friends, and FaceTime, that work well because they can be designed around the advantages of a closed

source platform. Although it is an advantage for a family or an organization to use common apps to communicate and share data easily, non-iPhone users are out of the loop with such apps.

One can also argue that Android has certain advantages because it has more apps available. Additionally, Android devices tend to be much less expensive than iPhones. Android allows third-party apps, but some people see third-party apps as a security problem instead of an advantage.

The good news is that both iOS and Android are robust and reliable systems. The best choice ultimately depends on the users and their communication needs. More good news is that some apps coming on the market enable easy communication and sharing between Android and iOS users.

## OS Installations and Upgrades in a Diverse OS Environment



**220-1102: Objective 1.9:** Given a scenario, perform OS installations and upgrades in a diverse OS environment.

### Boot Methods

The boot process involves loading the necessary OS files into RAM so that the computer becomes functional. Depending on the situation, different **boot methods** may be deployed. The OS can be stored on the local hard drive, but it can also be stored on a CD/DVD, on an external USB or eSATA drive, or on another computer on the network. Wherever it is stored, the computer needs to be told where to go to find the OS files. This is done in the BIOS/UEFI Boot Order settings. When booting, the PC looks in the preferred place for files and loads them into RAM; the computer then becomes operational. If the PC cannot find the files in the boot order, it moves on to the second place and then keeps looking until it finds an OS. [Figure 6-45](#) shows the boot order in typical BIOS. Keep in mind, though, that each vendor's boot order screen looks slightly different.



**Figure 6-45** BIOS Boot Order Menu

Many methods exist for booting a system during the installation process:



- **Optical disc (CD-ROM/DVD/Blu-ray):** Use this method to install Windows to an individual PC and to create a master PC from which disk images can be created.
- **Network/PXE boot (Preboot Execution Environment):** Use this method to install Windows to one or more systems that have working network connections. To use this method, network adapters must be configured to boot using the PXE boot ROM to a network location that contains an operating system image.

## Note

Netboot is a network boot technology developed by Apple. Netboot uses Boot Server Discovery Protocol (BSDP) to locate and install operating system files.

- **USB/eSATA boot (booting from a USB thumb drive):** Use this method when installing from a DVD is not feasible, such as installing Windows to a computer that lacks a DVD drive. The Windows USB/DVD Download Tool (available from [www.microsoft.com/en-us/download/windows-usb-dvd-download-tool](http://www.microsoft.com/en-us/download/windows-usb-dvd-download-tool)) can create a bootable

USB drive from a Windows ISO (.iso) image you have downloaded. If necessary, change the boot order in the system BIOS/UEFI firmware to permit booting from a USB drive.

- **Solid state/flash or internal hard drives (HDD/SSD):** This is the most common place for OS files to reside. After the OS is installed, it is important to change the boot order in BIOS/UEFI so that the computer looks here first for files and does not try to reinstall from the external source.
- **Internet based:** Downloading and installing over the Internet is an option. This involves downloading a server app and then downloading and creating the Windows ISO file. It is then possible to share the Windows installation folder and install Windows over the network connection.
- **External/hot-swappable drive:** Hot-swappable drives are attached in special drive bays that allow the hard disk to be changed out while the computer is running. When a computer is running, the OS is loaded into RAM so that the OS can reside on a hot-swappable drive and be changed out, as long as it is returned to the drive bay that is identified in BIOS/UEFI as the bootable drive.
- **Partition on the internal hard disk drive or SSD:** This option is similar to the internal hard drive above, but it involves a designated partition, or a section on the drive reserved for booting.

With each type of drive, the Windows installation files can be extracted or the ISO file can be used as an installation source.

## Types of Installations

Windows can be installed in a variety of ways. The most common methods follow:



- As an in-place upgrade to an existing version
- With the recovery partition (which resets the system to its original installed state)

- As a clean install to an empty hard drive or to the same partition as the current version
- As a multiboot, which means installing to unused disk space (a new partition) to enable a choice between the current version and the new version, as needed
- As a repair installation to fix problems with the current installation

The preceding installation options typically use the original distribution media or preinstalled recovery files.

Large-scale or customized installations might use the following methods:

- Unattended installation
- Remote network installation
- Image deployment

These installation options typically require the creation of an image file.

## Unattended Installation

In an attended installation, information must be provided at various points during the process. To perform an unattended installation, create the appropriate type of answer file for the installation type. Microsoft currently offers the Microsoft Deployment Toolkit (MDT) for automated installation of Windows. The MDT automatically creates and updates the Unattend.xml file (used to provide answers during the process) during the deployment.

Download the MDT from the Microsoft website:

<https://docs.microsoft.com/en-us/sccm/mdt/>.

## Types of Installations



## Upgrades

To perform an upgrade of the Windows 10/11 OS to the latest version, an *in-place upgrade* installation of Windows is recommended. Start the installation process from within the existing version of Windows. These in-

place upgrades do not delete previous installations, which means that the user can retain apps and settings as well as personal files.

## Note

To upgrade from Windows 10 to Windows 11, use an in-place upgrade if your machine is compatible (hardware specifications are listed in the upcoming section “Upgrade Considerations”). If it is compatible, follow these steps to upgrade in-place: Go to **Settings > Update & Security > Windows Update** and click the Check for Updates button. If Windows 11 is waiting for you, it can then be installed. Otherwise, later versions of Windows 10 might be available.

The exact upgrade paths between Windows versions vary according to the Windows edition currently in use. You can upgrade to the equivalent or better edition of Windows, but not a lower edition. The 32-bit versions can upgrade to 32-bit versions only; 64-bit versions can upgrade to 64-bit versions only.



## Clean Install

Before starting a ***clean install*** process, check the following:

- Make sure the drive for installation is placed before the hard drive in the boot sequence. The system needs to boot from the Windows distribution media if you are installing to an empty hard drive. You can perform a clean install of Windows from within an older version of Windows if you want to replace the older installation.
- If you will be installing to a drive that might require additional drivers (SATA, RAID, or third-party host adapters on the motherboard or in an expansion slot), have the drivers available on any type of removable media that the system supports.
- If you are installing from optical media, from a disk image (ISO, VXD, or VHDX), or within a virtual machine (VM), then after restarting the system with the CD or DVD media or image file in place, press a key when prompted to boot.

During the installation process, be prepared to confirm, enter, select, or provide the following settings, information, media, or options when prompted:

- **Custom installation:** Choose this option if performing a “clean boot” installation to an unused portion of the hard drive or wiping out the existing installation instead of upgrading it.
- **Edition of Windows you are installing:** If the incorrect version is entered, the installation cannot be activated.
- **Language:** Windows 10 is available in more than 100 different languages. Be sure the intended user’s language pack is selected prior to installation.
- **Location (home, work/office, or public):** The location information is used to configure Windows Firewall.
- **Network settings:** These settings are normally detected automatically for a wired connection. If your connection is wireless, make sure the SSID and password (encryption key) are available.
- **Partition location, partition type, and file system:** See the section “Partitioning Overview,” later in this chapter, for details.
- **Product key:** Some installations allow skipping this temporarily, but you must provide before you can activate Windows.
- **Time zone, time, and date:** These settings are normally detected automatically, but you can manually set them here.
- **Username and company name:** The company name is optional.
- **Workgroup or domain name:** This is a group of computers with common access to files and centralized administration and authentication.

## Note

The settings in this list are in alphabetical order. Operating systems prompt for this information at different points in the installation process.

At the end of the process, remove the distribution media. Windows then is ready to download the latest updates and service packs.

## Repair Installation

If a Windows operating system installation becomes corrupt, use a repair installation to restore working files and Registry entries without losing existing programs or information. Repair installations are available in Windows 10. Make a backup copy of your data files (stored in `\Users\Username` for each user of your PC) before you perform a repair installation, in case of problems.

### Note

The repair installation process is also known as an in-place upgrade.

To perform a **repair installation** of Windows 10 with a USB flash drive (which needs to be created before you start this process), follow these steps:



**Step 1.** Boot the computer normally and sign into the Administrator account. Disable any third-party security software to avoid interruptions of the upgrade.

**Step 2.** Insert the flash drive and run **setup.exe** to start the setup.

**Step 3.** When prompted, download and install updates.

**Step 4.** Accept the end user licensing agreement. The updates begin.

**Step 5.** When the updates are ready, click **Install** when prompted.

**Step 6.** Choose to keep personal files, if that is the preference.

**Step 7.** Let the Windows 10 Setup process run and repair Windows.

The rest of the installation proceeds as with a normal installation.

## Remote Network Installation

A **remote network installation** (which involves installing Windows from a network drive) begins by starting the computer with a network client and logging on to the server to start the process. To automate the process, Windows 10 can automatically be installed from a network drive by using Windows Deployment Services. Windows Deployment Services is included in newer Windows Server operating systems.

Server-based programs work along with the Microsoft Development Toolkit or Windows System Image Manager program. These programs are used to create an answer file that provides the responses needed for the installation.

## Image Deployment

An **image deployment** is the process of installing Windows from a disk image of another installation. This process is also called *disk cloning*. You can create a disk image by using a variety of tools, including Acronis True Image ([www.acronis.com](http://www.acronis.com)) and Seagate DiscWizard (which is partly based on Acronis True Image, available from [www.seagate.com](http://www.seagate.com)).

### Note

It is possible to burn a disc image file, which often has either an .iso or .img filename extension, to a USB flash or recordable CD or DVD by using Windows Disc Image Burner in Windows 10.

However, if you are deploying a disk image to multiple computers instead of as a backup of a single computer, consider these special issues:

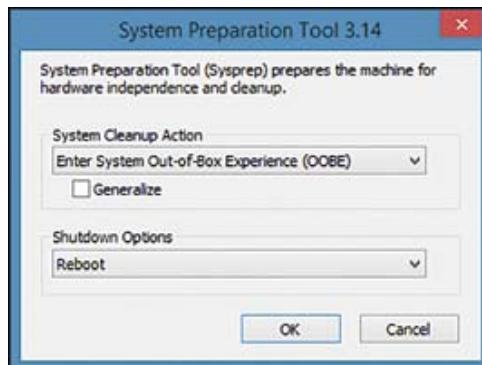
- **Hardware differences:** Traditional image cloning methods, such as those using Acronis True Image, were designed for restoration to identical hardware (that is, the same motherboard, the same mass storage host adapters, the same BIOS/UEFI configuration, the same Hardware Abstraction Layer [HAL], and the same Ntoskrnl.exe [NT kernel] file). For organizations that have different types and models of computers, this poses a problem.

- **Same security identifier:** A cloned system is identical in every way to the original, including having the same security identifier (SID). This can cause conflicts in a network.

To overcome these problems, use cloning programs designed to capture an image that can be deployed to different types of computers (laptops, desktops, and tablets) with different hardware and software.

For Windows 10, use the System Preparation Tool (Sysprep) to prepare the image for installation over many computers. Sysprep loads files and restarts the PC. If you select Generalize in Sysprep, Windows removes unique PC information, including the SID. When the install completes and the computer is restarted, a new SID is generated.

[Figure 6-46](#) shows the Sysprep window and the option to generalize the installation. Note the option to reboot at the end of the process.



**Figure 6-46** Starting the Sysprep Tool on a Windows 10 System

All cloning tools can work with a target drive that is the same size or larger than the original cloned system drive. Some can also work with a smaller drive; check the documentation for details.

## CAUTION

Do not use disk cloning to make illegal copies of Windows. Use disk-cloning software legally to make a backup copy of your installation. If you are duplicating the installation on another PC, be sure to clone a system created with a volume license for Windows, and make sure that you do not exceed the number of systems covered by that license; alternatively, make sure you use the correct license number (product key) for each

duplicate system. For more information about Windows licensing, see [www.microsoft.com/en-us/licensing/default.aspx](http://www.microsoft.com/en-us/licensing/default.aspx).

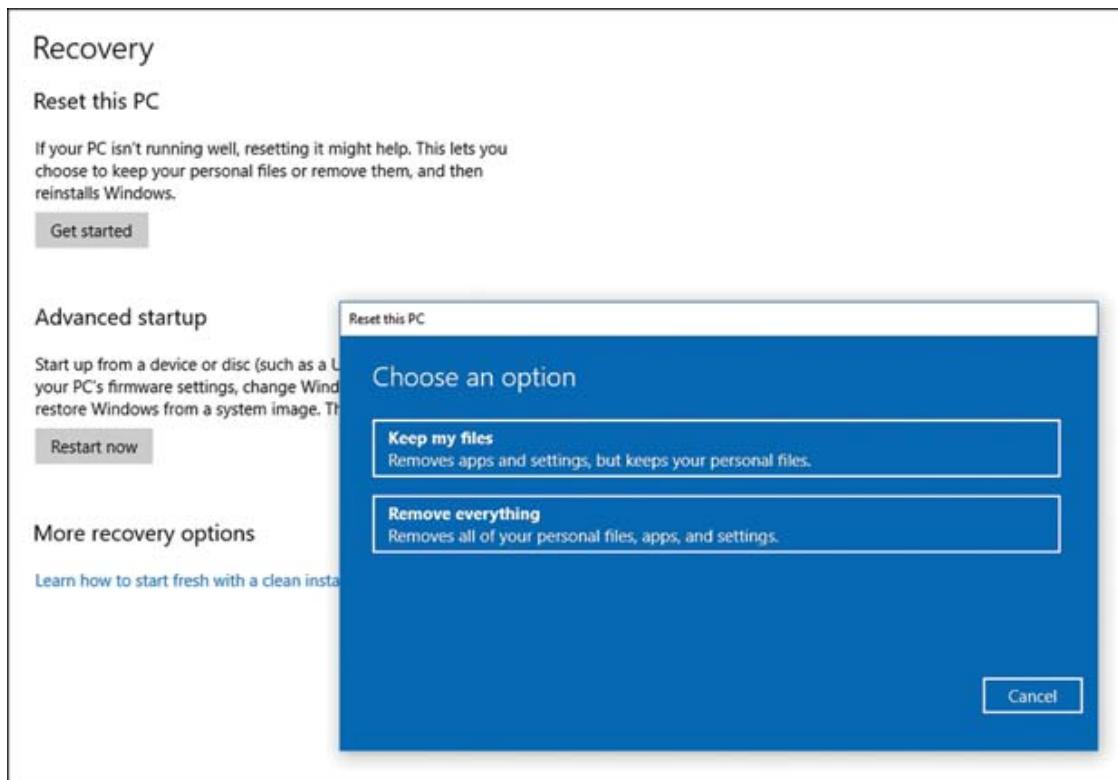
## Recovery Partition

When upgrading Windows or doing a clean install with Windows Setup, a **recovery partition** is created. The recovery partition is a space that holds the Windows Recovery Environment (WinRE), which can repair some common boot errors. WinRE is built into Windows 10 versions for desktop editions.

## Refresh/Restore

If a PC is underperforming or appears to be somehow infected by a virus, it might be a good idea to reset the PC to the factory default settings.

Resetting a PC in Windows 10 is a straightforward process. Go to **Settings > Recovery** and click Get Started under Reset This PC. When you click Get Started, you get two choices: Keep My Files or Remove Everything. Keep My Files is for a minor reset; it allows personal files to be kept while removing apps and any settings that have been changed. Remove Everything performs a major reset, removing all files; before you choose this option, you need to back up personal files. [Figure 6-47](#) shows the Recovery page, along with the window that appears when you click Get Started.



**Figure 6-47** The Recovery Window and the Reset This PC Window

## Other Considerations/Third-Party Drivers

When installing or updating an OS, it is important to think about updating drivers that support hardware used on the device. For example, a corrupt driver (or a driver made for a different version of the OS) can cause problems or, at worst, crash the system. If a hardware driver fails after an update, removing the driver from the Device Manager and reinstalling the latest driver version from the manufacturer is a good move.

Third-party drivers refer to drivers sourced from outside Windows, most commonly from a device manufacturer. The Windows OD contains a substantial library of default drivers for devices, such as network adapters and video and sound cards. For the most part, these drivers work fine, but installing a driver from the manufacturer can enhance the features or performance of a device.

## Partitioning Methods

Whether Windows is being installed to an empty hard drive or to a hard drive that has unassigned space (for multibooting), at least one new hard drive partition must be created. To do this successfully, you need to understand the differences between the following:

- Master boot record (MBR) and [GUID Partition Table \(GPT\)](#) partition tables
- Primary and extended partitions
- Extended partitions and logical disk drives
- Dynamic and basic disks

## Partitioning Overview

A hard drive cannot be used until it is prepared for use. Two steps are involved in preparing a hard drive:

**Step 1.** Create partitions.

**Step 2.** Format partitions (and assign drive letters).

A disk partition is a logical structure on a hard drive that specifies the following:

- Whether the drive can be bootable
- How many drive letters (one, two, or more) the hard drive will contain
- Whether any of the hard drive's capacity will be reserved for a future operating system or another use

Although the name *disk partition* suggests that the drive will be divided into two or more logical sections, every hard drive must go through a [partitioning](#) process, even if you want to use the entire hard drive as a single drive letter. All versions of Windows support two major types of disk partitions:



- **Primary partition:** A primary partition can contain only a single drive letter and can be made active (bootable). Only one primary partition

can be active. Although a single physical drive using MBR can hold up to four primary partitions, only one primary partition is needed on a drive that contains a single operating system. If you are installing a new operating system in a multiboot configuration with your current operating system, install the new operating system to a different disk partition than is used for the previous Windows version. If you are using a non-Windows operating system along with your current operating system, it should be installed into its own primary partition. A drive partitioned using GPT can have up to 128 primary partitions.

## Note

Depending on the layout and contents of your current disk partitions, you might be able to shrink the size of existing partitions with Windows Disk Management, to make room for a new primary partition, or you might need to use third-party software such as Acronis Disk Director or EaseUS Partition Master.

- **Extended partition:** An extended partition differs from a primary partition in two important ways:
  - An extended partition does not get a drive letter, but it can contain one or more logical drives, each of which is assigned a drive letter.
  - Neither an extended partition nor any drive it contains can be bootable.

Only one extended partition can be stored on each physical drive. Extended partitions are used only with MBR drives.

## MBR vs. GPT Partition Types

**Master boot record (MBR)** partitions are supported by classic ROM BIOS as well as UEFI firmware. MBR supports a maximum drive size of 2TB and up to four primary partitions.

A **globally unique ID partition table (GPT)** supports drives up to 256TB and up to 128 primary partitions. GPT is also more reliable than MBR because it protects the partition table with replication and a cyclic

redundancy check (CRC) of the partition table's contents. GPT also provides a standard way for system vendors to create additional partitions. GPT partition tables are supported by UEFI firmware.

To boot from a GPT drive, the system must have a 64-bit version of Windows. (Newer Windows Server versions also support GPT.) 32-bit versions of Windows can use GPT drives for data.

## Disk Preparation Using MBR

If a drive will be used by a single operating system using an MBR partition table, one of these three ways of partitioning the drive is used:

- **Primary partition occupies 100 percent of the physical drive's capacity:** This is typically the way the hard drive on a system sold at retail is used, and it is also the default for disk preparation with Windows. This option is suitable for the only drive in a system or an additional drive that can be used to boot a system, but it should not be used for additional drives in a system that will be used for data storage.
- **Primary partition occupies a portion of the physical drive's capacity, and the remainder of the drive is occupied by an extended partition:** This enables the operating system to be stored on the primary partition and the applications and data to be stored on one or more separate logical drives (that is, drive letters created inside the extended partition). This is a common setup for laptops but requires the partitioning process to be performed with different settings than the defaults. This configuration is suitable for the only drive or for the first drive in a multiple-drive system.
- **Extended partition occupies 100 percent of the physical drive's capacity:** The drive letters on the extended partition can be used to store applications or data, but not the operating system. An extended partition cannot be made active (bootable). This configuration is suitable for additional hard drives in a system (not the first drive); an extended partition can contain only one logical drive or multiple logical drives.

You can also leave some unpartitioned space on the hard drive for use later, either for another operating system or for another drive letter.

After a disk is partitioned, the drive letters must be formatted using a supported file system.

## Partitioning Using GPT

GPT partitioning creates one or more primary partitions. There are no extended partitions or logical drives on a GPT drive; each partition can be assigned a drive letter. However, only one partition can be active.

## Dynamic and Basic Disks

Windows supports two types of disks: basic and dynamic. A dynamic disk is more versatile than a basic disk because it can span two physical drives into a single logical drive, create striped or mirrored arrays, and adjust the size of a partition. However, during installation, Windows creates only basic disks. Only basic disks can be bootable.



## Creating Partitions During Windows Installation

When installing Windows 10 to an empty hard drive, you get a prompt for a location. To use all the space in the disk, make sure that the desired disk and partition are highlighted, and click Next.

To use only part of the space, click Drive Options (Advanced), click New, specify the partition size, and click Apply. Windows displays a message that it is creating an additional partition. Click OK to clear the message. A system-reserved partition is created, followed by the partition size you selected for Windows to use and the unused (unallocated) space.

To use an existing partition, highlight the desired partition and click Next.

### CAUTION

Be careful: Whatever partition you select for the installation will be formatted, and all data on that partition will be erased.

## **Formatting**

Quick formatting is an option with all versions of Windows. With new hard drives or existing drives that are known to be error free, you can use the quick format option to quickly clear the areas of the hard drive that store data location records.

With the full format option, Windows must rewrite the disk structures across the entire disk surface. This can take several minutes with today's large hard drives.

### **Note**

If you are concerned about the condition of a used hard drive that is being reused with Windows, use Windows chkdsk if the drive has been formatted to check its state. The drive vendor's disk diagnostic utility program also verifies the condition of a drive.

## **Upgrade Considerations**

Some configuration settings for Windows are made during installation; others are made afterward. The following sections describe the major issues to consider to complete the upgrade process.

## **Backup Files and User Preferences**

Before upgrading, a wise strategy is to back up the entire contents of the computer to a selected drive or to another local or network location. A backup program can create a compressed file to store backed-up information and user preferences.

Windows asks during an upgrade what to do with current files. They should migrate just fine, but a backup is always a good idea even under normal operations.

## **Application and Driver Support/Backward Compatibility**

After Windows is installed, it should be updated with the latest drivers. For individual PCs, the easiest way to perform these steps is to set up Windows Update for automatic updates.

However, if you are installing Windows for the first time and the system or motherboard was supplied with a driver disc, perform driver installation first before you run Windows Update.

## **Hardware and Application Prerequisites and Compatibility**

Before attempting to install any version of any OS, it is important to be sure that the hardware and applications to be used will work with (that is, are compatible with) the OS. This section briefly describes the process manufacturers use to ensure compliance and the steps PC techs take to make sure products comply.

### **Prerequisites**

When doing a clean install, it is important to make sure that your hardware meets the prerequisites for working with the software—usually a minimal amount of RAM and a certain level of processing power. However, the prerequisites are minimums; not having enough processing power and not having enough RAM are the most common causes of performance issues. Be sure to exceed the minimums so that the OS can smoothly operate.

The following list is a summary of the current requirements for Windows 10 and Windows 11.

#### **Windows 10**

- **Processor:** 1GHz or faster processor or System on a Chip (SoC)
- **RAM:** 1GB for 32-bit OS or 2GB for 64-bit OS
- **Hard drive space:** 16GB for 32-bit OS or 32GB for 64-bit OS
- **Graphics card:** DirectX 9 or later with WDDM 1.0 driver

- **Display:** 800×600
- **Internet connection:** Internet connectivity to perform updates and to take advantage of some features

## Windows 11

- **Processor:** Two or more cores on a compatible 64-bit processor or System on a Chip (SoC).
- **RAM:** 4GB.
- **Hard drive space:** 64GB or larger storage device.
- **Graphics card:** Compatible with DirectX 12 or later with WDDM 2.0 driver.
- **Display:** High-definition (720p) display that is greater than 9 inches diagonally; 8 bits per color channel.
- **Internet connection:** Windows 11 Home edition requires Internet connectivity and a Microsoft account. Switching a device out of Windows 11 Home in S mode also requires Internet connectivity.

Anything below these recommendations will likely result in a difficult install and poor performance. Upgrading to these standards or above is highly recommended.

## Windows Compatibility Program

Manufacturers have an interest in making sure their products will be usable by the world's largest OS audience, so they design their products to comply with the Windows Compatibility Program standards. This allows them to test their hardware and software products to ensure that they will work when the customer buys and installs them.

## Hardware and Application Compatibility

For a consumer, the easiest way to check for compatibility with a Windows OS is to consult Microsoft. For many years, Microsoft has maintained the Hardware Compatibility List (HCL), also called the Windows Compatibility Product List. The HCL provides information about manufacturers and drivers

that can be used (and not used) with Windows. With Windows 10, most previous equipment should run. The Microsoft Hardware Compatibility Checker matches compatible products for Windows and macOS (see <https://docs.microsoft.com/en-us/windows-hardware/drivers/dashboard/windows-certified-products-list>).

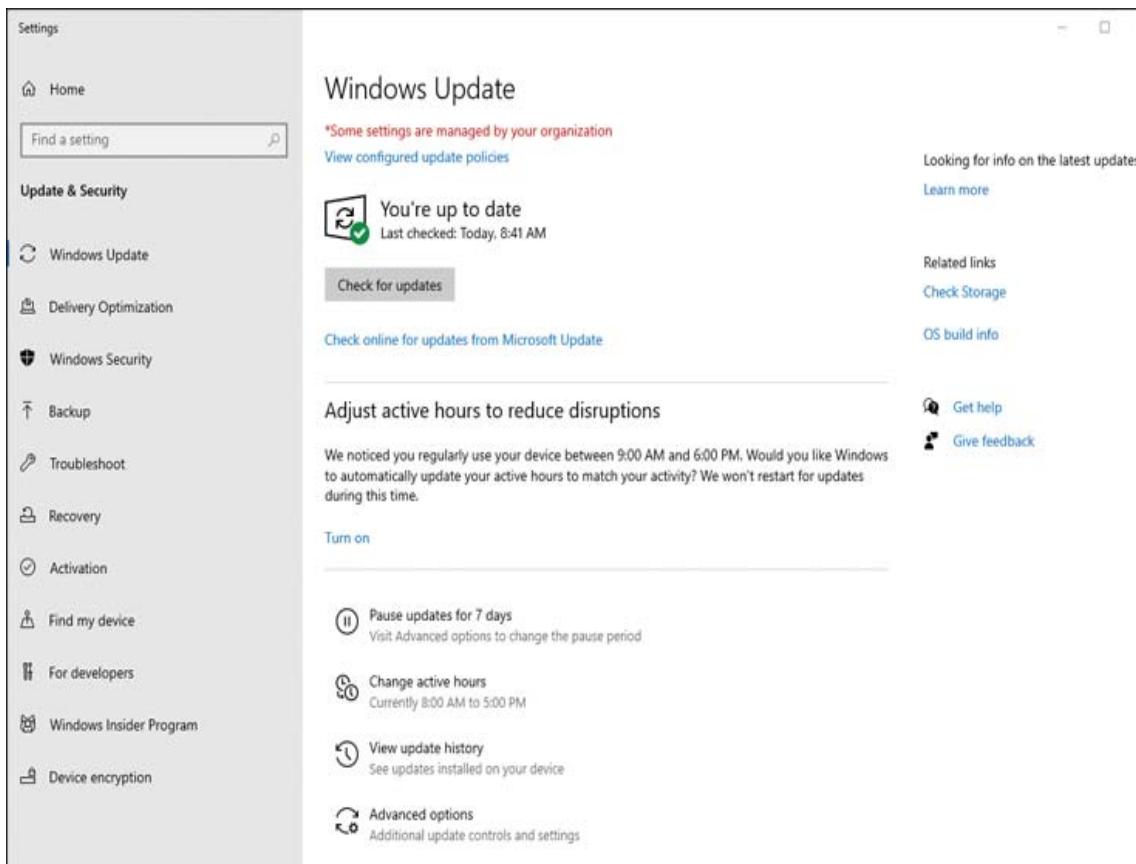
Most popular manufacturers submit drivers to Windows to allow for plug-and-play capability, but drivers usually need to be updated at some point in the device's life cycle. Whenever you are installing a device or an application, it is wise to check with the manufacturer's website for the latest update.

A program is written to work on a certain OS, and with each OS upgrade comes the possibility that a program will be running poorly or not at all. If you are running programs written for previous versions of Windows, you can check for compatibility with Windows 10 using the Compatibility Troubleshooter tool. In Windows File Explorer, right-click the program to be run and select Properties. Click the Compatibility tab, check Run This Program in Compatibility Mode, and select the OS previously used.

Another option in Windows 10 is to type **Run Programs** in the search bar and then select Run Programs Created for Previous Versions of Windows.

## Feature Updates

Windows includes a feature that keeps the software updated with fixes and security patches. The page can be found in **Settings > Update & Security > Windows Update** (see [Figure 6-48](#)).



**Figure 6-48** The Windows Update Page

Updates can be done manually by clicking the Check for Updates button, or an update schedule can be created.

## Update Life Cycle

Newer versions of the Windows OS are released every fall and spring. The life cycle for these Windows Update releases is 18 months, at which time Microsoft ends support of that update. When the support cycle ends, it is necessary to upgrade to a supported version to continue getting security and nonsecurity patches.

## Common Features and Tools of the macOS/Desktop OS

**220-1102: Objective 1.10:** Identify common features and tools of the macOS/desktop OS.

Although macOS is far less common than Windows in some corporate environments, macOS is very popular in educational and creative workplaces. To be a well-rounded computer technician, it is important to understand how the operating system differs from Windows and be able to perform basic commands and maintenance procedures.

## Installation and Uninstallation of Applications

The install and uninstall processes for macOS applications are fairly straightforward. The following sections describe the file types and process steps.

### File Types

Mac uses a fairly straightforward process for installing and uninstalling files that differs from the installation wizard found in Windows. The install file types used in the macOS are as follows:

- **.dmg (Disk Image) files:** Downloading a .dmg file is similar to downloading a complete installation kit for an application—similar to an ISO file in Windows. Everything necessary is contained in the file, including installation scripts and application files. Simply dragging a file to the hard drive ensures all necessary files are present. This drag-and-drop action completes all the installation tasks, similar to the installation wizard in the Windows environment. When the installation is complete, the .dmg file can be safely deleted.
- **.pkg:** These are compressed installation files and scripts, similar to the .zip files that the macOS uses for Mac software installs. The installation files are in the .pkg file, and there is no need to drag and drop them.
- **.app:** This file extension indicates that a file holds an executable application that will run on the macOS. The folder also holds information such as icons and other properties that the OS uses to make it functional.

## **App Store**

The App Store is the online market platform for Apple-approved applications. A user can purchase and download apps for the computer or iPhone and tablets and be sure that Apple has vetted the code for quality and security.

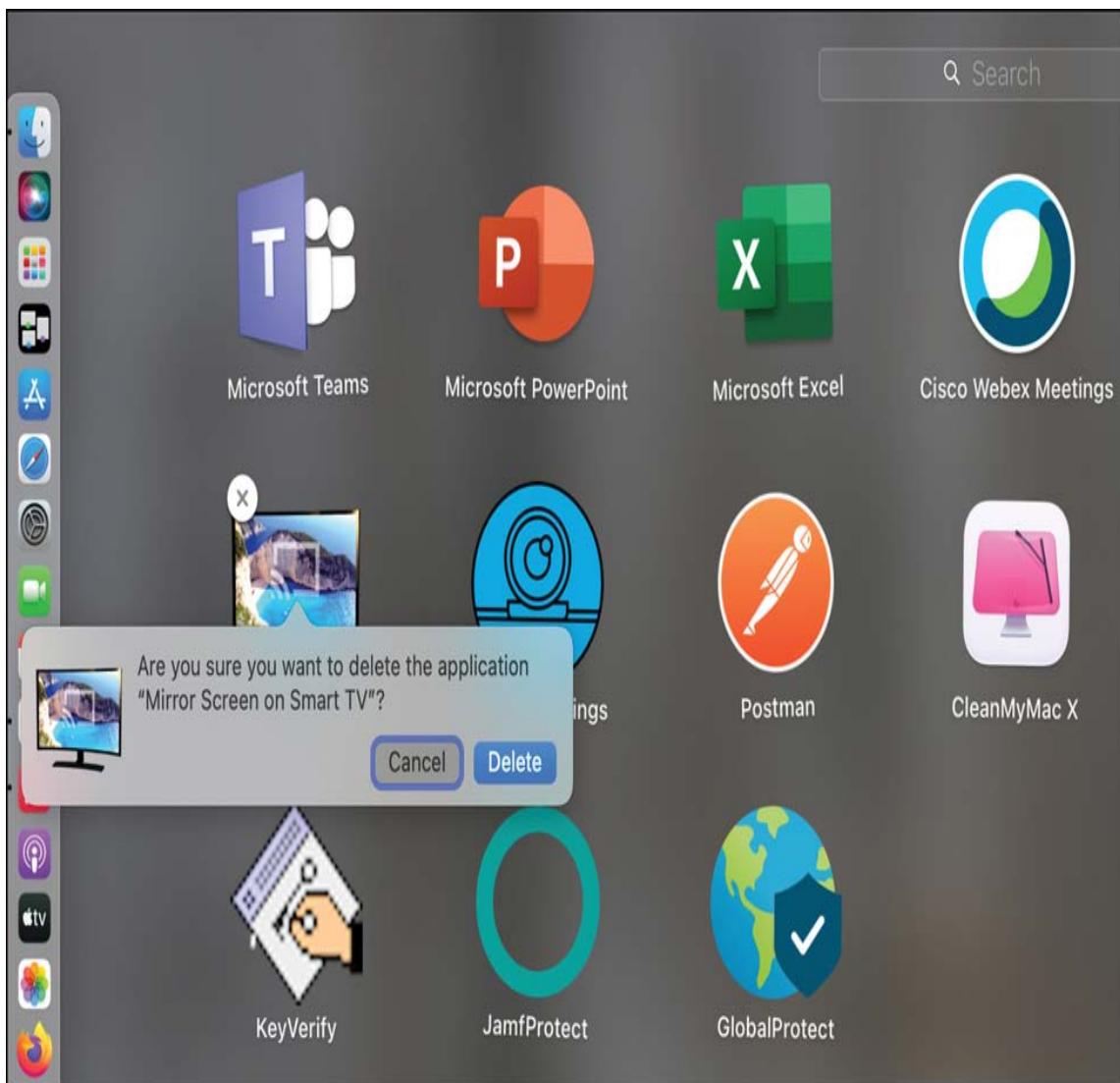
macOS has a variety of options for system updates in the App Store section of System Preferences. The App Store can be configured to automatically check for updates for apps and macOS, automatically install updates, and download apps installed on other macOS devices under the same user account.

To avoid confusion, note that the Apple Store is a place to purchase hardware (phones, computers, accessories, and services); the App Store is for purchasing applications.

## **Uninstallation Process**

Uninstalling apps from a Mac computer is not a complicated process. From the Finder menu, access the Applications folder. Locate the application to be deleted and drag it to the trash.

Another method is to select the Launchpad from the Dock. This displays all applications on the desktop; ones that can be quickly deleted show an X in the upper-left corner of their icon. Simply click the X and confirm (see [Figure 6-49](#)).



**Figure 6-49** Uninstalling from the Mac Launchpad (Third Icon from the Top on the Dock)

These quick methods do not completely uninstall files from the several different places app information is stored. The easiest way to do that is with third-party software such as CleanMyMac.

## Apple ID and Corporate Restrictions

Apple ID is the authentication process used to make sure authorized users are accessing the App Store and making software purchases. The Apple ID crosses platforms, and a user account can be used for purchases and access on an iPhone, an iPad, or a Mac computer.

Corporations can also have Apple ID accounts that they can assign to employees. The key difference between the personal account and the corporate account is that an administrator in the corporate environment can restrict access to the software and services when the user is working in the corporate environment.

## Best Practices

Best practices on a Mac are not different from those on any other OS. At one time, Apple computers were thought to be less vulnerable to virus infections, but that is no longer true. These steps should seem familiar by now.

## Backups

A full backup backs up the entire contents of the computer or selected drive to another local or network location. A backup program can create a compressed file to store backed-up information. With this type of backup, the backup program must run a restore utility to make the files usable again. Another type of backup program simply copies backup files to a different location, where they can be opened by the operating system.

Most backup programs can also run an incremental backup, which backs up only the files that have been created or changed after the last full backup.

Backup features to look for include the following:



- **Compression:** This reduces the amount of file space and also often decreases the amount of time needed to make a backup.
- **Support for incremental as well as full backups:** Good backup practice calls for periodic full backups, followed by backups of files that changed since the last full backup (incremental backups).
- **Local and network backup destinations:** Some backup utilities require additional configuration before a network backup can be performed.

macOS includes the **Time Machine** backup utility that must be configured and running to be useful in case data is lost.

To enable and configure Time Machine, follow these steps:



**Step 1.** Connect a suitable external disk to a macOS system.

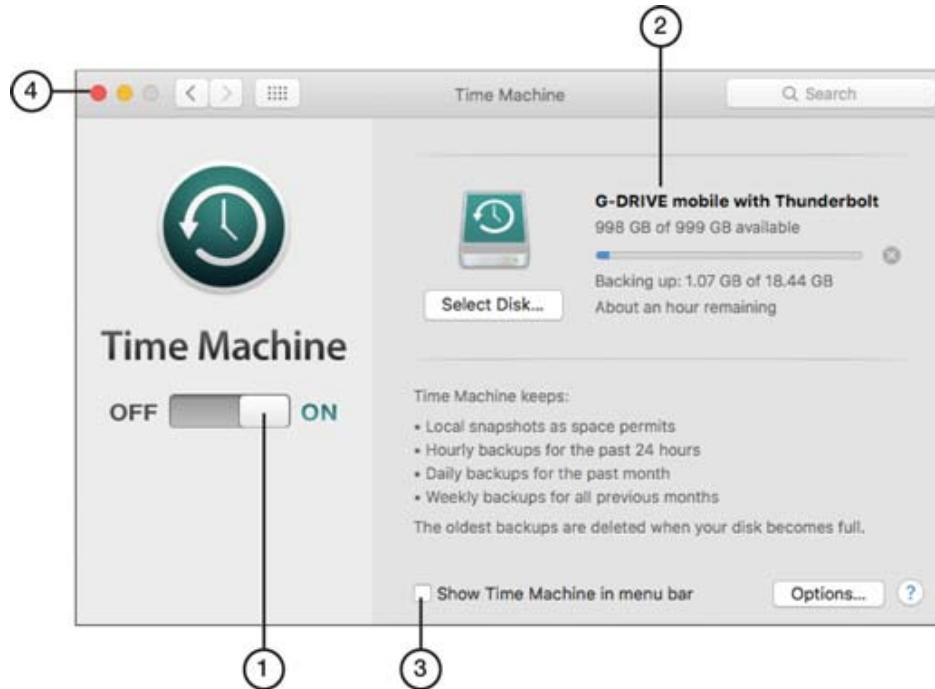
**Step 2.** When prompted, click **Use As Backup Disk**. You can also check the **Encrypt Backup Disk** box to protect the backup (see [Figure 6-50](#)).



1. Create and confirm password for encrypted Time Machine drive
2. Enter a password hint
3. Click to start encryption of Time Machine drive

**Figure 6-50** Selecting an External Disk for Use with Time Machine

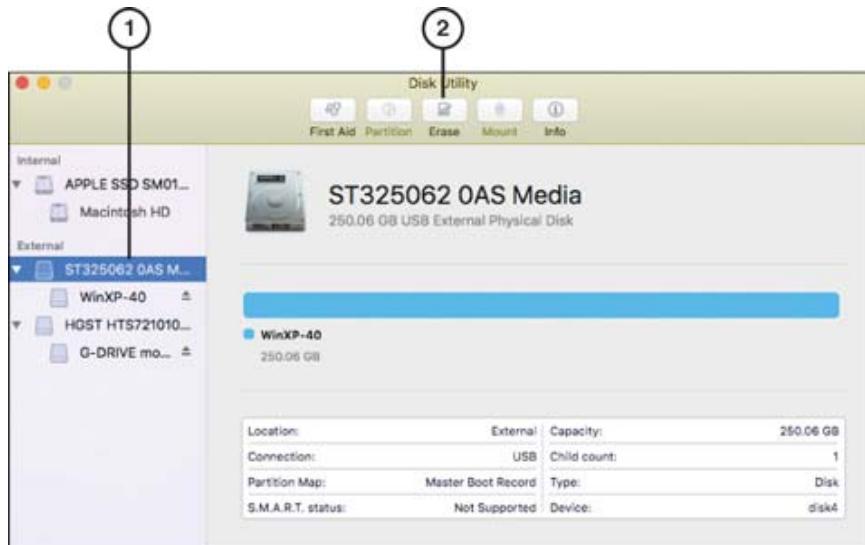
**Step 3.** If you selected the option to encrypt your backup in step 2, enter a password, confirm it, and enter a password hint. Click **Encrypt Disk** (see [Figure 6-51](#)).



1. Time Machine turned on
2. Progress bar and backup disk information
3. Check box to put Time Machine on menu bar at top of screen
4. Click to close (Red) or minimize (Yellow) Time Machine menu

**Figure 6-51** Encrypting the Time Machine Disk

**Step 4.** Make sure Time Machine is turned on (see [Figure 6-52](#)). After the selected disk is encrypted, the backup starts.



1. Click drive to erase
2. Click Erase to start process

## **Figure 6-52** Creating a Backup with Time Machine

Time Machine is designed to back up user files automatically. However, to create a disk image that can be restored in case of disaster, use Disk Utility.

## **Antivirus/Anti-malware Updates**

It was once widely believed that the macOS was immune to viruses and malware. Although macOS is not targeted nearly as much as Windows, an unprotected macOS computer can be used as an infection vector for Windows machines that connect to it.

ClamAV ([www.clamav.net](http://www.clamav.net)) is an open source antivirus app available for both macOS and Linux. Scans and updates can be automated with cron, and a GUI front end known as ClamTK is available. Well-known antivirus software usually has macOS versions as well as Linux and Windows versions.

Antivirus and anti-malware apps should be updated at least daily.

## **Updates/Patches**

macOS has a variety of options for system updates in the Software Update section of System Preferences (see [Figure 6-53](#)). The preferences can be configured to automatically check for updates for apps and macOS, automatically install updates, and download apps installed on other macOS devices under the same user account.

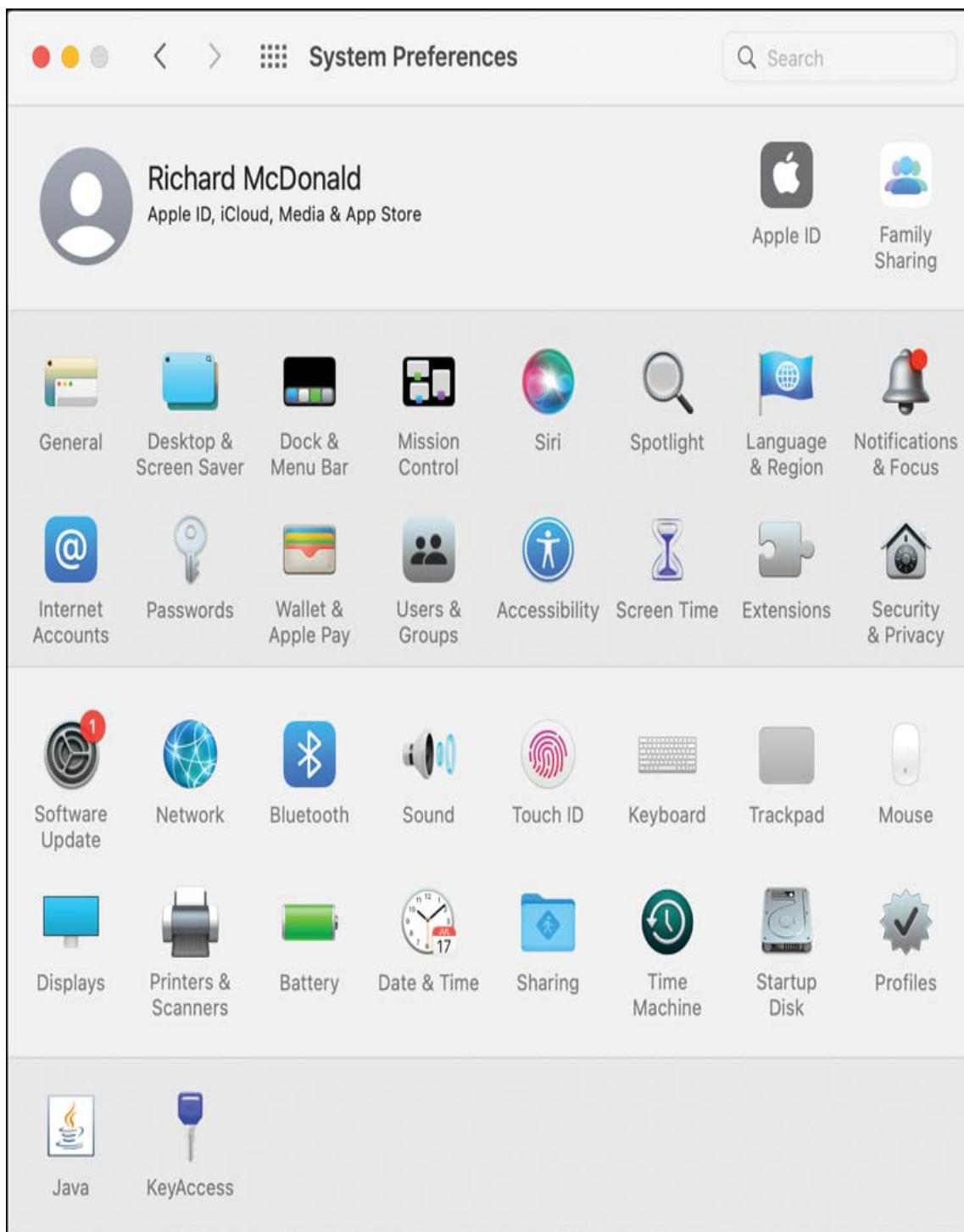


**Figure 6-53** The Software Update App from the System Preferences Menu

When updating software, the Mac or other device must be plugged into AC power. After downloading and installing the update, a password, fingerprint, or face ID is required after restarting.

## System Preferences

The System Preferences settings on a Mac can be accessed by selecting the gearwheel icon on the Dock or by using the Apple menu and selecting System Preferences. [Figure 6-54](#) shows an example of the System Preferences menu.



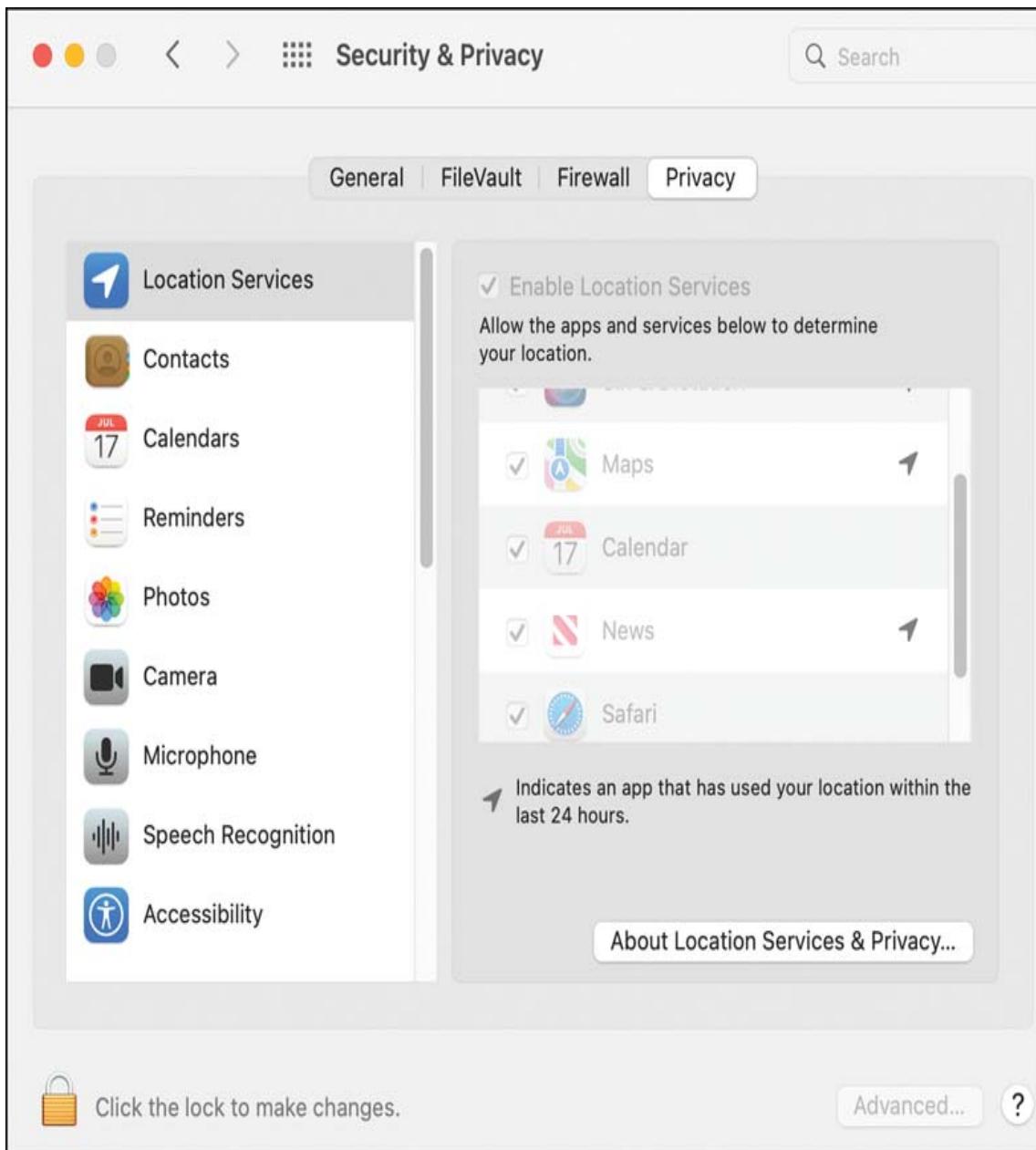
**Figure 6-54** The Systems Preferences Menu. The Red Number over the Software Update Indicates That a New Update Is Available (and That Auto-Updates Have Not Yet Been Configured).

The System Preferences menu varies, depending on the user and the apps installed. However, finding a particular setting is greatly simplified with the

search menu in the upper right. This menu is intuitive: Simply typing one or two letters of a setting highlights the preference that needs to be opened to change settings.

Some key preferences highlighted in the A+ objectives are as follows:

- **Displays:** Configuration of a display's settings, such as brightness and Night Shift, which warms the colors of a display in the evenings for potential sleep improvement.
- **Network:** Settings for Wi-Fi management, TCP/IP, DNS, and other network settings. Also has auto-join settings for commonly accessed networks.
- **Printers & Scanners:** Preferences for printers, print sharing, and scanning.
- **Security and Privacy:** Control over location services (see [Figure 6-55](#)). When enabled, the settings indicate which apps have used location services in the past 24 hours. Security services include firewall settings, FileVault (which automatically encrypts data on the disk), and password controls.



**Figure 6-55** Privacy Settings in the Security & Privacy Menu

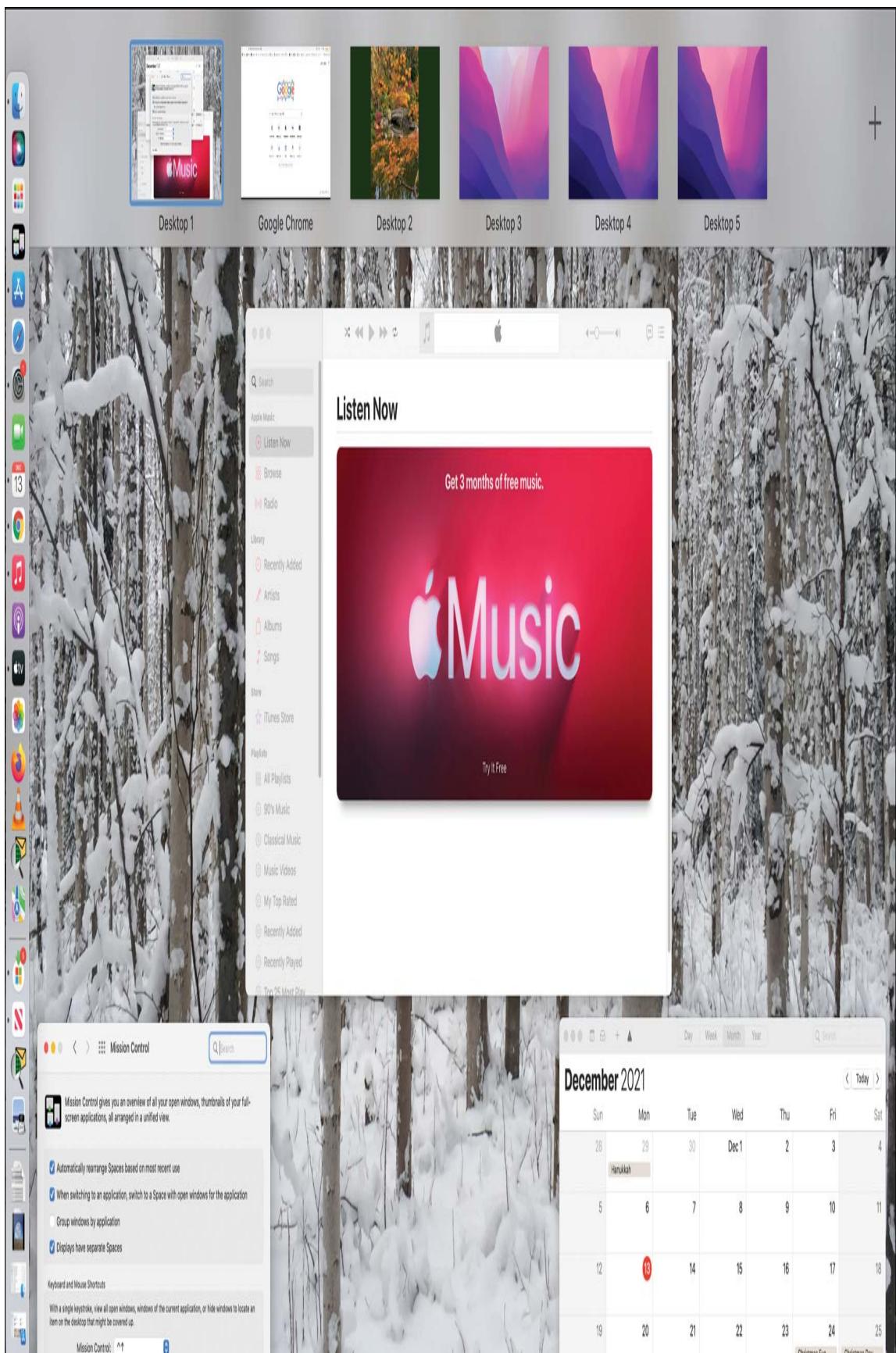
To change settings or to access advanced settings, the lock in the lower left must be unlocked with a password (or biometric) before you can make changes; it must then be relocked to apply the settings.

- **Accessibility:** Settings to configure the Mac to adapt to the user's vision, hearing, motor, and other requirements for ease of use.
- **Time Machine:** See the Time Machine coverage in the previous section.

## Features

macOS has a devoted following of users, and one reason is the many shortcuts and features included in the desktop experience. The A+ objectives feature the nine discussed here, but there are many more to be discovered:

- **Multiple desktops:** Users are not limited to one desktop for work. Several can be in use at one time, with workspaces running different applications (see the top of [Figure 6-55](#)). These desktops can be navigated by swiping up with three or four fingers on the trackpad, using the Control key with the left or right arrows, or using Mission Control.
- **Mission Control:** Mission Control facilitates a display of all open windows, available desktops, and other settings. Among these settings is the capability to use hot corners, in which mousing over a chosen corner of the screen opens a shortcut to a preselected feature, such as the Launchpad or Quick Notes. [Figure 6-56](#) depicts Mission Control (opened with the shortcut of Ctrl+up arrow).





**Figure 6-56** Privacy Mission Control, Displaying Available Desktops, the Dock, and Any Open Windows

- **Keychain:** This encrypted container on the Mac stores passwords, usernames, account numbers, and other private information. It provides security and ease when accessing sites that require authentication. Keychain works across platforms, so an update on a Mac updates the information in an iPhone on the same account.
- **Spotlight:** This is a highly intuitive search engine for documents, text references, and more. It does not reside on the desktop, but you can access it instantly by pressing Cmd+spacebar. Spotlight can be configured to search up to 18 different topics and areas, such as apps, documents, music libraries, and definitions. It can also be configured to not search items in the privacy settings.
- **iCloud:** iCloud is the Apple shared cloud storage product. For a monthly or annual fee, users can store documents and photos. iCloud is not confined to Mac users; it is available to Windows and Linux users as well.
- **Gestures:** This feature allows for an enhanced haptic- or touch-based mouse experience, with different configurable responses for swiping with one, two, or three fingers; using pinching motions; and so on. The gestures are configured under the Track Pad settings in System Preferences.
- **Finder:** The Finder is the key file management tool in the macOS. It provides a look at folders and subfolders (see [Figure 6-57](#)). In the figure, the Finder icon is highlighted on the Dock and then opened to Applications. The application subfolders display information and an installation .dmg file for the app.





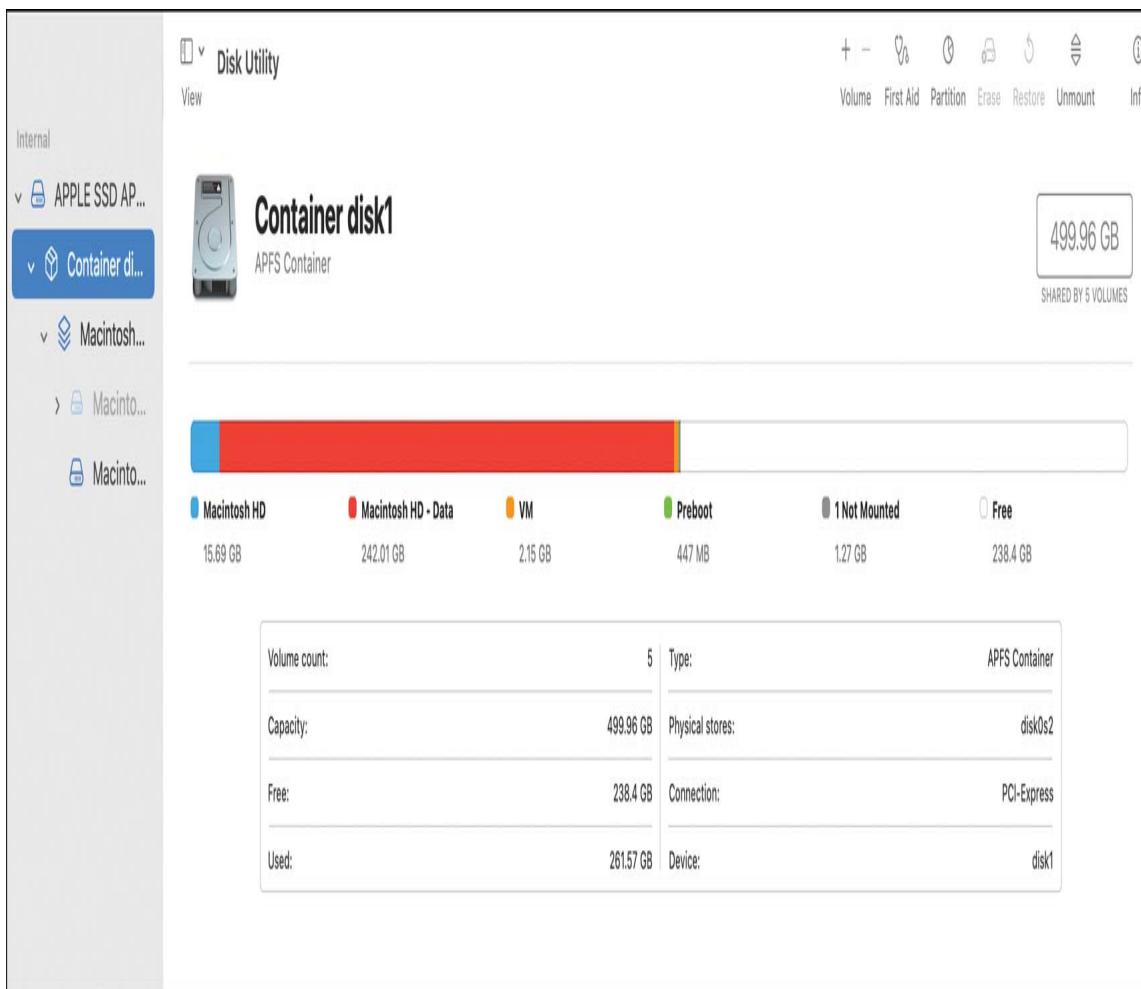
**Figure 6-57** The Finder

- **Remote Disc:** On earlier Macs, this feature allowed a device without an optical drive to access an optical drive on another computer. It was removed in 2019 with the Catalina 10.15 macOS update. On older Macs that have the Remote Disc feature, use the Finder to open the Remote Disc and then select the Mac or Windows computer that is sharing the optical drive. It plays as if it were locally attached.
- **Dock:** The Dock is the quick launch bar on a Mac, similar to the taskbar in Windows. It can be configured to launch apps or open folders or documents. It can be positioned on either side or the bottom of the desktop. [Figure 6-57](#) has the Dock on the left, accessing subfolders in the Applications folder. When the cursor is over the Dock icons the icon information is displayed.

## Disk Utility

[\*\*Disk Utility\*\*](#), shown in [Figure 6-58](#), allows for disk and file management in macOS. It creates blank disk images that can be used as containers for other files, including image backups. It also erases non-macOS drives and prepares them for use with macOS. Repairing, restoring, and mounting disks is also possible. Partitioning can happen here, but since iOS 10.13, Apple File System (APFS) formatted volumes automatically adjust as needed.





**Figure 6-58** APFS Disk Utility

Disk Utility is most easily accessed using Spotlight, the Launchpad, or Finder and searching for Disk Utility. To start Disk Utility at startup, press and hold Cmd+R until it starts.

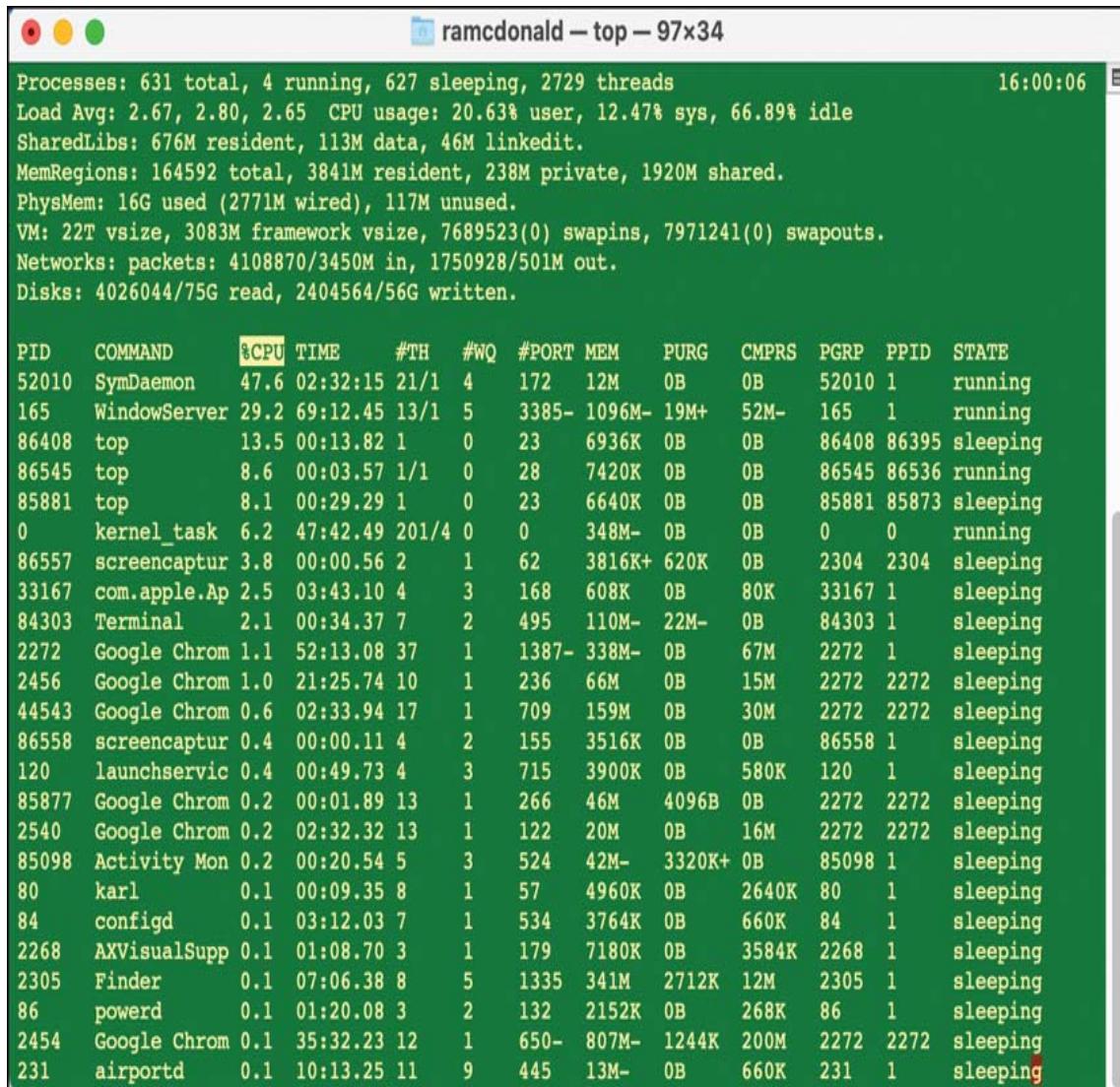
## FileVault

The **FileVault** tab enables and disables (with a password or biometric authentication) the automatic encryption of data on the computer (refer to Figure 6-55).

During setup, a recovery key is created in case the password is lost. If both the password and the key are lost, the data is permanently lost as well.

# Terminal

macOS includes a powerful **Terminal** app that opens a command-line environment. The macOS Terminal utility is used to run commands, scripts, and programs without a GUI. Terminal has its roots in a UNIX shell and can be used to manage other computers on a network. [Figure 6-59](#) depicts Terminal monitoring the top processes on a running Mac.



The screenshot shows a terminal window titled "ramcdonald — top — 97x34". The window displays system statistics and a list of running processes. The statistics include:

- Processes: 631 total, 4 running, 627 sleeping, 2729 threads
- Load Avg: 2.67, 2.80, 2.65 CPU usage: 20.63% user, 12.47% sys, 66.89% idle
- SharedLibs: 676M resident, 113M data, 46M linkedit.
- MemRegions: 164592 total, 3841M resident, 238M private, 1920M shared.
- PhysMem: 16G used (2771M wired), 117M unused.
- VM: 22T vsize, 3083M framework vsize, 7689523(0) swapins, 7971241(0) swapouts.
- Networks: packets: 4108870/3450M in, 1750928/501M out.
- Disks: 4026044/75G read, 2404564/56G written.

The process list is as follows:

PID	COMMAND	%CPU	TIME	#TH	#WQ	#PORT	MEM	PURG	CMPRS	PGRP	PPID	STATE
52010	SymDaemon	47.6	02:32:15	21/1	4	172	12M	0B	0B	52010	1	running
165	WindowServer	29.2	69:12.45	13/1	5	3385-	1096M-	19M+	52M-	165	1	running
86408	top	13.5	00:13.82	1	0	23	6936K	0B	0B	86408	86395	sleeping
86545	top	8.6	00:03.57	1/1	0	28	7420K	0B	0B	86545	86536	running
85881	top	8.1	00:29.29	1	0	23	6640K	0B	0B	85881	85873	sleeping
0	kernel_task	6.2	47:42.49	201/4	0	0	348M-	0B	0B	0	0	running
86557	screencaptur	3.8	00:00.56	2	1	62	3816K+	620K	0B	2304	2304	sleeping
33167	com.apple.Ap	2.5	03:43.10	4	3	168	608K	0B	80K	33167	1	sleeping
84303	Terminal	2.1	00:34.37	7	2	495	110M-	22M-	0B	84303	1	sleeping
2272	Google Chrom	1.1	52:13.08	37	1	1387-	338M-	0B	67M	2272	1	sleeping
2456	Google Chrom	1.0	21:25.74	10	1	236	66M	0B	15M	2272	2272	sleeping
44543	Google Chrom	0.6	02:33.94	17	1	709	159M	0B	30M	2272	2272	sleeping
86558	screencaptur	0.4	00:00.11	4	2	155	3516K	0B	0B	86558	1	sleeping
120	launchservic	0.4	00:49.73	4	3	715	3900K	0B	580K	120	1	sleeping
85877	Google Chrom	0.2	00:01.89	13	1	266	46M	4096B	0B	2272	2272	sleeping
2540	Google Chrom	0.2	02:32.32	13	1	122	20M	0B	16M	2272	2272	sleeping
85098	Activity Mon	0.2	00:20.54	5	3	524	42M-	3320K+	0B	85098	1	sleeping
80	karl	0.1	00:09.35	8	1	57	4960K	0B	2640K	80	1	sleeping
84	configd	0.1	03:12.03	7	1	534	3764K	0B	660K	84	1	sleeping
2268	AXVisualSupp	0.1	01:08.70	3	1	179	7180K	0B	3584K	2268	1	sleeping
2305	Finder	0.1	07:06.38	8	5	1335	341M	2712K	12M	2305	1	sleeping
86	powerd	0.1	01:20.08	3	2	132	2152K	0B	268K	86	1	sleeping
2454	Google Chrom	0.1	35:32.23	12	1	650-	807M-	1244K	200M	2272	2272	sleeping
231	airportd	0.1	10:13.25	11	9	445	13M-	0B	660K	231	1	sleeping

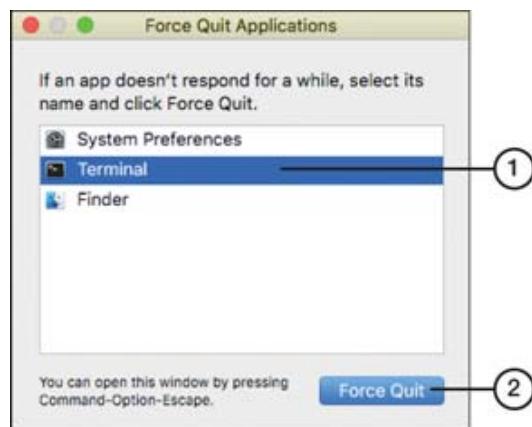
**Figure 6-59** Terminal on Mac

# Force Quit

The **Force Quit** feature in macOS enables the user to shut down a malfunctioning app.

To open the Force Quit application from the keyboard, press Cmd+Option+Esc.

Force Quit can also be started from the menu bar: Open the Apple menu and select Force Quit. You can also point at the app's icon in the Dock (at the bottom of the screen) and either right-click or click and hold it to bring up a menu with Quit as an option. From the Force Quit menu, select the app to stop (see [Figure 6-60](#)).



1. Select an app to force quit
2. Click Force Quit to close it

**Figure 6-60** Using Force Quit in macOS

## Common Features and Tools of the Linux Client/Desktop OS



**220-1102: Objective 1.11:** Identify common features and tools of the Linux client/desktop OS.

Linux operating systems are far less common than Windows on organizational desktops; however, they have an ever-growing presence as the OS on servers and other enterprise-level computers.



# Common Linux Commands

With more Linux systems showing up on corporate networks, computer technicians need to understand basic Linux commands. The following sections review the commands that can appear on the A+ exam.

To use these commands, open a Terminal session. Some commands must be run as root user. (To run commands as root, log in as root or use **sudo**.)

## ls

**ls** is the macOS and Linux equivalent to the Windows command **dir**. Use **ls -l** to list the contents of a directory (folder), including permissions and other information (see [Figure 6-61](#)).

```
msoper@localhost:/etc
File Edit View Search Terminal Help
-rw-r--r--. 1 root root      375 Sep 17 2015 trusted-key.key
drwxr-xr-x. 4 root root    4096 Oct 29 16:24 udev
drwxr-xr-x. 2 root root    4096 Jun 30 2015 udisks2
drwxr-xr-x. 2 root root    4096 Oct 29 16:23 unbound
-rw-r--r--. 1 root root     587 Jun 17 2015 updatedb.conf
drwxr-xr-x. 2 root root    4096 Oct 29 16:23 UPower
-rw-r--r--. 1 root root    1018 Jul 16 2015 usb_modeswitch.conf
drwxr-xr-x. 2 root root   20480 Oct 29 16:23 usb_modeswitch.d
-rw-rw-r--. 1 root root     28 Mar  2 19:19 vconsole.conf
-rw-r--r--. 1 root root     51 Aug 31 2015 vdpau_wrapper.cfg
-rw-r--r--. 1 root root    1982 Aug 20 2015 virt
drwxr-xr-x. 5 root root    4096 Oct 29 16:23 vmware-tools
drwxr-xr-x. 2 root root    4096 Oct 29 16:23 vpnc
-rw-r--r--. 1 root root    4925 Jun 18 2015 wgetrc
drwxr-xr-x. 2 root root    4096 Oct 29 16:23 wpa_supplicant
-rw-r--r--. 1 root root     0 Jun 18 2015 wvdial.conf
drwxr-xr-x. 6 root root    4096 Oct 29 16:24 XII
-rw-r--r--. 1 root root    589 Sep 14 2015 xattr.conf
drwxr-xr-x. 7 root root    4096 Oct 29 16:23 xdg
drwxr-xr-x. 2 root root    4096 Sep 10 2015 xinetd.d
drwxr-xr-x. 2 root root    4096 Oct 29 16:22 xml
drwxr-xr-x. 3 root root    4096 Oct 29 16:23 yum
drwxr-xr-x. 2 root root    4096 Oct 29 16:21 yum.repos.d
[msoper@localhost etc]$ ls -l
```

1. Directories are listed in blue
2. Press the up-arrow key to repeat the last command; press it again to repeat the previous one, and so on

**Figure 6-61** Using **ls -l** in Fedora 23 Workstation

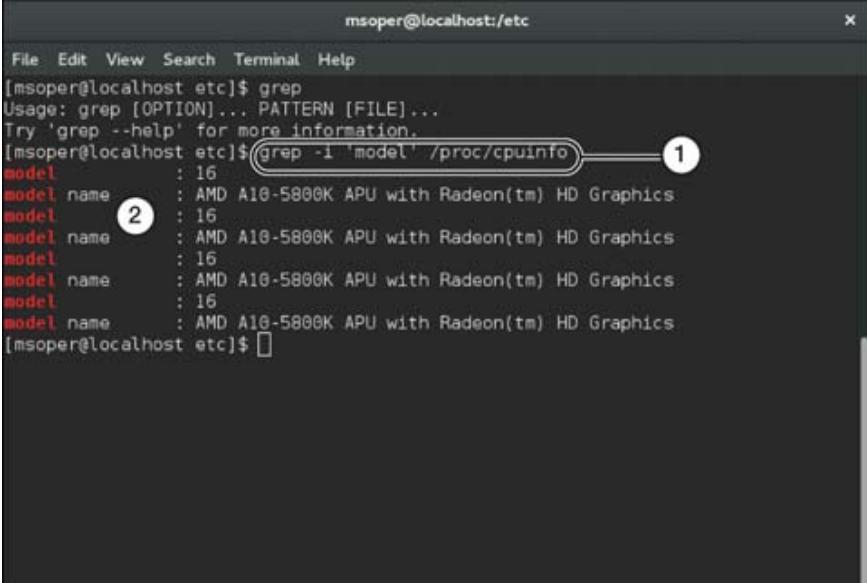
## grep

Use **grep** to perform text searches. The **grep** command line specifies what to search for and where to search.

**grep** can be used to find a specified word in one or more specified files. **grep** normally searches for exact matches (Linux and macOS are case sensitive), but it can be configured to ignore case with **-i**.

**grep** supports recursive searching—that is, searching in all files in directories (folders) beneath the current directory.

[Figure 6-62](#) shows **grep** being used to search for the word *model* in the /proc/cpuinfo directory (folder).



The screenshot shows a terminal window titled "msoper@localhost:/etc". The user has run the command `grep -i 'model' /proc/cpuinfo`. The output shows multiple occurrences of the word "model" in the /proc/cpuinfo file, each preceded by a red "model" and followed by a blue "name". A red circle labeled "1" is over the command line, and a blue circle labeled "2" is over the first occurrence of "model" in the output.

```
msoper@localhost:/etc$ grep -i 'model' /proc/cpuinfo
Usage: grep [OPTION]... PATTERN [FILE]...
Try 'grep --help' for more information.
[msoper@localhost etc]$ grep -i 'model' /proc/cpuinfo
model : 16
model name : AMD A10-5800K APU with Radeon(tm) HD Graphics
model : 16
model name : AMD A10-5800K APU with Radeon(tm) HD Graphics
model : 16
model name : AMD A10-5800K APU with Radeon(tm) HD Graphics
model : 16
model name : AMD A10-5800K APU with Radeon(tm) HD Graphics
[msoper@localhost etc]$ 
```

1. Searching for the word *model*
2. Matches

**Figure 6-62** Searching for Specific Text in a Folder by Using **grep**

## cd

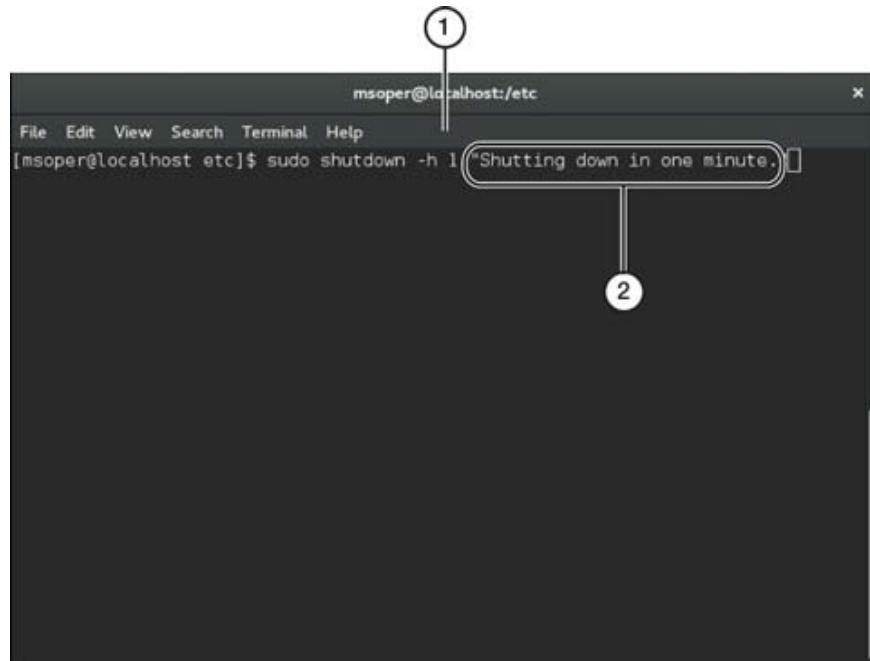
Use **cd** to change directories (folders). The syntax is different from the Windows command line: Linux uses the / slash, whereas Windows uses the \ slash.

Use **cd /etc** to change to the /etc folder.

Use **cd..** to move up one level.

## shutdown

Use **shutdown** to shut down the system. Figure 6-63 shows **shutdown** used along with options to specify when to shut down and when to broadcast a warning message. Note that the **sudo** command is used with this command because **shutdown** requires root access.



1. One minute (1) to shutdown
2. Message broadcast to all systems logged in to this computer

**Figure 6-63** Preparing to Shut Down a System

## pwd

**pwd** displays the name of the current/working directory.

## mv

Use **mv** to move files to a specified location, as in this example:

**mv thisfile.ext destination-folder**

## cp

Use **cp** to copy files to a specified location (using the syntax **cp filename /folder/ subfolder**) or to a different name in the same folder (for

example, **cp -i origfile copiedfile**). Use the **-i** option to be prompted in case the command would overwrite a file.

## rm

Use **rm** to remove (delete) files from the system (**rm filename**).

## chmod

Use **chmod** to change permissions of files and directories using the syntax **chmod permissions filename**. In [Figure 6-64](#), **chmod** is used to change permissions on the file test. The numbers that are used stand for different permissions. To learn more about these values, see the Chmod Calculator at <https://chmod-calculator.com>. Also note that, in [Figure 6-64](#), the command **ls -l** is used to display file permissions and the filename.

The screenshot shows a terminal window with the following session:

```
markesoper@markesoper-VirtualBox: ~/Desktop
markesoper@markesoper-VirtualBox:~/Desktop$ ls -l
total 0
-rw-r--r-- 1 markesoper markesoper 0 Mar 25 22:29 test
markesoper@markesoper-VirtualBox:~/Desktop$ chmod 444 test
markesoper@markesoper-VirtualBox:~/Desktop$ ls -l
total 0
-r--r--r-- 1 markesoper markesoper 0 Mar 25 22:29 test
markesoper@markesoper-VirtualBox:~/Desktop$ chmod 664 test
markesoper@markesoper-VirtualBox:~/Desktop$ ls -l
total 0
-rw-rw-r-- 1 markesoper markesoper 0 Mar 25 22:29 test
markesoper@markesoper-VirtualBox:~/Desktop$
```

Annotations with circles and numbers:

- Annotation 1: Points to the first `ls -l` command and its output.
- Annotation 2: Points to the second `chmod 444 test` command.

1. Using the `ls -l` command to see the file permissions changes made with `chmod`
2. Changing file permissions with `chmod`

**Figure 6-64** Changing Permissions for the File Test Using Ubuntu

## chown

Use **chown** to change file ownership using the syntax **sudo chown newowner filename**.

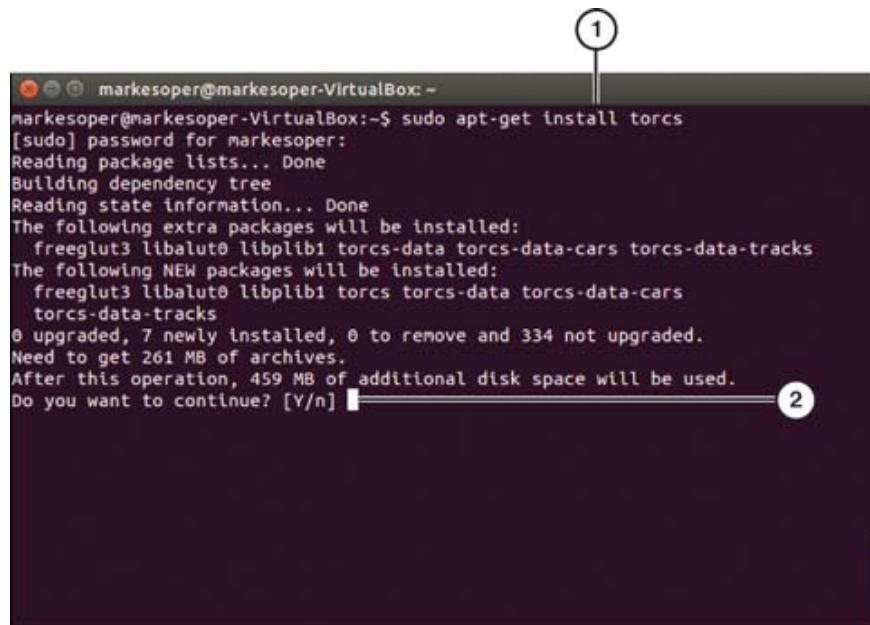
## **su/sudo**

Use **sudo** to run a command as another user. It is most commonly used by a user to run a command as root.

Use **su** to switch between accounts. Entering **su** without specifying options changes to root and prompts for the root password.

## **apt-get**

Use **apt-get** to install or manage Advanced Packaging Tool (APT) software packages, which are common in Debian-based distributions such as Ubuntu (see [Figure 6-65](#)). The **apt-get** command must be used with **sudo**. Use this syntax: **sudo apt-get function appname**.



```
markesoper@markesoper-VirtualBox:~$ sudo apt-get install torcs
[sudo] password for markesoper:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  freeglut3 libalut0 libplib1 torcs-data torcs-data-cars torcs-data-tracks
The following NEW packages will be installed:
  freeglut3 libalut0 libplib1 torcs torcs-data torcs-data-cars
  torcs-data-tracks
0 upgraded, 7 newly installed, 0 to remove and 334 not upgraded.
Need to get 261 MB of archives.
After this operation, 459 MB of additional disk space will be used.
Do you want to continue? [Y/n] 2
```

1. The function to perform is install
2. Answer Y to continue

**Figure 6-65** Installing torcs (The Open Racing Car Simulator) with **apt-get** on Ubuntu

## **YUM (Yellowdog Updater, Modified)**

**YUM** is an open-source utility that provides for automatic updates and package management in Linux.

## ip

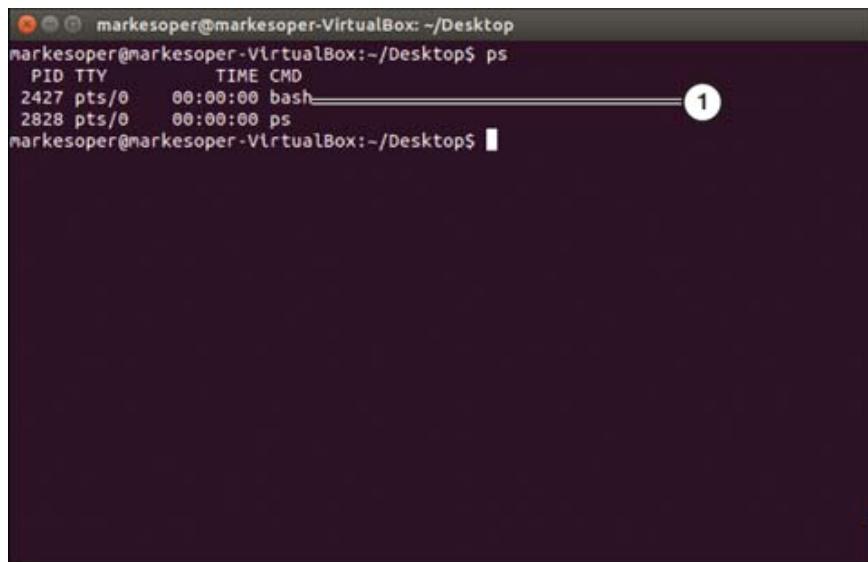
The **ip** command is used to manage network interfaces. It can bring up the network interfaces or shut them down, manage IP addresses, and look at routing and ARP tables.

## df (Disk Free)

The **df** command is used to display used and free space on disks. The command also has options for viewing file system size.

## ps

Use the **ps** command to list the processes and tasks running in the OS (see Figure 6-66).



A screenshot of a terminal window on a Linux desktop. The window title is 'markesoper@markesoper-VirtualBox: ~/Desktop'. The command entered is 'ps'. The output shows two processes: 'bash' with PID 2427 and 'ps' with PID 2828. The 'CMD' column shows the command name. A red circle with the number '1' is drawn around the 'CMD' column header.

```
markesoper@markesoper-VirtualBox: ~/Desktop$ ps
 PID TTY      TIME CMD
 2427 pts/0    00:00:00 bash
 2828 pts/0    00:00:00 ps
markesoper@markesoper-VirtualBox: ~/Desktop$
```

1. Current processes listed by name and PID.

**Figure 6-66** Listing Processes for the Current User with **ps**

## man

Linux distributions (distros) contain a manual (manpages) with options for each command. To view or print a command's manpage, use the command **man**. To learn more, see [www.linfo.org/man.xhtml](http://www.linfo.org/man.xhtml). To view manpages for Ubuntu (one of the most popular distros) online, see <https://manpages.ubuntu.com>.

## **top**

The **top** command provides summary information on resource use for tasks and processes in the form of a dashboard. It can also be used to monitor CPU and memory usage.

## **find**

The **find** command is used to find files and directories and information about them. You can search by name, date, owners, and so on.

## **DIG (Domain Information Groper)**

The **dig** command provides useful information on DNS servers for troubleshooting DNS issues.

## **cat**

**cat** is a utility command for writing text into files and printing file content.

## **nano**

**nano** is a command-line text editor with keyboard shortcuts and functions for editing files.

## **Best Practices**

To maintain any computer system, you should follow best practices related to the following:

- Scheduled backups
- Scheduled disk maintenance
- System updates and the App Store
- Patch management
- Driver and firmware updates
- Antivirus and anti-malware updates

The following sections discuss best practices in these areas for macOS and Linux.

## Scheduled Backups

Scheduled backups help prevent major data loss in case of system failure, accident, or loss. Backups can be used to safeguard the following:

- Contacts
- Email
- Media files (photos, videos, and music)
- Documents

The default backup app in macOS is Time Machine. Linux includes several utilities that can be used for backups. These include the command-line tar and rsync utilities. Others, including the grsync (GUI for rsync) and duplicity (command line and GUI available as Déjà Dup), are available from the repository for a Linux distribution or from the vendors.

### Note

The BackupYourSystem page on Ubuntu Linux Help (<https://help.ubuntu.com/community/BackupYourSystem>) provides a long list of command-line and GUI-based backup tools that also work with other Linux distros.

Scheduled backups should be run at times when the system is idle, such as overnight and on weekends.

## Backup Types

A full backup backs up the entire contents of the computer or selected drive to another local or network location. A backup program can create a compressed file to store backed-up information. With this type of backup, the backup program must run a restore utility to make the files usable again. Another type of backup program simply copies backup files to a different location, where they can be opened by the operating system.

Most backup programs can also run an incremental backup, which backs up only the files that have been created or changed after the last full backup.

Backup features to look for include the following:



- **Compression:** This reduces the amount of file space and often also decreases the amount of time needed to make a backup.
- **Support for incremental as well as full backups:** Good backup practice calls for periodic full backups followed by backups of files that have changed since the last full backup (incremental backups).
- **Local and network backup destinations:** Some backup utilities might require additional configuration before a network backup can be performed.

## Configuring a Backup App in Linux

The Ubuntu distributions have a preinstalled backup application that runs weekly and can also be configured to run daily. Backups can be kept as long as space permits, or for at least 6 months or a year. This backup utility is designed for new users.

Backup utilities based on tar, rdiff, and other Linux apps can require a great deal of scripting. One backup utility that helps create backup scripts by filling in the blanks is Backupninja. More information on Backupninja can be found at <https://linux.die.net/man/1/backupninja>.



## Antivirus

It's widely believed that Linux is immune to viruses and malware. Although Linux is not targeted nearly as much as Windows, an unprotected Linux computer can be used as an infection vector for Windows machines that connect to it.

ClamAV ([www.clamav.net](http://www.clamav.net)) is an open source antivirus app available for both macOS and Linux. Scans and updates can be automated with cron, and a

GUI front end known as ClamTK also is available. Well-known antivirus software usually has Linux and macOS versions as well as Windows versions.

Antivirus and anti-malware apps for Linux should be updated at least daily.

## Updates and Patches

If an organization has only a few Linux systems, running manual system updates with yum or apt-get might be sufficient for patch management. However, as the number of Linux systems increases, and when Linux systems are used for mission-critical functions such as web servers, better patch management methods are desirable.

If you use a script to check for and install updates to Linux or installed apps, the crontab utility can be used to set the task on a schedule that is run by the cron utility.

## Tools

As with Windows and macOS, key tools add ease and functionality to the OS. Two important tools in Linux are discussed here.

### shell/terminal

The **terminal** and **shell** tools in Linux are similar to the command shell (prompt) and PowerShell tools in Windows. The command line is the most direct and efficient access to the center of the OS, and PowerShell was designed to extend the power of the command shell, adding scripting functions and interoperability. The same is true of Linux. The terminal command opens a shell for typing commands. Linux shells, of which there are several, add similar functionality to the Linux terminal. The most popular Linux shell is Bash (Bourne Again Shell), but others are in use; these include PowerShell, which is now a fully functional cross-platform scripting language that works in Linux, macOS, and Windows 10 and 11.

To open Terminal in Linux, simply press Ctrl+Alt+T or type **terminal** in the search box.

## Samba

Linux and Windows machines can work together on a network, thanks to **Samba**. Samba is open source software that enables Linux machines to work in a Windows environment for file and print sharing. Samba also enables Linux machines to participate in Windows Active Directory as a controller or a member. More information on Samba is available at [www.samba.org/](http://www.samba.org/).

## Exam Preparation Tasks

As mentioned in the Introduction, you have several choices for exam preparation: the exercises here; [Chapter 10, “Final Preparation”](#); and the exam simulation questions in the Pearson Test Prep practice test software.

## Review All the Key Topics

Review the most important topics in the chapter, noted with the Key Topic icon in the outer margin of the page. [Table 6-9](#) lists these key topics and the page number on which each is found.



**Table 6-9** Key Topics for [Chapter 6](#)

Key Topic Element	Description	Page Number
<a href="#">Table 6-2</a>	Windows 10 Editions and Features	436
Section	Microsoft Command-Line Tools	438
<a href="#">Table 6-4</a>	Windows Command Prompt Commands	440
Section	format	443
Section	copy	445
Section	xcopy	446
Section	robocopy	446
Section	diskpart	447

<b>Key Topic Element</b>	<b>Description</b>	<b>Page Number</b>
Section	sfc	448
Section	chkdsk	449
Section	gpupdate	450
Section	Device Manager	456
<a href="#">Figure 6-14</a>	msinfo32 System Summary	464
Section	System Configuration Utility	467
Section	Registry Editor	469
<a href="#">Table 6-6</a>	Internet Properties Dialog Tabs	472
Section	Workgroup vs. Domain Setup	484
List	Creating a workgroup in Windows	485
Section	Network Shares	486
List	Mapping drives and folders	488
Steps	VPN connections	495
Steps	Configuring a wireless connection	496
Steps	Configuring a wired connection	497
Steps	Proxy settings	497
Section	System Requirements for Applications	501
Section	32-Bit vs. 64-Bit File Systems	501
Section	Workstation OSs	509
Section	Cellphone/Tablet Operating Systems	511
List	NTFS vs. FAT32	515
List	Methods to boot a system during the installation process	519
List	Types of Windows installations	520
Section	Upgrades	521
Section	Clean Install	521

<b>Key Topic Element</b>	<b>Description</b>	<b>Page Number</b>
Steps	Repair installation	523
List	Partitioning methods	527
Section	Creating Partitions During Windows Installation	529
List	Backup features	536
Steps	macOS: configuring Time Machine	537
<a href="#">Figure 6-58</a>	APFS Disk Utility	544
<a href="#">Figure 6-60</a>	Using Force Quit in macOS	546
Section	Common Linux Commands	546
List	Linux OS: backup features	554
Section	Antivirus	555

## Complete the Tables and Lists from Memory

Print a copy of [Appendix C, “Memory Tables”](#) (found online), or at least the section for this chapter, and complete the tables and lists from memory. [Appendix D](#), “Memory Tables Answer Key,” also online, includes completed tables and lists to check your work.

## Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

- [domain access](#)
- [workgroup](#)
- [Remote Desktop Protocol \(RDP\)](#)
- [BitLocker](#)
- [gpedit.msc](#)
- [in-place upgrade](#)
- [cd](#)

dir  
md  
rmdir  
ipconfig  
ping  
hostname  
netstat  
nslookup  
chkdsk  
net user  
net use  
tracert  
format  
xcopy  
copy  
robocopy  
gpupdate  
gpresult  
shutdown  
sfc  
[command name] /?  
diskpart  
pathping  
winver  
Task Manager  
Microsoft Management Console (MMC)  
Event Viewer (eventvwr.msc)  
Disk Management (diskmgmt.msc)  
Task Scheduler (taskschd.msc)  
Device Manager (devmgmt.msc)  
Certificate Manager (certmgr.msc)  
Local Users and Groups (lusrmgr.msc)  
Performance Monitor (perfmon.msc)  
Group Policy Editor (gpedit.msc)

System Information (msinfo32.exe)  
Resource Monitor (resmon.exe)  
System Configuration (msconfig.exe)  
Disk Cleanup (cleanmgr.exe)  
Registry Editor (regedit.exe)  
ease of access  
workgroup  
domain  
shared resources  
Windows Defender Firewall  
Internet Protocol (IP) addressing scheme  
subnet mask  
Domain Name System (DNS)  
gateway  
virtual private network (VPN)  
wireless wide area network (WWAN)  
proxy settings  
metered connections  
video random access memory (VRAM)  
Windows  
macOS  
Linux  
Chrome OS  
Android  
iOS  
iPadOS  
New Technology File System (NTFS)  
Extensible File Allocation Table (exFAT)  
File Allocation Table 32 (FAT32)  
Apple File System (APFS)  
Third Extended File System (ext3)  
Fourth Extended File System (ext4)  
product life cycle  
boot methods

clean install  
repair installation  
remote network installation  
image deployment  
recovery partition  
partitioning  
master boot record  
GUID Partition Table (GPT)  
.dmg files  
.pkg files  
.app files  
Time Machine  
Mission Control  
Keychain  
Spotlight  
iCloud  
Gestures  
Finder  
Remote Disc  
Dock  
Disk Utility  
FileVault  
Terminal  
Force Quit  
grep  
pwd  
mv  
cp  
rm  
chmod  
chown  
su/sudo  
apt-get  
yum

ip  
df  
grep  
ps  
man  
top  
find  
dig  
cat  
nano  
terminal  
shell  
Samba

## Answer Review Questions

- 1.** Which of the following statements best describes a workgroup?  
(Choose all that apply.)
  - a.** All the computers in a workgroup must be on the same subnet.
  - b.** File and printer sharing should be enabled on each computer in a workgroup.
  - c.** The workgroup should have a password.
  - d.** Each computer in a workgroup must have a user account for each user.
- 2.** Mark is redeploying a workstation for a new user in another building. It has been determined that the computer needs to be renamed for management purposes. Which one of the following options will allow him to make the change?
  - a.** Opening System Properties
  - b.** Typing Msinfo32 at the command line
  - c.** Opening the System Configuration utility
  - d.** Accessing the drive properties
- 3.** In the following table, indicate which command should be used to execute each task.

<b>Task</b>	<b>Command</b>
a. Open a command prompt	
b. View all the directories in a specified location	
c. Create a new folder	
d. Remove an empty folder	
e. Remove one or more files	
f. Stop running a specified task	
g. Copy single or multiple files	
h. Scan for errors and repair the hard drive	
i. Close a command prompt	
j. Create new partitions	
k. Display the help files for a specific command	
<b>1.</b> chkdsk	
<b>2.</b> cmd or command	
<b>3.</b> command/?	
<b>4.</b> del	
<b>5.</b> dir	
<b>6.</b> diskpart	
<b>7.</b> exit	
<b>8.</b> md or mkdir	
<b>9.</b> rd or rmdir	
<b>10.</b> taskkill	
<b>11.</b> xcopy, robocopy	
<b>4.</b> A client can browse the Web but is unable to print to a network printer. Which of the following statements best describes the most likely cause?	
<b>a.</b> The sharing options for the network profile need to be reconfigured.	

- b. The network adapter is configured to use half-duplex mode.
  - c. The Wi-Fi is disabled.
  - d. An alternative IP configuration is not complete.
- 5. Your network adapter is disabled. How is this indicated in Windows Device Manager?
  - a. The device is not listed.
  - b. An ! is displayed over the device icon.
  - c. A down-arrow icon is displayed over the device icon.
  - d. A ? is displayed over the device icon.
- 6. A client reports that the system is starting up very slowly. Which of the following utilities is best for determining what is going on?
  - a. Devices and Printers
  - b. Programs and Features
  - c. System Protection
  - d. System Configuration
- 7. Which of the following steps is necessary to turning on file sharing?
  - a. Open the Firewall application
  - b. Open the System Properties
  - c. Open the Network and Sharing Center
  - d. Open the System Configuration utility
- 8. You have created a shared folder on a network server. You have assigned a letter designation to the folder and made it available to all members of the Research department. This folder now appears as a drive letter on each user's computer. Which type of folder have you created?
  - a. Administrative share
  - b. Cloud share
  - c. Mapped network drive
  - d. VPN
- 9. In the following table, write the command used to open the respective utilities.

<b>Utility</b>	<b>Command</b>
a. Registry	
b. System Information	
c. System Configuration	
d. Microsoft Management Console	
	<b>1.</b> mmc <b>2.</b> msconfig <b>3.</b> msinfo32 <b>4.</b> regedit
<b>10.</b> Which of the following utilities is used to create a VPN?	
a. Network and Sharing Center	
b. Internet Options	
c. System Properties	
d. Windows Firewall	
<b>11.</b> Which of the following utilities do you use to see the items that are set to run automatically at a particular time?	
a. Task Scheduler	
b. Services	
c. Device Manager	
d. Performance	
<b>12.</b> Antonio is using his laptop in a restaurant and has set his network profile to Public. Which of the following is not available to him? (Choose all that apply.)	
a. File and printer sharing	
b. Access to downloaded documents	
c. Network discovery	
d. Media streaming	
<b>13.</b> Which of the following statements best describes a firewall?	

- a. A firewall is a specially constructed barrier in the server room that is meant to limit the spread of fire.
  - b. A firewall is a fire-suppression technology that uses plenum-grade cabling in ducts and ceiling spaces.
  - c. A firewall is a proxy server with a VPN connection.
  - d. A firewall is software or hardware that controls the flow of information between a computer and the Internet or another network.
- 14.** Which of the following can be configured as exceptions in Windows Defender Firewall? (Choose all that apply.)
  - a. Applications that are to be allowed through the firewall
  - b. Ports and port numbers to be opened
  - c. The IP address to be used
  - d. The subnet mask to be used
- 15.** What is the purpose of a subnet mask?
  - a. It allows computers to hide their IP addresses from others.
  - b. It translates addresses between IPv4 and IPv6.
  - c. It defines which IPv4 address bits are network bits and which are host bits.
  - d. It hides the default gateway from the local network.
- 16.** Which of the following is the backup utility for the macOS operating system?
  - a. tar
  - b. crontab
  - c. Time Machine
  - d. YUM
- 17.** What is the purpose of Disk Utility in macOS?
  - a. It prepares a disk to be used for storing image backups and other files.
  - b. It manages the network connection to the Internet.
  - c. It ejects a disk.
  - d. It manages remote storage in the cloud.

**18.** In the macOS or Linux terminal, which of the following is used to force quit an app by using its PID number?

- a. **kill**
- b. **Ctrl+Alt+Del**
- c. **end**
- d. **fq**

**19.** What is not true of Samba?

- a. It is open source.
- b. It allows Linux machines to join Active Directory.
- c. It enables print sharing across Linux and Windows machines.
- d. It is a backup utility for Windows and Linux.

**20.** Screen sharing, file sharing, and printer sharing are configured through which macOS utility?

- a. Control Panel
- b. System Preferences
- c. Sharing app
- d. Display

**21.** Which role does Mission Control play in macOS?

- a. It displays all open apps on multiple desktops.
- b. It installs an operating system on a virtual machine.
- c. It manages the flow of incoming and outgoing data across a network.
- d. It manages the flow of data through a firewall.

**22.** Which of the following macOS apps is used for sharing photos and documents and for data storage?

- a. Time Machine
- b. iCloud
- c. Apple Assist
- d. Spotlight

**23.** What is the name of the file manager used by macOS?

- a. Explorer

- b.** Search
  - c.** Finder
  - d.** File Explorer
- 24.** Which of the following refers to the row of icons of currently running apps at the bottom of the display screen in macOS?
- a.** Taskbar
  - b.** Menu bar
  - c.** Finder
  - d.** Dock
- 25.** Match the following Linux user commands with their descriptions.
- a.** su
  - b.** iwconfigapt-get
  - c.** cd
  - d.** ls
  - e.** chmod
  - f.** ps
  - g.** rm
  - h.** grep
  - i.** pwd
  - j.** yum
  - k.** chown

**Answer options:**

- 1.** Change file ownership
- 2.** Change folders
- 3.** Change permissions
- 4.** Delete files or folders
- 5.** Install or manage Advanced Packaging Tools
- 6.** List currently running processes
- 7.** Perform text/word searches
- 8.** Print (display) working directory

- 9.** Run commands as a different user (usually root)
- 10.** Show contents of a directory or folder
- 11.** Open-source utility for automatic updates in Linux

# Chapter 7

## Security

**This chapter covers the 10 A+ 220-1102 exam objectives related to security. These objectives may comprise 25 percent of the exam questions:**

- **Core 2 (220-1102): Objective 2.1:** Summarize various security measures and their purposes.
- **Core 2 (220-1102): Objective 2.2:** Compare and contrast wireless security protocols and authentication methods.
- **Core 2 (220-1102): Objective 2.3:** Given a scenario, detect, remove, and prevent malware using appropriate tools and methods.
- **Core 2 (220-1102): Objective 2.4:** Explain common social-engineering attacks, threats, and vulnerabilities.
- **Core 2 (220-1102): Objective 2.5:** Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.
- **Core 2 (220-1102): Objective 2.6:** Given a scenario, configure a workstation to meet best practices for security.
- **Core 2 (220-1102): Objective 2.7:** Explain common methods for securing mobile and embedded devices.
- **Core 2 (220-1102): Objective 2.8:** Given a scenario, use common data destruction and disposal methods.
- **Core 2 (220-1102): Objective 2.9:** Given a scenario, configure appropriate security settings on small office/home

office (SOHO) wireless and wired networks.

- **Core 2 (220-1102): Objective 2.10:** Given a scenario, install and configure browsers and relevant security settings.

The most important asset most companies own is their data. Data has become so important to business success that it is what most thieves seek. Because of the interconnected nature of the Internet, a security breach of a single device or network can lead to data theft, including the theft of client financial data that can greatly affect the lives of millions. Large-scale data breaches have brought large companies to bankruptcy, so data security is among the top concerns of business leadership. In this chapter, you learn about the multifaceted threats to security in the modern computing environment and how to mitigate them through the study of these CompTIA A+ Core 2 objectives. This chapter covers the following topics:

- **Physical security measures:** Physical security practices and their implementation
- **Logical security concepts:** Software-based security measures
- **Wireless security protocols and authentication:** Types of wireless security and authentication
- **Malware removal and prevention:** Methods and protocols for detection and prevention
- **Social engineering threats and vulnerabilities:** The various types of threats
- **Microsoft Windows OS security settings:** The important Microsoft security settings
- **Security best practices to secure a workstation:** Implementation of best practices
- **Mobile device securing:** Implementation methods for securing devices

- **Data destruction and disposal:** Methods and techniques for safely and securely disposing of hardware
- **Security configuration on SOHO networks:** Methods for configuring SOHO security
- **Browser security settings:** Secure settings and practices in browsers

## **“Do I Know This Already?” Quiz**

The “Do I Know This Already?” quiz allows you to assess whether you need to read the entire chapter. [Table 7-1](#) lists both the major headings in this chapter and the “Do I Know This Already?” quiz questions covering the material in those headings so that you can assess your knowledge of these specific areas. The answers to the “Do I Know This Already?” quiz appear in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes and Review Questions.”

**Table 7-1** “Do I Know This Already?” Section-to-Question Mapping

Foundation Topics Section	Questions
Security Measures	1–2
Wireless Security Protocols and Authentication	3
Malware Removal and Prevention	4
Social Engineering Threats and Vulnerabilities	5
Microsoft Windows OS Security Settings	6
Security Best Practices to Secure a Workstation	7
Securing Mobile Devices	8
Data Destruction and Disposal	9
Configuring Security on SOHO Networks	10

**CAUTION**

The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for the purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

- 1.** What kind of security breach is an access control vestibule (formerly mantrap) designed to foil?
  - a.** Biometric
  - b.** Tailgating
  - c.** Sleeping guard
  - d.** Shoulder surfing
  
- 2.** Say that you have been asked to improve security by adding a system that examines network packets to determine whether they should be forwarded or blocked. What function would you be most likely to add?
  - a.** MAC address filtering
  - b.** MAC address cloning
  - c.** Software firewall
  - d.** Multifactor authentication
  
- 3.** Which of the following is the most secure wireless protocol in use today?
  - a.** WEP

- b.** WEP3
  - c.** TKIP
  - d.** WPA3
- 4.** A user has unwittingly downloaded malware while also downloading a free application on a gaming site. What general term describes the unintentionally downloaded file?
- a.** Worm
  - b.** Trojan
  - c.** Ransomware
  - d.** Botnet
- 5.** Several computers on a network have been commandeered to launch an attack on a server on the Web. Which term best describes this situation?
- a.** Phishing
  - b.** DoS
  - c.** Spoofing
  - d.** DDoS
- 6.** Which setting allows the user the most privileges on a Windows network?
- a.** Modify
  - b.** Read and Execute
  - c.** Ultimate Use
  - d.** Write
- 7.** Which is the best example of a strong password?
- a.** dr0wssap
  - b.** Password9
  - c.** Pa5Sw0Rd5
  - d.** pA55wrds

- 8.** Which of the following is not an example of biometric authentication?
- a. Entering a password and answering a secret question
  - b. Apple FACE ID
  - c. Windows Hello
  - d. Touch ID
- 9.** Which method erases storage media but leaves the device intact?
- a. Data shredding
  - b. Degaussing
  - c. BitLocking
  - d. Incineration
- 10.** To help hide the identity of a wireless router, what should be changed from the default setting?
- a. Private IP address
  - b. MAC address filter
  - c. IP default gateway
  - d. Service set identifier
- 11.** Which of the following are considered password managers?  
(Select two.)
- a. Trusted sources
  - b. File hashing
  - c. Credential Manager
  - d. Keychain

## Foundation Topics

## Security Measures

**220-1102: Objective 2.1:** Summarize various security measures and their purposes.

Two basic categories of security exist: physical and logical. This section provides an in-depth look at both aspects of this vital topic.

## Physical Security

Physical security of IT equipment is a fundamental first factor in a secure network. As mentioned earlier, data is typically the most valuable asset in a company; leaving it in an unlocked area is dangerous in two ways. First, computer equipment is valuable. A thief might want the equipment for its face value, not caring about the valuable data that it contains or the harm its release might do to customers. Second, an unlocked door is an invitation for someone to install sniffing equipment and gain access to company network assets that lie well beyond the physical room left unattended. In the realm of physical security, an IT professional must understand and practice several protective measures.

## Access Control Vestibule

Some secure areas include an **access control vestibule** (formerly known as a mantrap), which is an area with two locking doors. A person might get past the first door by way of tailgating but likely will have difficulty getting past the second door, especially if there is a guard between the two doors. An access control vestibule essentially slows down the entry process, in hopes that any people sneaking in behind others will be thwarted before they gain entry to the secure area. If someone lacks the proper authentication, that person will be stranded in the access control vestibule until authorities arrive.

## Badge Reader

Badge readers are devices that can interpret the data on a certain type of ID. Although photo IDs are still best assessed by humans, other types of IDs add extra security that badge readers can govern.

ID badges and readers can use a variety of physical security methods, including the following:

- **Photos:** If the bearer of the card doesn't look like the person on the card, the bearer might be using someone else's card and should be detained.
- **Barcodes and magnetic strips:** The codes embedded on these cards carry a range of information about the bearers and can limit individuals' access to only authorized areas of buildings. These cards can be read quickly by a barcode scanner or swipe device.
- **RFID technology:** As with barcoded badges, cards with radio-frequency identification (RFID) chips can be used to open only doors that are matched to the RFID chip. They can also track movement within a building and provide other access data required by a security officer.

To prevent undetected tampering, ID badges should be coated with a tamper-evident outer layer.

## Video Surveillance

Cameras are ubiquitous, thanks to the explosive growth of the Internet of Things (IoT). They are affordable and can easily store recordings for security and historical reference. Video surveillance of secure areas is essential.

## **Alarm Systems**

Alarms are common in many areas of security, from failed drive alarms in computers to hacking attempts in firewalls. Less sophisticated but just as essential are physical alarms that alert security personnel when doors are open or cables are moved.

## **Motion Sensors**

When used with video and alarm systems, motion sensors can provide good physical security. Motion detectors can activate alarms and time-stamp events for tracking on video recordings.

## **Guards**

A determined and skillful thief can foil even the best security plans. The best way to deter a thief is to use a mix of technical barriers and human interaction. Guards can be deployed in different ways. When employees enter the work area in the presence of a guard, best practices most likely will be followed and everyone will scan in and be authenticated. Without a guard, people might hold the door open for others whom they recognize but who say they misplaced their IDs. Knowing that someone is watching carefully keeps honest people honest and deters dishonest people.

Another way to deploy guards is to have them watch several areas via security cameras that record access into and out of the buildings. Although this method is not as effective as posting a guard at each door, it allows fewer security guards to scan different areas for traffic behaviors that warrant further attention.

## **Door Locks**

Of course, the easiest way to secure an area is to lock doors. This seems like an obvious statement, but it is surprisingly common for people to simply wander into unauthorized areas. Some

organizations have written policies explaining how, when, and where to lock doors. Beyond the main entrances, you should also always lock server rooms, wiring closets, labs, and other technical rooms when they are not in use. Physical door locks might seem like a simple solution, but they can't be taken over by hackers.

## Equipment Locks

Most desktops, laptops, and other mobile devices such as projectors and docking stations feature a security slot. On a laptop, the slot is typically located near a rear corner (see [Figure 7-1](#)).



1. Security slot

**Figure 7-1** A Security Slot on a Laptop

This slot is used with a laptop cable lock, such as the one shown in [Figure 7-2](#). Laptop locks use a combination or keyed lock and are designed to lock a laptop (or other secured device) to a fixed location, such as a table. Keep in mind that many types of equipment locks can be used for lockers or even server rack systems.



**Figure 7-2** A Combination Laptop Security Lock

## Bollards

**Bollards** are short wood, metal, or concrete posts installed in sidewalks and driveways to allow pedestrian and bike traffic to pass while keeping larger vehicles away. They are often removable with key access, to allow maintenance vehicles and other necessary traffic to get close to buildings. Bollards are a passive way of keeping vehicles that could be listening for signals away from sensitive data centers. People coming and going from buildings also are easier to keep track of with video cameras.

## Fences

Of course, the most fundamental security device is a fence. Fences are usually subject to building codes, so effective design is important. They should be as tall as possible, sturdy, and monitored.

## Physical Security for Staff

This section highlights security methods and practices that allow access to those who need it and help keep out people (and their software) who try to compromise an organization's secure areas.

### Key Fobs

Key fobs can be used with a variety of security devices. Key fobs can contain RFID chips, and many are used as part of a two-step authentication process that works as follows:

- The user carries a key fob that generates a code every 30 to 60 seconds. Every time the code changes on the fob, it is also matched in the authentication server. In some cases, the user must also log into the fob to see the access code, for an extra layer of security.
- The user then logs into the system or restricted area, using the randomly generated access code displayed on the key fob's LCD display. The authentication server matches the current code and allows access.

A key fob used in this way is often referred to as a *hardware token*.

### Smart Card

A **smart card** is a credit card-sized card that contains stored information and possibly also a simple microprocessor or an RFID chip. Smart cards can be used to store identification information for use in security applications and to store values for use in prepaid

telephone or debit card services, hotel guest room access, and other functions. Smart cards are available in contact and contactless form factors.

Contactless cards are also known as *proximity cards*. Readers for these cards are usually wall mounted so that users can scan their cards within 6 inches of a reader.

A smart card–based security system includes smart cards, card readers that are designed to work with smart cards, and a back-end system that contains a database that stores a list of approved smart cards for each secured location. Smart card–based security systems can also secure individual personal computers.

To further enhance security, smart card security systems can be multifactor, requiring the user to input a PIN or security password and then provide the smart card at secured checkpoints, such as the entrance to a computer room.

## Keys

Keeping track of keys is essential. If keys are entrusted to a careless person or, worse, a dishonest employee, the entire security plan can fail. Document who has keys to server rooms and wiring closets, and periodically change the locks and keys. Cipher locks that use punch codes also enhance security. Using a combination of these methods provides greater protection.

## Biometrics

**Biometric security** refers to the use of a person's biological information, gathered from scans. The following main types are currently in use:

- **Retina (iris) scanning:** This highly accurate technology is nearly impossible to foil, but it requires specialized equipment and can be expensive.

- **Fingerprint scanning:** As with iris scanning, fingerprint scanning is highly accurate, but this type of biometric scan is much more affordable to implement. The scan gathers data on fingerprints and compares their features to data stored for matching. More than one fingerprint can be stored for reference.
- **Palmpoint scanning:** This scan is less accurate than fingerprint scanning because the palm scanner does not analyze the structure of the fingerprints; it merely gathers data on the size of the hand.

Facial recognition is not listed in the A+ objectives, but it might become more common as technology improves, cost drops, and hygienic practices become more widespread since the arrival of COVID-19. Facial recognition involves storing photographs, however, and privacy issues are arising as a result.

## Lighting

Maintaining well-lit areas is important, for many obvious and not-so-obvious reasons. With the advent of LED lighting, good lighting is no longer the cost and energy concern it used to be. Well-lit areas can provide safety for workers, enhanced readability of tiny labels when working with racks of equipment, and enhanced quality for video cameras and other security measures.

## Magnetometers

The term **magnetometer** is simply another name for a metal detector, common to all airports and many public areas. Highly sensitive areas generally have restrictions on weapons; a magnetometer can identify concealed weapons, to enforce the rules and reduce the likelihood of a violent incident.

## Privacy Screen

Privacy issues are important to any company that handles confidential data. When that data is being used on a workstation screen or mobile device, it needs to be protected from unintentional viewing. Data on a computer screen can be easily protected by installing a privacy screen, which is a transparent cover for a PC monitor or laptop display. It reduces the cone of vision, usually to about 30 degrees, so that only the person directly in front of the screen can see the content. Many of these screens are also antiglare, to reduce the user's eye strain.

## Logical Security Concepts

A computer is a combination of physical and logical systems, and security practices must address both of these sides of computing. The physical components of security addressed in the previous section are only part of a good security plan and will be ineffective if the security policies stop there. Addressing software (logical) security practices is essential as well.

## Principle of Least Privilege

Applying the **principle of least privilege** means giving users access to only what they require to do their jobs. Most users in a business environment do not need administrative access to computers and should be restricted from functions that can compromise security.

The principle of least privilege appears to be basic common sense, but it should not be taken lightly. When user accounts are created locally on a computer—especially on a domain—great care should be taken in assigning users to groups. Additionally, many programs ask during installation who can use and make modifications to the program; often the default is “all users.” Some technicians just accept the defaults when hastily installing programs, without

realizing that they are giving users full control of the program. It is an important practice to give clients all they need, but to limit their access to only what they need.

## Access Control Lists

**Access control lists (ACLs)** are lists of permissions or restriction rules for access to an object, such as a file or folder. ACLs control which users or groups can perform specific operations on specified files or folders.

## Multifactor Authentication

A **multifactor authentication (MFA)** system uses two or more authentication methods and is far more secure than single-factor authentication. For example, consider a person gaining access to a system by using a digital code from a fob and then typing a username and password. The combination of the password and the digital token makes it very difficult for imposters to gain access to a system. Multifactor authentication is more secure than earlier versions of software tokens, which could be stolen.

Factors of authentication are often broken down into something a user is (biometrics), something a user has (a token or access card), something a user knows (a personal identification number [PIN]), and where the user is located (geolocation). For example, automated teller machines (ATMs) use a common example of a multifactor authentication system, requiring both a “something you have” physical key (your ATM card) and a “something you know” PIN.

## Email

Email is the most common way to attack an organization because its employees might fall for phishing attacks (described in the section, “Social Engineering Threats and Vulnerabilities”). Filtering can

automatically organize email into folders, but from a security standpoint, its most important function is to block spam and potentially dangerous messages.

Email filtering can be performed at the point of entry to a network with a specialized email filtering server or appliance, as well as by enabling the spam- and threat-detection features that are built into email clients or security software.

Users can discard or quarantine spam or suspicious emails, as well as retrieve false positives that are actually legitimate messages from the spam folder and place them back into the normal inbox.

Email protocols should be secured to ensure that email is encrypted. For example, by default, POP and IMAP email protocols are not secure. Using secure protocols such as POP3S (port 995) or IMAPS (port 993) allows the incoming data from the client to be encrypted because they use an SSL/TLS session.

## Hard Tokens

A **hard token** is any physical device that a user must carry to gain access to a specific system. Examples are smart cards, RFID cards, USB tokens, and key fobs. (Key fob hardware tokens are explained earlier in this section.)

## Soft Tokens

As with key fobs, mentioned in the previous section on physical security, *software tokens* (or **soft tokens**) are part of a multifactor authentication process. The difference is that software tokens exist in software and are commonly stored on devices. For example, logging into a secure system might require sending a soft token via SMS message to a smartphone for code authentication. Both hard tokens and soft tokens can be used in multifactor authentication, as described earlier in this section.

## **Short Message Service**

Short Message Service (SMS) is the standard format of text messaging between devices. Products might have their own message formats (for example, Apple uses iMessage on its devices), but SMS is a standard. SMS is usually used for multifactor soft tokens, described earlier.

## **Voice Call**

Soft tokens can be authenticated with a voice callback. When a user logs in to a site, they might have to authenticate with a voice call and pressing a key provided by the service app on the phone. This is similar to the SMS login just described.

## **Authentication Application**

Multifactor authentication services provide apps that are downloadable to phones and other devices. This is an easy way to provide second-factor authentications after login. When logging into a restricted site, the service pushes a token to the user's registered device. Simply touching a confirmation button suffices for a fast and secure login.

## **Mobile Device Management**

Organizations that have many mobile devices need to administer them so that all devices and users comply with the security practices and policies in place. This is usually done with a suite of software known as **mobile device management (MDM)**. The MDM marketplace is quite competitive, and several solutions are available from companies such as VMware (AirWatch), Citrix (XenMobile), and SOTI MobiControl. These products push updates and allow an administrator to configure many mobile devices from a central location. Good MDM software secures, monitors, manages, and supports multiple different mobile devices across the enterprise.

# Active Directory

**Active Directory** is a Microsoft solution for managing users, computers, and information access in a network. It is based on a database of all resources and users that will be managed within the network. The information in the database determines what people can see and do within the network. A complete understanding of Active Directory is beyond the scope of this book, but every IT support person should know the basics of what it is and how it works. Here are the basics:



- **Login script:** When a user logs onto the network, Active Directory knows who that user is and runs a login script to make the assigned resources available. Examples of login tasks include virus updates, drive mappings, and printer assignments.
- **Domain:** The domain is a computer network or group of computer networks under one administration. Users log into the Active Directory domain to access network resources within the domain.
- **Group Policy:** This is a set of rules and instructions defining what a user or group of users can or cannot do when logged into the domain. A Group Policy Object (GPO) is a set of instructions assigned to a group of users or to certain machines on the network.
- **Organizational Unit (OU):** OUs are logical groups that help organize users and computers so that GPOs can be assigned to them. For example, a team of accountants might be assigned to an OU, and their GPO might give them special access to financial records.
- **Home folder:** This folder, which is accessible to the network administrator, is where the user's data and files are kept locally.

- **Folder redirection:** This allows for the work done by an OU to be saved on a common folder in the domain, as directed by the administrator instead of the user. For example, a policy might dictate that all work be kept in a common folder so that all members of a team can see the latest work and updates.
- **Security Groups:** These provide an efficient way to assign user rights and permissions to approved users who are accessing resources on the network. Group Policy (earlier in the list) can be used to assign rights to security groups. Permissions can be assigned to a security group for shared resources at specific levels of access.

## Wireless Security Protocols and Authentication



**Objective 2.2:** Compare and contrast wireless security protocols and authentication methods.

Wireless security has evolved over the past few years to adapt to the increasingly available tools that can hack into a wireless network. An administrator cannot safely install a wireless network using the default settings. The following sections describe the security options available on a wireless network.

### Protocols and Encryption

An encrypted wireless network relies on the exchange of a passphrase between the client and the wireless access point (WAP) or router before the client can connect to the network. Several standards for encryption have been used, as encryption methods have improved to keep ahead of hackers. Current protocols are known as Wired Equivalent Privacy (WEP). The first WEP version used the **Temporal Key Integrity Protocol (TKIP)**, which is now considered obsolete. Current versions are described as follows:

- **Wi-Fi Protected Access 2 (WPA2)** was released in 2004 and uses **Advanced Encryption Standard (AES)** encryption. WPA2's AES encryption is much stronger than the previous version: It uses 128-bit blocks and supports variable key lengths of 128, 192, and 256 bits. It allows up to 63 alphanumeric characters (including punctuation marks and other characters) or 64 hexadecimal characters. WPA2 also supports the use of a RADIUS **authentication** server in corporate environments.
- **Wi-Fi Protected Access 3 (WPA3)**, which was released in 2018, uses 128-bit encryption (192-bit in an enterprise version) and has a different method for sharing security keys than the other types of encryption. WPA3 is designed to add better privacy and protection against attacks on public Wi-Fi networks.

TKIP and AES encryption are quite different. TKIP is somewhat like WEP in design so that it can operate on legacy hardware that lacks computing power. TKIP is no longer considered sufficiently secure. AES is much more secure and has been adopted by the U.S. government as the encryption standard. Some important points to remember are that two versions of WPA2 exist: WPA2-Personal and WPA2-Enterprise. WPA2-Personal protects unauthorized network access via a password. WPA2-Enterprise verifies network users through a server. WPA2 Personal uses preshared keys. WPA3 also includes both a Personal version and an Enterprise version. WPA3 maintains equivalent cryptographic strength through the required use of 192-bit AES for the Enterprise version and optional 192-bit AES for the Personal version. WPA3 helps prevent offline password attacks by using Simultaneous Authentication of Equals (SAE). This still allows users to choose easier-to-remember passwords and, through forward secrecy, does not compromise traffic that has already been transmitted, even if the password becomes compromised.

# **Authentication**

Four different authentication methods are used for access to a wireless network: single-factor, multifactor, RADIUS, and TACACS+. These methods also apply to wired networks.

## **Single-Factor**

Single-factor authentication is basic username and password access to a computer or network. For years, this was sufficient—and it is still used in many environments. But the rise of online banking and shopping drew more advanced hacking methods, and single-factor authentication is now rare in online commerce.

## **Multifactor**

A multifactor authentication system uses two or more authentication methods and is far more secure than single-factor authentication.

## **RADIUS**

***Remote Authentication Dial-In User Service (RADIUS)*** dates back to the days of dial-up modem access to networks in the early 1990s. It has been widely distributed and is still in use, although it has been updated over the years. A user who wants to access a network or an online service can contact a RADIUS server and enter username and password information when requested. The server authenticates (or declines) the user and advises the network or service to allow the client in (or not).

## **TACACS+**

***Terminal Access Controller Access Control System (TACACS+)***

solved a problem that occurred as network use expanded in the 1980s. The name and acronym seem convoluted, but they describe the function and process pretty well. In early

network computing, when a user logged into a network, each time he or she accessed a different resource or host on that network, the user had to reauthenticate. Dial-up was slow, and logging in was a time-consuming process. With TACACS+, a user who was already authenticated into the network was automatically logged into other resources in the system as well. The network's access control system took care of the user's terminal access.

In its original form, TACACS is quite insecure, but Cisco has updated and re-released it in proprietary form as TACACS+.

## Kerberos

**Kerberos** is an open standard authentication protocol that is used between two clients (or a client and a server) and a third-party Kerberos Key Distribution Center server. The clients acquire a Kerberos key and can mutually authenticate across an unsecure network or the Internet.

Microsoft's version of Kerberos is the default method for Windows authentication for joining domains. Versions are also available on macOS, Linux, and other operating systems.

## Malware Removal and Prevention



**Objective 2.3:** Given a scenario, detect, remove, and prevent malware using appropriate tools and methods.

Wireless security has evolved over the past few years to adapt to the increasingly available tools that can be used to hack into a wireless network. An administrator cannot safely install a wired or wireless network using the default settings. The following sections describe some security threats and options available to mitigate those threats.



## Malware

Malicious software, or **malware**, is software designed to infiltrate a computer system and possibly damage it without the user's knowledge or consent. *Malware* is a broad term used by computer professionals to include viruses, worms, Trojan horses, spyware, rootkits, keyloggers, adware, and other types of undesirable software. The following sections describe some types of malware in more detail.

## Trojan

**Trojan** malware, also known as a Trojan horse, is a malware program disguised as a "gift"—usually popular videos or website links—that trick the user into downloading a virus that might be used to trap keystrokes or transmit sensitive information. Trojans are aptly named for the famous story of the wooden Trojan horse, an apparent gift that hid invading soldiers and allowed them to sneak inside the city gates of Troy.

## Rootkit

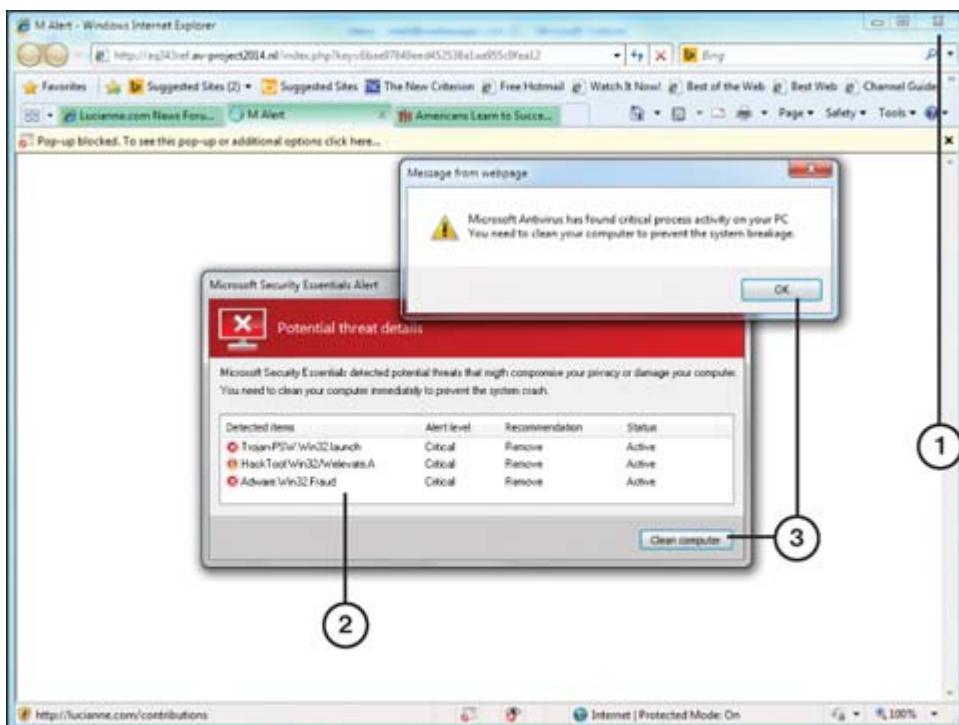
A **rootkit** is a set of hacking tools that makes its way deep into the computer's operating system or applications and sets up shop to take over the computer. Some rootkits do keylogging, some listen for banking information, and more complex ones completely take over a computer. A rootkit is a complex type of malware that is difficult to detect and remove with standard malware antivirus software. Sometimes wiping the drive and reinstalling the operating system is the only certain solution.

## **Virus**

Just as biological viruses can infect humans and cause all sorts of different illnesses, computer viruses can infect and damage computers. **Virus** is a generic term for any malicious software that can spread to other computers and cause trouble. Some viruses are more malicious than others, but all need to be guarded against with antivirus updates. Most virus attacks are spread with human assistance when users fall prey to phishing and carelessly open attachments. (Phishing is discussed in the section “Social Engineering Threats and Vulnerabilities,” later in the chapter.)

## **Spyware**

**Spyware** is software that spies on system activities and transmits details of web searches or other activities to remote computers. Getting multiple unwanted pop-up windows when browsing the Internet is a good indicator of spyware. Some pop-up windows show fake security alerts (as in [Figure 7-3](#)), in the hopes that a user will click on something and then either purchase rogue or fake antivirus software or just download more malware. Spyware can cause slow system performance.



1. The only safe place to click is the close browser button.
2. Fictitious threats.
3. Clicking either of these buttons might launch malware or spyware.

**Figure 7-3** A Fake Security Alert That Purports to Come from Microsoft

## Ransomware

**Ransomware** uses malware to encrypt the targeted computer's files. The ransom demand might be presented after you call a bogus technical support number displayed by a fake error message from the ransomware, or the ransom demand might be displayed onscreen. The ransom must be paid within a specified amount of time, or the files will not be decrypted.

A famous recent example of ransomware is the WannaCry virus, which spread throughout the world in 2017. It impacted Windows machines that had not been updated with security patches that would have prevented the spread of the attack.

An even larger attack is technically known as UNC2452 but more commonly known by how it was spread: through huge networks piggybacking on Solar Winds networking software. This virus is so exceptionally complicated that is thought to be the work of an unknown government.

## Keylogger

**Keylogger** viruses are especially dangerous because they track keystrokes and can capture usernames and passwords of unwitting users. A keylogger can be delivered via a Trojan horse, phishing, or a fake email attachment that the user opens. One way to foil these attacks is to require multifactor authentication because the second authentication factor changes, rendering the stolen password invalid.

## Boot Sector Virus

A **boot sector virus** is similar to a rootkit virus, in that it is embedded deep into the computer. In this case, the virus embeds itself into the initial code of the boot sector on a hard drive. Once there, it can be loaded into system memory on startup and initialize the hidden virus in other drives on the network. Current versions of BIOS and UEFI have built-in protection against boot sector viruses, and these viruses are less common than in decades past.

## Cryptominers

**Cryptominers** are viruses that take over the resources of an infected computer to mine cryptocurrency, usually bitcoin. This practice is also known as cryptojacking. Bitcoin mining is largely legal in most countries, but it is expensive in terms of power use and computer resources. Thus, miners sometimes try to force someone else to pay the costs of mining while they reap the benefit of earning cryptocurrency. Viruses can be delivered in Trojan horses, during phishing, and in browser-based attacks in which malicious code is put into a web page and runs when the browser visits the page.

Slow performance, high CPU usage, and higher network traffic are symptoms that a crypto virus might be onboard.

## Tools and Methods

The antivirus/anti-malware industry has worked hard to keep pace with the menace of hackers and ever-more-sophisticated viruses. The following sections discuss some of the tools and methods that are used to thwart hackers.

### Antivirus/Anti-malware

Protection against viruses and malware is necessary for every type of computing device, from mobile devices to servers. Computer protection suites that include antivirus, anti-malware, anti-adware, and anti-phishing protection are available from many vendors, but some users prefer a “best of breed” approach and choose the best available product in each category.

Antivirus/anti-malware programs can use some or all of the following techniques to protect users and systems:

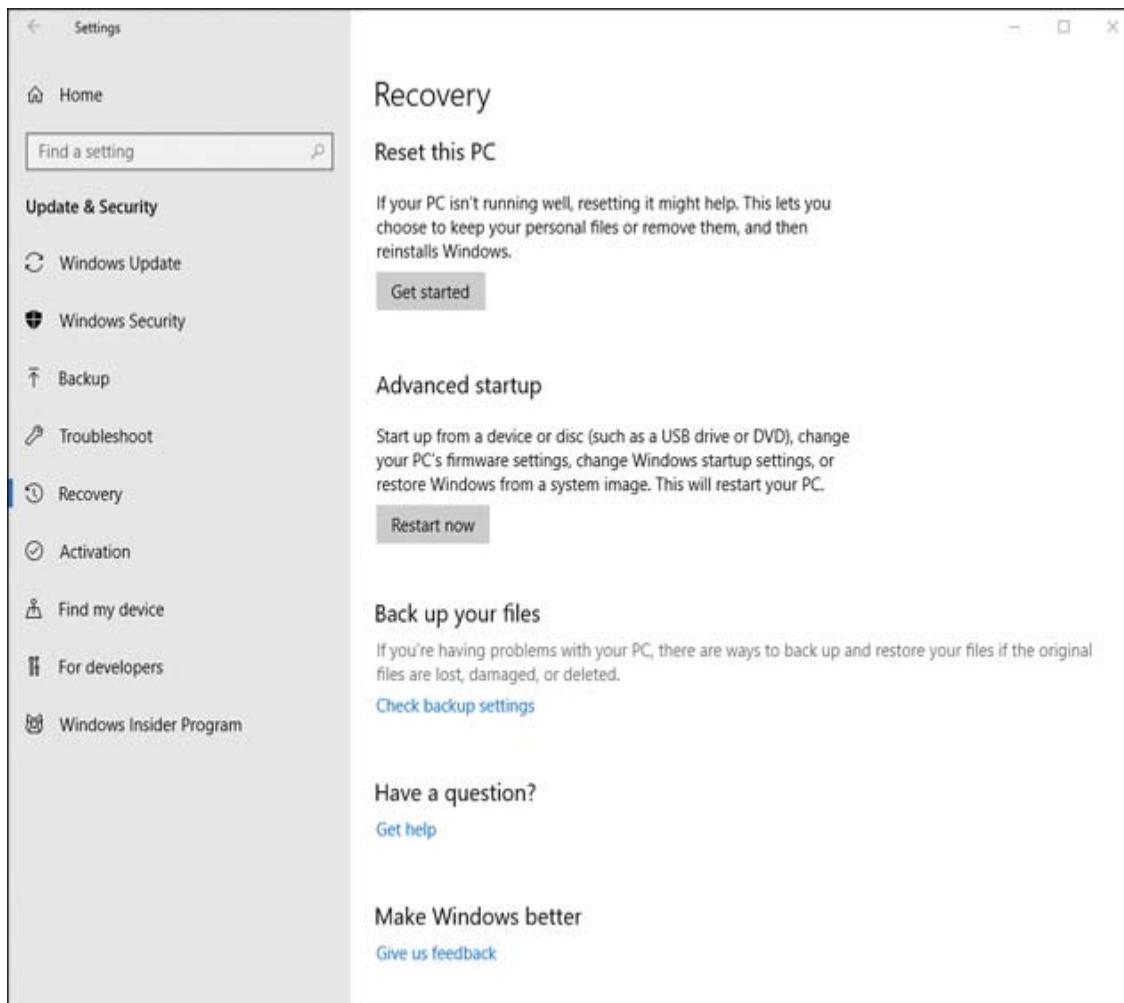


- Real-time protection to block infection
- Periodic scans for known and suspected threats
- Automatic updating on a frequent (usually daily) basis
- Renewable subscriptions to obtain updated threat signatures
- Links to virus and threat encyclopedias
- Inoculation of system files
- Permissions-based access to the Internet
- Scanning of downloaded files and sent/received emails

When attempting to protect against viruses and malware, the most important consideration is to keep your anti-malware application up-to-date. The second most important consideration is to watch out for unknown data, whether it comes via email, USB flash drive, a mobile device, or some other mechanism.

## Recovery Mode

**Recovery Mode** enables you to reset your PC or boot from a recovery disk. If resetting the PC is not sufficient, you can boot from a recovery disk to remove infected files and restore your original files. Access the recovery tools in Windows 10 by going to **Settings > Update & Security > Recovery**. Figure 7-4 shows the recovery tools page in Windows 10.



**Figure 7-4** Windows 10 Recovery Options

## User Education

Regardless of the sophistication of physical or digital security measures, a lack of user education can lead to security issues. Users should be educated in how to do the following:

- Ask for an ID when approached in person by someone claiming to be from the help desk, the phone company, or a service company.
- Ask for a name and a supervisor name when contacted by phone by someone claiming to be from the help desk, the phone company, or a service company.
- Use only official contact information for the help desk, phone company, and authorized service companies, and call the authorized contact person to verify that a service call or phone request for information is legitimate.
- Log into systems first and then give the technician the computer (instead of giving the technician all the login information).
- Change passwords immediately after service calls.
- Report any potential social engineering calls or in-person contacts, even if no information was exchanged. Social engineering experts can gather innocuous-sounding information from several users and create a convincing story to gain access to restricted systems.
- Keep antivirus, antispyware, and anti-malware programs updated.
- Scan systems for viruses, spyware, and malware.
- Understand the major malware types and techniques.

- Scan removable media drives (such as optical discs and USB drives) for viruses and malware.
- Disable Autorun and AutoPlay.
- Configure scanning programs for scheduled operation.
- Respond to notifications that viruses, spyware, or malware have been detected.
- Quarantine suspect files.
- Report suspect files to the help desk.
- Remove malware.
- Disable antivirus software when needed (such as during software installations) and know when to reenable antivirus software.
- Avoid opening attachments from unknown senders.
- Use anti-phishing features in web browsers and email clients.

## **Anti-Phishing Training**

Phishing is a well-known problem that continues to confound network security educators. Phishing requires naive or vulnerable users who are unfamiliar with how easily they can provide a home for malware or a virus. This is usually done by opening email that users do not carefully look at before opening, or giving away information that can help hackers access the network.

Training can involve weekly reports of phishing examples. Some IT departments even internally release “fake” phishing attempts to see if anyone responds and needs more training.

## **OS Reinstallation**

OS reinstallation is often a good solution for an infected computer. It is an involved process, but many viruses are so well hidden that it

can be the best solution.

Before performing the reinstallation:

- Isolate the computer from any network connections.
- Change all passwords that were used during the suspected time of infection, especially banking and work passwords. (There is no point in changing the computer's passwords because they will need to be reset during the installation.)
- Back up data files on an external hard drive. Don't back up the apps; the virus might reside in one of them.

During and after the reinstallation:

- Keep the computer off the network during the process.
- Ask for all updates available.
- Enable the firewall and install any other security software used on the network.
- Scan the external drive that contains the backed-up files, to make sure the virus is not reimposed in one of them.
- Enable automatic updates for the OS and antivirus software.

## Social Engineering Threats and Vulnerabilities



**Objective 2.4:** Explain common social-engineering attacks, threats, and vulnerabilities.

Botnets have made hacking so easy that any network can be tested by hackers thousands of times per day. Updated antivirus/anti-malware software and other software does the heavy lifting in

protecting networks and devices. Another constant threat to a computer network is users being manipulated or tricked into doing hackers' work for them. This hacking technique is known as social engineering. The following sections describe social engineering and other threats and vulnerabilities to networks.

## Social Engineering

Eight common ***social engineering*** techniques that all employees in an organization should know about are phishing, vishing, shoulder surfing, whaling, tailgating, impersonation, dumpster diving, and evil twin. The following sections describe each of these techniques.

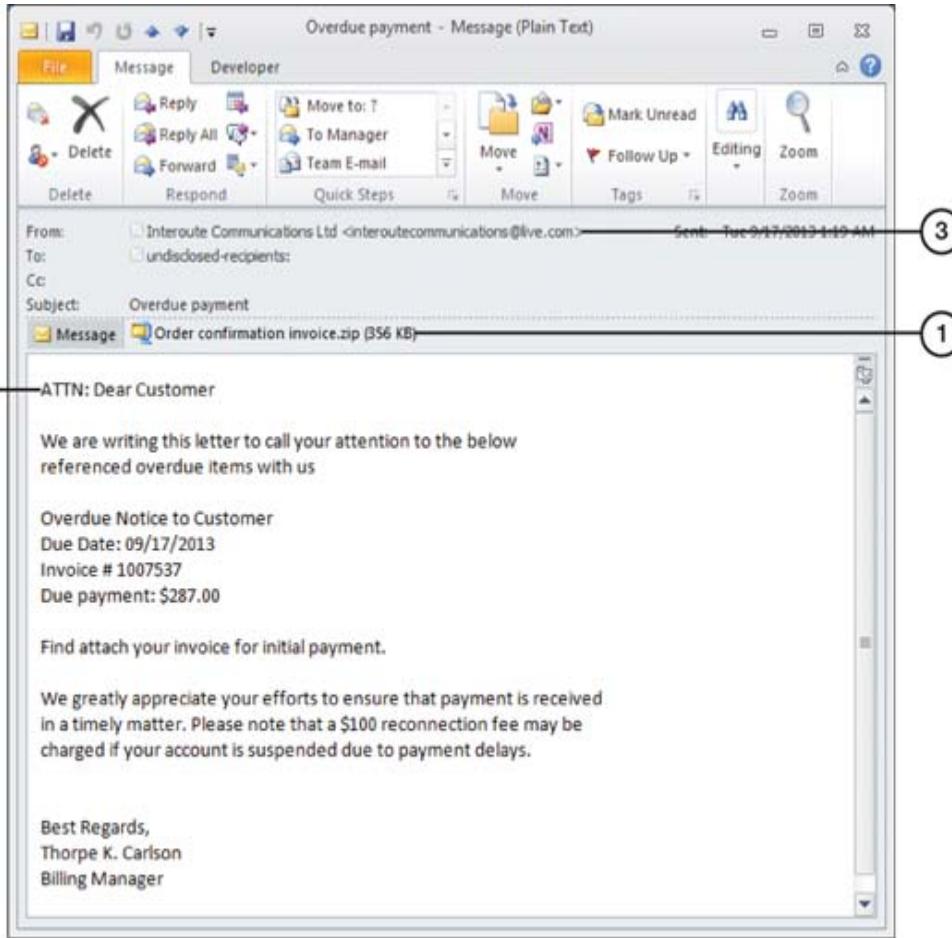
The key to mitigating these social engineering threats is a combination of ensuring employee awareness, implementing policies and protocols for handling sensitive internal information, and, whenever possible, using cybersecurity tools.

## Phishing

***Phishing*** involves creating bogus websites or sending fraudulent emails that trick users into providing personal, bank, or credit card information. A variation, phone phishing, uses an interactive voice response (IVR) system that the user is tricked into calling, to dupe the user into revealing information.

Phishing is a constant threat that administrators can address with awareness warnings that give examples of the latest threats and educate employees on identifying suspicious messages.

[Figure 7-5](#) illustrates a typical phishing email.



1. Zip archive files are frequently used by malware; open the file and your system is infected
2. Genuine emails from a company you work with will be addressed to a person or account number
3. Live.com is typically used by personal email, not company email

**Figure 7-5** A Message That Purports to Address an Overdue Payment but Shows Classic Signs of a Phishing Attack

## Vishing

**Vishing** involves leaving deceptive voice messages that appear to come from an internal source or other authority. These messages request confidential information, such as payroll or tax information. The attacks typically target a specific person, organization, or business. The best protection against vishing is to implement security practices that educate users on how to handle sensitive information within the organization.

## **Whaling**

**Whaling** is a specific type of phishing attack that goes after high-level employees (the big fish, or whale) in an organization, especially the CEO. The attacks tend to be more sophisticated and customized, appearing to come from a high-level executive at another company. Links inside the mail or website infect the computer belonging to leadership, granting access to more sensitive information and possible authorization for fund transfers.

## **Impersonation**

**Impersonation** is a type of social engineering similar to phishing, in which a hacker sends an email pretending to be someone the victim trusts. It can take time and research for the impersonator to figure out how to gain the target's trust. Impersonation, also known as business email compromise (BEC), is not restricted to email, but can happen on the phone or in person. Common sense and strict policies on how to communicate sensitive information can help prevent impersonation attacks.

## **Shoulder Surfing**

**Shoulder surfing** is the attempt to view physical documents on a user's desk or electronic documents displayed on a monitor by looking over the user's shoulder. Shoulder surfers sometimes watch the keyboard to see passwords being entered. They act covertly, looking around corners and using mirrors or binoculars. They might also introduce themselves to users and make conversation, in the hopes that the users will let down their guard.

A common protection against shoulder surfing is using a special privacy screen that limits the viewing range of a display. Employees should be trained to be aware of others who are able to see their screens and to leave screens locked when they are away from their workstations.

## Tailgating

**Tailgating** occurs when an unauthorized person attempts to accompany an authorized person into a secure area by following that person closely and grabbing the door before it shuts. This is usually done without the authorized person's consent; sometimes the authorized person is tricked into believing that the thief is authorized. If the authorized person is knowingly involved, the act is known as piggybacking. Mantraps, mentioned earlier, are designed to thwart tailgating.

## Dumpster Diving

Going through the trash seeking information about a network—or a person with access to the network—is called **dumpster diving**. This type of activity does not have to involve an actual dumpster, of course—just someone searching for any information that will help him or her socially engineer a way into a network. To limit the prospects of a dumpster diver, paper shredders or shredding services should be employed to keep data out of reach.

## Evil Twin

An **evil twin** attack involves setting up a fraudulent wireless access point on a network that imitates the legitimate AP for local users. The evil twin AP sometimes attacks the legitimate AP, so users are fooled into logging onto the evil twin. The twin can then sniff usernames and passwords and listen for other valuable information. Sometimes an evil twin can set up a fake portal that mimics the company site, to collect even more data on anyone who logs on.

## Threats

Any viable plan to protect a network and data must be based on a clear understanding of the threats that all IT networks face. This

section describes common threats and methods that outsiders use to compromise networks.

## DDoS

A **distributed denial of service (DDoS)** attack occurs when several (up to thousands) of computers have been compromised with special malware that turns them into bots. The bots then get directions from their new master to attack a network site with thousands of requests. The traffic is so overwhelming that the site is unreachable by normal traffic and is effectively shut down.

## DoS

A **denial of service (DoS)** attack involves one computer attacking a specific target with an overwhelming number of service requests. This is very similar to a DDoS attack, but without the bots. The messages coming from one source can still take down a network, at great cost to a business.

## Zero-Day

When legitimate software is sold and distributed, it might have unknown security vulnerabilities. When the flaws are discovered, the users put out alerts and the software company creates a patch. Sometimes hackers watch for those alerts and exploit the vulnerabilities before the patch is installed, hence the term **zero-day attack**.

## Spoofing

**Spoofing** is a general term for malware attacks that purport to come from a trustworthy source. Phishing, spear phishing, and rogue antivirus programs are three examples of spoofing.

## On-Path Attack

An **on-path attack** (formerly known as a man-in-the-middle [MiTM] attack) involves an attacker intercepting a connection while fooling the endpoints into thinking that they are communicating directly with each other. Essentially, the attacker becomes an unauthorized and undetected proxy or relay point; the attacker uses this position to capture confidential data or transmit altered information to one or both ends of the original connection.

## Brute Force

A **brute-force attack** involves cracking passwords by calculating and using every possible combination of characters until the correct password is discovered. The longer the password used, and the greater the number of possible characters in a password, the longer brute-forcing takes. One way an administrator can block brute forcing is to set authentication systems to lock after a specified number of incorrect passwords. Longer passwords also aid in the fight against brute-force attacks.

## Dictionary Attacks

**Dictionary attacks** involve attempting to crack passwords by trying all the words in a list, such as a dictionary. A simple list might include commonly used passwords such as 12345678 and password. Dictionary attacks can be blocked by locking systems after a specified number of incorrect passwords. Requiring more sophisticated passwords that do not include identifiable information such as birthdays or family names is also a strategy.

## Insider Threat

Many security procedures are designed to prevent people outside an organization from penetrating a network and making off with valuable data. However, a very real threat comes from insider threat,

in the form of dishonest or unhappy employees or a trusted vendor or contractor who has access to the network or the network infrastructure. Many incidents of corporate or government espionage and intellectual property theft have been performed by insiders with high levels of access. In fact, an insider can do much more harm than an outsider.

Preventing insider threats is difficult, but many of the monitoring and anti-phishing practices also protect against insider fraud.

It is a common corporate practice that when employees with access to the network are terminated or quit, their credentials are immediately rescinded and they have no further access to the buildings or the network.

## **Structured Query Language (SQL) Injection**

Structured Query Language (SQL) is a standard language for communication among databases. This language can be used to attack a database to steal important information such as credit card numbers, social security numbers, and other private data. It can also be used to simply attack a company or government and destroy or heavily damage databases so that they become useless. Database administrators must carefully design their databases to mitigate the threat of dangerous queries. In a **Structured Query Language (SQL) injection** attack, malicious code is inserted into strings that are later passed to a database server.

## **Cross-Site Scripting (XSS)**

**Cross-site scripting (XSS)** is a code-injection technique that uses client-side scripts. It involves tricking a user, often with a link in an email or through some other ruse. When an unsuspecting user clicks on the link, the attacker can inject malicious code into a web-based app. This code is then “trusted” in the user environment, but it can steal information stored in cookies or other valuable information.

The best defense against XSS is to have specific firewall settings on data types entering the systems and encrypting data leaving the system. This way, if information is stolen, the thief cannot read it.

## **Vulnerabilities**

A vulnerability is a weakness in an organization's security plan that can allow the previously mentioned threats to become real problems. Many of the vulnerabilities listed here should sound familiar by now, but they are briefly reviewed in the following sections.

## **Noncompliant Systems**

Noncompliant systems are systems that are tagged by a configuration manager application (for example, Microsoft's Endpoint Configuration Manager) as not having the most up-to-date security patches installed. Systems that do not have the most updated security patches are especially vulnerable to attacks. An example of this is a user attempting to log onto a corporate network with a personal computer that has not been updated to network standards that comply with the corporation's specifications.

## **Unpatched Systems**

Similar to noncompliant systems, an unpatched system will not protect against recently discovered and newly fixed zero-day vulnerabilities. When hackers know about these vulnerabilities, the attacks increase. Unpatched systems will be vulnerable to the attacks. Systems should be patched within one week of the release of a patch.

## **Unprotected Systems**

Similar to an unpatched system, an unprotected system that is missing firewalls and antivirus software (or outdated security

software) is vulnerable to the latest known virus information.

## EOL OSs

End-of-life (EOL) operating systems (OS) are dangerous to keep on a network. When software or hardware reaches EOL status, updates and patches are usually no longer available. Keeping equipment and operating systems up-to-date is part of a strong security plan.

## Bring Your Own Device (BYOD)

Bring your own device (BYOD) use on a restricted network can have some great productivity and cost benefits, but with them come serious risks. Any malware or vulnerabilities on personal devices can become a serious vulnerability when the device is granted access to the corporate network.

Network administrators need to be sure that any device allowed on the network is both updated and compliant with security practices. Many networks that allow BYOD activity require an online security check before they are granted access to the network. Personal device use should be restricted on a secure network.

## Microsoft Windows OS Security Settings



**Objective 2.5:** Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.

Microsoft has made several security settings and tools available in the Windows OS. These settings and tools allow users and administrators to control access to the computer, as well as to files and folders.

## Defender Antivirus

Windows comes with Microsoft **Defender Antivirus**, which is part of the Windows Security suite. To access Windows Security, go to **Start > Windows Security**. From the Security at a Glance window, select Virus & Threat protection. From the Virus & Threat Protection window, you can run a quick scan, select scan options, manage settings, and check for updates. You can even manage ransomware protection.

For real-world application and the A+ exam, ensure that you know how to activate and deactivate real-time protection (under Manage Settings), and understand how to keep your definitions up-to-date by selecting the Check for Updates link. Windows Defender is covered in more detail later in this chapter, in the section “Content Filtering.”

Microsoft offers a great resource for configuring Microsoft Defender Antivirus in Windows:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-antivirus-windows?view=o365-worldwide>

## Firewall

A **firewall** is a physical device or software program that examines data packets on a network to determine whether to either forward them to their destination or block them. A firewall can be a one-way firewall, which protects against inbound threats only, or a two-way firewall, which protects against both unauthorized inbound and outbound traffic. Most third-party firewall programs, such as ZoneAlarm, are two-way firewalls. A **software firewall** can be configured to permit traffic between specified IP addresses and to block traffic to and from the Internet except when permitted on a per-program basis.

A corporate network can use a proxy server with a firewall as the sole direct connection between the Internet and the corporate network and then use a firewall in the proxy server to protect the corporate network against threats.

Physical firewalls are specialized computers whose software is designed to quickly analyze network traffic and make forwarding decisions based on rules set by the administrator. Over time, that task has been incorporated more into software on the computers and into the OS design. An example is Windows Defender Firewall in Windows, which is discussed in the section, “Microsoft Windows OS Security Settings.”

Most current operating systems have some sort of firewall built in:



- As initially configured, the standard firewall in Windows is a one-way firewall. However, it can be configured to work as a two-way firewall. For more information about how it works, see the section “Firewall Settings,” later in this chapter.
- macOS includes an application firewall. In OS X 10.6 and newer, the application firewall offers additional customization options.
- Linux, starting with distros based on kernel 2.4.x and later, includes iptables to configure netfilter, its packet-filtering framework. To learn more, see [www.netfilter.org](http://www.netfilter.org). Many distros and third-party Linux apps are available to help make iptables and netfilter easier to configure.

## Activate/Deactivate

Windows Defender Firewall was covered in detail in Chapter 6, “Operating Systems.” However, we can’t stress enough how important a working knowledge of Windows Defender Firewall is for real-world application and the A+ exam. You should be familiar with

activating and deactivating (turning on and off) Windows Defender Firewall, and you should understand related port and application security settings and procedures.

To turn Windows Defender Firewall on or off in Windows 10, do the following:

- Step 1.** Select **Start > Settings > Update & Security > Windows Security > Firewall & Network Protection.**  
Open Windows Security settings.
- Step 2.** Select a network profile: **Domain network, Private network, or Public network.**
- Step 3.** Under Microsoft Defender Firewall, switch the setting to **On**.
- Step 4.** To turn off Windows Defender Firewall, switch the setting to **Off**. Turning off Microsoft Defender Firewall could make your device (and your network, if you have one) more vulnerable to unauthorized access. If you need to use an app that is being blocked, you can allow it through the firewall instead of turning off the firewall.

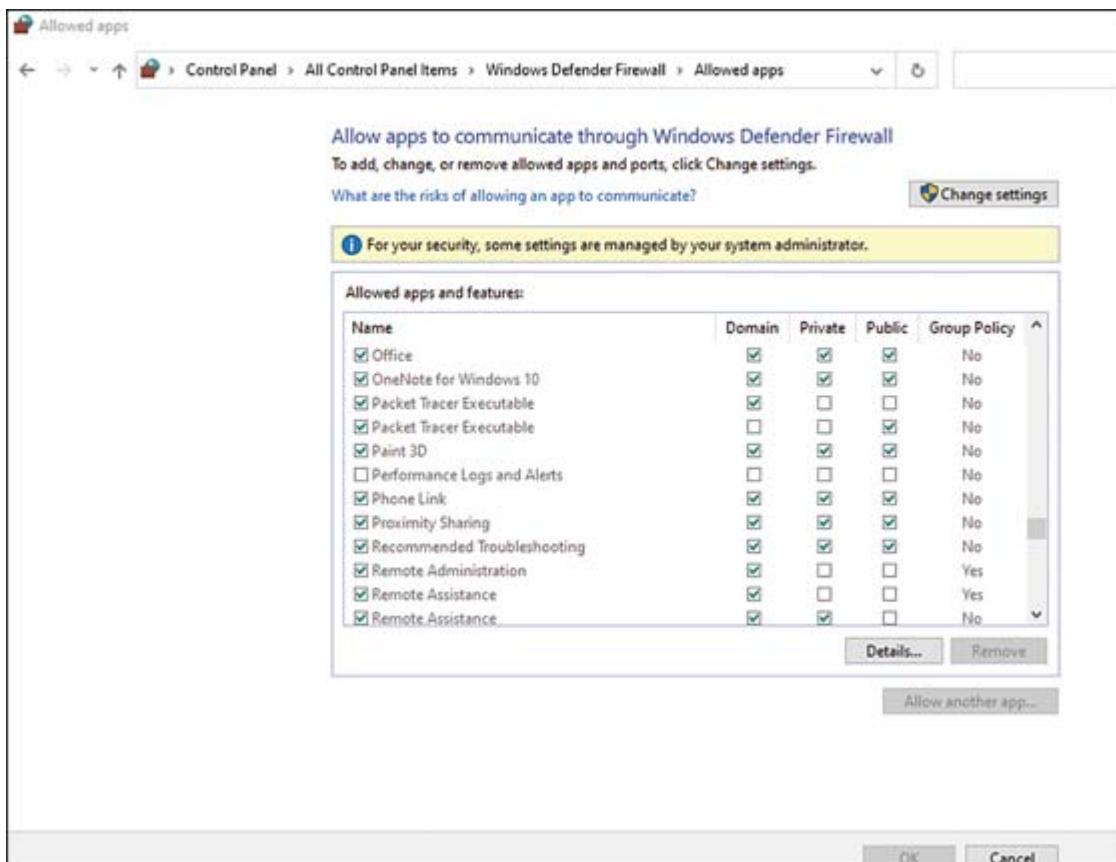
## **Port Security**

Managing port security refers to using a firewall appliance or a software firewall to prevent specified UDP or TCP ports from being used by a service, an application, a specific device, or all devices. Turning off unused ports makes it harder for hackers to find stealthy access into a machine.

## **Application Security**

Many applications are designed to update and communicate with other computers. Authorization for external communication can be managed in Windows Defender Firewall. When opening Windows Defender Firewall, select Allow an App or Feature Through Windows

Defender Firewall, to bring up the window shown in Figure 7-6. Each app and feature can be enabled or disabled from this menu.



**Figure 7-6** Managing Apps in Windows Defender Firewall

Microsoft also offers excellent detailed instructions for configuring Windows Firewall with Advanced Security at

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/windows-firewall-with-advanced-security>

## Access Control

The next sections discuss the purposes and principles of access control through the following:

- Users and groups

- NTFS vs. *share permissions*
- Shared files and folders
- System files and folders
- User authentication
- Run as administrator vs. standard user
- BitLocker
- BitLocker To Go
- Encrypting File System (EFS)

## Users and Groups

Users in Windows can be assigned to different groups, each with different permissions. The Local Policy settings (for local PCs) and Group Policy settings (for networked PCs connected to a domain controller running Active Directory) can restrict PC features by group or by PC. The 220-1102 exam covers some of the differences between the accounts.

## Local vs. Microsoft Accounts

When setting up a computer in Windows 10, you can choose whether to use a local account or a Microsoft account. Each has its own purpose, and you should know the difference.

- **Local account:** A local account is the same as the non-networked accounts that users experienced in previous editions of Windows. Configurable settings include the local username and password, desktop customization, access to Windows features, application installation, and the personalization of the desktop. Missing are the added features of the expansive Windows 10 online environment.

- **Microsoft Account:** Using a Microsoft account establishes an online relationship with Microsoft and allows for easier access to common Microsoft products such as Skype, Outlook, and even gaming features on Xbox. The username and password are not local preference, but rather the account email and associated password. A Microsoft account provides simplified setup and synchronization of additional devices, as well as easy access to the Windows Store. All Microsoft accounts can be combined and centrally managed.

## Standard and Administrator Accounts

Three standard account levels exist in Windows:

- **Standard account:** Standard accounts have permission to perform routine tasks. However, these accounts are blocked from performing tasks that involve systemwide changes, such as installing hardware or software, unless they can provide an administrator password when prompted by User Account Control (UAC).
- **Administrator account:** Users with an administrator account can perform any and all tasks.
- **Guest account:** The guest account level is the most limited. A guest account cannot install software or hardware or run existing applications; likewise, a guest account cannot access files in shared document folders or the Guest profile. The guest account is disabled by default. If it is enabled for a user to gain access to the computer, that access should be temporary, and the account should be disabled again when the user no longer requires access.

### Note

When a user is created using the Users applet in Windows, the user must be assigned a standard or administrator account. Guest accounts are used for visitors.

In Windows versions up to 8.1, the power users account is a specific account type that has more permissions than standard users but fewer than administrators. In those versions, power users have the same rights and permissions as standard users; however, a custom security template can be created if the Power Users group needs specific permissions, such as for the operation of legacy programs.

In Windows 10 and Windows 11, the Power Users group has been discontinued; however, it is available to assign for backward compatibility.

## NTFS vs. Share Permissions

Microsoft introduced the **New Technology File System (NTFS)** as an improved way to store files on disks over the FAT system of Windows 95. The changes in storage systems facilitated implementing file-level security in the form of permissions. Permissions control both local and network access to files and can be set for individual users or groups.

### Allow vs. Deny

Each permission has two settings: Allow and Deny. Generally, if you want a user to have access to a folder, you add that user to the list and select Allow for the appropriate permission. If you don't want to allow a user access, normally you simply do not add the user to a list. In some cases, an administrator must issue an explicit denial if the user is part of a larger group that already has access to a parent folder but needs to be kept out of a particular subfolder.

# Inheritance

The acts of moving and copying folders and files have different results, depending on permissions. For example, when you copy a folder or file to a different volume, the folder or file inherits the permissions of the parent folder it was copied to (the target directory). When you move a folder or file to a different location on the same volume, the folder or file retains its original permissions.

## File and Folder Attributes

File attributes are used in Windows to indicate how files can be treated. They can be used to specify which files should be backed up, which files should be hidden from the normal GUI or command-line file listings, whether a file is compressed or encrypted, and so on, depending on the operating system.

To view file attributes in Windows, right-click a file in File Explorer or Windows Explorer and select Properties. To view file attributes from the Windows command line, use the **Attrib** command.



## Shared Files and Folders

Shared files and folders have their permissions assigned from the Security tab of the object's properties sheet. Folder and file permissions vary by user type or group and can include the following:

- **Full control:** Grant complete access to the contents of the file or folder. When Full Control is selected, all of the following are selected and enabled automatically.
- **Modify:** Change file or folder contents.

- **Read & Execute:** Access file or folder contents and run programs.
- **List Folder Contents:** Display folder contents.
- **Read:** Access a file or folder.
- **Write:** Add a new file or folder.

## Permission Inheritance and Propagation

Permission inheritance and propagation describe how files and folders receive permissions.

If you create a folder, the default action is for the folder to inherit permissions from the parent folder—that is, any permissions that you set in the parent are inherited by any subfolder of the parent. To view an example of this, locate any folder within an NTFS volume (besides the root folder), right-click it, and select Properties; then access the Security tab and click the Advanced button. In Windows 10 or 11, the Advanced Security Settings dialog offers these buttons: Add, Remove, View, and Disable Inheritance.

You can also propagate permission changes to subfolders that are not inheriting from the current folder. To do so, select Replace All Child Object Permissions with Inheritable Permissions from This Object. Remember that folders automatically inherit from the parent unless you turn off inheritance, and you can propagate permission entries to subfolders at any time by selecting the Replace option.

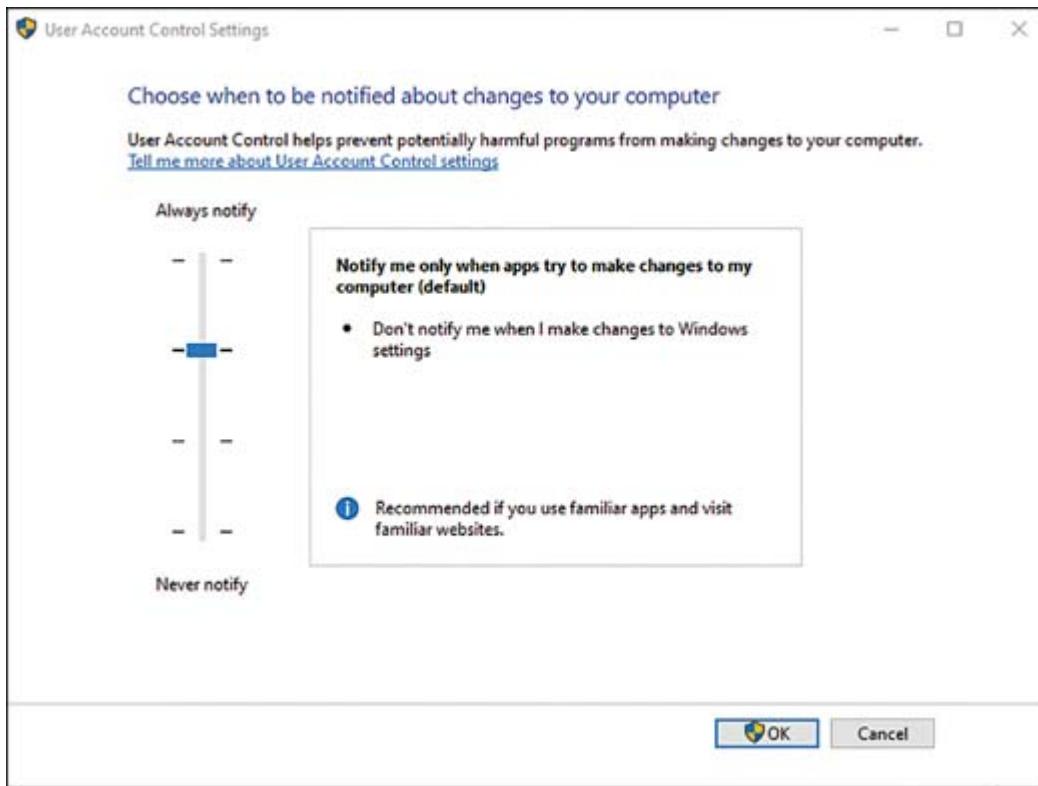
## Run as Administrator vs. Standard User

In Windows 10, press Windows+X and then click or tap Windows PowerShell to run in standard mode. An option to run as an administrator is also available.

## User Account Control

**User Account Control (UAC)** allows the end user to select a level of notifications concerning changes being made to the computer. The purpose of this tool is to prevent unauthorized changes to the computer; the varying levels are designed to allow end users to tailor notifications to their comfort level. UAC can be disabled, but it is better to define some level of notification than to have none at all.

To access the settings for UAC, simply type UAC in the Search area on the taskbar. Select UAC to see the UAC controls in [Figure 7-7](#).



**Figure 7-7** UAC Controls in Windows 10

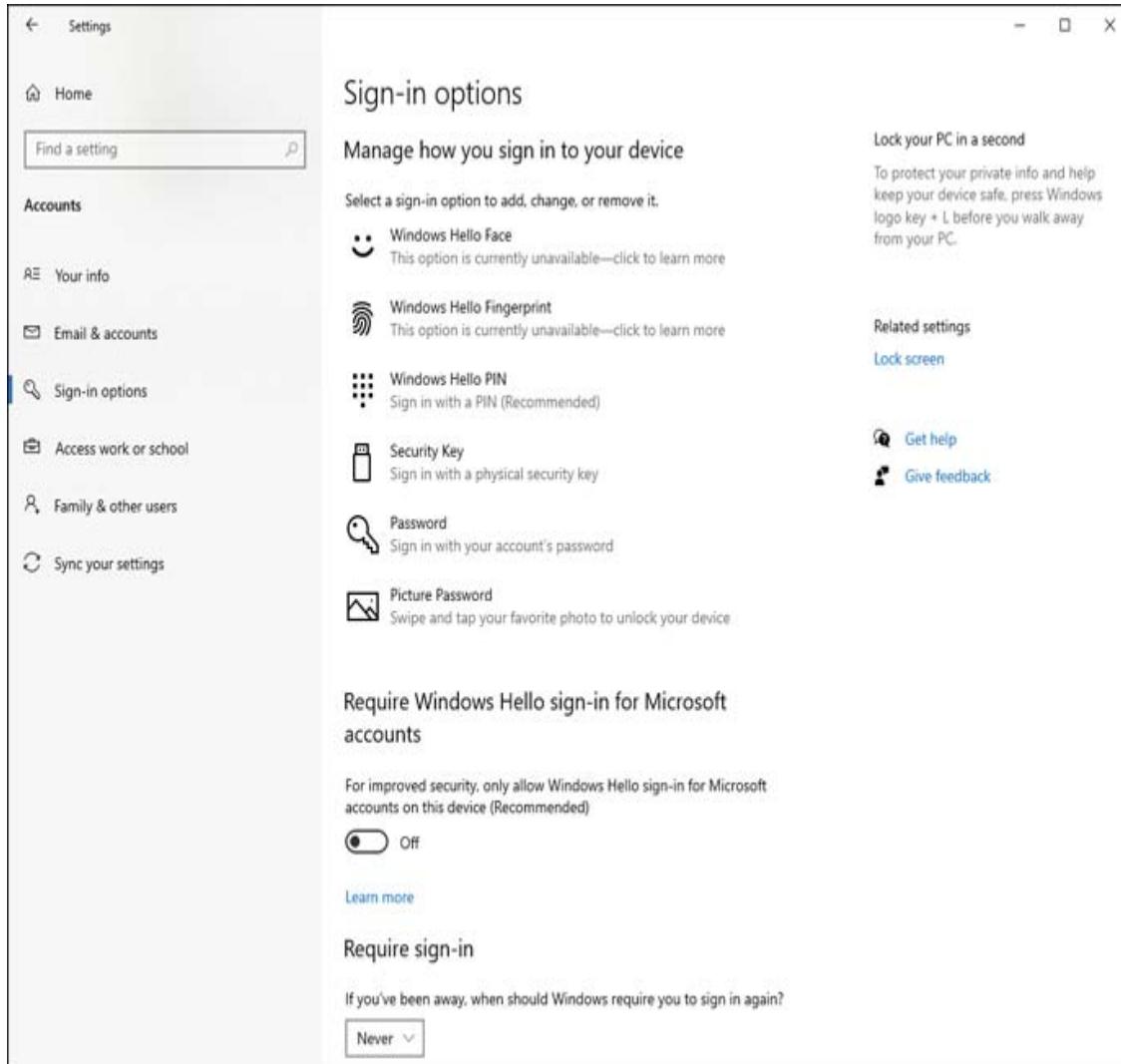
## Login OS Options

Authentication is the process of securely determining that the authorized persons accessing computers or the network are who they say they are. Windows includes a variety of authentication

protocols that can be used on a corporate network, including Kerberos, TLS/SSL, PKU2U, and NTLM.



Apple, Microsoft, and Google use mutual authentication for multiple services (also known as **single sign-on [SSO]**) to enable a single login that provides access to multiple services. For example, a single Microsoft Account login provides access to Outlook email, the Microsoft Store, and OneDrive. To make SSO possible in Windows, client IP addresses are mapped to usernames in Windows Active Directory. Similarly, a single Apple login provides access to iTunes, iCloud, and other services. A single Google login provides access to Gmail, Google Drive, and other services. Other Windows login OS options (besides username and password) include logging in with a PIN, a fingerprint, or even facial recognition. In Windows 10 and 11, you can manage how to sign into your device by going to **Settings > Accounts > Sign-in Options**. Here you can manage options such as facial recognition (Windows Hello), fingerprint recognition (Windows Hello), and Windows Hello PIN, as shown in [Figure 7-8](#).



**Figure 7-8** Windows Sign-in Options

## BitLocker

To encrypt an entire drive, you need some kind of full disk encryption software. Several options are currently available on the market; one option developed for business-oriented versions of Windows by Microsoft is called **BitLocker**. This software can encrypt the entire disk, which, after completed, is transparent to the user. However, BitLocker has some requirements, including the following:

- A Trusted Platform Module (TPM) chip, which is a chip residing on the motherboard that actually stores the encrypted keys.

or

- An external USB key to store the encrypted keys. Using BitLocker without a TPM chip requires changes to Group Policy settings.
- A hard drive with two volumes, preferably created during the installation of Windows. One volume is for the operating system (most likely C:), and it will be encrypted; the other is the active volume, and it remains unencrypted so that the computer can boot. If a second volume needs to be created, the BitLocker Drive Preparation Tool can assist you; you can download it from the Microsoft Download Center.

BitLocker software is based on the Advanced Encryption Standard (AES) and uses a 128-bit encryption key.

Since Windows Vista SP1, it has been possible to use BitLocker to encrypt internal hard disk volumes other than the system drive. For example, if a hard disk is partitioned as C: and D: drives, BitLocker can encrypt both drives.

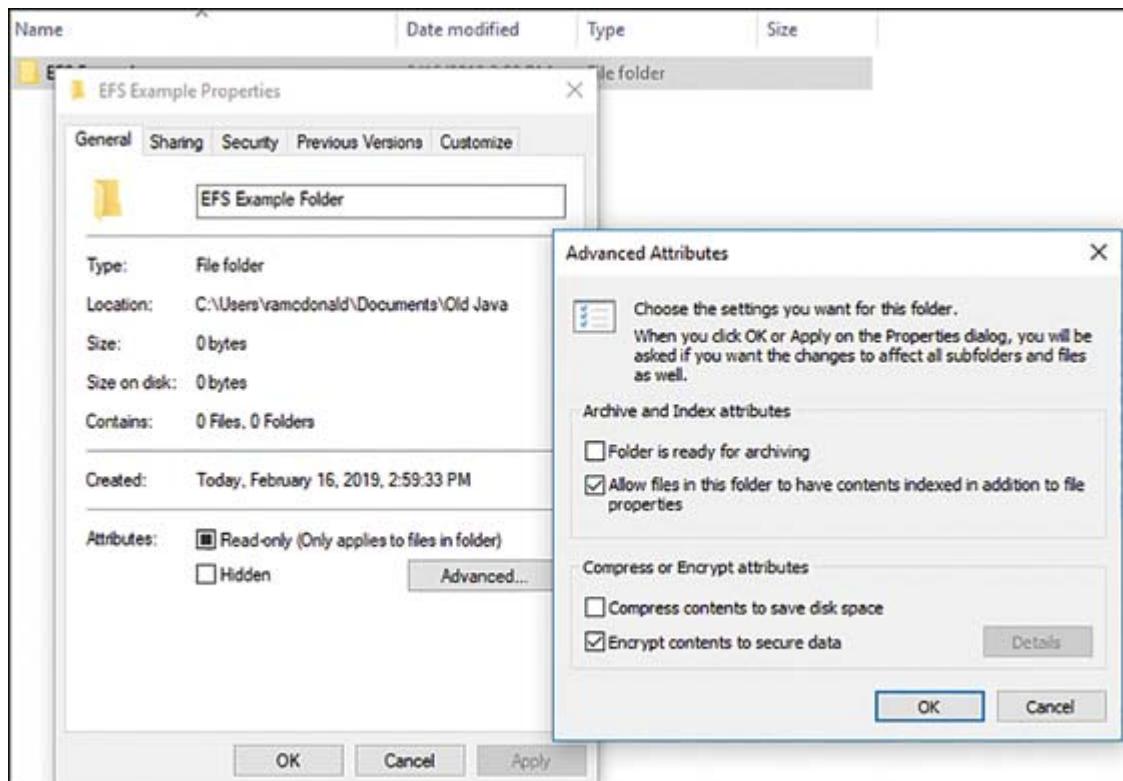
Windows 10 and 11 have several enhancements that make BitLocker more user friendly, but the essentials of BitLocker are the same as in Windows 7.

## BitLocker To Go

To enable **BitLocker To Go** on Windows 10 or 11, go to the **Control Panel > System and Security > BitLocker Drive Encryption**. For external drives, simply right-click the drive to encrypt and select Enable BitLocker to start the encryption process. During the process, you are prompted to specify a password or a smart card for credentials to access the drive's contents.

## EFS

Business-oriented editions of Windows include support for the **Encrypting File System (EFS)**. As Figure 7-9 shows, EFS can be used to protect sensitive data files and temporary files, and can be applied to individual files or folders. (When EFS is applied to folders, all files in an encrypted folder are also encrypted.)



**Figure 7-9** EFS Encryption Steps

EFS files can be opened only by the user who encrypted them, by an administrator, or by EFS keyholders (users who have been provided with the EFS certificate key for another user's account). Thus, the files are protected against access by hackers.

Files encrypted with EFS are listed with green filenames when viewed in Windows Explorer or File Explorer. Only files stored on a drive that uses NTFS can be encrypted.

To encrypt a file in Windows 10 or 11, follow this process:



**Step 1.** Right-click the file in File Explorer and select **Properties**.

**Step 2.** Click the **Advanced** button on the General tab.

**Step 3.** Click the empty **Encrypt Contents to Secure Data** check box. Figure 7-9 shows the steps for EFS encryption.

**Step 4.** Click **OK**.

**Step 5.** Click **Apply**. When prompted, select the option to encrypt either the file and parent folder or only the file, as desired, and click **OK**.

**Step 6.** Click **OK** to close the properties sheet.

To decrypt the file, follow the same procedure, but clear the **Encrypt Contents to Secure Data** check box in Step 3.

## Note

To enable the recovery of EFS encrypted files in the event that Windows cannot start, you should export the user's EFS certificate key. For details, see the Microsoft TechNet article "Create and Verify an Encrypting File System (EFS) Data Recovery Agent (DRA) Certificate," at <https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-and-verify-an-efs-dra-certificate>.

## Security Best Practices to Secure a Workstation



**Objective 2.6:** Given a scenario, configure a workstation to meet best practices for security.

Secure workstations are the foundation of secure networks. If an outside hacker or thief can access a workstation, the whole network can be compromised. The following sections cover the use of passwords, account management, and other methods to make workstations secure.

## Data-at-Rest Encryption

Because a company's most valuable asset is usually its data—whether in the form of customer information, trade secrets, or production information—it only makes sense to do whatever is possible to protect it. When data sits on a workstation, it can be compromised by gaining network access or can be physically stolen. One way to protect against these attacks is to have the data fully encrypted while it sits "at rest" on the workstation hard drive, on a server, or in the cloud. Having data robustly encrypted with RSA or AES methods ensures that, if the drives are compromised, the data will still be inaccessible.

Cloud providers such as Amazon Web Services (AWS), IBM, and Microsoft provide encryption options and services for data being stored on the cloud servers. Considering the potential losses stolen data can bring, stringent encryption practices make good sense.

***Data-at-rest encryption*** should be used on laptops and other systems that might be used outside the more secure corporate network environment. Laptops that contain unencrypted sensitive data have led to many data breaches.



## Password Best Practices

Not all passwords are equally secure; some are very easy to hack. Administrators must use stringent security policy settings and require users to follow strict guidelines for passwords they use to access the

network. The guidelines in the following sections reflect password best practices.

## Setting Strong Passwords

Guidelines for setting strong passwords should include requirements for minimum length and a mixture of alphanumeric and symbol characters. Every extra character in a password makes it much harder to hack. Using a password generator can make the creation of strong passwords easier. For example, the Norton Identity Safe Password Generator (<https://identitysafe.norton.com/password-generator>) offers highly customizable random passwords and can generate multiple passwords at the same time.

## Password Expiration

No matter how strong a password is, it becomes less secure over time. The longer a password is in use, the more susceptible it is to social engineering, brute-forcing, or other attacks. The risk of password discovery by unauthorized users is minimized through a password expiration policy under which passwords expire after a particular length of time and must be reset.

## Screensaver Required Password

To help protect computers from unauthorized use, users can be required to enter their password to return to the desktop after the screensaver appears. Users should also be required to lock their workstations so that a logon is required to return to the desktop.

In Windows, the screensaver required password setting (On Resume, Display Logon Screen check box) is located in the Screen Saver Settings window, which can be accessed from **Settings > Personalization** in Windows 10. In macOS, use the Desktop & Screen Saver menu to choose a screen saver; use Security & Privacy to require a password to unlock the system.

## **BIOS/UEFI Passwords**

BIOS/UEFI passwords prevent unauthorized users from changing settings. Note that they can be removed by resetting the CMOS. Some motherboards feature a jumper block or a push button to reset the CMOS. If this feature is not present, the CMOS can be reset by removing the CMOS battery for several minutes. Chapter 3, “Hardware,” covers the configuration of BIOS/UEFI security settings in more detail.

## **Requiring Passwords**

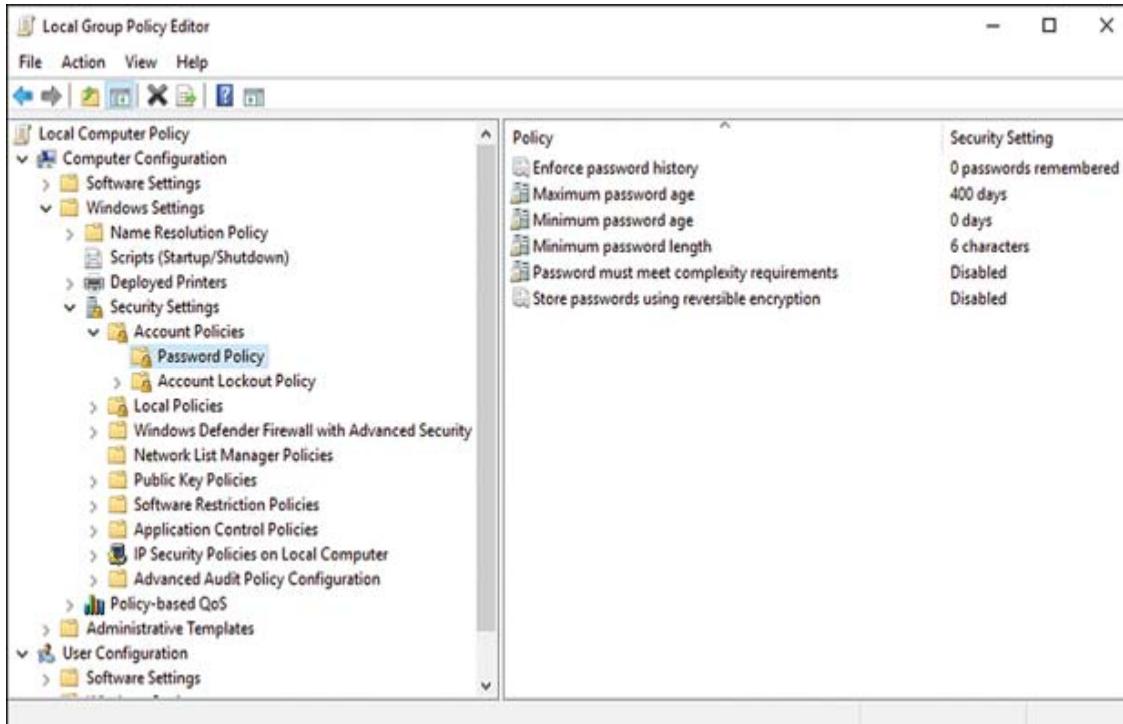
PC users should be trained to use passwords to secure their user accounts. Administrators can require this through the Local Security Policy and Group Policy in Windows. Users should be informed in advance that passwords are about to expire so that users can change passwords early and avoid being locked out at an inconvenient time.

Passwords can be set up to require users to do the following:

- Change passwords periodically, to keep them fresh and secure.
- Enforce a minimum password length, to keep passwords strong.
- Require complex passwords that include a mixture of letters, numbers, and special characters.
- Prevent old passwords from being reused continually by tracking past passwords and not allowing them.
- Wait a certain number of minutes after a specified number of unsuccessful logins has taken place before being able to log in again.

To create a password or adjust password settings in Windows 10, go to **Settings > Accounts > Sign-in Options**. To change or enforce password policy settings, go to the following location by using the Group Policy Management Console: **Computer Configuration >**

**Windows Settings > Security Settings > Account Policies > Password Policy.** Figure 7-10 shows the path to these settings.



**Figure 7-10** Password Policy Settings

## End-User Best Practices

The practices in this section might seem so common sense that they do not warrant mentioning, but lazy practices develop in a workplace and become fertile ground for attacks. End users should have these practices embedded into their work practices.

## Use Screensaver Locks

Automatic screen locking can be configured to take effect after a specified amount of idle time, to help safeguard a system if a user forgets to lock the system manually. Before screen locking can be used, accounts must have the screen lock feature enabled. In Windows 10, go to **Settings > Personalization > Lock Screen**.

In Windows, users can lock their screens manually by pressing Windows+L on the keyboard or by pressing Ctrl+Alt+Del and selecting Lock Computer. In Linux, the keys to use vary by desktop environment. In macOS, use Ctrl+Shift+Eject or Ctrl+Shift+Power (for keyboards without the Eject key).

## **Log Off When Not in Use**

Leaving a computer logged in and unattended is an open invitation to trouble. End users are accountable for activity on their computer when they are away, and logging off is a simple way to protect both the user and the company.

## **Secure/Protect Critical Hardware**

Everyone knows someone who has lost a computer or other mobile device—or, worse, had it stolen. The headaches this can cause are also well known, including financial disaster and job termination. End users should never leave their devices unattended, even for a minute; that time is all it takes for disaster to strike. If end users must part with devices, they must be sure that the devices are securely locked in a trusted area before they leave.

## **Secure Personally Identifiable Information (PII)**

Loss of an access code, a social security number, or any other personally identifiable information (PII) can be as disastrous as losing a device. Identity theft can ruin a person financially and be nearly impossible to completely recover from. Storing PII in encrypted folders is a wise move.



# **Account Management**

When combined with workstation security settings, user account settings help prevent unauthorized access to the network. The account management settings described in the following sections can enhance security.

## **Restricting User Permissions**

User permissions for standard users prevent systemwide changes, but additional restrictions can be set with Group Policy or Local Security Policy.

## **Login Time Restrictions**

To prevent a user account from being used after hours or before the start of business, use login time restrictions to specify when an account can be used.

## **Disabling Guest Account**

The guest account in Windows is a potential security risk, so it should be disabled. If visitors need Internet access, a guest wireless network that does not connect to the business network is a good replacement.

## **Failed Attempts Lockout**

Password policy should specify that a user will be locked out after a specified number of failed attempts to log into an account. A lockout policy can also incorporate a timeout policy that specifies how long the user must wait after an unsuccessful login before attempting to log in again.

## Changing Default Usernames and Passwords

Default administrator usernames and passwords for SOHO routers or other devices or services that have default passwords should be changed. Default usernames and passwords are available in documentation for these devices, so it is easy for an attacker to find the defaults and use them to take over routers or other devices that are still set to the default passwords.

## Disabling Autorun/AutoPlay

Autorun is a feature that enables programs to start automatically when a CD or USB drive or flashcard is connected to a computer. AutoPlay is a similar feature that offers enhanced options in a Windows environment. Both Autorun and AutoPlay allow the user to select what kinds of programs, updates, and syncs can take place. When you disable Autorun, an optical disc or USB drive will not automatically start its autorun application (if it has one), and any embedded malware thus will not have a chance to infect the system before you scan the media. AutoPlay is a similar feature that pops up a menu of apps to use for the media on an optical drive or USB flash drive.

The easiest way to turn off AutoPlay in Windows is to open the AutoPlay applet in **Settings > Devices > AutoPlay** and toggle the button off. [Figure 7-11](#) shows the AutoPlay Settings window in Windows 10. [Figure 7-12](#) shows how to turn off AutoPlay from the Group Policy settings.

The screenshot shows the Windows Settings application interface. On the left, there's a sidebar with a back arrow, the word "Settings", a home icon, and a search bar labeled "Find a setting". Below the search bar is a section titled "Devices" containing icons for "Bluetooth & other devices", "Printers & scanners", "Mouse", "Touchpad", "Typing", "Pen & Windows Ink", "AutoPlay" (which is selected), and "USB". The main content area is titled "AutoPlay". It includes a toggle switch labeled "On" under the heading "Use AutoPlay for all media and devices". Below this are sections for "Choose AutoPlay defaults" which lists "Removable drive" (set to "Choose a default"), "Memory card" (set to "Choose a default"), and "Apple iPhone" (set to "Take no action"). There are also "Related settings" links for "Default app settings" and "Have a question?" with a "Get help" link.

← Settings

Home

Find a setting

Devices

- Bluetooth & other devices
- Printers & scanners
- Mouse
- Touchpad
- Typing
- Pen & Windows Ink
- AutoPlay
- USB

## AutoPlay

Use AutoPlay for all media and devices

On

### Choose AutoPlay defaults

Removable drive

Choose a default

Memory card

Choose a default

Apple iPhone

Take no action

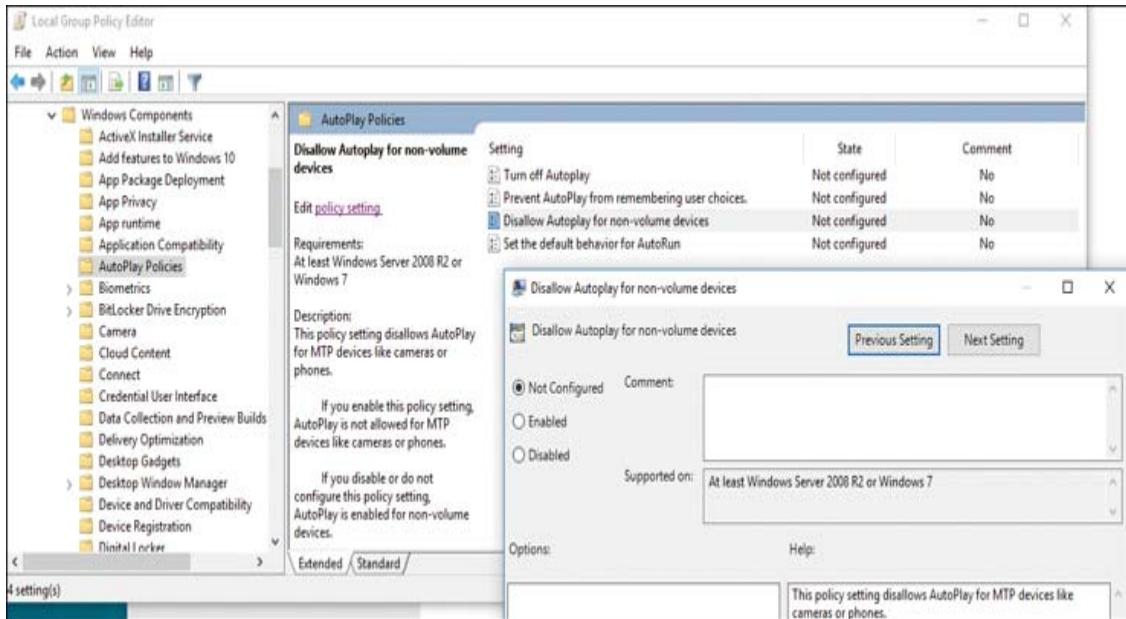
### Related settings

[Default app settings](#)

### Have a question?

[Get help](#)

**Figure 7-11** AutoPlay Settings in Windows



**Figure 7-12** Disabling AutoPlay in the Group Policy Settings

To disable Autorun in Windows by using Local Group Policy, complete the following steps:

**Step 1.** Click **Start** and, in the search field, type **gpedit.msc** to open the Local Group Policy Editor.

**Step 2.** Navigate to **Computer Configuration > Administrative Templates > Windows Components > AutoPlay Policies**.

**Step 3.** Double-click the **Turn Off Autoplay** setting to display the Turn Off Autoplay configuration window.

**Step 4.** Click the **Enabled** radio button and then click **OK** to enable the policy named Turn Off Autoplay.

## Note

Laptops that do presentations might require AutoPlay.

For security reasons, macOS does not support any type of Autorun feature, but it is possible to select apps that you want to run on startup. To edit this list, select **Apple menu > System Preferences > Users and Groups > Login Items**.

In Linux, you can disable Autorun on systems that use the Nautilus file manager by changing the properties on the Media tab to enable Never Prompt or Start Programs on Media Insertion and disable Browse Media When Inserted.

## Securing Mobile Devices



**Objective 2.7:** Explain common methods for securing mobile and embedded devices.

Mobile devices have evolved to the point that they can hold as much valuable data as any workstation. Add to this their compact and easy-to-conceal design and the high cost of the devices, and it becomes clear why mobile devices pose a serious security threat. The following sections cover methods and practices that can mitigate mobile device threats.



### Note

For the 220-1102 exam, be familiar with these concepts:

- Screen locks
- Remote wipes
- Locator applications
- Remote backup applications

- Failed login attempt restrictions
- Antivirus/anti-malware
- Patching/OS updates
- Biometric authentication
- Full device encryption
- Multifactor authentication
- Authenticator applications
- Trusted sources vs. untrusted sources
- Firewalls
- Policies and procedures

## Screen Locks

The first step in securing a mobile device is to set a numeric passcode or another type of screen lock. Such a passcode locks the device, making it inaccessible to everyone except those who know the passcode—and experienced hackers. A screen lock can be a pattern that is drawn on the display, a PIN (passcode lock), or a password. A very strong password is usually the strongest form of screen lock. The screen lock setting can be accessed on an Android device by going to **Settings > Security**. On iPhone 12, go to **Settings > FaceID & Passcode > (enter the current passcode)**. The navigation varies between Android and iPhone versions, but the settings here apply to both types of phones, unless otherwise noted.

You can select how long the phone waits after inactivity to lock; this is usually set to 3 or 5 minutes, but in a confidential environment, it might be appropriate to set this to Immediate. To enable Auto-Lock, go to **Settings > General > Auto-Lock** and select a number of

minutes. If this is set to Never, the device will never sleep, negating the security of the passcode and using valuable battery power. The default setting is 2 minutes. On an iPhone, Auto Lock is available under the Display Settings area.

In addition to the default timeout, devices can be locked by quickly pressing the power button. If this is configured, the passcode must be supplied whenever a mobile device comes out of a sleep or lock state and whenever it is first booted.

Some devices support other types of screen locking, including a fingerprint lock (in which the user's fingerprint is matched against a list of authorized user fingerprints) and a face lock (in which the user's face is matched against a list of authorized user faces).

Windows Hello, a Windows feature supported on some devices, is an example of a face lock. Face ID is the Apple version that is supported on newer versions of iPhone and iPad Pro.

A swipe lock app immediately locks a device when the user swipes the display to one side.

The next option on the Security screen is Visible Passwords. If this option is checked, the device shows the current letter of the password being typed by the user. This type of setting is vulnerable to shoulder surfers (people looking over your shoulder to find out your password) and should be deselected so that only asterisks (\*) are shown when the user types a password.

A Credential Storage option also is available. By default, secure credentials are dropped when a session is finished. (An exception to this rule is a Gmail or other similar login.) However, if Use Secure Credentials is checked and a user accesses a website or an application that requires a secure certificate, the credentials are stored on the device. A user can set a password here so that only he or she can view or clear credentials or install credentials from a memory card. The use of secure credentials is usually configured

only if a user needs access to confidential company information on the Internet.

Passcode locking can be accessed on iPad and iPhone devices by going to **Settings > Passcode** and tapping Passcode Lock to display the Passcode Lock screen. Tap Turn Passcode On to set a passcode.

## Remote Wipes

A lost or missing mobile device is a serious security threat. A hacker can get past passcodes and other screen locks, which means it's just a matter of time before the hacker has access to the data. An organization with confidential information should consider enabling a **remote wipe** of a device. As long as the mobile device still has access to the Internet, the remote wipe program can be initiated from a desktop computer to delete all the contents of the remote mobile device.

Some devices (such as the iPhone) have a setting that causes the device to be erased after a certain number of incorrect password attempts (10, in the case of the iPhone). Third-party apps also are available for download for most mobile devices and can wipe the data after a specified number of attempts. Some apps configure a device to automatically take a picture after three failed attempts and email the picture to the device owner. Examples of software that can accomplish this include Google Sync, Google Apps Device Policy, Apple Data Protection, and third-party apps such as Mobile Defense. In some cases, such as with Apple Data Protection, the command that starts the remote wipe must be issued from an Exchange server or mobile device management (MDM) server. Of course, you should have a backup plan in place as well so that data on the mobile device is backed up to a secure location at regular intervals. This way, if the data needs to be wiped, you know that you can recover most or all of the data. The type of remote wipe program, backup

program, and policies on how these are implemented can vary among organizations.

## **Locator Applications**

By installing or enabling a locator application or service such as Android Device Manager, Lookout for iOS or Android, or Find My iPhone (or Find My App and AirTag), a user can track down a lost device. These apps can be operated from any other phone that has a similar app installed, as long as the power is on and geolocation is working.

## **Remote Backup Applications**

A mobile device is backed up in two ways: using a USB connection to a desktop or laptop computer, or to the cloud by using a remote backup application.

The Apple iCloud offers a free cloud backup service for a limited amount of data (currently, 5GB), with more space available by subscription. iTunes, which can be used for USB-based backup, backs up the entire device to a hard drive at no additional cost.

Android users have free backup for email, contacts, and other information via Google Cloud. However, backing up photos, music, and other content and documents must be performed either manually via USB or with a file sync to the cloud, using a service such as Dropbox or another third-party app.

Both iOS and Android users can use popular third-party, cloud-based backups that are also supported for macOS and Windows, such as Carbonite ([carbonite.com](http://carbonite.com)) and iDrive ([idrive.com](http://idrive.com)).

## Failed Login Attempts Restrictions

Most mobile devices include failed login attempt restrictions. If a person fails to enter the correct passcode after a certain number of attempts, the device locks temporarily and the person must wait a certain amount of time before attempting the passcode again. If the person fails to enter the correct passcode again, on most devices, the timeout increases. As mentioned earlier, multiple failed logins can result in a remote wipe of the hard drive.

## Antivirus/Anti-malware

Just as there is antivirus software for PCs, *antivirus/anti-malware* software exists for mobile devices. These are third-party applications that need to be paid for, downloaded, and installed to the mobile device. Some common examples for Android include McAfee VirusScan Mobile, AVG, Lookout, Dr. Web, and NetQin.

iOS works a bit differently than Android. iOS is a tightly controlled operating system. One benefit of being a closed-source OS is that writing viruses for it can be more difficult, making it somewhat more difficult to compromise. But no OS is truly safe from compromise. For the longest time, no antivirus software existed for iOS, but Apple now allows the download of previously unavailable applications and software that Apple did not authorize.

## Patches and OS Updates

Patches and OS updates help protect mobile devices from the latest vulnerabilities and threats. By default, you are notified automatically about available updates on Android and iOS-based devices. However, you should know where to go to manually update these devices as well:

- For Android, go to **Settings > General > About Device > Software Update** or **Settings > System > About Device**

**> Software Update > Check for Updates.**

- For iOS, go to **Settings > General > Software Update**.

Large organizations that have many mobile devices should use a mobile device management (MDM) suite. McAfee and many other companies have MDM software suites that can take push updates and configure many mobile devices from a central location. Decent-quality MDM software secures, monitors, manages, and supports multiple different mobile devices across the enterprise.

## **Biometric Authentication**

Both current and older Android and iOS devices can use biometric authentication through the use of add-on fingerprint readers or iris readers.

Recent and current iOS devices have built-in support for fingerprint reading with all Touch ID feature-enabled phones and iPad versions.

Face locks, such as Microsoft Windows Hello and Apple Face ID, are also considered a type of biometric authentication.

## **Full-Device Encryption**

With full-device encryption, your data is not accessible to would-be thieves unless they know the passcode. Apple iOS devices feature full-device encryption that is activated when a passcode is assigned to the device. For more about this and other iOS security, Apple provides an iOS Security guide at

<https://support.apple.com/guide/security/welcome/web>.

Android 12 supports both full-disk encryption and file-based encryption. File-based encryption is encryption on individual files, meaning that each file has a separate encryption key so that all the phone resources do not have to be tied up in the encryption process.

## **Firewalls**

Android does not include a firewall, so third-party apps must be used to provide protection against unwanted Internet traffic. Google Play offers many free firewall apps for Android.

Apple does not include a firewall because the design of iOS uses a feature called sandboxing that runs apps in a separate protected space.

## **Policies and Procedures**

Many individually owned mobile devices are now being used on corporate networks. Because these devices were not configured by the corporation, they can potentially present security threats. To prevent threats, organizations need to address these issues in their policies and procedures.

## **BYOD vs. Corporate-Owned Devices**

The following are benefits of bring your own device (BYOD) policies:

- No hardware cost to the organization
- Higher usage because employees are satisfied with their selected device
- Greater productivity

Potential drawbacks include the following:

- Hidden costs of management and security
- Possibility that some employees will not want to buy their own devices

Corporate-owned personally enabled (COPE) is a model in which the company owns the device and sometimes allows the employee to use it for personal use. This model is of great benefit to the

organization because the devices are preapproved and are typically similar in model. They are thus easier to manage and control with mobile device management (MDM) or mobile application management (MAM) policies.

## Profile Security Requirements

Whether an organization uses corporate-owned mobile devices, BYOD, or a mixture, setting and following profile security requirements is important for achieving increased productivity without incurring significant risks. Issues involved include specifying approved devices and operating system versions, requiring passwords and lock screens, requiring device encryption, addressing support issues, and determining when and how to remove company information when an employee leaves the organization.

## Internet of Things

***Internet of Things (IoT)*** devices, such as smart home devices, security cameras, and AI assistants such as Alexa and Google Home, have become so pervasive that they can be found in almost every household and SOHO. These devices might be useful or fun, but they come with risks to your network if precautions are not taken.

IoT devices do not have industry standards for security, so each device opens a different door to a hacker. Because the devices tend to be insecure, the best solution is to secure them when they join the network.

Steps that can make IoT devices safer are similar to other security practices mentioned elsewhere in this chapter:

- Enabling authentication and/or changing default passwords to make them more secure
- Keeping the devices updated to the latest software or firmware

- Isolating them on their own subnet or network, to control access to servers and other devices that hackers might seek out

## Data Destruction and Disposal

220-1102  
Exam

**Objective 2.8:** Given a scenario, use common data destruction and disposal methods.

Even after computers, mobile devices, and even some types of printers have reached the end of their useful lives, the hard drives inside contain potential security risks. Risks also lie in flash drives, external drives, and optical media. To prevent confidential company or client information from being accessed from a computer or another device that is being disposed of for resale, recycling, or deconstruction for parts, follow the methods described in the next sections.

### Note

For the 220-1102 exam, you should understand the importance of these methods:

- Physical destruction methods
- Recycling or repurposing best practices
- Outsourcing concepts

## Physical Destruction Methods

Physical destruction turns a mass storage device into small pieces that cannot be reconstructed, making the data inside unrecoverable. Methods include the following:



- **Shredder:** Some office-grade shredders can destroy optical media. Electronics recyclers use heavy-duty shredders made for hard disks and mass storage devices, to reduce storage devices, tape, or other types of media into small bits.
- **Drill/Hammer:** Remove the hard disks and destroy their platters with a drill, hammer, or other device; then recycle the scrap.
- **Electromagnetic (*degaussing*):** Tools such as electromagnetic degaussers and permanent magnet degaussers can permanently purge information from a disk. The drive is physically intact, but all data, formatting, and control track data is missing. Use this type of physical destruction if you want to use a drive for display purposes.
- **Incineration:** Incineration of tape and other types of magnetic and optical media is allowed in some areas and available from various companies.

Data-recycling companies that destroy hard drives or other storage devices can provide a certificate of destruction to prove compliance with local laws or institutional policies.

## Recycling or Repurposing Best Practices

As long as the data on a hard drive or other mass storage device can be rendered unrecoverable, destroying the media itself is not necessary. The following are some best practices for recycling and repurposing:



- **Low-level format vs. standard format:** The standard format used in operating systems is a quick format. This type of

format clears only the root folder. The rest of the data on the disk can be recovered until it is overwritten. A long format rewrites the disk surface. However, data recovery programs available from many third-party firms can recover data from a formatted drive. A low-level format that creates the physical infrastructure where data will be stored on a disk is performed by the drive manufacturer before the drive is shipped and cannot be performed in the field.

- **Overwrite:** Some disk maintenance programs from mass storage vendors include options to overwrite a hard disk's or SSD's data area with zeros. Data recovery programs can often recover data that has been overwritten in this fashion.
- **Erasing/drive wiping:** To ensure the complete destruction of retrievable data on a storage device, the data must be overwritten with a program that meets or exceeds recognized data-destruction standards, such as the U.S. Department of Defense (DoD) 5220.22-M (which requires seven passes) or Peter Gutman's 35-pass maximum-security method. These programs, referred to as drive wipes, destroy existing data and partition information to prevent data recovery or drive forensic analysis. Use this method when maintaining the storage device as a working device is important for repurposing (such as for donation or resale). A variety of commercial and freeware programs can be used for this task, which is also known as disk scrubbing or disk wiping.

## Outsourcing Concepts

Countless examples of problems and lawsuits have arisen from the improper handling of data and equipment. Equipment that is simply thrown away or recycled often puts valuable company resources in the hands of complete strangers who can do what they want with the data.

Companies should have data destruction policies in place, including paper shredding and hard drives. It is usually economically beneficial to outsource this destruction task to a third-party vendor who has invested in the proper equipment and training of staff. Outsourcing to a qualified company ensures that the methods used are secure and safe and that the data disposal is legal. Most companies do not dispose of enough equipment or data to warrant investing in destruction equipment or specialized staff.

Another advantage of outsourcing to a qualified company is that the company can certify that the destruction is complete and was done correctly and then issue an official ***certificate of destruction/recycling*** to confirm the destruction of the material. This shows business partners and government regulators that care was taken to comply with safety practices and local laws.

## Configuring Security on SOHO Networks



**Objective 2.9:** Given a scenario, configure appropriate security settings on small office/home office (SOHO) wireless and wired networks.

Both wireless and wired small office/home office (SOHO) networks are important to businesses of all sizes, as well as individual users. However, they represent significant vulnerabilities if they are not properly secured. The following sections explain how the different encryption methods work and detail the additional steps that must be taken to completely secure a wireless network.

### Home Router Settings

To be secure and navigate the Internet safely in today's world, specific security settings must be considered when installing and

configuring a home router. The following are some important guidelines for SOHO wireless and wired networks.

## Change Default Passwords

The documentation for almost all WAPs and wireless routers lists the default administrator password. This documentation can be readily downloaded in PDF or HTML form from vendor websites. Because an attacker can use this information to take over the device, it is essential to change the default to a private password. Most routers use the Administration or Management dialog for the password and other security settings.

### TIP

To further secure a router or WAP, configure the device so that it can be managed only with a wired Ethernet connection.

## IP Filtering

Settings that control access to the network by analyzing IP traffic are known as Access Control Lists (ACLs). Basic settings on a SOHO are fairly easy to implement by simply knowing what types of IP protocols and traffic will be allowed. For example, many large networks deny ping traffic by filtering out ICMP protocol traffic on the networks. Traffic can be filtered by traffic type or by IP address. In general terms, **IP filtering** lets you control what Internet Protocol (IP) traffic is allowed into and out of your network.

## Firmware Updates

Most SOHO router vendors issue at least one **firmware update** during the lifespan of each model of WAP and wireless router. Updates can solve operational problems and add features that enhance Wi-Fi interoperability, security, and ease of use. To

determine whether a WAP or wireless router has a firmware update available, follow these steps:



- Step 1.** View the device's configuration dialogs to record the current firmware version. Also note the router's model number and revision from the back or bottom of the device.
- Step 2.** Visit the device vendor's website to see whether a new version of the firmware is available.
- Step 3.** Download the firmware update to a PC that can be connected to the device with an Ethernet cable.
- Step 4.** Connect the PC to the device with an Ethernet cable.
- Step 5.** Navigate to the device's firmware update dialog.
- Step 6.** Follow the instructions to update firmware.

## Content Filtering

The IT department is responsible for compliance to the acceptable use policy of IT infrastructure, as well as making sure that inbound and outbound content is in line with expectations. Shielding the network from errant users who would exploit inappropriate content on the Web or in email is necessary.

**Content filters** on routers help control access to inappropriate websites and can filter by address or other keywords of concern. These filters can be applied to both inbound or outbound traffic and, depending on the router, permit different levels of control for individual users.

## Physical Placement/Secure Locations

In a SOHO network environment, physical security refers to preventing unauthorized use of the network. The same basics of

physical security apply in a SOHO network in a large office environment:



- Secure the network equipment in a locked wiring closet or room.
- Disable any unused wall Ethernet jacks by either disabling their switch ports or unplugging the patch panels in the wiring closet.
- Route network cables out of sight, in the walls and above the ceiling. Having them out of sight cuts down on the chances that someone will tap into the network.
- Lock doors when leaving.
- If possible, dedicate a lockable room as a workspace in a home office, to protect company devices and other resources from the hazards of daily family life, such as children and pets.

## **Dynamic Host Configuration Protocol (DHCP) Reservations**

The DHCP server built into almost all home routers is responsible for giving out IP addresses to all computers on the network that request one. Restricting DHCP is one way to control access to the network.

Most DHCP servers can reserve IP addresses for specific computers and other devices, such as printers, by mapping the device's physical MAC address and matching it to a constant IP address. **Dynamic Host Configuration Protocol (DHCP) reservations** allow the network administrator to manage devices and control IP leases for outside users. These reservations can also be used on IP phones and IoT devices.

Static IP addresses, configured by the network administrator and not DHCP, are still important for network stability. Devices such as switches, printers, and servers should have static addresses so that they are available when a DHCP server is down.

## Static WAN IP

The wide area network on a SOHO is the connection to the Internet Service Provider (ISP). The **static WAN IP address** is provided by the ISP and is applied (usually automatically) to the “Internet” port on the router. The address is “static” because it does not change and does not expire as a leased dynamic address does. This address is on a different network from the local SOHO addresses because it belongs to the ISP’s router.

## Universal Plug and Play

**Universal Plug and Play (UPnP)** was designed to allow devices on a home or SOHO local area network (LAN) to easily connect and cooperate with other devices on the LAN. As a similar example of Plug and Play, consider a printer being plugged into a computer: The Plug and Play capability of the OS finds a device driver and allows the device to interact. UPnP scaled up this idea to a LAN, to allow gaming devices, smart home IoT devices, and virtual assistants to work on a LAN. UPnP does not scale further up to enterprise networks.

This benefit of easy setup of devices comes with security flaws. Especially concerning is the UPnP use of port forwarding and its lack of authentication. If it is exploited from the outside, port forwarding grants access to devices on the LAN; this should not be universally enabled, but it comes enabled by default on many routers. The best approach is to protect the SOHO LAN by disabling port forwarding and taking on the task of manually setting up devices on the SOHO LAN.

## Screened Subnet

A **screened subnet**, formerly known by CompTIA as a demilitarized zone (DMZ), allows outside traffic through to a particular IP address on a LAN. In a SOHO router, any device assigned to the DMZ receives traffic that is not specified for a particular device. Using a DMZ host makes sense for gaming and other types of traffic when you cannot specify in advance the ports needed. However, the DMZ host must have its own firewall because DMZ hosts are not protected by the router firewall.



## Wireless-Specific Security

The default settings for a wireless network should be changed to provide security. The following sections discuss these issues.

### Changing the Service Set Identifier (SSID)

The service set identifier (SSID) can provide a great deal of useful information to a potential hacker of a wireless network. Every wireless network must have an SSID; WAPs and wireless routers typically use the manufacturer's name or the device's model number as the default SSID. If a default SSID is broadcast by a wireless network, a hacker can look up the documentation for a specific router or the most common models of a particular brand and then determine the default IP address range, the default administrator username and password, and other information that makes it easy to attack the network.

To help “hide” the details of your network and location, a replacement SSID for a secure wireless network should not include any of the following:

- Your name

- Your company name
- Your location
- Any other easily identifiable information

An SSID that includes obscure information (such as the name of your first pet) is a suitable replacement.

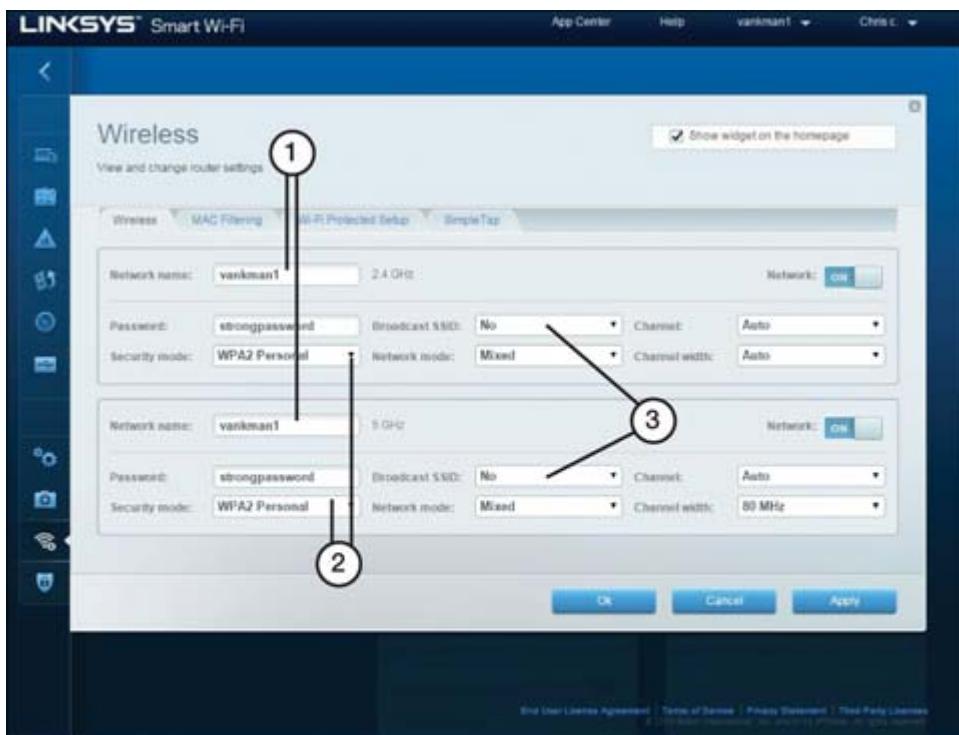
## Encryption Settings

The importance of setting encryption to the latest possible standards is covered earlier in this chapter, in the section “Wireless Security Protocols and Authentication.” The information there applies to SOHO networks as well because a SOHO can be set up as an extension of a business. In such a case, all security policies from the business should apply at the SOHO extension as well.

## Disabling SSID Broadcast

Disabling SSID broadcast is widely believed to be an effective way to prevent a wireless network from being detected, and the A+ certification exam shares that opinion. But this approach is not always enough. Even though disabling SSID broadcast prevents casual bandwidth snoopers from finding your wireless network, Microsoft does not recommend disabling SSID broadcasting as a security measure because serious hackers can use certain methods to discover networks.

[Figure 7-13](#) illustrates a Linksys router configuration dialog in which several of these security recommendations have been implemented.



1. User-assigned SSID in place of factory default
2. WPA2 Personal security mode selected
3. SSID broadcast disabled

**Figure 7-13** Configuring a Router with Alternative SSIDs, WPA2 Encryption Enabled, and SSID Broadcast Disabled

## Disabling Guest Access

The guest account in a wireless network is a potential security risk, so it should be disabled. If visitors need Internet access, a separate guest wireless network that does not connect to the business network is a good replacement.

## Changing Channels

Wireless frequency channels can overlap with neighboring channels. If this happens, consider changing the channel to one that is farther away. You can also reduce the transmit power of the wireless channel being used, to limit access to a smaller area. This can help

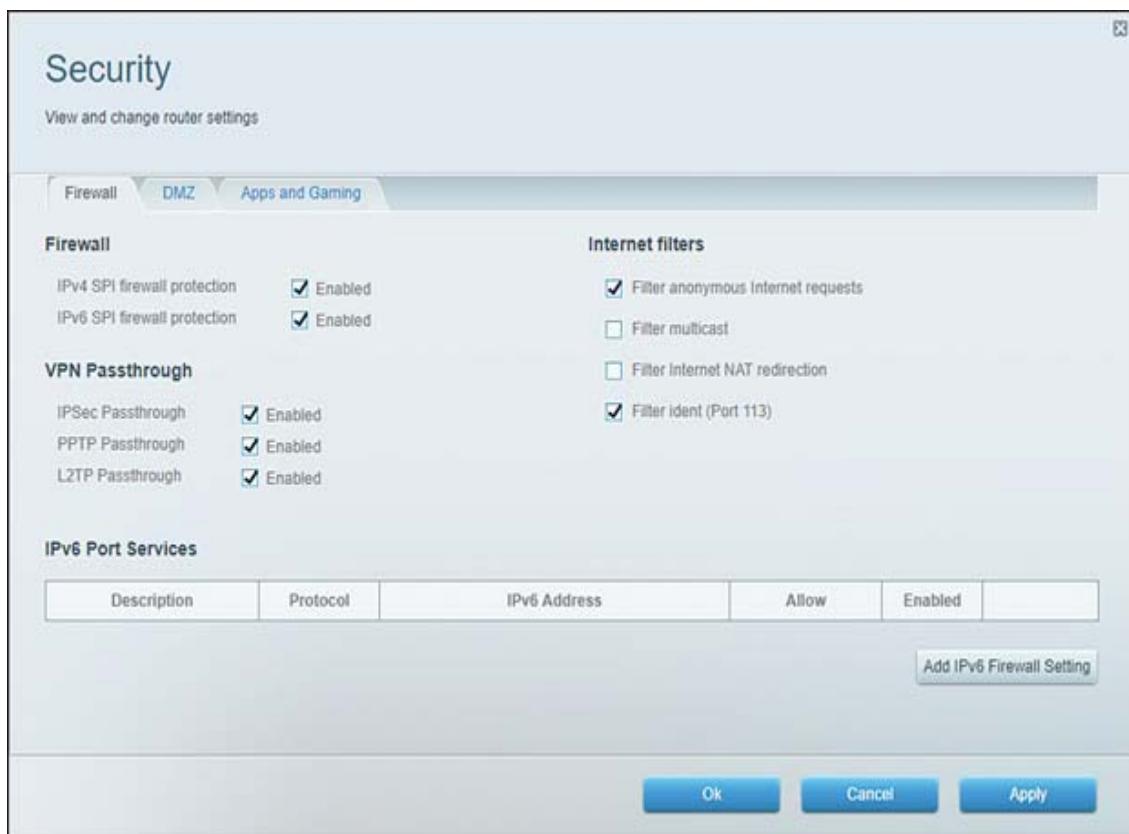
keep malicious outsiders or rogue employees from connecting to a SOHO router.

## Firewall Settings

By default, most WAPs and wireless routers use a feature called Network Address Translation (NAT) to act as simple firewalls. NAT prevents traffic from the Internet from determining the private IP addresses that computers on the network use. However, many WAPs and wireless routers offer additional firewall features that can be enabled, including the following:

- Access logs
- Filtering for specific types of traffic
- Enhanced support for VPNs

See the router manufacturer's documentation for more information about advanced security features. [Figure 7-14](#) shows an example of firewall settings.



**Figure 7-14** Firewall Settings

## Port Forwarding/Mapping

Use **port forwarding** (also known as **port mapping**) to allow inbound traffic on a particular TCP or UDP port or range to go to a particular IP address rather than to all devices on a network. A basic example is an FTP server that is internal to a LAN. The FTP server might have the IP address 192.168.0.250 and might have port 21 open and ready to accept file transactions (or a different inbound port could be used). Clients on the Internet that want to connect to the FTP server would have to know the IP address of the router, so the clients might connect with an FTP client using the IP address 68.54.127.95 and port 21. If an appropriate port-forwarding rule is in use, the router sees these packets and forwards them to 192.168.0.250:21, or whatever port is chosen. Many ISPs block this type of activity, but port forwarding is a common and important method in larger networks.

## Disabling Ports

Blocking TCP and UDP ports, also known as *disabling ports*, is performed with a firewall app such as Windows Defender Firewall with Advanced Security. Hackers take advantage of unused ports sitting idle on a network, and disabling unnecessary ports makes it harder to access your domain.

## Configuring Browser and Relevant Security Settings



**Objective 2.10:** Given a scenario, install and configure browsers and relevant security settings.

The web browser is arguably the most commonly used app in daily use. Web browsers such as Google Chrome, Microsoft Edge, Apple Safari, and Mozilla Firefox are used billions of times a day for everything from sending emails; communicating live with family, friends, or coworkers; and conducting banking and other highly confidential transactions. Knowing how to install, update, configure, and secure commonly used browsers is a skill that every tech should possess. Entire books have been written regarding web browser configuration and security; this section focuses on the current objectives for the CompTIA A+ exam.

## Browser Download and Installation

When downloading browser software (or any app, for that matter), you should do so only from trusted sources. [Table 7-2](#) displays reliable, trusted source Internet reference links where you can safely download the most popular web browsers in use today. Notice the secure *HTTPS* at the beginning of each URL.



**Table 7-2** Trusted Web Browser Download Links

Browser	Link
Microsoft Edge	<a href="https://www.microsoft.com/en-us/edge">https://www.microsoft.com/en-us/edge</a>
Chrome	<a href="https://www.google.com/chrome/">https://www.google.com/chrome/</a>
Firefox	<a href="https://www.mozilla.org/en-US/firefox/new/">https://www.mozilla.org/en-US/firefox/new/</a>
Safari	<a href="https://support.apple.com/downloads/safari_(macOS_only)">https://support.apple.com/downloads/safari (macOS only)</a>

Installing a trusted web browser is typically a straightforward process. The following are general steps to install Google Chrome, which is currently the most popular browser, on a Windows-based system. Most web browser installations follow a similar process:

**Step 1.** Download the installation file.

**Step 2.** If prompted, click **Run** or **Save**.

If you choose Save, start installation with either of these methods:

- Double-click the download.
- Click **Open File**.

**Step 3.** You might be asked, “Do you want to allow this app to make changes to your device?” Click **Yes**. In Windows 10 or 11, a Chrome window opens up when everything is complete.

If you have used a different browser, such as Microsoft Edge or Safari, you can import your settings into Chrome.

Keep the following points in mind when downloading web browsers or any other apps over the Internet:

- Websites that have a URL that begins with *HTTPS* are considered secure and trusted. Remember that Hypertext Transfer Protocol Secure (HTTPS) is a secure extension to the HTTP protocol. HTTPS uses secure port 443, while HTTP uses unsecured port 80.
- If you receive an “Untrusted Certificate” pop-up message when accessing a website, it means that your current browser doesn’t know whether the website is authentic or fake. Invalid or fake SSL/TLS certificates often indicate that a malicious website is present.

## Note

Be sure to download programs and files from trusted sources, or sources that you know are legitimate (for example, Microsoft.com, Google.com, Mozilla.org, Apple.com, and so on, as noted in [Table 7-2](#)).

## Hashing

**Hashing** verifies that the contents of files are unaltered. A hash is often created on a file before it is downloaded; then another hash is created after the download. The two values are compared to make sure the contents are the same. When downloading files—particularly upgrades, patches, and updates—be sure to check and verify the hash values.

Hashing is also important if you store a browser installation file for a later installation because you want to ensure that the installation file has not been tampered with. You can do this by creating a Secure Hash Algorithm (SHA) hash of the executable installation file and storing it for later use. When it is time to install from the executable

installation file, you can run hashing to verify the signature of the file. The details of hashing are beyond the scope of A+. To learn more, visit <https://csrc.nist.gov/projects/Hash-Functions>.

## Untrusted Sources

The previous section on hashing provided an example of using an SHA hash to verify the integrity of a stored browser executable file. If the hash signature matches, the installation file is trusted. If the hash does not match, it is said to be untrusted. This is a perfect example of an untrusted source. You should always download installations from trusted sources and then protect them with file hashing, to detect any malicious activity or tampering.

## Extensions and Plug-ins

Extensions and plug-ins are used to customize web browsers. They add features and functionality and allow you to customize and personalize your web browser. Extensions typically represent source code, while plug-ins are executables. Extensions add functionality to a web browser as a whole, while plug-ins add extra features to particular web pages. Although good (trusted) extensions and plug-ins add functionality and features, bad (untrusted) ones can cause great harm to your system. They can use up system resources, insert ads, redirect web searches, and even collect your personal data.

You can view the extensions that are installed in Microsoft Edge by entering **edge://extensions** in the address bar. To view extensions installed to Google Chrome, enter **chrome://extensions** in the address bar. From these locations, you can also enable or disable extensions or search for others.

### Note

Microsoft Edge and Google Chrome now primarily use extensions and have nearly eliminated using plug-ins. However, Mozilla Firefox still uses both extensions and plug-ins.

## **Password Managers**

A password manager is an application that stores passwords that you use for various websites or services. Password managers are often local programs that run within the operating system. They can also be provided by open source third-party companies such as KeePass or commercial providers such as 1Pssword and Roboform. Commercial managers involve a nominal cost, but they are often more manageable for less experienced users.

Credential Manager is the password manager for Windows and Microsoft Edge. Google Chrome and Mozilla Firefox use built-in credential managers. macOS uses Keychain as its password manager. These tools store web credentials and OS credentials.

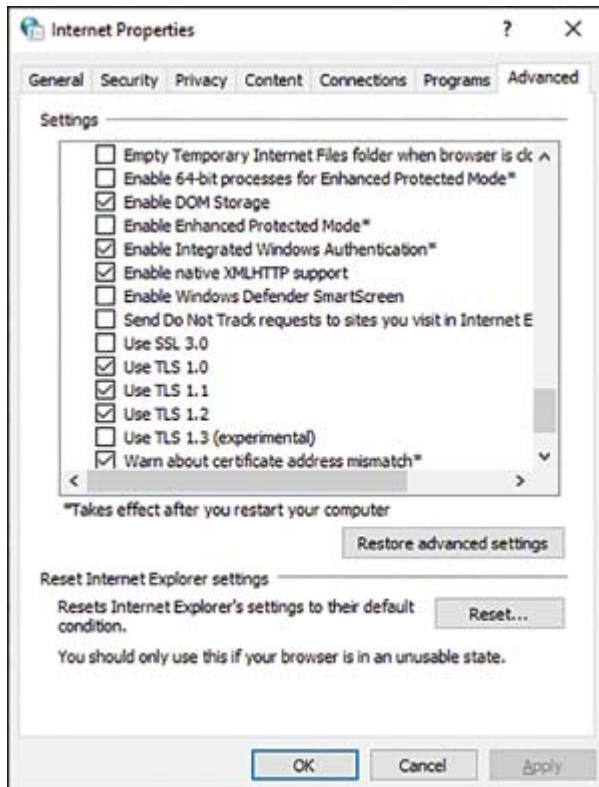
## **Secure Connection/Sites—Valid Certificates**

Using a secure Internet connection and connecting to websites that use valid certificates is critical to ensuring the health and safety of your data and your system. Several technologies help you stay as safe as possible when traversing the world through a web browser. For the purposes of A+ certification, the next sections focus on TLS and HTTPS.

## **Transport Layer Security (TLS)**

TLS is the most widely adopted protocol used to encrypt communications between web apps and web servers and ultimately protect sensitive data in motion (transit). TLS 1.2 is widely used; 1.3 is the latest version, but it is listed as experimental at the time of this writing. To see the various TLS versions in Windows, access

**Internet Options > Advanced**, as shown in [Figure 7-15](#). These TLS settings apply to both Google Chrome and Microsoft Edge.



**Figure 7-15** Internet Options TLS Versions

## Hypertext Transfer Protocol Secure (HTTPS)

As previously mentioned, websites that have a URL that begins with *HTTPS* are considered secure and trusted. This is important here as well. Remember that Hypertext Transfer Protocol Secure (HTTPS) is a secure extension to the HTTP protocol, which is not trusted. If you do not see a padlock in your browser's URL address bar, you are not using HTTPS and the web page is not safe. You should immediately close your session.

Speaking of the padlock in your browser, right-clicking the padlock enables you to view certificate information about your connection. You can see whether the certificate is valid, determine whether the

connection is secure, and view details about the connection protocol in use.

## Settings

Securing browsers with the appropriate settings helps you avoid many system security problems, including spyware, ransomware, and other malicious activities. It is important to configure your client web browsers for ease of use and to ensure that your customers are aware of security threats that loom on the Internet.

## Pop-up Blocker

Pop-up blockers prevent pop-ups from appearing when users visit a website. Most popular browsers, such as Microsoft Edge and Google Chrome, have pop-up blocker capabilities built in and block pop-ups by default. However, in some cases, you might actually want to allow pop-ups.

To configure pop-ups and redirect settings in Microsoft Edge, perform the following steps:

**Step 1.** Tap **Settings**.

**Step 2.** Select **Site Permissions**.

**Step 3.** Select **Pop-ups and Redirects**.

**Step 4.** Toggle **Pop-ups and Redirects** off to block pop-ups, or toggle it on to allow pop-ups on your device.

To configure pop-ups and redirect settings in Google Chrome, perform the following steps:

**Step 1.** Open Chrome.

**Step 2.** At the top right, click **More (three vertical dots) > Settings**.

**Step 3.** Click **Privacy and Security > Site Settings**.

**Step 4.** Click **Pop-ups and Redirects**.

**Step 5.** Choose the option you want as your default setting.

## **Clearing Browsing Data**

Clearing browser data involves using an extension to the browser that allows you to remove browser data such as history, cache, and cookies from a browser toolbar. From the toolbar, you have an option to clear all browser data or selectively remove various information or data types for clearing. Clearing cached files and images (described next) can help fix problems you might have with accessing web pages. Clearing cookies, for example, can help with privacy concerns. Remember that clearing browsing data removes all website-based temporary files stored on the local system, such as browsing history, cookies, passwords, and cache.

To clear browser data in Microsoft Edge, select **Settings** and then click **More > Settings > Privacy, Search, and Services**. Under Clear Browsing Data, select **Choose What to Clear**.

To clear browser data in Google Chrome, follow these steps:

**Step 1.** On your computer, open Chrome.

**Step 2.** At the top right, click **More**.

**Step 3.** Click **More Tools**. Clear the browsing data.

**Step 4.** Choose a time range, such as Last Hour or All Time.

**Step 5.** Select the types of information you want to remove.

**Step 6.** Click **Clear Data**.

## **Clearing the Cache**

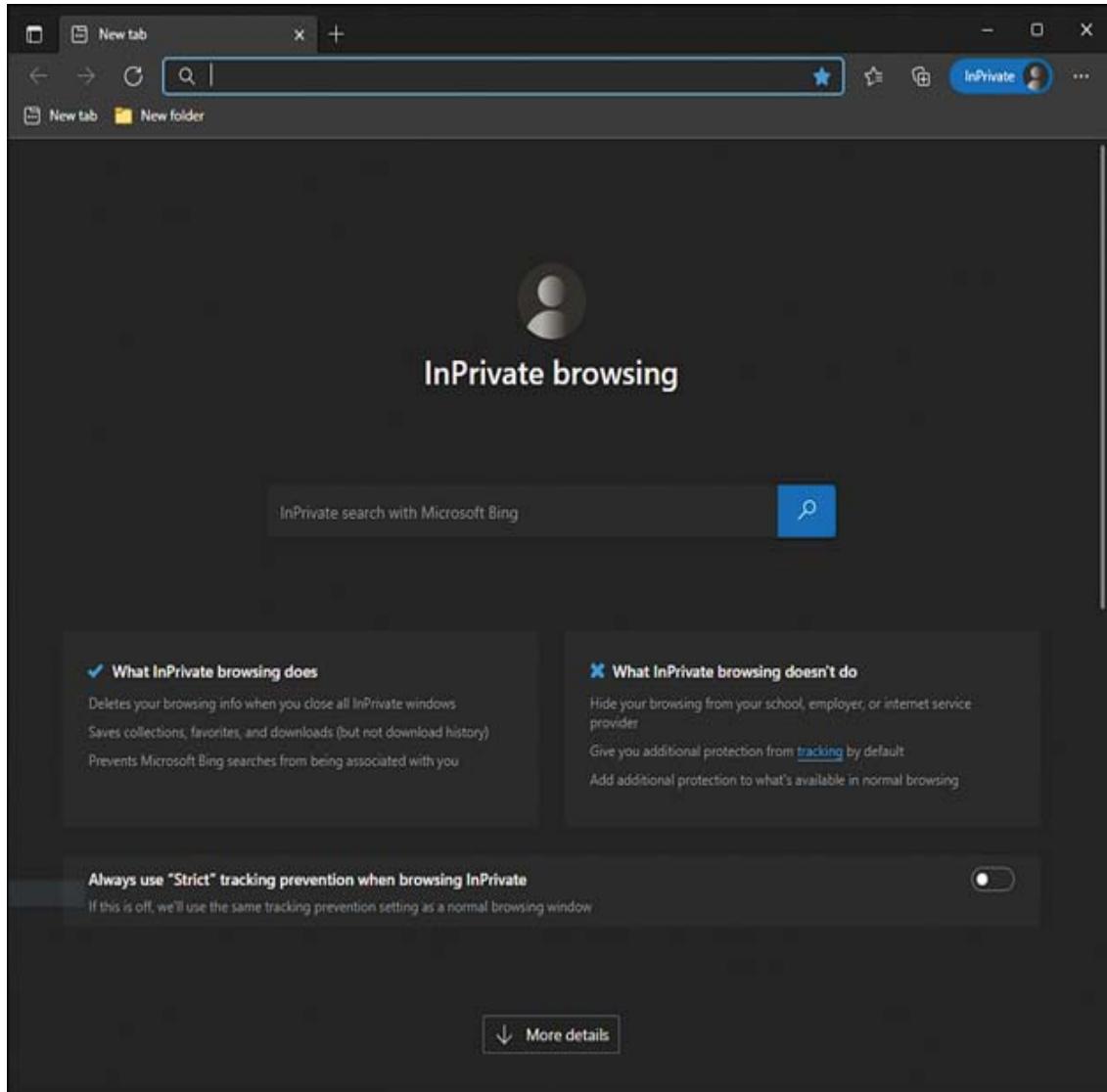
When web pages are accessed, the information is stored in the cache. This process occurs so that if the data is needed again, it can

rapidly be accessed from local storage. This caching process means fewer trips to the Internet to access the same information. Clearing the cache is sometimes necessary if the latest copy of the web page is required. This is often the case during web page development or if you need to access the same website but use different credentials or logon information. Clearing the browser cache removes images and forms, which prevents you from using old forms and ultimately protects your personal information. This is similar to the previously mentioned action of clearing browser data, but it primarily has to do with images and forms.

## Private Browsing Mode

Private browsing mode is a feature of web browsers that does not store web browsing data or information. In fact, when you close private browsing mode, all browsing data and information is removed or destroyed. In Microsoft Edge, private browsing is called InPrivate browsing; in Google Chrome, it is called Incognito mode. To enter InPrivate mode on Microsoft Edge, click the three dots in the upper-right corner of the window and then select New InPrivate Window. The screen turns dark when you enter InPrivate browsing, as shown in [Figure 7-16](#). In the Safari app on a Mac computer, you can choose **File > New Private Window** to use private browsing. For the A+ exam, you should know how to initiate private browsing in Edge and Chrome.





**Figure 7-16** InPrivate Browsing in Microsoft Edge

## Sign-in/Browser Data Synchronization

Because most people access data on various devices, including desktops, laptops, and smart devices, it is extremely important for data to be synced across all devices so that the same information is available. In the old technology days, this involved copying a file to media and then copying that file to each device to have an up-to-date copy. These days, *browser data synchronization* is a cloud service that almost all browser vendors offer for sharing settings and

information across all devices. As long as you sign in with a valid user account, your data is synced across all your devices.

## Note

Be sure to keep work data and personal data separate. In some instances, a browser data sync might be against company policy (for example, if you sync your personal device to a work system). Always check your company policy before you comingle personal settings and data with company settings and data.

## Ad Blockers

An **ad blocker** is a tool that integrates with a web browser and uses filtering to block specific advertisements. Ad blockers assist with online privacy and help to avoid spyware-infected ads. Implementing ad blockers is considered good security practice. In fact, the NSA and Cybersecurity and Infrastructure Security Agency recently released important guidance recommending the use of ad blockers as an important security measure.

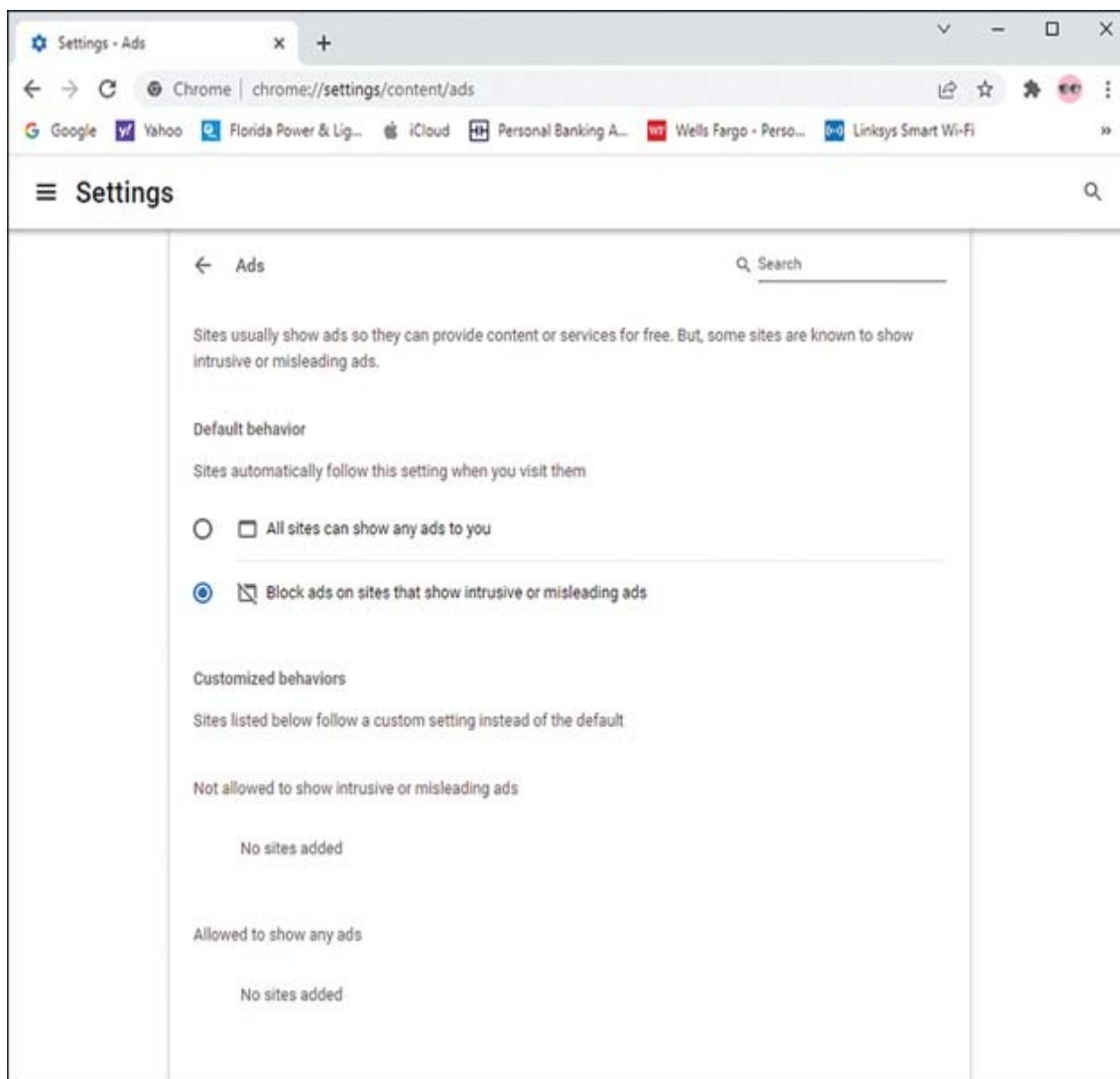
To adjust ad blocker settings in Google Chrome, do the following after you open the Chrome browser:

**Step 1.** At the top right, click **More (three vertical dots) > Settings**.

**Step 2.** Click **Privacy and Security > Site Settings**.

**Step 3.** Click **Additional content settings > Ads**.

[Figure 7-17](#) displays ad blocker settings in Google Chrome.



**Figure 7-17** Ad Blocker Settings in Google Chrome

Many (if not most) third-party ad-blocking programs are offered for free. For example, AdBlock is a free add-on to Microsoft Edge that blocks pop-ups, video promotions, and other distracting ads.

## Exam Preparation Tasks

As mentioned in the Introduction, you have several choices for exam preparation: the exercises here; [Chapter 10, “Final Preparation”](#); and the exam simulation questions in the Pearson Test Prep practice test software.

# Review All the Key Topics

Review the most important topics in the chapter, noted with the Key Topic icon in the outer margin of the page. [Table 7-3](#) lists these key topics and the page numbers on which each is found.



**Table 7-3** Key Topics for Chapter 7

Key Topic Element	Description	Page Number
List	Active Directory basics	581
List	Wireless protocols and encryption types	582
Section	Malware	584
List	Antivirus/anti-malware protection techniques	587
Section	Social Engineering Threats and Vulnerabilities	590
List	Built-in OS firewalls	598
Section	Shared Files and Folders	603
Paragraph	Single sign-on (SSO)	604
Steps	Encrypting files	607
Section	Password Best Practices	608
Section	Account Management	612
Note	Securing mobile devices	615
List	Physical destruction methods	621
List	Recycling/repurposing best practices	622

<b>Key Topic Element</b>	<b>Description</b>	<b>Page Number</b>
Steps	Updating SOHO router firmware	624
List	Physical security best practices in a SOHO network environment	625
Section	Wireless-Specific Security	626
Table 7-2	Trusted Web Browser Download Links	630
Figure 7-16	InPrivate Browsing in Microsoft Edge	637

## Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

access control vestibule  
 bollards  
 smart cards  
 biometrics  
 magnetometers  
 principle of least privilege  
 access control list (ACL)  
 multifactor authentication (MFA)  
 hard token  
 soft token  
 mobile device management (MDM)  
 Active Directory  
 Temporal Key Integrity Protocol (TKIP)  
 Wi-Fi Protected Access 2 (WPA2)  
 Advanced Encryption Standard (AES)  
 authentication

Wi-Fi Protected Access 2 (WPA3)  
Remote Authentication Dial-In User Service (RADIUS)  
Terminal Access Controller Access Control System Plus  
(TACACS+)  
Kerberos  
malware  
Trojan  
rootkit  
virus  
spyware  
ransomware  
keylogger  
boot sector virus  
cryptominers  
recovery mode  
social engineering  
phishing  
vishing  
whaling  
impersonation  
shoulder surfing  
tailgating  
dumpster diving  
evil twin  
distributed denial of service (DDoS)  
denial of service (DoS)  
zero-day attack  
spoofing  
on-path attack  
brute-force attack  
dictionary attack

Structured Query Language (SQL) injection  
cross-site scripting (XSS)  
Defender Antivirus  
firewall  
software firewall  
share permissions  
New Technology File System (NTFS)  
User Account Control (UAC)  
single sign-on (SSO)  
BitLocker  
BitLocker To Go  
Encrypting File System (EFS)  
data-at-rest encryption  
remote wipe  
antivirus  
anti-malware  
Internet of Things (IoT)  
degaussing  
certification of destruction/recycling  
IP filtering  
firmware update  
content filters  
Dynamic Host Configuration Protocol (DHCP) reservations  
static WAN IP address  
Universal Plug and Play (UPnP)  
screened subnet  
port forwarding/mapping  
hashing  
ad blocker

## Answer Review Questions

- 1.** Andre was running late for work and left his security badge in his car. Instead of taking the time to return to his car and risk being late, he waited by the outer door and walked in behind another employee. The other employee did not know Andre and was irritated with him for following so closely, so she didn't allow Andre to follow her through the inner door to work. He had to return to his car for the badge. What security concepts were involved in this scenario? (Choose two.)

  - a.** Security guard
  - b.** Tailgating
  - c.** Access control vestibule/mantrap
  - d.** Shoulder surfing
- 2.** Alexa was working her shift in the server room when an alarm went off on a server that belonged to a vendor from another company. She was unable to get to the reset button on the server. What likely prevented her from accessing the server whose alarm was going off?

  - a.** Lack of a key fob
  - b.** Rack-level security
  - c.** Lack of authentication
  - d.** Privacy screen
- 3.** Match the type of malware to its description.

Description	Type of Malware
<b>1.</b> Infects and rewrites files. Replicates automatically, with no user intervention.	
<b>2.</b> A method of hiding malware from detection programs.	

Description	Type of Malware
3. Tracks web browsing. Uses pop-ups to attract a user's attention.	
4. Encrypts target files and then demands payment to unencrypt files.	
5. Infects and rewrites files. Replicates itself if a user executes the file.	

Answer options:

- a. Spyware
  - b. Virus
  - c. Worm
  - d. Rootkit
  - e. Ransomware
4. As an IT professional, you should be sure to employ security best practices. Which of the following is not a best practice?
- a. Strong passwords for user accounts
  - b. Antivirus/malware protection
  - c. Changing the default password on a WAP
  - d. WEP encryption
5. Which of the following is generally the most difficult form of security for a malicious hacker to overcome?
- a. Firewall
  - b. Encryption
  - c. Biometrics
  - d. Physical lock and key
6. Biometrics include the use of which of the following? (Choose all that apply.)

- a. Fingerprint scan
  - b. RFID
  - c. Retinal scan
  - d. Token
- 7.** Which of the following is not a type of token?
  - a. Key fob
  - b. Cable lock
  - c. RFID card
  - d. Smart card
- 8.** Which of the following is a program that either blocks or allows data packet delivery to network addresses?
  - a. DHCP server
  - b. Key fob
  - c. Firewall
  - d. Network server
- 9.** Which of the following is a characteristic of a strong password? (Choose all that apply.)
  - a. No more than six characters
  - b. Lowercase only
  - c. Use of symbols
  - d. Use of numbers
- 10.** Mike was called to a workstation that was running slowly. After interviewing the user and asking about recent activity, Mike determined that the user had opened a fake email and reset his password. Which of the following was the user most likely involved in?
  - a. Tailgating
  - b. Dumpster diving

- c. Phishing
  - d. Shoulder surfing
- 11.** Fred determined that encryption was the best solution for keeping his USB flash drive safe while on the road. Which security product satisfies this need?
  - a. Recovery Console
  - b. Single sign-on (SSO)
  - c. BitLocker To Go
  - d. USB 3 Lockup
- 12.** Ellen works at home as an accountant. She noticed her wireless network slowing and wondered whether her neighbors had started using her network for streaming. Which security practices can she employ to ensure that her neighbors don't gain access to her network and that her clients' files are protected? (Choose two.)
  - a. Change the default IP address on the default gateway
  - b. Change the network name and disable the SSID broadcast
  - c. Use MAC address filtering
  - d. Change the Netflix password
- 13.** Jen has been tasked with repurposing laptops used by the human resources department. What can she do to make sure important personnel information cannot be compromised?
  - a. Overwrite
  - b. Low-level format
  - c. Standard format
  - d. Drive wipe
- 14.** Hiro is able to log into his account at work but cannot see the work his team is doing for an advertising client. He did not have any trouble before he went on vacation. What is a reasonable explanation for this problem?

- a. Share permissions were updated while he was gone.
  - b. Hiro was locked out due to inactivity
  - c. It took Hiro three tries to log into his computer, and his permissions were suspended after the second attempt.
  - d. The boss thought Hiro was leaving the company, so his account was disabled.
- 15.** Which of the following is used to verify that the contents of files are unaltered?
  - a. Trusted sources
  - b. Hashing
  - c. Pop-up blockers
  - d. Private browsing mode

# Chapter 8

## Software Troubleshooting

**This chapter covers the five A+ 220-1102 exam objectives related to Microsoft Windows OS troubleshooting, PC security, malware removal, mobile OS and application operational and security issues, and related topics. These objectives may comprise 22 percent of the exam questions:**

- **Core 2 (220-1102): Objective 3.1:** Given a scenario, troubleshoot common Windows OS problems.
- **Core 2 (220-1102): Objective 3.2:** Given a scenario, troubleshoot common personal computer (PC) security issues.
- **Core 2 (220-1102): Objective 3.3:** Given a scenario, use best practice procedures for malware removal.
- **Core 2 (220-1102): Objective 3.4:** Given a scenario, troubleshoot common mobile OS and application issues.
- **Core 2 (220-1102): Objective 3.5:** Given a scenario, troubleshoot common mobile OS and application security issues.

Given the widespread use of mobile devices, troubleshooting is now more than just solving problems with computers. However, many of the same principles apply, whether solving problems with computers, peripherals, or mobile devices: knowledge of products and operating system functions, understanding of the tools needed to diagnose and repair problems, and a determination to avoid data loss except when unavoidable. This chapter helps you apply these principles.

## **“Do I Know This Already?” Quiz**

The “Do I Know This Already?” quiz allows you to assess whether you need to read the entire chapter. [Table 8-1](#) lists both the major headings in this chapter and the “Do I Know This Already?” quiz questions covering the material in those headings so that you can assess your knowledge of these specific areas. The answers to the “Do I Know This Already?” quiz appear in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes and Review Questions.”

**Table 8-1** “Do I Know This Already?” Section-to-Question Mapping

<b>Foundation Topics Section</b>	<b>Questions</b>
Troubleshooting Common Windows OS Problems	1–3
Troubleshooting Common PC Security Issues	4–6
Best Practice Procedures for Malware Removal	7
Troubleshoot Common Mobile OS and Application Issues	8–9
Troubleshoot Common Mobile OS and Application Security Issues	10

### **CAUTION**

The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for the purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

- 1.** Kate is experiencing inconsistent web access; sometimes her access is down for a few minutes at a time. She does not lose a connection to her local network, but she can't browse. Which System Settings can she check to see her local network and Internet status?

  - a.** Network Connections
  - b.** Internet Update
  - c.** Network Status
  - d.** Ethernet
- 2.** Which message could indicate that incompatible hardware is installed or that there are registry problems during the boot sequence?

  - a.** A BSOD error
  - b.** A "Wirefault" message during booting
  - c.** A red X on the Taskbar
  - d.** A "Network Not Found" message
- 3.** Which of the following should be considered when a warning displays that the computer is low on memory? (Choose all that apply.)

  - a.** The amount of RAM
  - b.** Swap file/page file settings
  - c.** Changing the virtual memory settings
  - d.** Checking resources in the Task Manager
- 4.** What kind of malware can cause home page settings to change?

  - a.** Pop-ups
  - b.** Browser redirection
  - c.** WannaCry
  - d.** Rapidly opening windows

5. Which warning is intended to prevent using apps from a fraudulent source?

  - a. Certificate
  - b. System update
  - c. Neither A nor B
  - d. Both A and B
6. What is the main purpose of a bootable antivirus program?

  - a. It allows continuous scanning for malware.
  - b. It can run scans without an OS.
  - c. It checks the BIOS/UEFI for viruses.
  - d. It scans the OS as it loads.
7. What is the second step in the best practice procedures for removing malware?

  - a. Identify symptoms.
  - b. Disable System Restore in Windows.
  - c. Quarantine infected systems.
  - d. Update anti-malware software.
8. Ivan is trying to stream music on his cellphone, but his usual app is not working. What should his *first* step be?

  - a. Keep his finger on the app icon until it wiggles and then delete it.
  - b. Restart the phone.
  - c. Shut down the phone.
  - d. Update the app.
9. Lorna likes to stream TV shows on her phone while she is on the bus. One day her service slows down, and she can't watch her shows. Why might Lorna's phone slow down so much?

  - a. Lorna changed her bus route and now goes a different way to work.

- b. Lorna watched so much TV this month that her provider throttled her data rate.
  - c. Lorna forgot to pay her bill.
  - d. Lorna's phone provider merged with a cable company, and that company decided to change her service.
- 10.** Eric wants to customize his phone's user experience beyond what his phone company provides. What must he do to make these changes to the OS?
  - a. Eric must download special malware for his phone.
  - b. Eric must order special updates from the cell provider.
  - c. Eric can't do this; it is illegal.
  - d. Eric must jailbreak his phone.

## Foundation Topics

# Troubleshooting Common Windows OS Problems



**220-1102: Objective 3.1:** Given a scenario, troubleshoot common Windows OS problems.

Troubleshooting is an essential skill for a PC technician. The capability to recognize and remediate OS issues starts with concepts covered in this section.

## Common Symptoms

Windows OS has countless lines of code and several processes working simultaneously. Occasionally, some processes fail and cause

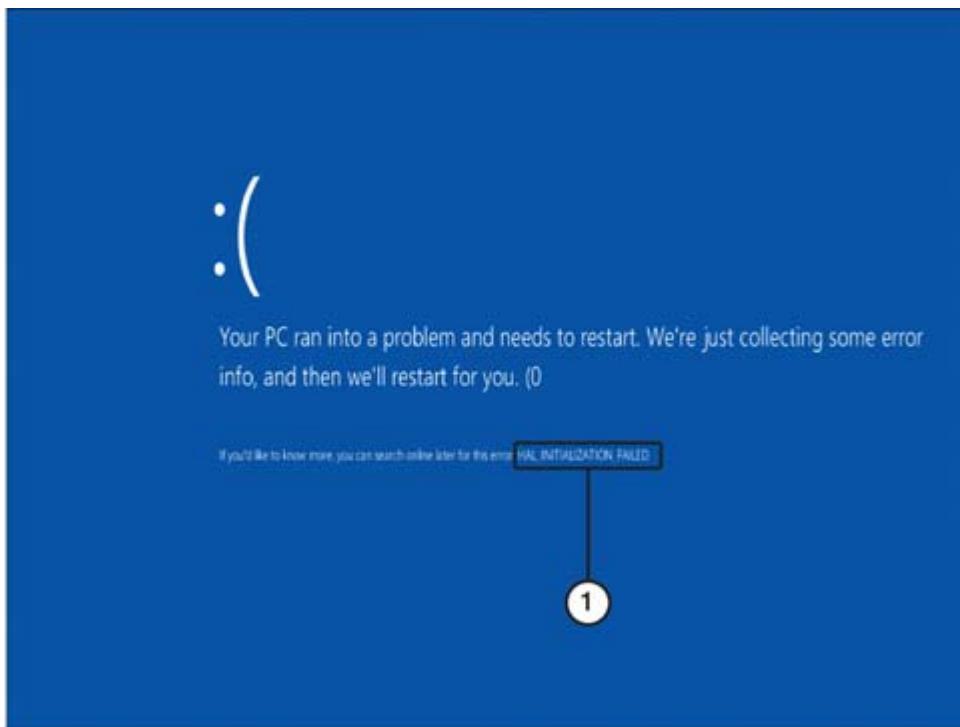
problems for the whole system. Performance then is impacted in many possible ways, ranging from slow performance to system crashes. This section introduces some of the more common OS problems and tells how they can be recognized.

## BSOD

Proprietary crash screens such as the Windows STOP error (**blue screen of death [BSOD]**) can be caused by operating system, application, or hardware errors.

If Windows is configured to reboot when a STOP error occurs, the system will continuously reboot until the error is resolved. To leave a STOP error message onscreen until you decide to restart the system, clear the Automatically Restart check box in the System Failure setting in the Startup and Recovery section of Advanced System Properties. This is accessed via **Control Panel > System > Advanced System settings**. Under Startup and Recovery, select Settings. More details and depictions of this are highlighted in [Chapter 5, “Hardware and Network Troubleshooting.”](#)

In Windows 10, STOP errors look like the example in [Figure 8-1](#). The STOP error is listed by name.



1. STOP error message

**Figure 8-1** A Windows 10 STOP Error

## Note

Regardless of when a STOP/BSOD error occurs, your system is halted by default. If the computer does not restart on its own, you must turn off the system and turn it back on. Before you do that, however, record the error message text and other information so that you can research the problem if it reoccurs. For more information, see the next section, “Causes of BSOD Errors.”

## Causes of BSOD Errors

BSOD errors can be caused by any of the following:

Key  
Topic

- **Incompatible or defective hardware or software:** Start the system in **Safe Mode** and uninstall the last hardware or software installed. Acquire updates before you reinstall the hardware or software. Exchange or test memory. Run SFC/scannow to check for problems with operating system files.
- **Registry problems:** **System Restore** can also be used to revert the system and registry to an earlier state.
- **Viruses:** Scan for viruses and remove any that are discovered.
- **Miscellaneous causes:** Check the Windows Event Viewer and also check the system log. Research the BSOD with the Microsoft Support website.

## Researching BSOD Causes and Solutions

To determine the exact cause of a STOP error, note the number or name of the error (for example, “STOP 0x0000007B, HAL INITIALIZATION FAILED”) and look it up at the Microsoft support website: <https://support.microsoft.com>. When you search for the error, be sure to specify the version of Windows in use.

### Note

STOP errors are often referred to with a shortened version of the error code or by name. For example, the shortened version of a 0x0000007B error is 0x7B.

### TIP

Unfortunately, you can't take a screen capture of a BSOD for printing because a BSOD completely shuts down Windows. In this situation, a digital camera or smartphone can be used to record the exact error message.

The solution might involve one or more of the following changes to your system:



- Changing the system registry. Sometimes you can download an automated registry repair tool to perform these changes for you. Whether you make the changes manually or automatically, back up the registry first.
- Removing a newly added component.
- Replacing components such as memory.
- Upgrading an application.

## Sluggish Performance

A slow system or sluggish performance can be caused by many issues in Windows. [Table 8-2](#) lists some possible causes and solutions.



**Table 8-2** Slow/Sluggish System Performance Causes and Solutions

---

### Windows System Performance Troubleshooting

---

Problem	Solution
System is not configured for maximum performance	To solve this problem, set the Power setting to High Performance using the Power options icon in the notification area or the Power options in the Control Panel. This option is not available on tablets.

---

## **Windows System Performance Troubleshooting**

---

<b>Problem</b>	<b>Solution</b>
Drive containing paging file and temporary files is nearly full or badly fragmented	Use Disk Cleanup in the drive properties to remove unwanted files, check the drive for errors, and defragment the drive. If you have more available space on a different drive, use the Advanced tab in the system properties to change the location of the paging file and temp files.
System is overheating and CPU is running at reduced speed	Remove dust and dirt on the CPU and system fans. Check for adequate airflow through the system. Change back to the Balanced power setting.
Memory is running low	Add RAM; this fixes many performance problems. For better performance, exceed the minimums recommended for the version of Windows in use.
Sudden performance drop occurs	Check for viruses and malware; this is especially important if performance has suddenly plunged.
Registry error messages appear	The program CCleaner is widely used for this task.

---

## **Boot Problems**

Boot problems such as failure to boot can be caused by several issues, including incorrect boot order configuration in the BIOS/UEFI, corrupt or missing boot files, missing driver files, or even a failing CMOS battery.

Windows uses the bootmgr and BCD files during the startup process. If these files are corrupted or missing, the corresponding error messages appear:

- **bootmgr is missing:** This message appears if the bootmgr file is missing or corrupt. This black screen likely will also include the message “Press Ctrl+Alt+Del to Restart”; however, doing so probably will not fix the issue.
- **The Windows Boot Configuration Data file is missing required information:** This message means either that the Windows Boot Manager (bootmgr) entry is not present in the Boot Configuration Data (BCD) store or that the Boot\BCD file on the active partition is damaged or missing. Additional information you might see on the screen includes File: \Boot\BCD and Status: 0xc0000034.

A missing bootmgr file can be repaired in two ways:

- Boot to the System Recovery options and select the Startup Repair option. This should automatically repair the system and require you to reboot. To access the options in Windows 10, locate the Advanced Startup Settings menu.
- Boot to the System Recovery options and select the Command Prompt option. Type the **bootrec /fixboot** command, as shown in [Figure 8-2](#).



```
c:\Administrator:X:\windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

X:\Sources>bootrec /fixboot
The operation completed successfully.

X:\Sources>
```

## **Figure 8-2** Repairing BOOTMGR.exe from the Windows Recovery Environment's Command Prompt

For more about these steps, see <https://support.microsoft.com/en-us/kb/2622803>.

To repair the BCD store, use this short process:

- Step 1.** Boot to the System Recovery options and select the **Startup Repair** option. Windows should automatically repair the system and require you to reboot. If not, move on to the second step.
- Step 2.** Boot to the System Recovery options and select the **Command Prompt** option. Type **bootrec /rebuildbcd**.
  - a.** If the Bootrec.exe tool runs successfully, Windows presents you with an installation path for a Windows directory. To add the entry to the BCD store, type **Yes**. A confirmation message appears, indicating that the entry was added successfully. Restart the system.
  - b.** If the Bootrec.exe tool can't locate any missing Windows installations, you must remove the BCD store and then re-create it. To do this, type the following commands in the order shown here and press Enter after each command:

[Click here to view code image](#)

```
Bcdedit /export C:\BCD_Backup  
ren c:\boot\bcd bcd.old  
Bootrec /rebuildbcd
```

## **Frequent Shutdowns**

Continuous reboots can be caused by problems with the power supply or by a Windows or other operating system configuration setting:

When the Power Good line to the motherboard carries a voltage that is too high or too low, the processor resets, shutting down the system and rebooting it. Test the power supply voltage levels; replace the power supply if Power Good tests out of specifications.

Intermittent failures of other USB external devices or of internal devices can be caused by damaged data cables, power supplies or connectors, or ports.

To troubleshoot these problems, follow these steps:

**Step 1.** Shut down the device (and the computer, if the device is internal) and replace the data cable with a known-working replacement. If a USB device is plugged into a front-mounted USB port or a USB port on a card bracket, check the USB header cable connections to the motherboard.

**Step 2.** Turn on the device or computer.

**Step 3.** Test the device over time. If the device works correctly, the problem is solved.

**Step 4.** If steps 1–3 did not resolve the problem, use the original data cable and try plugging it into a different internal or external port. Repeat steps 2–3.

**Step 5.** Try steps 1–4 again, but this time use a replacement power connector or AC adapter.

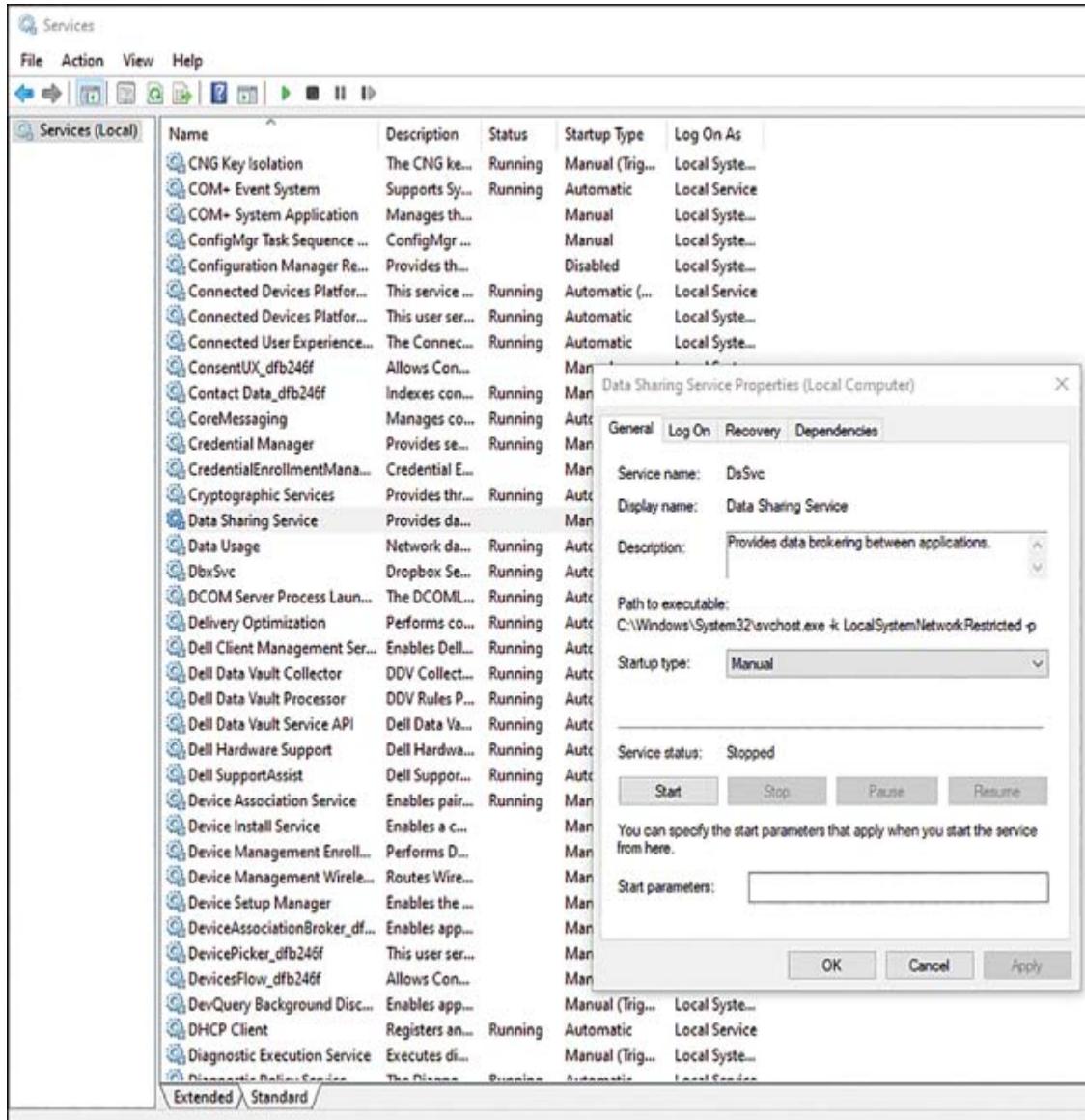
**Step 6.** When you find the defective component, the problem will stop. If the problem is not resolved with different data cables, connectors, or power supplies/AC adapters, the device itself needs to be replaced.

Intermittent or frequent shutdowns are often a software issue. Updating drivers is a reliable fix. Also check the sleep mode settings in Windows 10, to make sure the computer is not simply going to sleep.

## Services Not Starting

Remember that services are the numerous background applications running in Windows that perform the minor tasks that keep Windows 10 running. Dozens of services run in Windows 10, including even more extended services that support the Windows services. From time to time, one of these services might fail to load when booting. One common reason is that so many services are running that a non-Windows service interrupts a Windows service during the boot process. To view the available services, go to the Run command box (Windows+R) and type **services.msc**.

From the Services menu, select the service that is experiencing a problem and check its status. If it is disabled, right-click the service and click Start to enable it. [Figure 8-3](#) shows that the Data Sharing service in the Services console is disabled. Clicking Start on the General tab should enable it; if not, the Recovery tab (see [Figure 8-3](#)) offers further options to restart the service. These options are available by right-clicking the service and selecting Properties.



**Figure 8-3** Services Manager

Other possible approaches include using Windows Recovery (WinRE) in the advanced setup menu. (This works in both Windows 10 and 11.) Three possible ways to access WinRE are as follows:

- From the login screen, click Shutdown; then hold down the Shift key while selecting Restart.
- Click **Start > Settings > Update & Security > Recovery**. Under Advanced Startup, click Restart Now.

- Boot to recovery media.

Another option is to boot in Safe Mode and troubleshoot the Services.

If problems persist, try running the System File Checker (from an elevated mode) and then reboot.

System Restore (**Settings > Windows Update > Advanced Options**) can be used if the previous efforts fail. A last resort is to reset the PC (**Settings > Update and Security > Recovery**).

## Application Crashes

Applications can misbehave or crash for a variety of reasons.

Applications are written to work with operating system software, and well-written applications rarely have problems in that environment. Keep in mind, however, that OS software is constantly being updated for security and other reasons, and usually a lag occurs between the OS and application revisions. During that update lag, many possibilities can go wrong.

Microsoft is constantly updating Windows 10 with code and patches that work with specific applications. These patches do not necessarily install automatically. You can customize these updates in Windows Update settings. To access these settings in Windows 10, go to **Start > Settings > Update & Security**. If needed, the Advanced Options tab is available.

Also available from the Update and Security page in Settings is the Troubleshoot tool, which offers a way for Windows 10 to self-diagnose and repair problems.

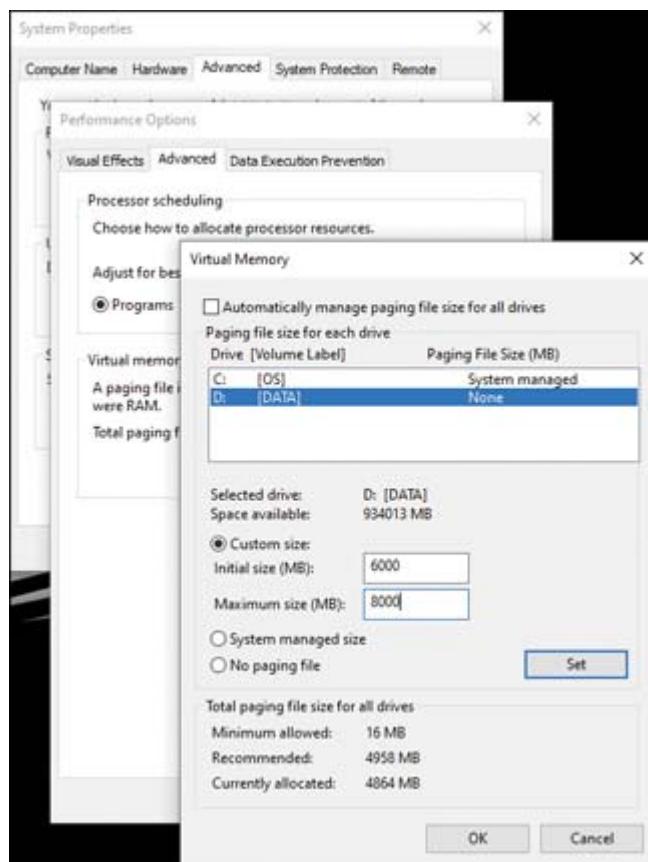
To access these settings in Windows 10, go to **Start > Settings > Update & Security > Troubleshoot**. Options for managing how to run Troubleshoot automatically are available in the drop-down list.

If you encounter application errors, also check with the application developers to see if updates are available. Software “patches” are small updates that can fix known problems until a full version update is available. If patches are not available and the software is essential to the business, you might need to roll back the OS update to improve performance. Of course, updates happen for a reason; if security issues arise from rolling back an update, be sure to address those in some other way, if possible.

Drivers for peripheral devices and video and graphics cards can be another source of application issues. Windows Updates usually include the drivers, but the manufacturers have them as well. Uninstalling a driver and then replacing it can often solve a problem.

## Low Memory Warnings

If Windows issues a warning stating “Your computer is low on memory,” the likely cause is that not enough memory resources exist for all the tasks the computer is trying to perform. The computer might be under-resourced (see [Chapter 3, “Hardware,”](#) for more on adding RAM) or some application (or even a virus) might be demanding more processing power than should be allowed. [Figure 8-4](#) depicts the following steps that address low memory warnings by adjusting allotted virtual memory.



**Figure 8-4** Virtual Memory

The first step in addressing this warning is to visit the Task Manager and see where the resources are being allotted. If unused or unnecessary applications are open and are demanding memory space and CPU time, shut them down so that you can free up resources. As applications are closed, more memory becomes available. If an unrecognized app is using memory, research the app or service to see if it is necessary. If no information is available, scanning for a virus or **malware** is a good idea.

Another option is to increase virtual memory, which means assigning some hard drive space to perform as RAM.

To increase virtual memory, follow these steps:

**Step 1.** Press Windows+X and then select **System**.

**Step 2.** Select **Advanced System Settings**. This opens the System Properties page.

**Step 3.** Select the **Advanced** tab and choose **Settings** under the Performance tab to open the Performance Options window.

**Step 4.** Choose the **Advanced** tab and select **Change** under Virtual Memory to access the allocation settings.

## USB Controller

The warning “Not Enough USB Controller Resources” indicates that too many USB devices (or, more likely hubs) are trying to access a limited number of endpoints in the USB controller. This is more common with USB 3.0 devices than USB 2.0 devices because, in greatly simplified terms, USB 3.0 can demand more resources.

The following are quick fixes for this issue:

- Disconnect unnecessary hubs or devices from the computer to free up endpoints in the controller.
- If possible, move some devices or external hubs from USB 3.0 to USB 2.0 ports (or simply use a USB 2.0 cable from the computer to a USB hub). This should free up some access to the controller.
- Add a USB host controller in a PCIe slot.
- Reinstall the Universal Serial Bus Host Controllers.

For a deeper dive into how to reinstall USB host controllers, see <https://thegeekpage.com/not-enough-usb-controller-resources/fix>.

To troubleshoot USB problems, follow these steps:

**Step 1.** Shut down the device (and the computer, if the device is internal) and replace the data cable with a known-working replacement. If a USB device is plugged into a front-

mounted USB port or a USB port on a card bracket, check the USB header cable connections to the motherboard.

**Step 2.** Turn on the device or computer.

**Step 3.** Test the device over time. If the device works correctly, the problem is solved.

**Step 4.** If steps 1–3 did not resolve the problem, use the original data cable and try plugging it into a different internal or external port. Repeat steps 2–3.

**Step 5.** Try steps 1–4 again, but this time use a replacement power connector or AC adapter.

**Step 6.** When you find the defective component, the problem will stop. If the problem is not resolved with different data cables, connectors, or power supplies/AC adapters, the device itself needs to be replaced.

## System Instability

The underlying issues that cause system instability could be the same or similar to the issues mentioned in the previous sections. However, if the PC runs slowly or is intermittently sluggish, and if additional RAM (or page file management), startup program management, and updates have not resolved the issue, you can take a few more steps:

- Free up disk space in Storage Settings (**Settings > System > Storage**).
- Pause syncing. Synchronization of OneDrive, Dropbox, or other cloud storage can intermittently use up resources, causing slow traffic and sluggish loading of apps. Try temporarily pausing the synchronization and check for performance improvement.
- Check/scan for virus or malware problems.

- Recent updates and changes might be the issue. Restoring from a System Restore point can remove troublesome programs without removing your personal files.

## No OS Found

If an operating system cannot be located, boot into the BIOS/UEFI and check that the computer is looking in the correct place for the OS. The drive hosting the OS should be in the first option to boot.

Loose cables are another common problem that can cause a boot to fail. If the boot option settings are correct in the BIOS/UEFI, check the cables; sometimes cables look connected but are not seated properly.

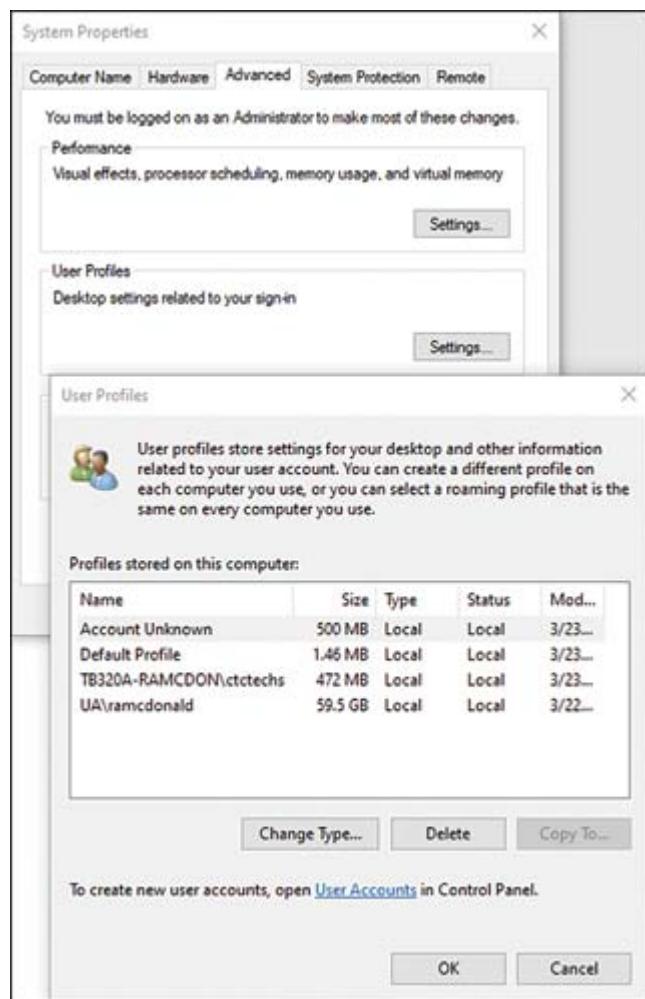
Resetting the BIOS/UEFI is also an option. The BIOS?UEFI menu has options for restoring defaults.

## Slow Profile Load

A user profile contains personalized settings for devices such as the mouse and keyboard, Windows-based applications, and desktop files and settings. Sometimes a user notices that one profile loads much more slowly than other profiles.

One reason for a slow-loading profile is that many large files and folders are stored on the desktop and need to be loaded as part of the profile. Storing these large files in My Computer or another drive reduces the load time.

To check the size of a user profile, use the Run dialog box or the search tool and enter **sysdm.cpl**. This brings up the System Properties menu in [Figure 8-5](#).



**Figure 8-5** Checking User Profiles

From the System Properties menu, select the Advanced tab and then select Settings under User Profiles. The User Profiles information displays as shown in the second window of [Figure 8-5](#).

## Note

One profile is much larger than the others. In this case, you should suggest to this user that cleaning up the desktop will likely avoid slow profile issues.

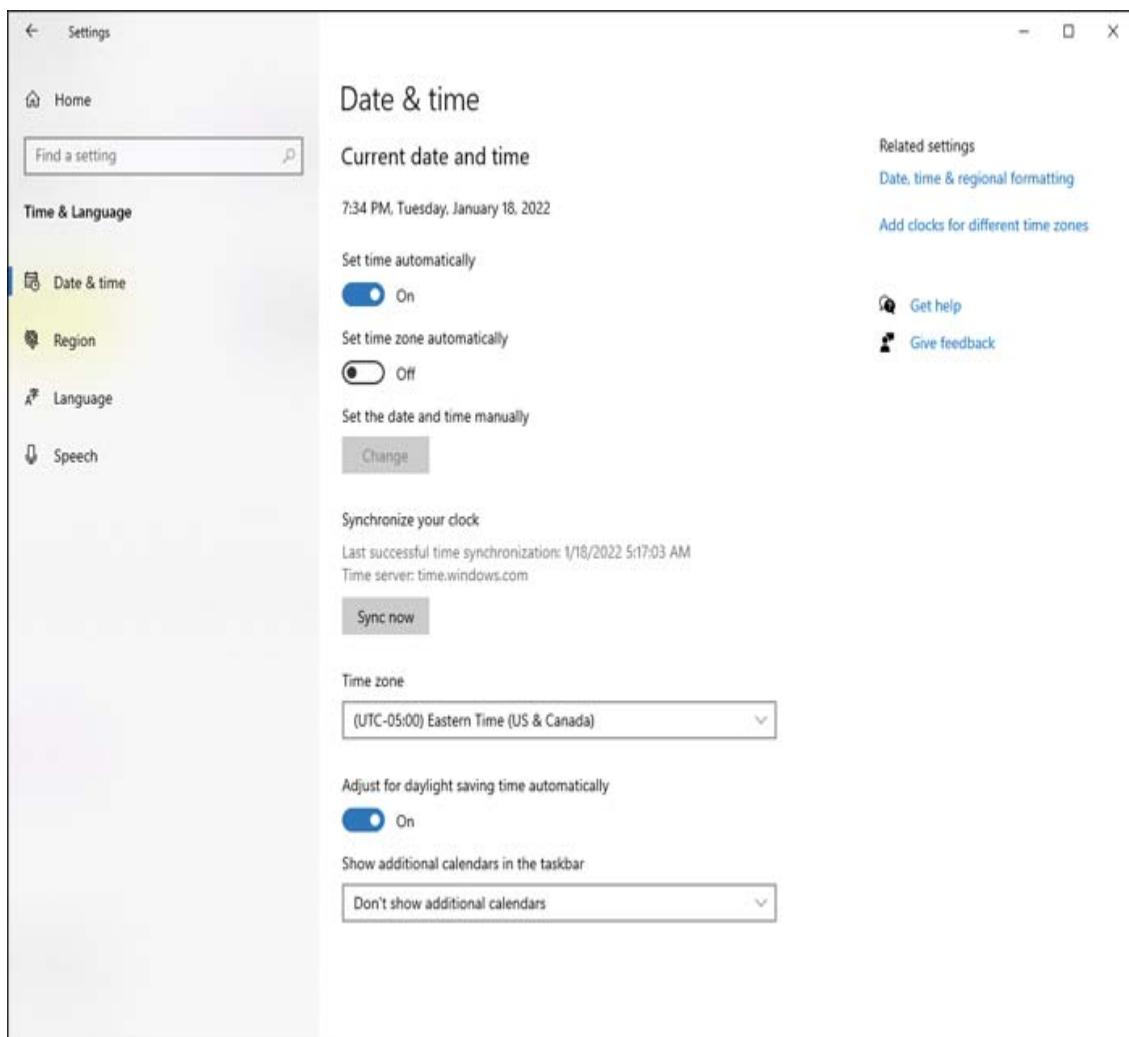
## Time Drift

**Time drift** occurs when the clock for one computer or server does not agree with the clocks of other computers it interacts with. This can cause several issues that can be hard to detect. For example, event logs used to troubleshoot can have the wrong time stamps, and other computers or servers, both local or on the Web, can experience secure transaction issues or authentication issues.

The easy fix here is to set a computer's time to align with the time used by the National Institute of Standards and Technology (NIST), found at [www.time.gov](http://www.time.gov). This site even provides a calculation of the difference between the device's clock and the NIST time. Use this clock to reset the time on the computer.

A computer network should have all its devices running on the same time. This can be done by establishing a clock server in a network and running NTP (the Network Time Protocol) on all devices.

Time settings, as well as the option to manually synchronize the clock, are found under **Settings > System > Date & Time**, as Figure 8-6 shows. Note that, in the example, the source for the time setting is the server located at <http://time.windows.com>.



**Figure 8-6** Time Settings

## Common Troubleshooting Steps

This section lists common Windows OS troubleshooting steps that have been described throughout the book. The list starts with simple first steps and progresses through increasingly complex steps. You should be familiar with these steps for the examples you might see on the A+ exam.

- **Reboot:** Rebooting is always a good first step, especially if the device has been running for an extended time.

- **Restart services:** From the Run menu, type either **services.msc** or **services** in the search bar and then open the Services app. Select the application and stop or restart as needed.
- **Uninstall/reinstall/update applications:** Go to the Microsoft Store app, select Account, and then select App Updates. The store can update apps automatically.
- **Add resources:** Always remember, few actions can improve a PC's performance more substantially than adding more RAM.
- **Verify requirements:** New versions of software and upgrades to hardware can make current specifications obsolete. RAM, storage, and power supply issues can creep into an upgraded system.
- **Perform a system file check:** Select Windows+X/PowerShell (Admin). Type **sfc /scannow** (include the space after sfc).
- **Repair Windows:** Rebooting while pressing F11 (on most machines) brings up Windows 10 Advanced Starting Options. Select **Troubleshoot > Advanced Options > Startup Repair**.
- **Run Windows Recovery (WinRE):** Click **Start > Settings > Update & Security > Recovery**. Under Advanced Startup, click **Restart Now**.
- **Perform a System Restore:** Pressing Reboot+F11 (on most machines) brings up Windows 10 Advanced Starting Options. Select **Troubleshoot > Advanced Options > System Restore**.
- **Reimage:** Pressing Reboot+F11 (on most machines) brings up Windows 10 Advanced Starting Options. Select **Troubleshoot > Advanced Options > System Image Recovery**.
- **Roll back updates:** Reboot+F11 (on most machines) brings up Windows 10 Advanced Starting Options. Select

**Troubleshoot > Advanced Options > Uninstall Updates.**

## Rebuild Windows Profiles

User profiles contain desktop backgrounds and files, icons, and other personal data that can bloat a profile and cause it to load slowly when booting. If other profiles load quickly, too much data might be the problem. Manage the profile data by reducing data in the profile or removing it.

### Note

Removing a profile is not possible while working inside it. Instead, you must access a different profile (or create another one, if necessary).

It is possible to delete a profile without deleting a user account. When you have finished deleting a profile, restarting generates a new profile for the user account.

The steps for rebuilding a Windows profile are as follows (refer to [Figure 8-5](#)):

**Step 1.** To delete a user profile, use the Run dialog box or the search tool and enter **sysdm.cpl**. This brings up the System Properties menu shown in [Figure 8-5](#).

**Step 2.** From the System Properties menu, select the **Advanced** tab and then choose **Settings** under User Profiles. The User Profiles information displays, as in the second window of [Figure 8-5](#).

**Step 3.** Select the profile and then click the **Delete** button.

**Step 4.** In the Registry Editor (regedit in the search bar), delete the user profile found at the end of the following path:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ProfileList.

**Step 5.** Reboot.

## Troubleshooting Common PC Security Issues

**220-1102: Objective 3.2:** Given a scenario, troubleshoot common personal computer (PC) security issues.



This section helps you deal with PC security issues, including common symptoms of malware infections and software tools to battle malware. Special attention is given to network connectivity because that is among the most common problems IT technicians face.

### Common Symptoms

Trying to cover every PC security issue you might encounter in the field is a fool's errand. Instead, this section covers the most common PC-related security issues that might appear in an A+ exam question, paying special attention to network access.

Before you do anything else, check connectivity on other devices on the network. If none of the devices can connect, then take these measures.

In Windows 10, a red X icon appears on the taskbar next to the network icon when connectivity issues arise. Sometimes the failure is not the network: The security settings might not allow access to the network.

The first step is to check connectivity on other devices on the network. If only one device is affected, disconnect that device from

its wireless network and then reconnect to it. For a wired network, restart the computer.

Other troubleshooting tasks related to network access are as follows:

- Verify the name of the assigned or desired network. A hotspot might be down, causing problems authenticating to another access point.
- In Windows 10, click the network icon in the taskbar to open the Network Status window. A Troubleshoot button appears there if you are not connected.
- For connection problems with any OS, turn off the broadband modem or access device, wait about a minute, and then turn the modem or device back on. Then turn off the router, wait about a minute, and turn the router on again. If the problem was with the broadband modem or access device, this should solve the problem. If this does not solve the problem, contact the ISP; the problem might be on the ISP network.

[Table 8-3](#) describes other security issues that can arise and suggests approaches for repairing them. Be sure to know these symptoms for the 220-1102 exam.



**Table 8-3** Common Symptoms of PC Security Issues

Symptom	Possible Causes
No access to the network	Internet connectivity problems that do not affect all computers and devices on the network could be caused by malware. Run troubleshooters to repair the problem. If the problem continues to occur, scan the systems.

Symptom	Possible Causes
Desktop alerts	<p>The Notifications and Quick Actions center is easily accessed on the taskbar next to the time and date. Notifications can be edited by going to <b>Settings &gt; System &gt; Notifications and Actions</b>. Options include connectivity, VPN, network, and settings notifications, as well as notifications from apps. OS updates also can be sent here. A regular check of the Notifications and Quick Actions center can help keep small problems from turning into big ones.</p>
False alerts regarding antivirus protection	<p>Security alerts from Windows Defender or from your OS might indicate malware infection or other problems. Sometimes alerts that pop up without any notification in Defender or the Action Center are attempts to infect your system by tricking you into clicking a phishing link in the pop-up. Scan the system.</p> <p>Rogue antivirus programs look like legitimate antivirus programs but actually are designed to infect your system or phish users for personal information. Uninstall any such program and scan the computer.</p>
Altered system or personal files	<p>Malware infections might rename system files (such as msconfig, regedit, and taskmgr) that can help block malware.</p> <p>Files can go missing or be renamed on your storage devices if they are corrupted, infected with malware, unknowingly hidden, or automatically moved by a program without user acknowledgement. Files that have actually disappeared and have not been moved or artificially hidden can often be recovered with</p>

Symptom	Possible Causes
	undeletion software that scans the hard drive for files that are no longer recorded in the file allocation table, the storage device data that tracks where files start and end. Undeleted malware-infected files can reinfect a system if they are not properly cleaned before use.
Unwanted notifications within the OS	Notifications can be easily managed in Windows 10 by going to <b>Settings &gt; System &gt; Notifications &amp; Actions</b> . From this page, you can customize notifications and alerts from Windows and from individual apps that are installed.
OS update failures	A common reason OS updates fail is lack of disk space. Make sure ample free disk space is available; some updates can be quite large. Also make sure that automatic updates are not blocked by antivirus protection settings.

## Browser-Related Symptoms

Often the performance of the preferred browser can indicate problems with malware infection or fraudulent apps on the device. [Table 8-4](#) lists browser issues and their possible causes.

**Table 8-4** Browser-Related Symptoms

Symptom	Possible Causes
Random or frequent pop-ups	If the browser has pop-up blocking enabled but pop-ups are still showing up, the system might be infected with malware. If many pop-ups are displayed onscreen rapidly and they keep showing up even as they are closed, the system is almost

Symptom	Possible Causes
	certainly infected and needs to be scanned immediately.
Certificate warnings	Operating systems and browsers use digital certificates to determine the valid sources of apps and drivers. Certificates that have been obtained fraudulently from a certificate authority can be used to launch malware attacks.
Browser redirection	Browser redirection, also known as browser hijacking, takes place when the home page setting for your browser is changed without your permission. Some free apps offer to change your browser home page during installation, but you can opt in or opt out of the change. If an app changes your browser home page without notifying you, it could be malware. Scan the system.

## Best Practice Procedures for Malware Removal

**220-1102: Objective 3.3:** Given a scenario, use best practice procedures for malware removal.



Removing malware will be a common task for a support technician for the foreseeable future. These steps are best practices to follow each time the task is undertaken.

Follow this seven-step procedure to remove malware—and know it well for the A+ exam:

**Step 1. Investigate and verify malware symptoms.** Use [Table 8-4](#) to identify symptoms.



**Step 2. Quarantine infected systems.** Disconnect the system from wired and wireless networks, and suspect any media that has touched the system as being possibly infected.

**Step 3. Disable System Restore in Windows.** Disable System Restore at this point so that it doesn't run, and create a restore point with infected files before the system is cleaned. Some malware programs use System Restore to reinfect systems. System Restore is designed to help recover from user error or system crashes, not spread malware.

**Step 4. Remediate the infected systems.** Use a different system to change passwords for network access, ecommerce, and social media. Back up data, in case the system must be reformatted. Check the backup for malware before reinstalling it. This process involves the following substeps:

- a. **Updating *anti-malware software*:** To update anti-malware on a quarantined system, download offline update files on a different system, copy them to a USB flash drive, and install the updates on the quarantined system.
- b. **Using scanning and removal techniques (such as **Safe Mode** and the preinstallation environment):** Run scans and remove threats in Safe Mode or WinRE. If a quarantined system's antivirus/anti-malware software cannot be updated, the apps themselves might be infected or blocked by malware. Download the files needed to create a CD or USB bootable anti-malware disc or USB drive on a different system.

**Step 5. Schedule scans and run updates.** Update anti-malware and antivirus software, and run full scans with both. If the infection source is known by name, first use a

specific removal tool (if available) and follow that with full scans. Scan with more than one tool to ensure that the infection has been removed.

**Step 6. When the system is clean, enable System Restore and create a restore point in Windows without copying infected files.** This step simply involves reenabling System Restore and manually creating a clean restore point in Windows.

**Step 7. Educate the end user.** Discuss principles of avoiding malware infections with end users. If the infection vector (the way the virus accessed the computer, such as by email, flash drives, or a downloaded app) is known, discuss it specifically. Also provide general guidance for safe computing (for example, avoiding the use of orphan USB flash drives, not opening attachments from unknown sources, using real-time antivirus software, and scanning systems weekly).

## Troubleshoot Common Mobile OS and Application Issues

**220-1102: Objective 3.4:** Given a scenario, troubleshoot common mobile OS and application issues.



[Table 8-5](#) describes some of the common mobile OS and application issues, along with some likely troubleshooting steps to take.



**Table 8-5** Common Symptoms of Mobile OS and Application

## Issues

Symptom	Troubleshooting Step(s)
App fails to launch	Delete the app and reinstall it.
App fails to close or crashes	Delete the app and reinstall it. Force-stop the app (methods vary by phone or device). Clear the app's cache and data (Settings menu).
App fails to update	If the app pauses during the update, a file might have been corrupted in transit. Delete the app and repeat the download and install procedures.
App is slow to respond	If rebooting does not fix this problem, check the available storage and delete old or unused data. When a phone nears storage capacity, it can lag.
OS fails to update	This is likely a storage issue. Check for space, and make enough room for the update to download and launch.
Battery life issues arise	Many features that run in the background can limit the battery life of a phone or device. For example: <ul style="list-style-type: none"><li>■ Make use of battery optimizing information and settings such as Low Power Mode.</li><li>■ Reduce the brightness of the screen.</li><li>■ Identify apps that use more power, and manage them.</li><li>■ Turn off alert sounds and vibrations.</li></ul>

Symptom	Troubleshooting Step(s)
Phone or device randomly reboots	<ul style="list-style-type: none"> <li>■ Charge the phone or device before it runs out of power. One strategy is to occasionally run the battery down to 10–15 percent capacity and then charge it fully.</li> </ul> <p>Close any apps not in use. Determine whether an installed app is the problem by restarting in Safe Mode, removing the most recent app, and then restarting. If problem persists, repeat for other recent apps.</p>
Screen does not autorotate	<p>Access the control center (with an iPhone, swipe down from the upper-right corner; on an Android device, swipe down from the top). Tap the rotation lock icon to toggle the setting.</p> <p>Also check the Display settings and make sure the display is Standard and not Zoomed; the zoom can prevent the screen from rotating.</p>

## Connectivity Issues

Symptom	Troubleshooting Step(s)
<b>Bluetooth</b>	For both iPhone and Android, the most common solution is to “forget” the device that is failing to pair from the cache.
Wi-Fi	Check that signal strength is good. Sometimes walking away from a strong signal activates cellular data and drops the Wi-Fi connection.

Symptom	Troubleshooting Step(s)
	Verify the networks and authentication. Be aware that crowds at large events can overwhelm Wi-Fi (and cell) data systems.
<b>Near-field communication (NFC)</b>	Make sure NFC is enabled in the Control Center (for iPhone models up to 11—in subsequent models, NFC is always on and no setting is available). NFC is good for only a few inches. To connect, be sure that the reader and the phone are nearly touching.
AirDrop	<i>For iPhone/iPad:</i> Make sure the receiving device is both compatible and discoverable. AirDrop works only when the receiving device is turned on and its screen is awake. AirDrop uses Bluetooth and Wi-Fi; make sure they are enabled. Check that Airplane mode is off.

For all issues in [Table 8-5](#), the first steps are the same:

**Step 1.** Remove accessories and external battery packs.

**Step 2.** Restart the phone or device.

**Step 3.** Update the OS and the apps.

Sometimes OS updates impact the functions of installed apps.

Phones and other mobile devices might operate in many unexpected ways. [Table 8-5](#) describes several problems and their possible solutions.

## Note

These steps assume that the phone or device has been restarted and updated.

# Troubleshoot Common Mobile OS and Application Security Issues

220-1102  
Exam

**220-1102: Objective 3.5:** Given a scenario, troubleshoot common mobile OS and application security issues.

Because of their limited storage, memory, and reliance on wireless and cellular networking, mobile devices are subject to many issues that do not affect more robust devices. The following security issues, which can appear on the exam, reflect the challenges of day-to-day mobile use.

## Security Concerns

Key Topic

As always, security practices are a key topic of the A+ exam. The concerns listed in the following sections are ways in which hackers might try to skirt security settings.

## Android Package (APK) Source

As with any software for a device, a key security practice is to check the reliability of the source for a file before downloading. **Android Package (APK) source** files can be corrupted by hackers and distributed. Unwary users can unwittingly download APK files loaded

with malware or Trojan horses that are ready to install in their Android system.

## Developer Mode

Developer mode is available in Windows 10 and on the Android mobile OS. The purpose of Developer mode is to allow someone developing applications to test the applications. Developer mode in Windows is found in **Settings > Update & Security > For Developers**. On Android devices, it varies by release, but Developer mode is intentionally complicated to keep users from accidentally going into the environment on the phone. Exploring Developer mode is not necessarily dangerous, but the user experience is different in that environment and caution is necessary.

## Root Access/Jailbreak

**Jailbreaking** an iPhone OS means acquiring access to the root files for the purpose of customizing the iOS, adding portability between cell providers, and possibly bypassing paywalls for apps. Jailbreaking is mostly done by hacking hobbyists who like to customize phones.

Although jailbreaking is not illegal, it can provide access to illegal behavior. Still, jailbreaking involves serious risks. Bypassing the manufacturer's secure design adds inherent risks for malware. Additionally, changing code and installing other software will likely cause iOS instability and often voids the manufacturer's warranty.

Android devices are relatively easy to root (that is, to gain root access to) so that users can install different operating systems and continue to use their cellular and data connections. On the other hand, gaining the same sort of access to an iOS device requires jailbreaking it, which means that the device might henceforth be blocked from getting future updates.

Unauthorized **root access** can be dangerous, and it is a risk incurred when users download apps that do not come from Google

Play. These apps do not properly follow the permissions rules and might elevate permissions without the user's knowledge or consent. Running a device in Developer mode (used for software and service development and testing) disables most safeguards. On current versions of Android, several steps are required to enable Developer mode, so this is difficult to do accidentally.

Jailbreaking an iOS device or rooting an Android device puts the device and its information at much higher risk than with a normally functioning device.

## Bootleg/Malicious Application Spoofing

**Application spoofing** occurs when a malicious application imitates a legitimate application and tricks users into revealing passwords or other sensitive information as they interact with the false app. This process is similar to a phishing attack. Application spoofing can be sophisticated and requires that users be ever aware of how they are sharing sensitive information.

Spoofing can also be used to generate extra ads and overrun a user's experience with pop-ups.

## Common Symptoms



The following symptoms should be familiar; many are similar to the PC issues covered in the first section of this chapter. These symptoms indicate problems in PCs and mobile devices that can occur as a result of security issues. When the user experiences these symptoms, it is time to heighten the awareness of security habits, check for updates, and scan for viruses. A few new troubleshooting steps and fixes follow this list:

- High network traffic

- Sluggish response time
- Data usage limit notification
- Limited Internet connectivity
- No Internet connectivity
- High number of ads
- Fake security warnings
- Unexpected application behavior
- Leaked personal files or data

## Slow Data Speeds

Slow data speeds can be caused by a number of factors:

- **No connection to a cellular network:** Check the network indicator at the top of the smartphone or cellular-equipped tablet to determine the network connection type.
- **A weak cellular or Wi-Fi signal:** With Wi-Fi, switch to a stronger SSID signal, if possible. With 4G and 5G, use a cell tower scanner to locate a stronger cell tower.
- **“Unlimited” data plan speed caps after reaching speed or data limits per billing period:** Some providers that offer “unlimited” data plans drastically reduce speed after a certain level of data is transferred during a billing period. Check data usage, and set up a warning to display before you reach this goal. Alternatively, consider switching to a different plan.

## Leaked Personal Files/Data

To prevent personal files or data from being discovered if your mobile device is lost, follow these steps:

**Step 1.** Enable encryption.

**Step 2.** Enable options to lock and wipe your device in case of loss.

**Step 3.** Avoid attaching to open Wi-Fi networks.

**Step 4.** Use a VPN for secure connections if you must use an open Wi-Fi network.

**Step 5.** Disable Wi-Fi tethering or connection sharing services if they are not in use.

## Data Transmission Over Limit

Exceeding the amount of data included in your cellular plan can be expensive. To avoid unexpected bills, periodically check data usage. On Android, go to **Settings > Connections > Data Usage**. Scroll down to see which apps are using the most data. Ensure that Set Data Limit is turned on to set a limit and give you a warning about exceeding the limit.

On iOS, go to **Settings > Cellular > Cellular Data Usage**. Use the sliders to disable any apps that should not be using cellular connections. Turn off cellular data if no data allowance is left in the current period.

If you see unusual amounts of data usage, the device could be infected with malware.

## Tools

Mobile users and techs have a wide variety of software tools available to help boost performance and security, including the following:

- **Anti-malware:** Both Android and iOS devices can be protected with anti-malware apps—some free and some paid—from the same vendors who protect desktop and laptop systems. Every mobile device should be protected, if for no other reason than

that a mobile device can be used as an infection vector for any other device it connects to. Check Google Play and the App Store for anti-malware apps from AVAST, AVG, Kaspersky Labs, Norton, McAfee, Bitdefender, AVIRA, ESET, and many others.

- **App scanner:** App scanners monitor the permissions and use of apps. During the installation process for an app, the user sees a long list of permissions the app is being granted. An app scanner can help determine whether an app is safe to use.

## Factory Reset/Clean Install

Before retiring a device, or to eliminate apps that might put privacy at risk, perform a factory reset on the device. This can be followed by a clean install of desired apps, if necessary.

If the device is not yet encrypted, set up a PIN to automatically encrypt the device.

For Android:

**Step 1.** Make sure Back Up My Data and Automatic Restore are enabled.

**Step 2.** Go to **Settings > Personal > Backup and Reset > Factory Data Reset.**

**Step 3.** Review the warnings and click **Reset Device.**

The device is returned to its factory configuration. All data and device updates are removed from the device. To restore the data to the device, using the data backed up to Google in step 1, follow the steps on the screen.

For iOS:

**Step 1.** Install the latest version of iTunes on your host PC or macOS computer.

**Step 2.** Start iTunes.

**Step 3.** Connect your device to the computer via the charge/sync cable. Trust the device or enter a passcode, if prompted.

**Step 4.** Select your device.

**Step 5.** Back up its contents. Be sure to select **Transfer Purchases** for content purchased from iTunes, back up the Health & Activity data stored on your device in encrypted form, and start your backup.

**Step 6.** To erase the device, go to **Summary > Restore**.

**Step 7.** Tap **Restore** again to erase your device and reload it to its original factory condition.

Before you uninstall a misbehaving iOS app, try updating it.

## Exam Preparation Tasks

As mentioned in the Introduction, you have several choices for exam preparation: the exercises here; [Chapter 10, “Final Preparation”](#); and the exam simulation questions in the Pearson Test Prep practice test software.

## Review All the Key Topics

Review the most important topics in the chapter, noted with the Key Topic icon in the outer margin of the page. [Table 8-6](#) lists these key topics and the page number on which each is found.



**Table 8-6** Key Topics for [Chapter 8](#)

Key Topic Element	Description	Page Number
List	Causes of BSOD Errors	651

<b>Key Topic Element</b>	<b>Description</b>	<b>Page Number</b>
List	Resolving BSOD Errors	652
<a href="#">Table 8-2</a>	Slow/Sluggish System Performance Causes and Solutions	652
<a href="#">Table 8-3</a>	Common Symptoms of PC Security Issues	665
List	Seven-step procedure to remove malware	667
<a href="#">Table 8-5</a>	Common Symptoms of Mobile OS and Application Issues	669
Section	Security Concerns	670
Section	Common Symptoms	672

## Complete the Tables and Lists from Memory

Print a copy of [Appendix C, “Memory Tables”](#) (found online), or at least the section for this chapter, and complete the tables and lists from memory. [Appendix D, “Memory Tables Answer Key,”](#) also online, includes completed tables and lists to check your work.

## Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

[blue screen of death \(BSOD\)](#)

[Safe Mode](#)

[System Restore](#)

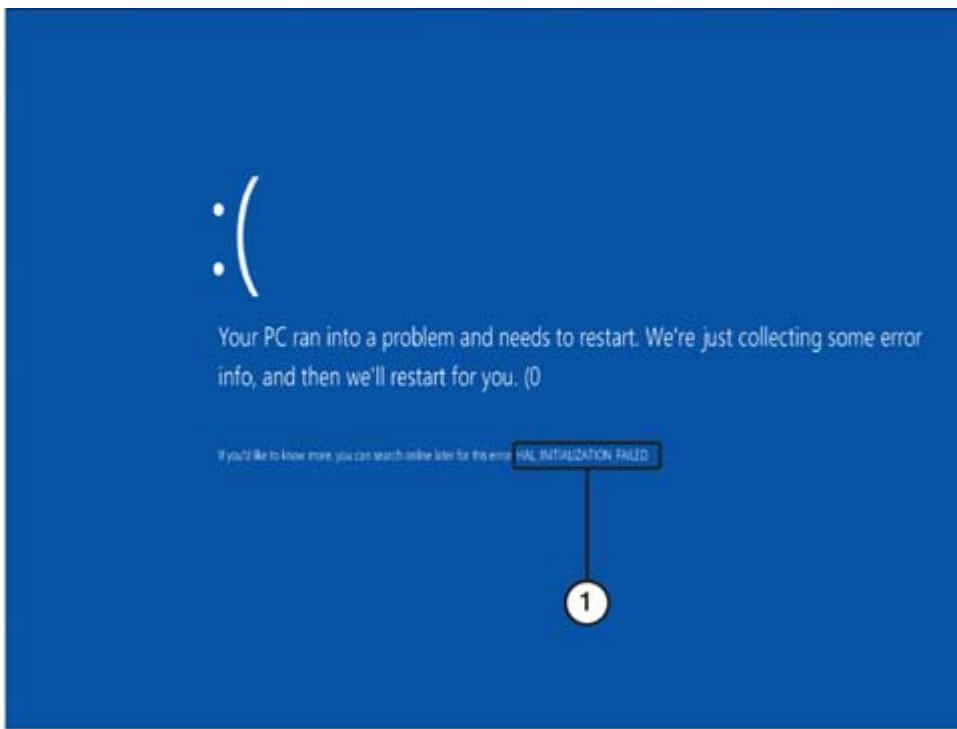
[malware](#)

[anti-malware software](#)

Bluetooth  
near-field communication (NFC)  
Android package (APK) source  
jailbreaking  
root access  
application spoofing

## Answer Review Questions

- 1.** Which operating system is displaying this message?



1. STOP error message
- a. macOS
  - b. Windows 10
  - c. Linux
  - d. Android
- 2.** Why is a lack of free space causing a problem for the system?

- a. The hard drive is running out of space and cannot store any more files.
  - b. At least 10 percent free space is needed for a swap file.
  - c. The hard drive does not have enough free space to upgrade to the latest version of the operating system.
  - d. The applications need more space to run.
- 3. How do you try to repair a missing or corrupt BOOTMGR file on a Windows system?
  - a. Use the System Recovery options.
  - b. Use the Advanced Boot options.
  - c. Reboot the computer and edit the BIOS/UEFI startup program.
  - d. Download a new BOOTMGR file from the Internet.
- 4. Which of the following procedures best describes how to access the Task Manager?
  - a. Press Ctrl+R.
  - b. Press Ctrl+Alt+Delete and then select Task Manager.
  - c. Press Ctrl+R and then select Task Manager.
  - d. Press Alt+F1 and then select Task Manager.
- 5. Which of the following could be causes of poor system performance on a Windows computer? (Choose all that apply.)
  - a. The drive that contains paging and temporary files is nearly full.
  - b. Dust and dirt are restricting airflow, and the CPU is overheating.
  - c. Too many services are configured to start automatically during startup.
  - d. Minimum memory requirements have been met but not exceeded.

- 6.** Put the steps of the malware removal process in order by matching each of the following descriptions to one of the following steps (including the two parts for step 4).

<b>Step</b>	<b>Description</b>
<b>1.</b>	
<b>2.</b>	
<b>3.</b>	
<b>4a.</b>	
<b>4b.</b>	
<b>5.</b>	
<b>6.</b>	
<b>7.</b>	<ul style="list-style-type: none"><li><b>a.</b> Schedule scans and run updates.</li><li><b>b.</b> Disable System Restore (in Windows).</li><li><b>c.</b> Update the anti-malware software.</li><li><b>d.</b> Quarantine the infected systems.</li><li><b>e.</b> Educate the end user.</li><li><b>f.</b> Enable System Restore and create a restore point (in Windows).</li><li><b>g.</b> Investigate and verify malware symptoms.</li><li><b>h.</b> Scan and use removal techniques (Safe Mode, preinstallation environment).</li></ul>

- 7.** In which of the following locations do you find the log files that Windows creates to describe information, warnings, and errors on your system?

- a.** Device Manager
- b.** Event Viewer

- c. Finder
  - d. Recovery Environment
- 8. System Restore is used to do which of the following?
  - a. Restore the system to its original configuration.
  - b. Remove apps that are not from the Microsoft Store and reinstall apps that are from the Microsoft Store.
  - c. Use a system image to restore the computer to its original condition.
  - d. Create a restore point with which to restore the computer to an earlier point in time.
- 9. Which Windows utility is used to disable any programs and services that run when the computer boots?
  - a. regedit
  - b. msconfig
  - c. sfc
  - d. msinfo32
- 10. Which of the following can generate a STOP/BSOD error on a local desktop computer?
  - a. Incompatible/defective hardware
  - b. A virus infection
  - c. Registry configuration problems
  - d. A remote cloud server dropping a connection during a download
- 11. Which of the following is the most common remedy for a mobile device not pairing with a known Bluetooth device in the cache?
  - a. Use encryption on your mobile devices.
  - b. Clear the cache by choosing to “forget” the device.
  - c. Use a VPN whenever possible.

- d.** Disable Wi-Fi tethering.
- 12.** Which of the following problems might occur when you install third-party apps on a mobile device? (Choose all that apply.)

  - a.** Unexpectedly high resource utilization
  - b.** Unauthorized root access
  - c.** Unauthorized location tracking
  - d.** Unauthorized camera or microphone activation

# Chapter 9

## Operational Procedures

**This chapter covers the nine A+ 220-1102 exam objectives related to operational procedures, with a focus on safety, environmental controls, change management, documentation, privacy, and other concepts. Even the best-planned networks experience problems, and an important IT skill is knowing how to recognize trouble and then manage it for minimum network impact. These objectives may comprise 22 percent of the exam questions:**

- **Core 2 (220-1102): Objective 4.1:** Given a scenario, implement best practices associated with documentation and support systems information management.
- **Core 2 (220-1102): Objective 4.2:** Explain basic change-management best practices.
- **Core 2 (220-1102): Objective 4.3:** Given a scenario, implement workstation backup and recovery methods.
- **Core 2 (220-1102): Objective 4.4:** Given a scenario, use common safety procedures.
- **Core 2 (220-1102): Objective 4.5:** Summarize environmental impacts and local environmental controls.
- **Core 2 (220-1102): Objective 4.6:** Explain the importance of prohibited content/activity, and privacy, licensing, and policy concepts.
- **Core 2 (220-1102): Objective 4.7:** Given a scenario, use proper communication techniques and professionalism.

- **Core 2 (220-1102): Objective 4.8:** Identify the basics of scripting.
- **Core 2 (220-1102): Objective 4.9:** Given a scenario, use remote access technologies.

Up to this point, the focus of this book has been the hardware and software technical skills that an A+ certified technician can be expected to have in an IT position. However, a successful employee in the technical field must also be adept at communication and organizational skills. This chapter focuses on these “soft skills” that often make the difference between an adequate technician and a valuable employee. Scripting and use of remote technologies are covered as well.

## **“Do I Know This Already?” Quiz**

The “Do I Know This Already?” quiz allows you to assess whether you need to read the entire chapter. [Table 9-1](#) lists both the major headings in this chapter and the “Do I Know This Already?” quiz questions covering the material in those headings so that you can assess your knowledge of these specific areas. The answers to the “Do I Know This Already?” quiz appear in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes and Review Questions.”

**Table 9-1** “Do I Know This Already?” Section-to-Question Mapping

<b>Foundation Topics Section</b>	<b>Questions</b>
Best Practices and Documentation	1
Change Management	2
Workstation Backup and Recovery Methods	3
Explain Common Safety Procedures	4–7
Environmental Impacts and Appropriate Controls	8

Foundation Topics Section	Questions
Addressing Prohibited Content/Activity and Privacy, Licensing, and Policy Concepts	9–12
Communication Techniques and Professionalism	13
Scripting Basics	14–15
Remote Access Technologies	16

## CAUTION

The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for the purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Jennifer has asked for a document showing the LANs and IP addresses in the building. What kind of document did she request?
  - a. IP address directory
  - b. Logical topology
  - c. Netspace directory
  - d. Physical topology
  
2. Enrique has been asked to attend a meeting to report on how proposed network changes will affect his workgroup. Which term best describes the meeting he will attend?
  - a. Scope impact meeting
  - b. CIO roundtable
  - c. Change management meeting

- d. Disaster prevention meeting
- 3. What concept is addressed with the 3-2-1 rule?
  - a. Network connectivity procedures
  - b. Electrical safety procedures
  - c. Administrative password procedures
  - d. Data backup procedures
- 4. According to building codes, what does every grounded outlet used for computers connect to?
  - a. The neutral circuit in the wiring closet
  - b. A copper pipe buried underground
  - c. The hot wire circuit cutoff
  - d. A UPS in the server room
- 5. Gina was upgrading graphics cards on 10 PCs in a design office. After she removed the old cards, she had to use scissors before installing the new ones. Why would she need scissors in her tech bag?
  - a. To trim the plastic tabs off the power connectors
  - b. To cut “installed on” tags noting the date to mail back to the manufacturer
  - c. To cut the tape on the bubble wrap around the new cards
  - d. To open antistatic bags
- 6. What is the purpose of an ESD strap?
  - a. To equalize potential
  - b. To seal antistatic bags
  - c. To ground PC power supplies while unplugged
  - d. To eliminate electromagnetic interference on the fiber lines
- 7. When a workstation installation creates a tripping hazard, which best practice is not being practiced?

- a. Cable management
  - b. Disaster prevention
  - c. Acceptable use policy
  - d. Self-grounding
- 8. Eric comes across a box containing a chemical in use in the building that has spilled in the main aisle of the warehouse. What should he do before sweeping it up?
  - a. Call 911
  - b. Rope off the area and evacuate the building
  - c. Consult the chemical hot sheet
  - d. Consult the MSDS
- 9. Jacob is upset because he can use a particular app on only three of his four computers. His fourth computer is capable of running it, but he doesn't want to pay more. Which of the following are keeping him from just adding the app to his machine without paying more? (Choose two.)
  - a. DRM
  - b. GDPR
  - c. EULA
  - d. PHI
- 10. Which is not a type of regulated data?
  - a. PCI
  - b. GDPR
  - c. DRM
  - d. PII
- 11. What is the name for a set of procedures that an investigator follows when examining a technology incident?
  - a. Incident response
  - b. AUP

- c. DRM
  - d. EULA
- 12.** Which of the following are examples of appropriately dealing with a customer's confidential and private materials? (Choose two.)
  - a. Mary asks a client to move her handbag away from the work area.
  - b. Bob turns off his cellphone when talking to customers.
  - c. Alexandria is assisting in a doctor's office and asks for insurance files to be removed from the workstation.
  - d. Ali refuses an offer to eat lunch in the discounted employee cafeteria.
- 13.** Which of the following is an example of unprofessionalism in a customer service environment?
  - a. Wearing khaki shorts to work in a bank's IT department
  - b. Asking a customer with an accent to repeat what he or she said
  - c. Using a cellphone to ask a colleague for an opinion
  - d. Clarifying customer statements
- 14.** Which programming language is the file extension .sh associated with?
  - a. Python
  - b. PowerShell
  - c. 3-2-1
  - d. Linux
- 15.** Which of the following creates a secured tunnel over a public network?
  - a. Telnet
  - b. VPN

- c. EULA
  - d. MSDS
- 16.** Which of the following is a proprietary desktop sharing application?
- a. DRM
  - b. RDP
  - c. EULA
  - d. MSDS

## Foundation Topics

### Best Practices and Documentation

220-1102  
Exam

**220-1102: Objective 4.1:** Given a scenario, implement best practices associated with documentation and support systems information management.

A technician must be a good communicator, and one of the most important forms of communication in an IT career is to provide documentation. Any experienced technician can tell stories of how proper documentation could have saved time and money on a job. This section explains how different types of documentation help keep an organization running smoothly long after a technician has left the building.

### Ticketing Systems

Technical support ***ticketing systems*** come in a wide variety of formats. Each business or institution must take care to choose a system that both makes the technical processes run smoothly and

helps the clients, whether customers or coworkers, feel that their needs are addressed and problems are resolved in a professional manner.

Some support systems require taking information over the phone; others require customer initiation online. Each organization must determine what works best in its own environment. This section does not dwell on the best style of support system, but instead looks at seven content areas that are common to most support documentation requests.

## **User Information**

Getting names correct is important, of course, but so is gathering user information about where users work or how they are using the technology being supported. This information informs the support technician on the nature of the problem.

## **Device Information**

Be specific about the device in question. Identifying a specific device or software that is not working will save valuable time if an onsite visit is necessary. The location, ID number, and name of a contact person all are helpful.

## **Description of Problems**

Precise descriptions are essential. Saying that a device "is not working right" is not really helpful. "My network connection is uneven and drops every few minutes" does far more to isolate the problem and identify proper help.

## **Categories**

Provide a list of problem categories for users to choose from, with an Other option at the end. Most users are not aware of the categories

or support specialties the support staff uses, so providing a list is helpful. The following are examples of categories on a support ticket:

- User account support (password, login, and permissions support)
- Network/Internet access
- Slack or email
- Software support (listing names of supported software)

## Severity

Severity helps the support team prioritize tickets so that the most critical issues are supported first. Levels typically look similar to this listing, including brief descriptions of the needed priority to help the client get the proper support:

- **Urgent:** Normal production work has stopped. This often impacts an entire office if an outage has occurred.
- **High:** Some loss of capability to perform normal work tasks.
- **Average:** Inconvenience to workers or customers, but the company is managing to get by at substandard levels.
- **Low:** No impact on the ability to work, but maintenance could be required.

## Escalation Levels

Depending on the size and scope of a support center, different levels (or tiers) of support are offered. Common problems that are fairly easy to resolve are assigned a low level; more complex problems that require special support skills and experience can be escalated to higher levels. The following are the three most common levels:

- **Level 0:** The customer/client can resolve the issue with online tools and documentation. An example is using a utility for password reset.
- **Level 1:** An agent has access to support software and support scripts (predefined steps to help users). An example is starting a script with "Is the machine plugged in and powered on?" and then moving to more technical details.
- **Level 2 (or higher):** Support staff employs specialized skills and usually more experience. Examples are software specialists and network specialists.

## **Clear, Concise, Written Communication**

Written and oral communication skills are also important technical skills. Communicating calmly and helpfully with clients and other support staff is a major part of what makes a good support technician. Clear communication in these areas is essential:

- **Problem description:** This involves getting examples and details on how the problem is manifesting itself to the user.
- **Progress notes:** Multiple people might be trying to resolve an issue, especially if a problem has been escalated. It is essential to make sure everyone is working from the same information.
- **Problem resolution:** This is the hardest communication step. After working to resolve a problem and get the user back to work, technicians often face pressure to move on to the next issue. However, complete documentation of the issue will help support staff recognize future issues with devices or identify areas where training is needed.

## **Asset Management**

Organizations of all types need to be accountable for the money and other resources they spend on technology. The term *asset* is used

because the equipment is often expensive and considered part of the company's value.

*Inventory lists* contain a detailed history of all the hardware and software purchased for company use.

A *database system* tracks the assets in inventory. Depending on the size of the organization, this task can be managed with a small database, such as a simple spreadsheet, all the way to a specialized database, with staff assigned to track the assets for technical, budget, and tax purposes. The database should account for when assets were purchased, how and where they were used, and, eventually, how they were disposed of.

The IT department usually must receive and document equipment with durable asset tags. These tags are typically customized, including the name of the organization along with a barcode and serial number used to create an asset database. They are most often made of a metalized polyester that should last as long as the computer asset is expected to be in use.

An asset tag allows the company to track who is assigned to the device and who is responsible for the equipment. This database is also used to track warranty information and repairs. Using a barcode scanner is the most convenient way to keep track of the equipment while it is in use in the company.

The *procurement lifecycle* describes a method for planning purchases and the expected life of technical assets bought for the company. This is generally done for larger purchases, such as servers, switches, and major software implementations, but not so much for consumables, such as cables and keyboards. The lifecycle can vary widely, depending on the asset. For example, servers might have a life expectancy of a few years before newer technologies necessitate replacement, whereas the infrastructure that holds the server—rack, cooling fans, and battery backups—might have a longer lifecycle expectancy. The IT department is responsible for

documenting the equipment at the end of its usefulness as it goes out of inventory and is sold, donated, or destroyed.

Warranty and licensing need to be tracked as assets because they add value to the equipment. Warranty information can help in planning for the procurement lifecycle, as well as avoid unnecessary purchases of broken machines.

Licensing agreements must be tracked so that users do not fall out of compliance and either lose access to the services provided by the license or become liable for misuse.

As mentioned earlier, tags and databases can be used to track assigned users of assets. It is surprisingly easy to lose track of assets when personnel changes or company reorganizations occur. Assigning users is also a way of assigning responsibility for security of the asset, lessening the chance of theft or misuse of company assets.

## Types of Documents

Several standard documents are essential for an IT department. Documentation of the network infrastructure and addressing, use policy, and compliance procedures are described in the sections that follow.

## Acceptable Use Policy (AUP)

An **acceptable use policy (AUP)**, as it pertains to user safety and security procedures, is designed to keep a network safe from outside intruders. Acceptable use goes even further when it comes to computer best practices within a company. Each organization should define what it considers to be acceptable use of its computing resources within its network. For example, government networks generally are not available for private use, so private email might not be allowed on work computers. Inappropriate use of the Web has

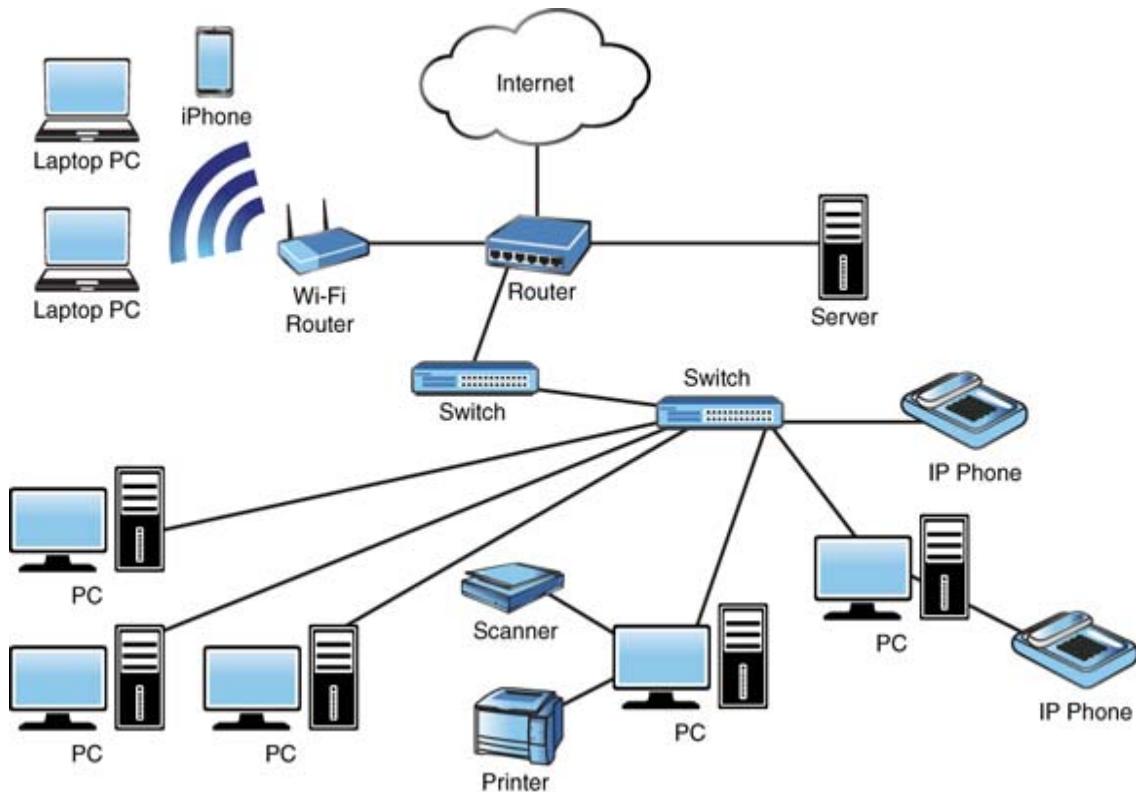
been a problem in workplaces since the Internet became common in business.

For legal protection of the company, acceptable use rules need to be established and then agreed to by users (usually with a signature). An AUP document is often signed during the onboarding process when an employee is hired.

## Network Topology Diagrams

When a technician is called into a building to service a computer or a network of computers, one of the first tasks is to understand how the network is supposed to work. A **network topology diagram** is essentially a map of a network that shows how equipment is physically arranged in the building and logically connected as a network.

A physical topology diagram uses representational icons to depict types of equipment such as laptops, PCs, servers, wireless access points, switches, and routers. It can also show how computers and printers are arranged, as well as the physical cables that connect them together. [Figure 9-1](#) shows an example of a basic physical topology diagram with computers connected on a network.



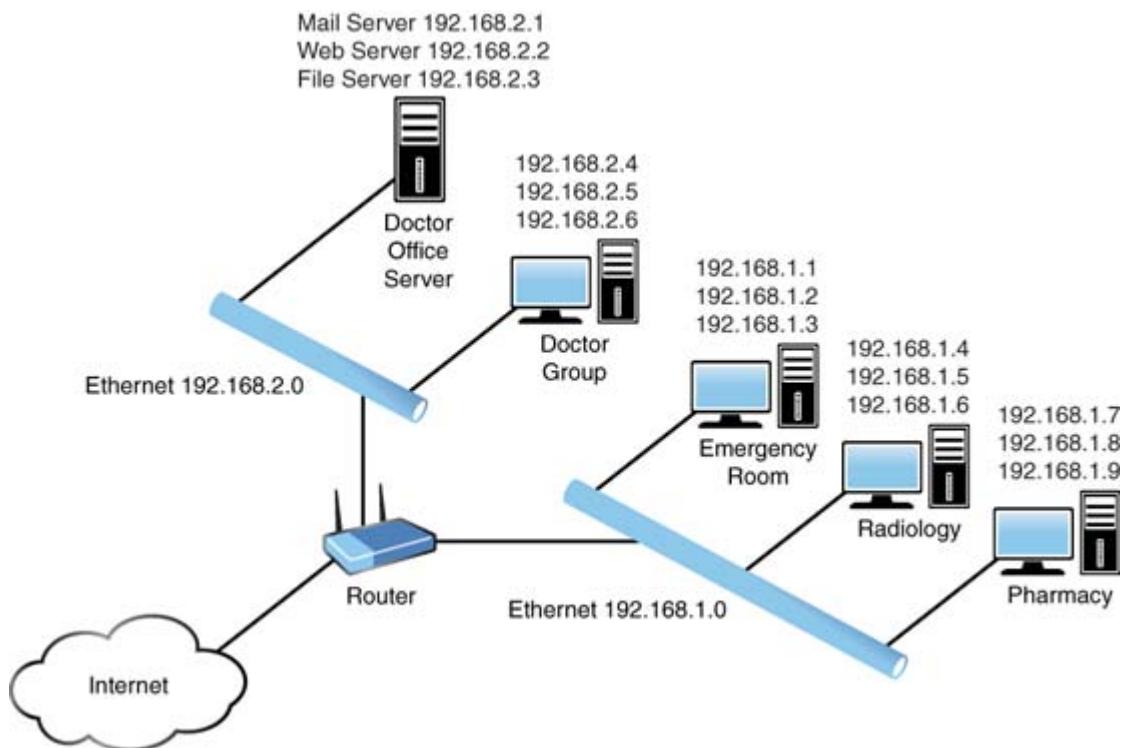
**Figure 9-1** A Physical Topology Diagram

A *physical topology diagram* also maps wireless access ports and wiring closets. The diagram might “zoom in” and depict a single room or floor. Technicians can use a physical topology diagram to find a device they have been called to service. Techs can also use the diagram to see what other equipment, such as printers, security cameras, and switches, are in use and where to find them.

Alternatively, physical topologies might “zoom out” and give the general design of a building, including wiring closets on floors and the point-of-presence (PoP) for connectivity to the ISP. These cut sheets should be posted in secure wiring closets but, for security reasons, not made available to the general public.

A *logical topology diagram* depicts a network’s design, including how computers are grouped together into local area networks (LANs). A logical diagram might include a basic map of wiring closets and general areas of the building, but instead of focusing on computers, this diagram pinpoints network IP addresses. This is beneficial

because troubleshooting Internet connectivity is a major part of the IT workday; knowing which network the devices should be on saves time in troubleshooting. [Figure 9-2](#) shows a logical topology diagram of a medical facility.



**Figure 9-2** A Logical Topology Diagram

## Regulatory and Compliance Policy

Compliance with local government regulations is a necessary part of legal and safe electronics and technology work. Many regulations govern workplaces, and they vary in different areas. For example, electronics recycling is subject to local disposal laws, and privacy concerns for client data are increasingly coming under regulatory scrutiny. Construction codes for electrical and ventilation design are also subject to local rules.

It is important to make all users of technology aware of procedures and then document those procedures. Consider some ways in which this occurs:

- **Splash screens:** These screens display logos or policies that “welcome” a user at startup or login. These might be accompanied by a checkbox requiring the acknowledgment of certain rules before the user can access the company resources.
- **Incident reports:** When a rule or law has been broken, an incident report is necessary so that the company can track its legal responsibilities. This allows the company to plan for training and to comply with laws as necessary.
- **Standard operating procedures (SOP):** Most large organizations have a SOP manual, sometimes known as a policy or employee manual, to document the proper ways a company does business. These are often updated and become the subject of recurrent employee training. Examples of procedures in a SOP follow:
  - Procedures to track licensing for software installations
  - Password policies
  - New user setup checklists
  - End user termination policies

## Knowledge Base and Articles

Reading and research also are technical skills. Being an IT technician means being in a constant state of learning, and a good technician knows how to find answers to unusual problems. Keeping a library of articles and links to helpful resources is essential.

A whitepaper is a type of resource that is common in technical fields. A whitepaper differs from other types of writing, in that it focuses on a complex technical topic and tries to make it understandable to the average reader. Companies often publish whitepapers on new technologies or products they are presenting to the public so that they can influence decision makers. Knowledge bases can also

consist of links to commonly accessed support forums where fellow IT professionals go to seek and give technical support.

The easiest way to access knowledge base articles and whitepapers is to go to the support site for a product or do a search for a topic. An example of a documentation support site is the AWS CloudFormation documentation site, at <https://docs.aws.amazon.com/cloudformation/index.xhtml>.

## Change Management



**220-1102: Objective 4.2:** Explain basic change-management best practices.

Change is a constant force in the field of IT. That force needs to be managed well so that change can improve processes in the organization and avoid potential perils. For example, if a data manager wants to make changes to a loan management software system in a bank, the manager must first make sure that the marketing department, which might rely on the loan data, has software that works with the new system. Otherwise, improving loan management could cause problems for the marketing department.

**Change management** is the process of preparing for and controlling changes in a network, including planning, staffing, organizing, and getting feedback from impacted stakeholders. Change management is studied by IT and business organizations such as the Information Technology Infrastructure Library (ITIL) and ISO/IEC 20000, which produce change process guidelines for their members.

## **Documented Business Processes and Practices**

Knowing how a company performs its many tasks can help create a map of how the change should be implemented. It cannot be assumed that everyone can do without services while the network is down. In addition, tremendous overlap in network use also likely exists. For example, changes to the production end of a business could unintentionally impact other parts. An IT manager might believe that an old server is useless, not realizing that it serves as a backup server for another department.

Even small changes to a network need to have a well-planned implementation. Change management puts planning at the forefront and engages IT people and users from across the organization. It is important that all users of a network be aware of changes that will come and understand, based on detailed analysis, how those changes will impact their functions. For example, a software change made to benefit sales or marketing functions might have an adverse effect on how accounting tracks company expenses. Understanding the full impact of a change across the organization is essential, and that knowledge must be brought to the change board members.

Many parts of an organization use the IT infrastructure in different ways, and it is necessary to have a document that records how it is used. This means creating a record of who uses the network, what parts they use, and how they impact other users.

## **Rollback Plan**

The **rollback plan** (also called a backout plan) is a document that lets the change administrators restore the network to the service level that was present before the change. Sometimes even the best plans can have unintended consequences on a network, or a planned upgrade might fail. When this happens, it is important to have an exact document that tells all the planned steps and logs the configuration codes necessary to get back to normal.

## **Sandbox Testing**

A digital sandbox, such as a virtual machine (VM) environment, is an offline area where changes and ideas can be tested before they are applied to live production networks. By replicating the work environment in a sandbox, any flaws in the change can be identified before implementation.

## **Responsible Staff Member**

One designated person generally coordinates changes with stakeholders throughout the organization. This person, called the change lead, can communicate planned changes to different departments so that they can check for possible impact or problems that could cause unintended consequences to other parts of the network or organization.

## **Change Management**

As previously defined, change management is the process of preparing for and controlling changes in a network, including planning, staffing, organizing, and getting feedback from impacted stakeholders. When changes occur, it is important to record what was changed and how it was accomplished. The change documentation can include a backout plan to implement in case trouble arises at a future date. This document needs to be available for anyone who wants to make further changes to the network. The following sections document some of the finer details of change management.

## **Request Forms**

Departments that want to plan or implement changes in their part of a larger network must submit a form, usually located in the standard operating procedures manual, to the designated person responsible for changes to the overall network. The form should require

descriptions of the proposed change, the costs (both technical and financial), and the benefits of the change. The form can then be used as a basis for communication with other stakeholders in the organization.

## Purpose of the Change

Clarity in purpose is essential for a successful network change or migration. First, knowing the purpose of the project helps limit the scope of change and keeps it from getting larger than necessary. Second, users will be inconvenienced, so they need to be brought into the process to identify issues and help make the change successful.

## Scope the Change

*Scope* refers to the extent of the *impact* of a change. Scope must be determined so that all affected users and managers do not suddenly lose the capability to work when a change is implemented. Scoping a change means creating a detailed plan itemizing processes and settings that will stay the same after the change (for example, application settings needed to perform core functions), hardware or software that will go away, and the changes that have a mixed outcome (meaning some benefit, such as efficiency, but also some drawbacks, such as layoffs of loyal employees).

## Date and Time of the Change

Be sure to announce the date and time of a change well in advance so that others can plan as well. These plans usually call for changes to occur during downtime at night, when the fewest users will be impacted, especially if a system outage is expected.

## Affected Systems/Impact

A key purpose in managing change carefully is to avoid unintended problems for various systems that are in place. For example, choosing the time of a change is important; making a change at the same time a payroll run is being processed could cause problems for not just payroll, but the employees who are depending on timely paychecks. Thus, it is important to identify all systems that will be affected by the changes and to mitigate the impact to their tasks.

## Risk Analysis

Some level of risk is always present when making changes to a network. A goal of change management is to identify the risks and mitigate them. Examples of risks that IT managers plan for include delays, lower-than-expected quality, and use of more resources. When the risks are identified, managers and planners can work to neutralize them.

A change manager might assign a risk level of high-, medium-, and low-risk categories and then manage the team resources according to the potential impact on the organization.

**Risk analysis** is often performed using either qualitative or quantitative analysis methods. A qualitative risk assessment can involve brainstorming, focus groups, surveys, and similar processes to determine asset worth and valuation to the organization. Uncertainty is also estimated, allowing for a relative projection of qualitative risk for each threat. Risk levels can be assigned a numeric value based on their position in a risk matrix/heat map that plots the probability (very low to very high) and impact (very low to very high). Numeric values can be assigned to each state (very low = 1, low = 2, moderate = 3, and so on) to perform a quasi-quantitative analysis, but because the categories are subjectively assigned, the result remains qualitative. A quantitative assessment is less subjective; the process requires assigning a value to all the various

components. To perform a quantitative risk assessment, an estimation of potential losses is calculated.

## Change Board Approvals

The change board (also known as a change advisory board, or CAB) is a group gathered from areas of the organization that will be impacted by the planned changes. The task of the change board is to analyze requests for change (RFCs) and study the benefits and risks of implementing changes. The change manager works under the authority of the change board and gives approval for the manager to proceed with the necessary work to be done. Members of the change board are usually leadership-level employees who understand the impact that requested changes will have on the work in their respective areas.

## End User Acceptance

The end users of the network will be the final arbiters of success or failure in the change migration. Those planning and implementing the change should be informed, but because all users will have a role, they need to be involved, too. Managers might need to schedule training time, and users might have to accept and endure a learning curve. The more ownership they can have in the process, the more likely the users will tolerate the hardship of the process.

## Workstation Backup and Recovery Methods



**220-1102: Objective 4.3:** Given a scenario, implement workstation backup and recovery methods.

Throughout this book, we have mentioned that data is usually the most important asset that a company has to protect. Loss or breach of data can paralyze a company and bring it down. Disasters, by

definition, are sudden and cause great damage. They are often nature driven and cannot be avoided. The best an organization can hope for in planning for a disaster is to have a system that can fail well and provide a reasonable path to recovery.

## Backup and Recovery

Four main types of data backup exist:



- **Full:** A full backup backs up the entire contents of the computer or selected drive to another local or network location. Because every file is copied, this backup takes the longest and uses the most storage.
- **Incremental:** These backups copy only data that has changed since the last backup. If a full backup is performed every Saturday, then an incremental backup could be run each day of the week, recording one day of activity each time. This way, backups are current but a full backup does not have to run each day.
- **Differential:** These backups record changed data since the last full backup. These backups can be done often to ensure that data backups are very current.

A differential backup includes all data that has changed since the last full backup, regardless of whether or when the last differential backup was made, because this backup does not reset the archive bit, a file attribute used to track incremental changes to files for the purpose of the backup. An incremental backup includes all the data that has changed since the last incremental backup. An incremental backup is incomplete for full recovery without a valid full backup and all incremental backups since the last full backup. For example, if the server dies on Thursday, four tapes are needed: the full backup from

Friday and the incremental tapes from Monday, Tuesday, and Wednesday. A full backup copies all selected files and resets the archive bit.

- **Synthetic:** These backups are similar to full backups, except that they are actually reconstructed in software from a full backup in the past and then modified with the incremental backups that have occurred since the full backup. The benefit is reduced storage needs for backup data.

## Backup Testing

Testing backups is important: The worst time to find out that your scheduled backups are not working properly is when they are needed to recover data. Testing backups ensures that the needed data is available when a backup is necessary. It also enables IT staff to practice restoration so that they have this skill in place when it is most needed.

Each organization must determine the necessary frequency of testing. Testing not just data, but also infrastructure such as backup power supplies, is a good plan.

In the days when tape backups were run, testing backups was a time-consuming task. Thanks to cloud storage, network-attached storage (NAS) solutions, and virtualization, the process is much easier today.

## Account Recovery Options

It is easy to lose track of all the accounts people keep in their daily digital lives. As we increase the roles of digital work and recreation in our daily lives with shopping, banking, TV subscriptions, online storage, medical records, and access to networks where we work, the need for accounts and authentication becomes more vital. Losing access to an account can result in anything from a mere

inconvenience that requires a password recovery process, to a full disaster after being cut off from financial or medical services.

Account recovery can take many forms, depending on the account and who is responsible for its safekeeping. No matter who is responsible, smart account holders know how to get out of trouble before trouble occurs. Having a plan in place to recover your digital life if laptops or phones are lost, stolen, or destroyed allows you to recover quickly and keep records secure until the devices are back online.

Most personal accounts from vendors can be recovered in one of several ways:

- Submitting an account email address on the login page and having a password recovery link sent via email
- Having a tech support agent reset an account with a temporary password that must be reset upon login
- Answering secret questions with answers provided during account setup

For example, subscribers to Microsoft online user accounts in Windows can have their accounts shut down if Microsoft sees signs of unusual activity. When an account is disabled, users can sign into their Microsoft account and follow instructions to get a security code. Similarly, a bank might lock down a credit card if it sees unusual purchasing patterns; then either the bank contacts the customer or the account holder must contact a bank agent to verify purchases.

At work, users count on the system administrator to help them get back online. Windows Active Directory and nearly all other enterprise-level server solutions have administrative tools to recover deleted user accounts.

Data is fragile by nature, and many problems can arise, resulting in corrupt or unusable data on a computer or mobile device. Our increasing reliance on data makes backups essential even for home

users. Fortunately, backing up any computing device is easier than ever.

Windows, Linux, and macOS have systems in place to make backing up and, if necessary, restoring data a fairly routine process. Several ways of backing up images are available, including backing up to the cloud, using a backup service, and creating a network-attached storage (NAS) system for a network.

Three levels of data backup exist. They are listed here and described in more detail in the following sections:

- **System image:** Making a copy of an entire disk, including the Windows image
- **File-level backup:** Backing up or archiving files such as documents, reports, and pictures
- **Critical application backup:** Backing up applications needed to restore business after a disaster

## System Image

A system image backup includes everything on the drive, including the operating system (which is the system image). This backup can be used to restore a failed computer if a failure occurs. This is a full backup and is also known as a “snapshot” of everything on a drive at a given time. The time of the snapshot becomes the restore point in the recovery process.

After the OS is installed, the data files are recovered. If backup space is an issue, doing a system image backup might not be the best choice: The OS takes up considerable space, and there is likely already a copy of the OS that can simply be reinstalled. In recent years, however, storage prices have dropped and the OS process for backup has been simplified, so backing up with a system image is a more common choice now. [Chapter 8, “Software Troubleshooting,”](#) details this process.

## File-Level Backup

Files are generally the data saved by users when they use applications. File backups can be documents, media files (such as video or music), and pictures. Keeping just the data takes up less space than backing up the applications as well. As with the OS, most applications can be restored from the original disks or downloaded again; then the files can be recovered. See [Chapter 8](#) for procedural details.

## Critical Applications

Determining what files are considered critical varies depending on the organization, but generally these are the first files that will be restored after a disaster, to get operations up and running again. This can be accomplished with a system image or with virtual machines (VMs) that can be loaded to run quickly.

## Backup Rotation Schemes

It is important to manage and organize data backups in a manner that allows reliable access to current and historical data. To make sure that data is safe and accessible, plan for where and when data will be archived, as explained in the following sections.

## Onsite vs. Offsite Backups



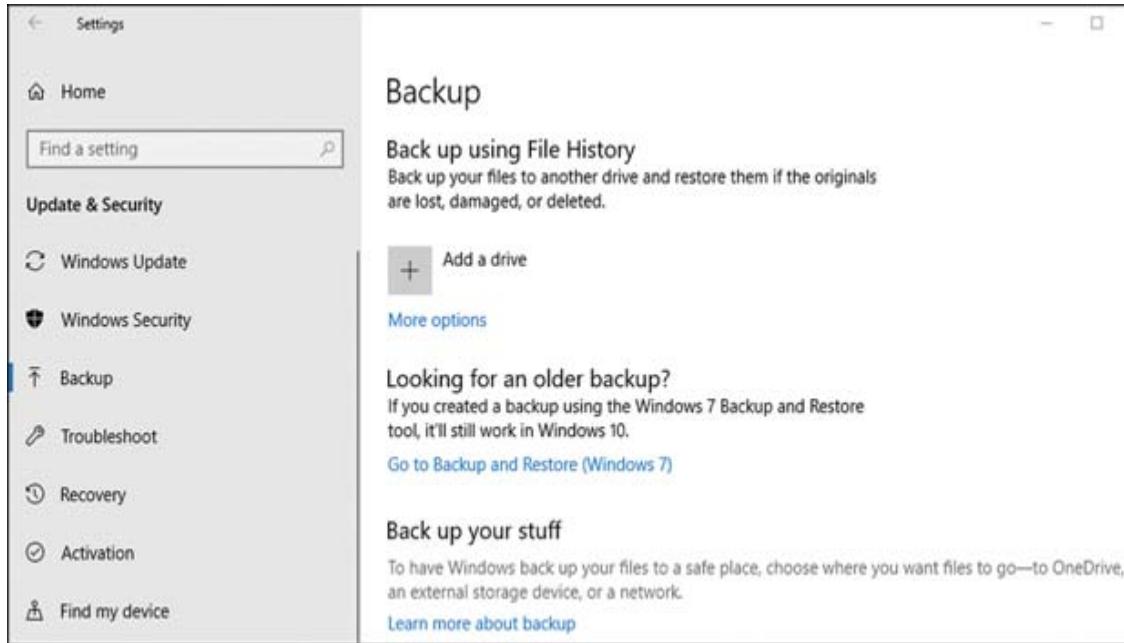
Where data is stored is a vital consideration. Storing it in at least two places prevents a potential data loss due to fire, flood, human error, or system failures. Keeping a copy of backed-up data onsite ensures easy access on a daily basis. Onsite storage can be on servers, stored hard drives, backup tapes, or other storage media.

Keeping a redundant copy of backed-up data offsite guards against a physical disaster wiping out important data. Offsite storage can be in a cloud or could involve backed-up media in another data center far enough away that it is not impacted by the same fires, floods, or storms that could harm the primary data center. Keeping the remote data offline also protects against hacking.

The easiest way to back up data on workstations is to use an external drive (hard drive or USB flash drive) with a redundant backup on the cloud.

For an external drive backup, mount a USB flash drive (or an external hard drive) and drag the files into the drive window. Unmount/eject the USB drive and store the flash drive. Then copy the files to a flash drive for backup.

The Windows Backup and File History utilities and Time Machine in macOS easily back up files and system images to external hard drives. With an external hard drive plugged into a USB port, start the backup utility and select the drive. When the backup is complete, store the drive in a safe, dry environment until the next backup is to be performed. Scheduled backups should be run at times when the system is idle, such as overnight and on weekends. [Figure 9-3](#) shows the first steps of Windows 10 Backup using the File History utility to store or retrieve files.



**Figure 9-3** Windows 10 Backup

macOS includes Time Machine, an automatic backup utility that can create hourly backups for 24 hours and that saves those hourly backups as daily backups and maintains weekly and monthly versions. Go to System Preferences to enable and configure Time Machine:

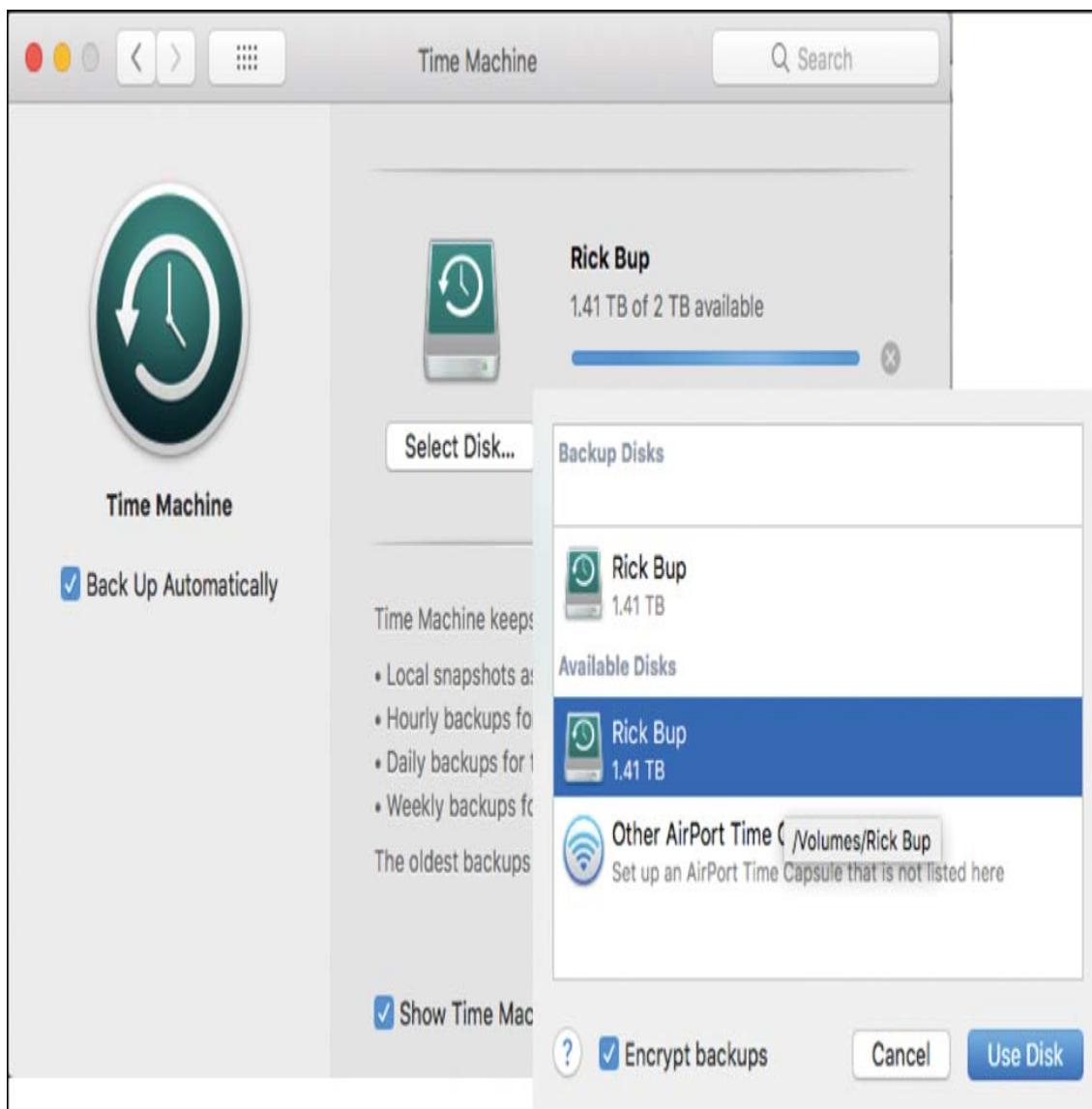
**Step 1.** Connect a suitable external disk to a macOS system (see [Figure 9-4](#)). In this example, Rick Bup is an external drive connected via USB.



**Figure 9-4** macOS Time Machine Backup Utility

**Step 2.** Click **Backup Disk**.

**Step 3.** In the new window that appears, check the **Encrypt Backups** box to protect the backup (see the insert of Figure 9-5).



**Figure 9-5** Selecting and Encrypting an External Disk (Rick Bup) in Time Machine

**Step 4.** Enter a password, confirm it, and enter a password hint. Click **Encrypt Disk**.

**Step 5.** Make sure Time Machine is turned on. After the selected disk is encrypted, the backup starts.

Linux includes several utilities that can be used for backups. These include the command-line tar and rsync utilities. Others, including grsync (which is a GUI for rsync), duplicity (which is available as a

command-line utility and also as a GUI called Deja Dup), are available from the repository for a Linux distribution or from the vendors.

## Note

The BackupYourSystem page on Ubuntu Linux (<https://help.ubuntu.com/community/BackupYourSystem>) provides a large list of command-line and GUI-based backup tools that also work with other Linux distributions.

The process of backing up files or images to the cloud can be managed by a cloud backup service that syncs the drives on a schedule you choose. The following are common names in the increasingly crowded cloud provider arena:

- Amazon Drive
- Dropbox
- Google Drive
- OneDrive app in Windows

These options provide varying levels of storage space, encryption services, and price points. Each has an introductory level for personal use that provides free or discounted storage space and bigger plans for business-level customers.

All of these services mimic a flash drive or external drive by mounting a virtual drive on the desktop for accessing files. As with any other drive window on the computer, files can be copied or moved by simply dragging them to or from the cloud drive window. User data can also be accessed via the provider's web page. [Table 9-2](#) compares the storage of files in the cloud versus local storage.

**Table 9-2** Comparing Cloud vs. Local Storage

Factor	Cloud Storage	Local Storage	Advantage
Media	Web	Tape, CD, USB, hard drives	None
Cost	As-needed subscription	Hardware, utilities, external location costs, and administrative overhead	Cloud
Accessibility	On-demand access to files	Must be physically stored and secured in a separate location	Cloud
Safety	Secure, but requires Web access	Secure when properly handled	None
Flexibility	Capability to back up any computer or file; restores files on demand	Capability to back up only local computers; requires physical access to restore files	Cloud

As you can see from [Table 9-2](#), there are increasing advantages to using the cloud, but the benefits of secure local storage have not completely disappeared. Add to this mix the possibility of internal clouds, and the lines become even less clear. A good backup plan is not restricted to either of these options and instead involves taking advantage of the benefits of each.

## Grandfather-Father-Son (GFS) Backup

## Rotational Scheme

The **grandfather-father-son (GFS)** rotation method describes keeping three different generations, or types of backups, in various places. The name is simply an easy way to remember that full backups (grandfather—perhaps a monthly backup stored redundantly offsite) can be combined with a weekly backup (father—also sent offsite) and a daily incremental backup (son). This scheme is popular because of the minimal use of time and storage for the smaller backups.

Increased use of cloud storage simplifies the process of offsite storage so that storing all three backup types both onsite and offsite can be easily done.

### 3-2-1 Backup Rotational Rule

The **3-2-1 backup rule** or scheme is an easy way to define the practice of keeping backups:

- **3:** Keep one primary copy plus two backup copies of data.
- **2:** Keep two methods of storage for the data (for example, local and cloud).
- **1:** Keep one local backup offsite, in case of fire or storm damage to a facility.

## Explain Common Safety Procedures



**220-1102: Objective 4.4:** Given a scenario, use common safety procedures.

Workplace safety should be the primary concern of every employee at every level in an organization. Most organizations have safety

plans and procedures that directly apply to the work performed by a PC technician. These technicians need to be aware of not only data safety and security but also physical safety. This section covers basic safety procedures common for a PC technician.

Computer safety involves keeping computers safe from failure and keeping technicians safe while working in a dangerous environment. The following concepts are covered in this section:

- Preventing electrostatic discharge
- Working with electricity safely
- Handling toxic waste
- Protecting personal and physical safety

## Equipment Grounding/Proper Power Handling

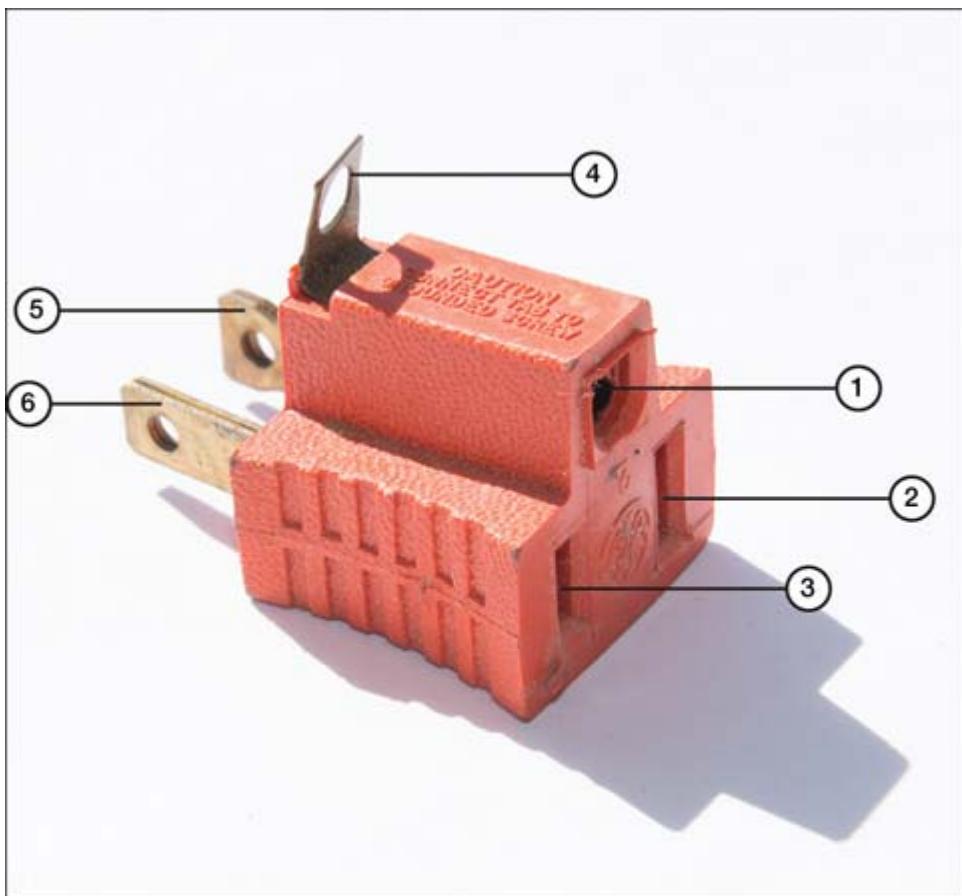


Construction codes require every building with electrical service to be grounded. *Grounding* an electrical system means making a direct connection from the building's electrical service to the earth so that dangerous voltage from line surges and lightning strikes will find its way into the earth instead of injuring people, damaging equipment, or causing a fire. Every grounded outlet in a building has a direct connection to a metal grounding electrode that goes several feet into the earth. Using proper grounding outlets provides an element of safety for both the user and the computer. [Figure 9-6](#) shows a common grounded outlet. Grounded outlets have three prongs in almost all areas of the world.



**Figure 9-6** A Common Grounded Outlet (Image © Jason Kolenda, Shutterstock)

When a grounded outlet is not available, a grounded-to-ungrounded adapter (see [Figure 9-7](#)) can be used for temporary setups if the loop on the adapter can be connected to a working ground (such as a grounding screw or a copper wire wrapped around a metal pipe).

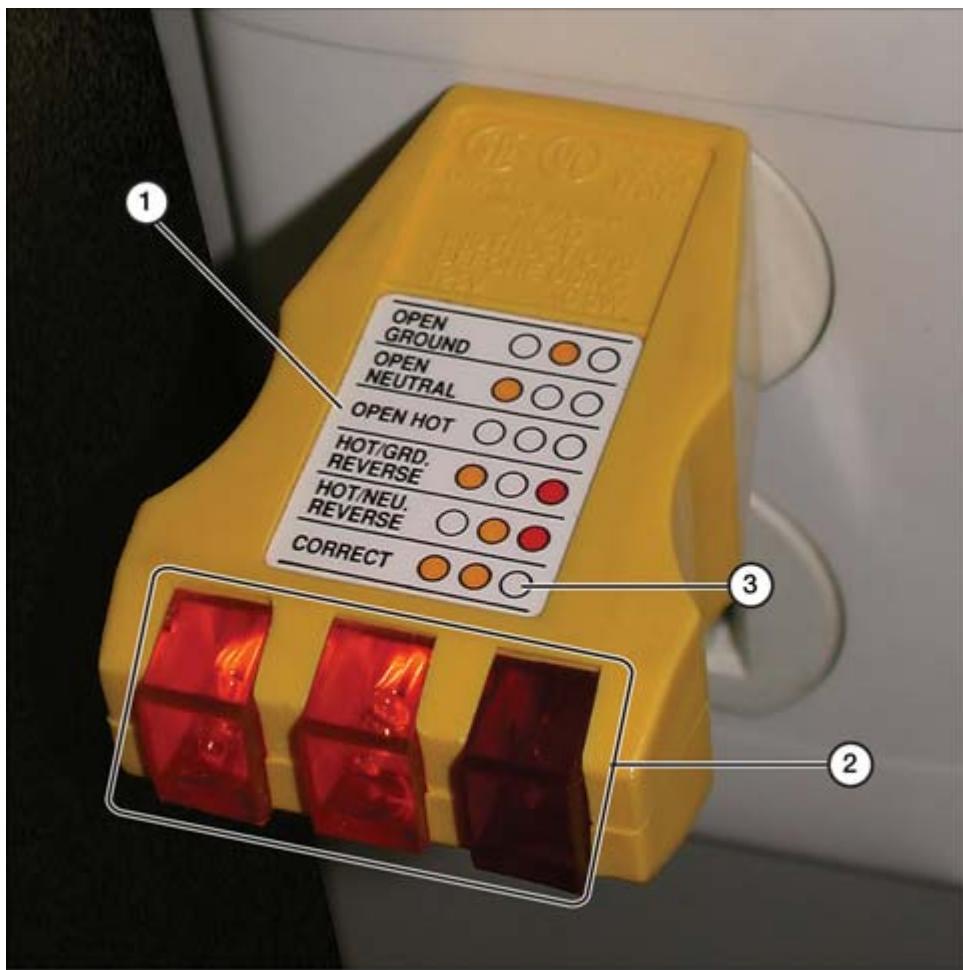


- |                      |                  |
|----------------------|------------------|
| 1. Ground connector  | 4. Ground loop   |
| 2. Neutral connector | 5. Neutral prong |
| 3. Hot connector     | 6. Hot prong     |

**Figure 9-7** Using a Ground Screw or Wire to Provide a Safe Connection for Grounded Equipment

In the United States, grounded 120V AC electrical outlets have been required by code since 1962. Thus, a more likely issue in residential and office environments is the possibility of an improperly installed grounded outlet: one in which the ground line does not connect to a ground.

The easiest way to determine proper building wiring, including grounding, is to use an electrical outlet tester such as the one shown in [Figure 9-8](#).



1. Outlet tester legend
2. Test lights
3. Legend indicates wiring is correct

**Figure 9-8** Using an Electrical Tester to Determine Whether an Outlet Is Properly Wired and Grounded (Earthing)

## Proper Component Handling and Storage

Key Topic

During the building, upgrading, repairing, or teardown of electronic and computer equipment, many potential opportunities arise for equipment to be damaged or destroyed by **electrostatic discharge (ESD)**.

ESD is the silent enemy of computer equipment. ESD might be too low for humans to detect, but it is still strong enough to damage electronic components. The human body constantly builds up static electricity—even when sitting at a desk. Additionally, the drier the atmosphere is, the more easily static electricity builds. [Table 9-3](#) shows the ESD potential at different humidity levels and activities.

**Table 9-3** ESD by Activity and Relative Humidity

<b>Activity</b>	<b>Relative Humidity</b>		
	<b>55%</b>	<b>40%</b>	<b>10%</b>
<b>Normal Activities</b>			
Walking on carpet	7500V	15,000V	35,000V
Walking on vinyl floor	3000V	5000V	12,000V
<b>Workbench Repair and Packing Tasks</b>			
Completing typical worker tasks at an electronics bench	400V	800V	6000V
Removing computer chips from a plastic tube	400V	700V	2000V
Removing computer chips from a vinyl tray	2000V	4000V	11,500V
Removing computer chips from Styrofoam	3500V	5000V	14,500V
Removing a bubble pack from a printed circuit board (motherboard, video card, and so on)	7000V	20,000V	26,500V
Packing motherboards, video cards, or other printed circuit boards in a foam-lined box	5000V	11,000V	21,000V

Equipment can be damaged by ESD of 700V or higher. [Table 9-3](#) demonstrates that even ordinary activities can cause levels of ESD that are dangerous to components. As humidity decreases, the voltage released during ESD climbs.

Without ESD protection, static electricity seeks to discharge to anything else that has a different electric potential—especially metallic items such as circuit boards. Casually picking up an expensive video card can possibly damage it. This damage could cause a complete failure or intermittent issues that are difficult to troubleshoot. Make things easier for yourself by employing antistatic measures at all times. There are four keys to protection:

- Antistatic bags
- ESD straps
- ESD mats
- Self-grounding

## **Antistatic Bags**

When removing a component from a computer, immediately place it in an antistatic bag and put it off to the side (see [Figure 9-9](#)). Parts should never be lying around outside an antistatic bag. Normal bubble wrap bags do not constitute antistatic protection, so be sure to use proper antistatic bags. Some bubble wrap is antistatic and is labeled as such.



1. Antistatic bag
  2. micro PCIe card inside anti-static bag

**Figure 9-9** Using an Antistatic Bag to Protect a microPCIE Wireless Network Adapter

After placing an item in an antistatic bag, place it in a protective box to avoid physical impact damage.

## **ESD Straps**

An ESD strap is designed to equalize the electric potential of the user and the device the strap is clipped to, such as the interior of a computer. Equalizing the electric potential prevents ESD because ESD is the movement of electricity between two objects with different electric potential.

An ESD strap has two pieces:

- An elastic or hook-and-loop strap with a built-in metal snap backed by a metal plate.
- A coiled flexible cable with a matching snap at one end and an alligator clip at the other end. The snap contains a 1-megohm resistor, which can help prevent injury in case of electrical discharge.

To properly use an ESD strap, follow these steps:

**Step 1.** Place the elastic or hook-and-loop strap around one wrist, with the flat metal plate against the skin.

**Step 2.** Adjust the strap until the metal plate stays in place as you move your wrist.

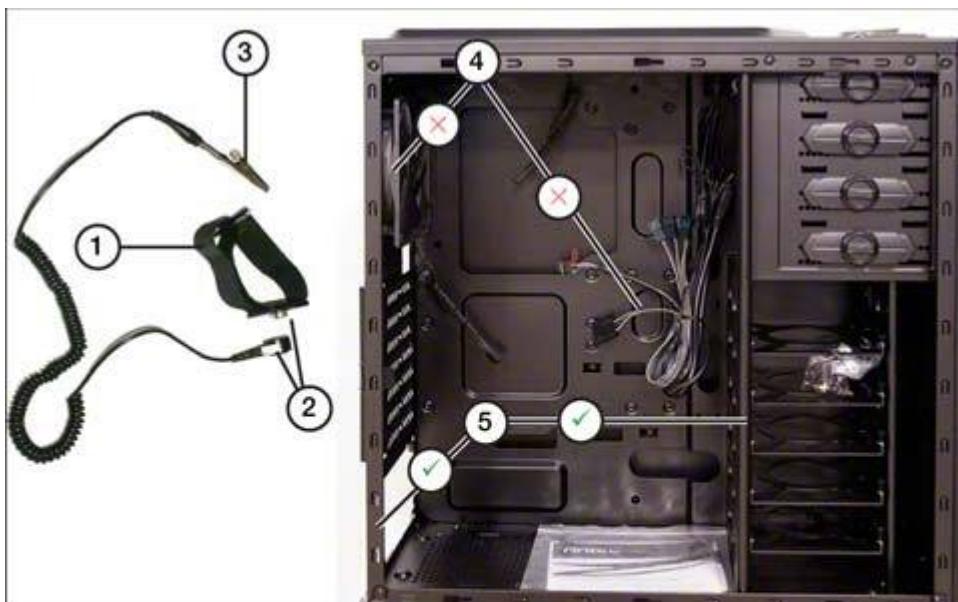
**Step 3.** Snap the cable to the strap around your wrist.

**Step 4.** Open the alligator cable and clamp it to the unpainted metal on the object you are servicing.

The strap around the wrist with the metal plate, snap, and cable equalizes the electrical potential between you and the object you are servicing, to prevent ESD.

[Figure 9-10](#) illustrates a typical ESD strap and suitable locations for attaching it to a computer.





1. Adjustable wrist strap
2. Snap cable to wrist strap
3. Clamp alligator clip to unpainted metal components on the device being serviced
4. Not suitable (plastic fan or coated wires)
5. Suitable (metal chassis frame or drive bay frame)  
Green check (indicates suitable locations for strap)  
Red X (not suitable locations)

**Figure 9-10** Using an ESD Strap to Prevent Damaging ESD When Working on Electronics

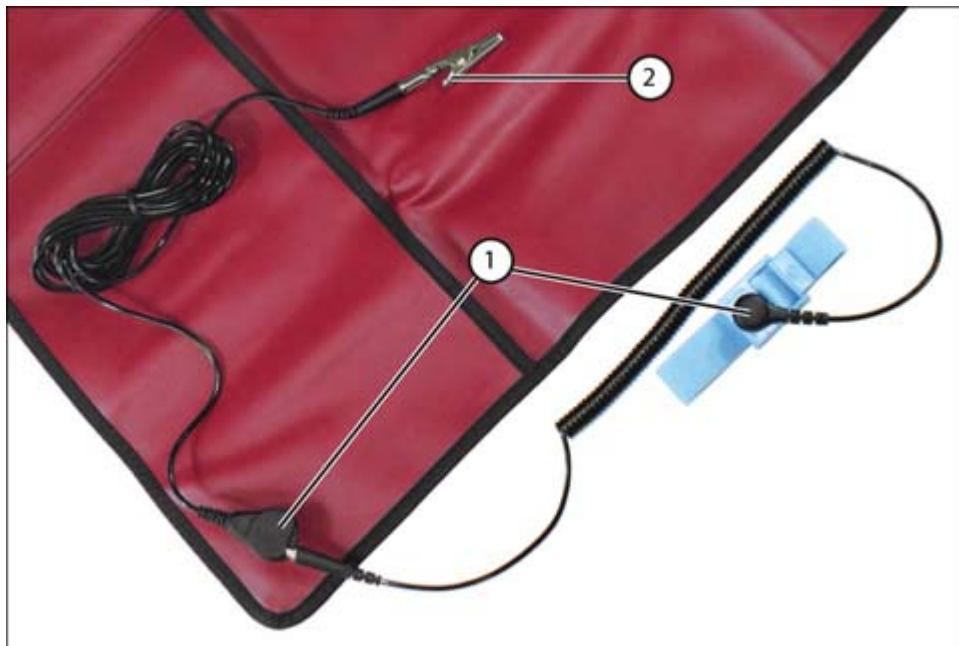
## ESD Mats

The next level of protection for bench repairs and upgrades is to use an ESD mat. An ESD mat can be connected to a device being repaired using one of the following methods:

- A cable with an alligator clip
- A cable with a loop designed to be held in place by a case screw, but with the cable snapped to the mat instead of to your wrist

As with an ESD strap, the end of the cable that snaps to the mat has a 1-megohm resistor built into it.

The ESD mat shown in [Figure 9-11](#) is bundled with an ESD strap. Some versions use antifatigue material suitable for floor use.



1. Resistors built into cables
2. Attach this clip to equipment being serviced

**Figure 9-11** Using an ESD Mat for Additional Protection Against Damaging ESD

## Self-Grounding

In some instances, it might be necessary to work on equipment without any ESD protection. In such cases, self-grounding is a way to protect the equipment being worked on.

Self-grounding involves touching a nearby metal component before touching the device being serviced (for example, touching a metal portion of a chair before picking up a component or opening the device). Before opening a computer, you can self-ground by touching an unpainted portion of the case with both hands before you install or uninstall a component. Do this every time before you touch a component. If no other antistatic options are available, this technique can be used as a last resort.

## Note

Remember to keep the computer unplugged while working inside it. Disconnect the power or turn off the computer using the power switch (if there is one) before you work on the system. You might not know whether the AC outlet is wired properly. By simply disconnecting the power, you eliminate any chance of a shock.

## Other ESD and Safety Precautions to Take

When working with electronics, consider these precautions:

- When handling components or cards, hold them by the edge or bracket. Do not touch the chips, contacts, or other circuitry.
- When handling components, stay stationary. Do not shuffle your feet or move more than necessary while installing or removing the component.
- Remove jewelry and wear protective clothing. In some labs, technicians wear antistatic nylon jumpsuits. For the average person, wearing rubber-soled shoes can also help prevent ESD.
- If possible, work in an area with no carpet. Carpet is perhaps the leading cause of high electrical potential that leads to ESD.
- Avoid using AC-powered tools near a computer. Use battery-powered devices (such as a multimeter) only when necessary.

# **Compliance with Local Government Regulations**

Compliance with local government regulations is a necessary part of legal and safe electronics and technology work. Check with your local municipality for recommended electronics recycling locations that comply with an ISO 14001 certification. Follow regulations for ventilation and other workplace issues as well.



## **Personal Safety**

In this section, we discuss methods for keeping a bench technician safe while working on computer and electronics equipment.

### **Disconnect Power First**

Electricity is a hazard to both computers and humans. Cautiously approach any encounter with electricity. Always be sure to disconnect power before repairing a PC.

### **Remove Jewelry**

Remove jewelry of all kinds (rings, necklaces, earrings, and so on) before working on a computer. Do not allow jewelry to come into contact with any components.

### **Lifting Techniques**

Use safe lifting techniques to avoid injury. When lifting a large or heavy item, stand close to the item, squat down to the item by bending the knees, grasp the item firmly, keep the back straight, and slowly lift with the legs, not the back. Be sure not to twist the body, and keep the item close to the body, to help prevent back injuries.

When moving items, it is best to have them stored at waist level so that minimal lifting is necessary. The Occupational Safety and Health Administration (OSHA) has plenty of guidelines and recommendations for physical safety at the workplace; see [www.osha.gov](http://www.osha.gov).

## **Weight Limitations**

Know your weight limitations, to avoid injury. Incorrectly lifting heavy items can cause many types of injuries. As a general rule, if an item is heavier than one-quarter of your body weight, you should ask someone else to help. Approach a box and move it slightly, to gauge whether help is needed to move it safely. Lifting is among the most common causes of worker injuries.

## **Electrical Fire Safety**

With electrical fire safety, the safest measures are preventive ones. Buildings should be outfitted with smoke detectors and fire extinguishers. The proper type of fire extinguisher for an electrical fire is a Class C extinguisher. CO<sub>2</sub>-based BC fire extinguishers are common and relatively safe to humans, but they can cause damage to computers. If equipment needs to be protected more, an ABC Halotron extinguisher should be used. Server rooms and data centers often are protected by a larger special hazard protection system that uses the FM-200 clean agent system. This clean agent does not cause damage to servers and other expensive equipment and is also safe for humans.

If you see an electrical fire, use the proper extinguisher and attempt to put it out. If the fire is too big for you to handle, dial your country's emergency number (911 in the United States). Then evacuate the building. Afterward, you can notify building management, your supervisor, or other facilities people. If the fire involves a live electrical wire, it should be shut off at the source. Do not attempt this with bare hands, and make sure that your feet are

dry and that you are not standing in any water. Use a wooden stick, board, or rope. If this is not possible, contact the supervisor or building management so they can shut down power at another junction.

If you find an apparently unconscious person underneath a live wire, do not touch the person. Again, attempt to move the live wire with a wooden stick or similar object. Never use anything metal, and do not touch anything metal while you are doing it. After moving the wire, call 911 and immediately contact your superiors. While waiting, attempt to administer first aid to the person.

Always follow company policy and local government regulations for handling emergencies.

## **Cable Management**

Cable management is even more important outside a computer than it is inside. Routing power cables and data cables inside a PC is important for providing good airflow for cooling. However, cables outside the computer can be a trip hazard. Any external USB cables should be routed so that they do not interfere with the normal activity of employees. More important, network cables should be stationary and routed away from walking areas.

Local governments have rules for how networking and telecommunications wires should be installed, and many municipalities require a license to install any of these cables. When running network cables for new computers, first check local regulations and see whether a licensed installer is required for compliance with local government regulations. Make sure that cables do not pose trip hazards and, if possible, are not run near any electrical devices or wires.

## **Safety Goggles**

Wear safety goggles when performing computer repairs, cleaning, or upgrades, to avoid eye injuries from dust, dirt, flyaway screws or bolts, solder, or other threats. The U.S. standard for protective work eyewear is ANSI Z87.1-2010. Eye protectors that meet this standard can be rated for nonimpact or impact (Z87+) applications, so choose according to the risks involved in your specific application.

In other countries, determine the relevant standards for industrial protection when selecting safety goggles.

## **Air Filter Mask**

If a job being performed requires metal machining, buffing, sanding, soldering, waste processing, recycling, or painting as part or all of your technology-related work, an air filter mask might be required for safety.

The U.S. National Institute for Occupational Safety and Health (NIOSH) standards for particulate filtering respirators include the following filter series:

- **N:** Not resistant to oil
- **R:** Resistant to oil
- **P:** Oil proof

The highest ratings available are P100 (99.97 percent efficiency against oil and non-oil particulate aerosols, to meet HEPA standards), R95 (95 percent efficiency against oil and non-oil particulate aerosols), and N95 (95 percent efficiency against non-oil particulate aerosols). Some filters can also block ozone.

Check the particulate hazard types associated with a task before selecting an R-series or N-series filter, or choose a P100 filter. Some masks can accept any of these filter types.

# Environmental Impacts and Appropriate Controls

220-1102  
Exam

**220-1102: Objective 4.5:** Summarize environmental impacts and local environmental controls.

IT equipment is not restricted to climate-controlled data centers, and an IT professional must be aware of how different environments can impact the performance of a computer or network.

For the 220-1102 exam, you need to know how to control temperature and humidity, what an MSDS is and how to use it, and how to deal with dust and debris when it comes to computers.

## Material Safety Data Sheet (MSDS)

Key Topic

A **material safety data sheet (MSDS)** is a document that gives information about particular substances, such as the toner in a laser printer's toner cartridge. Any product that uses chemicals is required to have an MSDS. An MSDS includes the following information:

- Proper treatment if a person comes into contact with or ingests the substance
- How to deal with spills
- How to properly handle and dispose of the substance
- How and where to store the substance

### Note

The term *MSDS* was updated to *SDS* (Safety Data Sheet). Both terms are seen in common use, but SDS is the current standard.

## TIP

MSDS personal protection ratings are designed to inform the consumer of the safe way to handle the material.

The recommendations for ratings A–D are as follows:

- **Rating A:** Safety glasses
- **Rating B:** Safety glasses and gloves
- **Rating C:** Safety glasses, gloves, and apron
- **Rating D:** Face shield, eye protection, gloves, and apron

Most companies have their MSDS documents online. For example, accessing [www.hp.com/us-en/hp-information/sustainable-impact/document-reports.xhtml](http://www.hp.com/us-en/hp-information/sustainable-impact/document-reports.xhtml) and searching for HP MSDS takes you to all the MSDS documents for Hewlett-Packard inkjet cartridges, toner cartridges, cleaners, digital projector and printer lamps, batteries, and so on. MSDS documents are usually in PDF format, so be sure to have Adobe Reader or another PDF reader installed.

Generally, substances that contain chemicals should be stored in a cool, dry place, away from sunlight. “Cool” means at the lower end of the OSHA guideline, about 68 degrees Fahrenheit (20 degrees Celsius). Often this involves a storage closet that sits away from the general work area and outside the air filtration system. Such a closet is also usually less humid than other parts of the building.

As far as disposal goes, any substance with an MSDS should not be thrown away when you are finished with it. It should usually be recycled according to the procedures documented in the MSDS. This recycling can occur by interacting with the local municipality (in the

case of batteries) or by returning items directly to the manufacturer or vendor (in the case of ink/toner cartridges).

Know what to do when someone is adversely affected by a product that contains chemicals. A person might have skin irritation from coming into contact with toner particles or a cleaner that was used on a keyboard or mouse. As a technician, it is your job to find out how to help such a person. If you do not have direct access to the MSDS, contact your organization's facilities department or building management. Perhaps the cleaning crew uses a particular cleaning agent that you are not familiar with, and only the facilities department has been given the MSDS for it. Proactively reviewing all MSDS documents is best, but in this case, you probably won't have access to the document. Collaborate with the facilities department to get the affected person the proper first aid, and, if necessary, take the person to the emergency room. Finally, remove the affected device (if it is a keyboard or mouse, for example) and replace it with a similar device until you can get the original device cleaned properly.



## Toxic Waste Handling/Disposal

The CompTIA A+ certification exam addresses three types of safe handling for computer-related toxic waste:

- Batteries
- Toner
- Other devices and assets, such as CRT displays, cellphones, and tablets

The following sections provide guidance on toxic waste handling.

## Recycling Batteries

Be sure to properly dispose of batteries. Nickel-cadmium (Ni-Cad), nickel-metal hydride (NiMH), and lithium-ion (Li-Ion) batteries for cellphones, computers, and other electronics should not be discarded as trash; neither should lead-acid cells used in UPS battery backup units. If these items are not recycled properly, they will become toxic waste.

These batteries can be safely recycled in several ways, to avoid environmental threats:



- For small numbers of rechargeable batteries or devices that contain rechargeable batteries, use a recycling drop-off station (such as a drop-off station at an electronics retailer).
- For large numbers of rechargeable batteries, devices, or UPS devices with batteries, contact an electronics recycler in your area.
- Some batteries can be returned directly to the manufacturer for recycling.
- During storage and transport, make sure battery contacts are prevented from touching each other. Check and follow regulations regarding the shipment of Li-Ion batteries, which pose a potentially high fire and explosion hazard in some environments.

## Toner

Toner bottles and cartridges for laser printers and copiers should be recycled instead of discarded. Unlike with batteries, users can earn money or credits toward additional purchases by recycling toner bottles and cartridge products at local office supply stores or toner

recycling shops. Although inkjet cartridges are not recognized as toxic waste, they also should not be discarded; they can be turned in for credit at office supply stores or inkjet cartridge remanufacturers. Some manufacturers include a prepaid label in the box containing the ink, for easy returns.

After removing the old toner cartridge, use a specially designed toner vacuum to remove loose toner from inside the printer before inserting the new cartridge.

## **Cellphones and Tablets**

As mentioned previously, batteries for cellphones and tablets should be recycled. But before you dispose of these devices, be sure that any personal or company data is safely deleted and the SIM card is removed. Data to check for includes contacts, messages, downloads, pictures, and voicemails. Browser data should be cleared as well.

## **Temperature and Humidity Level Awareness and Proper Ventilation**

You should be aware of the temperature and humidity measurements in your building. You also should be thinking about airborne particles and proper ventilation. Collectively, OSHA refers to this as air treatment. Air treatment involves removing air contaminants and controlling both room temperature and humidity. Although no specific government policy covers this, recommendations suggest a temperature range of 68–76 degrees Fahrenheit (20–24 degrees Celsius) and a humidity range of between 20 percent and 60 percent. Remember that a higher humidity level means a lower chance of ESD, but conditions might get a bit uncomfortable for workers; a compromise must be sought. If the organization uses air handlers to heat, cool, and move the air, it will be somewhat difficult to keep the humidity much higher than 25–30 percent.

## **Proper Ventilation**

An organization should use local exhaust (to remove contaminants generated by the organization's processes) and introduce an adequate supply of fresh outdoor air through natural or mechanical ventilation. For air treatment, organizations should use filtration devices, electronic cleaners, and possibly chemical treatments activated with charcoal or other sorbents (that is, materials used to absorb unwanted gases). Most filtration systems use charcoal and HEPA filters. These filters should be replaced at regular intervals. Air ducts and dampers should be cleaned regularly, and ductwork insulation should be inspected periodically.

If a considerable level of airborne particles remains, portable air filtration enclosures can be purchased that also use charcoal and HEPA air filters or that possibly utilize ultraviolet light to eliminate particles. These enclosures are commonly found in computer repair facilities because of the amount of dust and debris sitting in computers that are awaiting repairs. Some organizations even provide masks or respirators for their employees.

## **Compressed Air and Vacuum Systems**

A PC workbench can be equipped with a compressed air system and vacuum system. This way, the PC tech can blow out the dust and dirt from a computer while, at the same time, vacuuming it. Otherwise, the best approach is generally to take the computer outside when cleaning it.

## **Power Surges, Under-voltage Events, and Power Failures**

Reliable power delivery at a consistent level is essential in protecting electronic equipment such as computers and televisions. Even in communities with quality power delivery, power surges and sags endanger computers. An electrical outlet might be properly wired

(see the section “Equipment Grounding,” earlier in this chapter), but other threats can affect the well-being of computers or other devices connected to the outlet:

- Power surges
- Under-voltage events
- Power failures

## Surge Suppressors

A surge suppressor is designed to block power surges from damaging the equipment plugged into it. **Power surges** are defined as overvoltage events that last no more than 50ms and that can reach voltage levels as high as 6000V and 3000A.

Surge suppressors are rated in joules to indicate the amount of energy a surge suppressor can absorb before failing. All other factors being equal, the higher the joule rating, the better. However, keep in mind that a unit with multiple metal-oxide varistors (MOVs) on each power lead might provide better protection than a single large MOV.

MOVs absorb power surges and gradually wear out. Although many (but not all) surge suppressors have lights that indicate when protection has failed, only a few models stop providing power if protection fails.

Pay attention to how many computers are connected to a surge suppressor. Add the combined wattage or volt-amp ratings of the devices to be plugged into the surge suppressor, and compare that to the maximum that the surge suppressor can support. Usually, a surge suppressor can handle two basic computers and two monitors. However, a high-powered device such as a laser printer should get its own surge suppressor.

Surge suppressors should be replaced every three to five years, or right after an event that damages the MOVs, such as a nearby

lightning strike, frequent power flickers, burn marks, or smoke in any outlet on the unit.

## Battery Backup Units



Power failures (total loss of power) and under-voltage events (sustained voltage drops of as much as half the rated output) stop computers and peripherals from working. Unfortunately, if computers and peripherals lose power in the middle of backups, updates, or reports, files can be corrupted. The solution is to use a battery backup uninterruptible power supply (UPS).

Battery backup units are rated in two ways: volt-amps (VA) and Watts (W). Different battery backup units with the same wattage rating can vary in terms of the VA rating. However, the usual calculation for comparing the W and VA ratings is to assume that  $VA \times .60 = W$ . Thus, a UPS with a 1000VA rating provides about 600W of power.

In addition to providing enough power to run connected devices (such as a computer, a display, and USB devices, but not a laser printer), a UPS needs to be able to run on battery an appropriate amount of time before the UPS shuts it down. This is called the runtime. Some vendors and third-party websites (for example, [www.easycalculation.com/physics/classical-physics/ups-power-requirement.php](http://www.easycalculation.com/physics/classical-physics/ups-power-requirement.php)) provide calculators that use input watts or amperage draws to calculate the UPS size needed. To increase runtime, select a unit with a larger VA or W rating.

### Note

Do not use the battery-backed outlets on a UPS for devices such as laser printers. These power-hungry devices can quickly drain

the UPS battery or damage the unit. For such devices, use the surge-suppressed outlets that are not connected to the battery.

[Table 9-4](#) provides a quick review of what the 220-1102 exam requires you to know about dealing with power surges, blackouts, and brownouts.



**Table 9-4** Electrical Conditions and Protective Measures

Type of Electrical Condition	Description	Protective Measure
Power surge	Overvoltage event lasting less than 50ms. Up to 6000V and 3000A.	Surge suppressor
Under-voltage event	Sustained voltage drop of up to half the normal voltage. Can last for minutes to hours.	UPS
Power failure	Total loss of power for an extended period of time.	UPS or generator

## **Addressing Prohibited Content/Activity and Privacy, Licensing, and Policy Concepts**



**220-1102: Objective 4.6:** Explain the importance of prohibited content/activity, and privacy, licensing, and policy concepts.

Network administrators face several challenges in keeping a network safe and secure. Although many tools and procedures are used to

prevent misuse of resources, security incidents are bound to happen. Not all of them come from outside the network. In fact, some of the most perilous threats come from users inside the organization who violate security rules or rules of acceptable use.

Managing user content, activity, and privacy is challenging because users and managers do not all understand these concepts in the same way. An organization must create a well-defined policy that spells out what is and is not acceptable use and practice. The policy also must define the consequences of not complying with the organization's standards while using its equipment. This section details the process of responding to violation incidents.

For the sake of studying the incident response process, prohibited content and activity can be defined as follows:

- Any content stored on a company-owned or company-managed computer, mobile device, or network that is contrary to organizational policy
- Any activity performed or received by a company-owned or company-managed computer, mobile device, or network that is contrary to organizational policy

When someone has been found to have acted inappropriately, having a response and process in place protects both the organization and the users.



## Incident Response

Incident response is the set of procedures that any investigator follows when examining a technology incident. The initial response and documentation are important because the information and evidence gathered guides the rest of the process.

## First Response

When an incident is reported, the responder's first task is to identify exactly what happened. The responder must first *identify* whether this is a simple problem that requires troubleshooting or an incident that needs to be escalated. The key to any problem solving is understanding what problem needs to be resolved.

For example, if a person has prohibited content on a computer, this can be considered an incident. As part of first response, the incident should be escalated to the violator's supervisor, with reporting on exactly what was found. Copyrighted information, malware, inappropriate content, and stolen information can all be considered prohibited.

After identifying the problem, the incident must be *reported through proper channels*. Reporting through proper channels might include law enforcement if the incident involves fraud or the security of private customer information. Then steps must be taken to ensure *data/device preservation*. This often means making a backup of the computer's image using special software to ensure data integrity and preservation. However, depending on the organization's policies, a better approach could be to leave everything as is and wait for a computer forensics expert or a security analyst. It is important to preserve the scene so that a specialist can collect evidence.

## Documentation

Documenting everything that is found and anything that happens after the initial report is essential. If the organization does not have set reporting formats, then writing down the details and taking pictures is appropriate. Any and all information should be available to the supervisor. If the first responder is able to fix the problem and no other specialists are required, the *documentation process* can continue through to the completion of the task (and beyond, while monitoring the system). Documentation should include any

processes, procedures, and user training that might be necessary to avoid a similar incident in the future.

## Chain of Custody

If preserving evidence is required, one way of doing this is to set up a **chain of custody**, the chronological documentation or paper trail of evidence. It should be initiated at the start of any investigation and should include tracking the evidence/documenting process; identifying who had custody of the evidence, all the way up to litigation (if necessary); and verifying that the evidence has not been modified or tampered with.

### Note

A PC tech normally does not get too involved with investigations, but the A+ exam covers the basic concepts of incident/first response, documentation, and chain of custody.



## Licensing/Digital Rights Management (DRM)/End-User License Agreement (EULA)

All types of software licensing issues can complicate your life as a PC tech. It's important to realize that carelessness with licensing could put your company in financial and legal jeopardy.

The following are some issues to watch out for:

- The limitations created by digital rights management (DRM)
- End-user license agreements (EULAs)
- Open source vs. commercial licenses

- Personal vs. enterprise licenses

## DRM

**Digital rights management (DRM)** is the general term for software or service mechanisms that limit the end user's rights to copy, transfer, or use software or digital media. The following are some examples of DRM:

- Restrictions on digital music playback when the music has been burned to an audio CD, such as with Apple Music
- Limits on the number of systems that can use an application at the same time, such as Adobe Creative Cloud or Microsoft Office 365

When upgrading a system that is running DRM-based apps, it is important to determine in advance how the upgrade might affect DRM issues. In some cases, moving to a new OS might be transparent to the DRM system; in other cases, the DRM system might require the user to confirm the license.

When removing from service a system that is running DRM-based apps, it is important to determine in advance how to properly move the DRM-based apps or DRM-limited files to another system. Authorization might need to be removed from the system before a new system can be authorized to use the app.

## EULA

An **end-user license agreement (EULA)** restricts how an app can be used and what transfer rights are available. If an app was preinstalled on a system, its licensing might not allow the app to be moved to another system. Be sure to check the EULA for a particular app or for an operating system with bundled apps to determine what can legally be done with the operating system and apps when the

original computer is withdrawn from service or upgraded to a new operating system.

## **Understanding Open Source and Commercial Licenses**

According to the Open Source Initiative website (<https://opensource.org/osd>):

Generally, open-source software is software that can be freely accessed, used, changed, and shared (in modified or unmodified form) by anyone. Open source software is made by many people, and distributed under licenses that comply with The Open Source Definition.

Linux operating system distributions (known as *distros*) and Linux apps are some of the most well-known examples of open source software.

Open-source software can be used for commercial purposes and can even be sold. However, **open-source licenses** require the sellers of open source software to not limit the rights of purchasers to use, change, or share the software. For example, the rights obtained when Company A starts using Software X must be passed on to Company B when Company A sells any version of Software X, and so on. These rights include source code.

### **Note**

The Open Source Initiative website offers a variety of OSI-approved licenses that can be used as models for licensing; see <https://opensource.org/licenses>.

Most commercial software other than open source can be called closed source. For example, Microsoft Windows, Apple macOS,

Adobe Creative Cloud, and Microsoft Office are examples of operating systems and apps that use commercial licenses. Unlike an open source license, which permits free use, modification, and sharing of source code, commercial licenses do not cover source code (the actual instructions used to make the software). They also limit how licensees can use object code (the program). For example, Adobe Creative Cloud subscriptions can be used on two computers (for example, a work and a home or travel computer), but not at the same time. If a third computer has Adobe Creative Cloud installed, Adobe permits Creative Cloud apps to run on the additional device if the other computers' licenses are deactivated by Creative Cloud.

## Personal vs. Enterprise Licenses

**Personal use licenses** are software licenses provided for computers purchased at retail or online stores and downloaded or packaged apps designed for use by individuals. Essentially, these licenses limit the use of the software to one or a very small number of computers in the same household (for example, antivirus utilities designed for up to five Windows, macOS, or mobile devices).

**Corporate use licenses** can differ from personal software licenses in several ways:

- Software covered by enterprise licenses includes management and security features designed for the enterprise.
- Software covered by enterprise licenses have much different rules for software upgrades than personal-licensed software.
- Software covered by enterprise licenses can be licensed per seat, per device, per processor, or in other ways.
- Some personal software licenses, such as for Microsoft Office Home and Student, are specifically restricted from being used in business.

The company can face serious fines if software licensing terms are not followed. A supervisor should be notified if a technician is asked to violate the terms of a license.

## Valid Licenses and Non-expired Licenses

A *valid license* means that the user has agreed to the software developer's terms of use. This is also known as *subscription-based licensing*. These terms can include a recurring payment agreement based on time or the number of users. The agreement should also detail how software will become unusable if the subscription is not renewed.

An alternative to subscription licensing is a *non-expiring license*, also known as a *perpetual* license. This simple license grants the user ongoing permission to an application, with no expiration date.

## Regulated Data

Four types of data are regulated and must be protected by network administrators. They are listed with the acronym first because that is how they are referred to in the field:



- **PII:** Personally identifiable information, such as a person's name, address, driver's license number, credit card numbers, and social security number
- **PCI:** Payment Card Industry standards that are in place to protect credit cardholders' data, including card numbers and address and credit information
- **GDPR:** General Data Protection Regulation, enacted in Europe to protect several types of data, including health, biometrics, genetics, and criminal history

- **PHI:** Protected health information (a part of the HIPAA law), which covers health status as well as payment methods, account numbers, and beneficiaries

Any organization that holds or uses this type of information is responsible for protecting it from identity thieves. Many serious (and very expensive) data breach cases have happened in recent history, and some of them have had crippling effects on the companies that lost data. A computer technician's role in protecting data includes the following:

- Configuring systems to use secure cloud storage instead of locally stored sensitive information on laptops and mobile devices
- Configuring and using strong encryption on wireless networks and point-of-sale (POS) systems
- Using full-disk encryption such as BitLocker, BitLocker To Go, or similar products on laptops and mobile devices that store or access sensitive data
- Configuring hardware and software firewalls to protect sensitive data
- Educating users on methods to remove personally identifiable information from documents, photos, and other files that might be shared or posted online

Of course, it is important to protect users and the organization by keeping up with recent developments in both knowledge and application of these policies and best practices. Understanding them is necessary for the A+ exam.

## Communication Techniques and Professionalism



**220-1102: Objective 4.7:** Given a scenario, use proper communication techniques and professionalism.

Of all the technical skills PC support technicians should have in their toolkit, strong communication skills are among the most enduring and vital. No matter what version of software or generation of hardware is in use, effective written and oral communication is needed to identify and document issues and to train users in how to function in their technical environment. Employers consistently rank communication as the most desirable “soft skill” (as opposed to hard technical skill) they look for when hiring new employees. This section highlights aspects of communication and professionalism expected of a PC support technician.

## Professional Appearance and Attire

IT support technicians project the image of their organization when they are called upon to support a client, whether that client is a customer or a fellow employee. Every organization has its own culture, and expectations of appearance (beards, hair, tattoos, and so on) can vary quite a bit. It is important to be aware of this even more when visiting clients outside the organization.

Attire, or clothing choice, is also part of an organization’s culture. The main point to keep in mind with clothing choice is that it reflects respect for the environment you will be working in more than it involves personal comfort or fashion statements.

Some employers opt to give technicians some sort of uniform so that they can be easily recognized. Other companies simply offer guidelines, such as the following:

- **Formal:** This means dress slacks, dress shirt, and a tie. This attire is most often required when supporting institutions that

have the same expectations for all employees, such as government or financial institutions.

- **Business casual:** This term is a bit less defined and varies by region. It most often means corduroy or khaki-type pants (not blue jeans), or perhaps clean and untorn jeans with a collared shirt. The employer should set these expectations early in the hiring process, but if they are unclear, techs should err on the safe side: Dressing up is always better than dressing down when working with others.

## **Use Proper Language and Avoid Jargon, Acronyms, and Slang When Applicable**

Using proper language is one way to instill confidence in the people you are trying to help. Proper language is whatever is customary and professional in your work environment. Cursing and swearing are never considered acceptable, even if some people at work speak this way. Speak clearly and in a simple, concise, and respectful manner.

Use proper English and avoid slang. Also avoid computer jargon and acronyms, such as WPA3 or TCP/IP, that might confuse the customer.

## **Maintain a Positive Attitude/Project Confidence**

Customers watch technicians while they work on their problems, and they can lose confidence when the tech sounds or looks worried. Similarly, a bad service tech projects arrogance by rejecting or brushing aside questions and comments; a good one maintains an attitude that the problem will be solved. A customer is reassured when a technician is confident that the right tools and resources will solve the problem.

## **Actively Listen, Take Notes, and Avoid Interrupting the Customer**

The key to getting information from a customer is *active listening*, a conversational skill that includes making eye contact, taking notes, and encouraging open-ended answers without interrupting. Listen carefully to what someone has to say about a problem he or she is experiencing. What the person says might provide clues about the reason for the problem. Even when a customer admits to being a nontechnical person or even a technophobe, listen carefully.

## **Be Culturally Sensitive**

Nations, organizations, and departments all have cultures—ways of communicating, rituals to follow, and definitions of good manners. Cultural sensitivity helps prevent barriers to good communications. Be sure to use the appropriate honorific titles (Mr., Ms., Mrs., and so on), pick up on visual and verbal cues, and use professional titles when applicable (doctor, professor, and so on). When a person has an accent and is hard to understand, concentrate and ask the person to repeat anything that you do not understand.

## **Be on Time**

Punctuality is probably the most important ingredient in customer relationships. If you have to be late, contact the customer. Also consider contacting your supervisor, depending on how late you are. Clients always highly value reliability.

## **Avoid Distractions**

Don't let your cellphone, an event on TV, or the view out the corner office window get between you and a solution. Avoid distractions and interruptions when talking with customers. Stay focused on what your customer is telling you, and the solution will be easier to

find. Don't talk with other coworkers while interacting with customers. Don't use social media sites or use text messaging for non-work-related issues; when you send a text to ask for help, make sure your customer knows why you are sending a text. Avoid personal interruptions except in an emergency. Respect the customer's time, and save personal calls for breaks or when the job is finished. Customers usually pay by the hour, and they deserve every minute of your attention.

## **Dealing with Difficult Customers or Situations**

Solving technology problems is difficult, and customers can make it harder. These tips should help mitigate a difficult situation:

- **No matter how tough the problem (or the customer) is, avoid arguing with customers or getting defensive:** The job is to solve the customer's problem, and doing that well sometimes takes a lot of patience.
- **Do not minimize or dismiss customers' problems:** Problems that seem simple to a technician can be very difficult for a customer. Keep in mind that every person with a broken PC might be losing valuable personal or business data; they might even lose enough data to wipe out a business.
- **No matter how incorrect their actions are or how poor their judgment is, avoid being judgmental of your customers:** Again, focus on the problem and look for a solution. Forming opinions based on your personal feelings usually has a bad outcome.
- **Clarify customer statements:** Ask the customer open-ended questions to further identify the issue and narrow the scope of the problem. Clarify by repeating the problem back to the customer. Restate the issue to verify everyone's understanding of the problem.

- **Do not disclose experiences on social media:** A customer relationship is to be valued. Gossiping on social media tells the customer that you do not value customer privacy.

## **Set and Meet Expectations/Timeline and Communicate Status with the Customer**

Many of the communication skills discussed in this section come together in the process of setting and meeting customer expectations. Expectations and communication can be strengthened in many ways, including the following:

- Coming in the door with a smile and getting right to work on determining the problem sets the tone for the customer's experience. Clearly state the problem, the plan is to fix it, how long it will take, and, if known, any extra costs. Clients always appreciate minimal surprises.
- Create a timeline of the steps and when you expect to meet them. Communicate the status with the customer often.
- If applicable, offer different repair/replacement options and allow the customer to select the one that works best in the situation.
- Provide and organize proper documentation of any services and products that are offered. When the job is complete, document the problem, process, and solution.
- Follow up with the customer at a later date to verify continued satisfaction.

## **Dealing Appropriately with Customers' Confidential and Private Materials**

Whether working in the customer's office or at a workbench, remember that the customer's computer information, printouts, and

other information is the customer's, and such data needs to be kept private. In many cases, this is not just good practice, but the law.

Asking a customer to move confidential materials such as bank statements, accounting information, legal documents, and other private company information to another area protects you from any suspicion later. Private materials that personally belong to the customer should also be moved out of the way.

## Scripting Basics



**220-1102: Objective 4.8:** Identify the basics of scripting.

PC technicians are often called upon to work on, configure, and update many computers or other devices at one time, and that can mean repeating the same tasks on each machine. Waiting for long processes to run or updates to install on each machine can take a lot of time. Writing a script with all the commands and inputs enables you to run the updates automatically, saving valuable time and money.

Programming is an important technical skill, but it is beyond the scope of the CompTIA A+ exam. However, being able to identify the basics of scripting is important because the capability to run scripts as a PC technician or an administrator is an invaluable asset.

## Script File Types

Script files are text files that contain instructions or commands that a computer follows to perform a task. They can be straight text commands for an OS, or they can be written in a scripting language (a limited kind of programming language) that can be run on the computer and interpreted by the operating system. The operating system then performs the commands in the script to complete the

tasks. [Table 9-5](#) identifies and briefly describes the six common scripting languages required for the A+ exam. You should be able to recognize them by their file extensions.



**Table 9-5** Basic Scripting Languages

---

**Extension   Language   Basic Information**

---

<b>.bat</b>	Windows batch file	Batch files are script files that are strictly Windows based. They are text files that contain commands or instructions for the command-line interpreter to execute. The instructions in a batch file can be interpreted only by the Windows operating system.
<b>.ps1</b>	PowerShell	Windows PowerShell is a tool to help technicians and network administrators automate support functions through the use of scripts and snippets. Windows 10 and 11 ship with PowerShell.
<b>.vbs</b>	VBScript	VBScript, a scripting language developed by Microsoft, is considered a subset of the Visual Basic programming language. It was designed specifically for use with Microsoft Internet Explorer. It gives web pages a level of interactivity.
<b>.sh</b>	Linux shell script	A shell script is a text file that contains a sequence of commands for a Linux- or UNIX-based system. Shell scripts might not run correctly on a Windows system. Linux has had several shells;

---

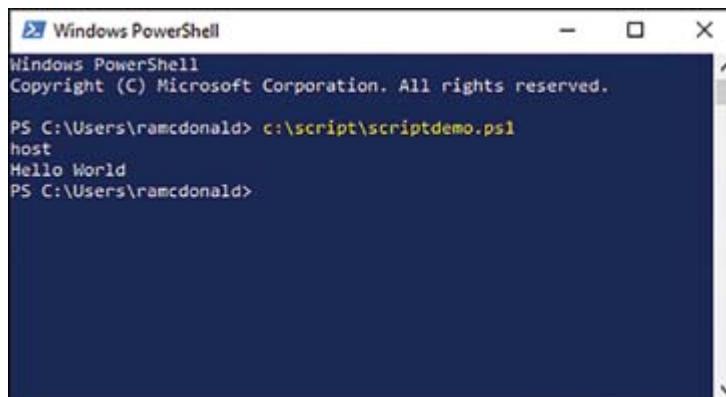
## Extension Language Basic Information

---

		BASH (Bourne-Again Shell) is the most common of them.
<b>.py</b>	Python	Python is often a good choice for those beginning to learn programming. It is relatively easy to learn, and Python scripts can run on most operating systems. For example, Windows Shell is known as Python Interactive Shell.
<b>.js</b>	JavaScript	JavaScript is a programming language that has many uses today. It is valuable for creating scripts because it can be run on any operating system. It is usually written into web pages to create client interactions; JavaScript is read by the browser. Creating and running command-line JavaScript requires installing Node.js.

Scripts can be opened and read or edited in basic text editors such as Notepad, or in special programming environments that assist with commands and testing of scripts. These are often referred to as shells, and they are designed to assist in script writing. [Figure 9-12](#) shows a basic “Hello World” script in Windows PowerShell. Note that the file was written in Notepad and saved as scriptdemo.ps1, using the filename extension for PowerShell. The entire text of the script is:

“Hello World”

A screenshot of a Windows PowerShell window titled "Windows PowerShell". The window shows the following text:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\ramcdonald> c:\script\scriptdemo.ps1
host
Hello World
PS C:\Users\ramcdonald>
```

The window has a dark blue background and a light gray border.

**Figure 9-12** Basic Script in Windows PowerShell

## Use Cases for Scripting

The purpose of scripts is to automate tasks commonly performed by a technician. Using tasks saves time, not only in typing out the script, but also in ensuring the reliability of the input and avoiding unintended consequences from bad code. [Table 9-6](#) lists seven common use cases where scripts are useful.



**Table 9-6** Use Cases for Scripting

Case	Description	Examples
Performing basic automation	Saves time inputting commands on individual machines	Using installation scripts when setting up new workstations
Restarting machines	Reboots without human input	Installing updates or patches
Remapping network drives	Redirects resources on workstations	Easing the process of system upgrades
Installing applications	Runs a script with license keys and permissions	Allowing simultaneous

<b>Case</b>	<b>Description</b>	<b>Examples</b>
		installations on workstations
Automating backups	Implements scheduled backups	Backing up several machines with one script
Gathering information/data	Logs resource use or user logins	Monitoring resources for network planning
Initiating updates	Ensures security with scheduled updates and patches	Scheduling checks for security patches

## Other Scripting Considerations

A common frustration for people new to scripting is “fat fingering” a script with a wrong character or number and having even this type of small error cause the script to fail. All computer languages follow strict command structures and syntax; although shells take away some of the burden, syntax still needs to be correct. When entering a script into a production environment, be sure that it has been tested in a sandbox environment first. Not doing so could result in harmful effects on the production network:

- **Unintentionally introducing malware:** This can be done by not checking imported scripts with security software.
- **Inadvertently changing system settings:** Remember that computers do not question what they are told to do. If bad scripting instructions change security or other system settings, that could open the door to disaster.
- **Browser or system crashing due to mishandling of resources:** Sometimes a poorly written script can instruct the computer to run a task that is beyond the power of a machine to handle. If the CPU is busy running a loop in a bad script, it

does not have resources for other important tasks. Again, sandboxing should help prevent these types of errors.

This brief introduction to scripting covers the basics mentioned in the CompTIA A+ objectives, but there is much more to learn. The following links provide more information about scripting in PowerShell, Linux, Python, and JavaScript:

<https://docs.microsoft.com/en-us/powershell/scripting/windows-powershell/ise/how-to-write-and-run-scripts-in-the-windows-powershell-ise?view=powershell-7.2>

<https://help.ubuntu.com/community/Beginners/BashScripting>

[www.python.org](http://www.python.org)

[www.javascript.com](http://www.javascript.com)

## Remote Access Technologies



**220-1102: Objective 4.9:** Given a scenario, use remote access technologies.

A technician commonly needs to access client computers or virtual computers remotely. The machines might be in another part of the network operations center or at the homes of clients working in other parts of the world. Remote access allows a user to see and control what is going on in another computer or device in a different location. Examples of using remote access include the following:

- A support technician accessing a client's computer to troubleshoot or update a PC.
- A network administrator adjusting settings on a server in another part of the network.

- A network administrator needing to access a router, switch, firewall, or other network device to manage traffic. (These devices usually do not have keyboards or monitors for input or output.)

A few protocols and applications have long been used for remote access, and third-party applications have become more prevalent. This section describes examples of remote access technology.

## Methods/Tools

Several methods exist for connecting remote computers, each developed for a specialized need or environment. This section discusses the most common methods for remotely accessing and managing remote computers and networks.

### RDP

**Remote Desktop Protocol (RDP)** was developed by Microsoft to allow a user to securely connect to a remote computer in order to perform services or support another user. The protocol allows for encrypted access with screen capture, mouse, and keyboard functions. Common tasks with the remote connections are support and management of remote computers. RDP is based on a client/server model. The user is the client, and the remote Windows computer enables the RDP server. The remote computer serves a graphic capture of the screen to the support tech. The support tech can manipulate the mouse and keyboard of the remote computer as well. If a remote worker needs tech support, the technician can then instruct the worker to enable the RDP server (if it isn't already enabled) and remotely see what is going on. This can greatly reduce the cost of tech services in a company.

RDP is a proprietary Microsoft protocol that is preinstalled on Windows, but macOS and Linux versions of both server and client are available as well. To enable Remote Desktop in Windows 10, go

to **Settings > System > Remote Desktop**. Remember that RDP uses port 3389, which needs to be opened in the firewall. [Chapter 6, “Operating Systems,”](#) discusses RDP in detail.

Windows 10 Remote Desktop Connection App is the most current tool for connecting a computer running Windows 10 Pro to another computer or device (iOS, Android, or Windows) that is also running the Remote Desktop App. The client device must enable the Remote Desktop Connection. To enable it in Windows 10, go to **Settings > System** and choose Remote Desktop Connection to toggle the enable setting. On iOS or Android, open the Remote Desktop Connection and select the desired PC for the connection.

## Note

This type of software is known as thin client software because only the mouse movement, keyboard activity, and screenshot captures are sent across the network, requiring very low bandwidth. Citrix, working with Microsoft, was the pioneer of thin client software, but many other vendors now compete in the market.

## VPN

A ***virtual private network (VPN)*** connection creates a secure tunnel over a public network, such as the Internet, between two computers (see “VPN Connections” in [Chapter 6](#) for more detail).

## Virtual Network Computing

***Virtual network computing (VNC)*** is common in desktop support. It allows a support agent to remotely control mouse and keyboard inputs to a client’s computer.

## **SSH**

**Secure Shell (SSH)** allows data to be exchanged between computers on a secure channel. This protocol offers a more secure option than FTP and Telnet. The Secure Shell server uses TCP port 22.

## **Remote Monitoring and Management**

**Remote Monitoring and Management (RMM)** tools enable technicians to monitor and manage remote networks. This usually involves installing special tools called **agents** that collect data and report it back to the management team for data analysis. RMM solutions are primarily designed to help large managed IT service providers (MSPs) remotely manage and administer customer computers and networks.

## **Microsoft Remote Assistance**

**Microsoft Remote Assistance (MSRA)** is the Windows utility for offering or accepting remote assistance. In Windows, it can be enabled by accessing the run menu (Windows+R) and typing **MSRA**.

As with Remote Desktop Connection, MSRA must first be enabled under System Properties with specific information on who is allowed to connect. If the computer is part of an enterprise network, MSRA options might not be available if other help applications are proscribed by management.

When the app opens, options to invite a connection or to accept a connection request appear.

## **Third-Party Tools**

For years, a market has existed for specialized tools or the third-party development of terminal services such as Telnet and SSH, as well as FTP. Some tools are free, and others have free client software but paid server software; still others are pay only. Often a free 30-day download is available to individuals but not to companies.

Sometimes Windows incorporates third-party tools into the OS, but the options available can vary from those of the third parties that created the tools. For example, PuTTY ([www.putty.org](http://www.putty.org)) is an open source application that provides connectivity software for Telnet and SSH connections.

## **Screen-Sharing and Videoconferencing Software**

Screen-sharing and videoconferencing software came into wide public use during the COVID-19 pandemic, when remote working and learning became the norm. Pre-pandemic, a clearer distinction was made between screen sharing and videoconferencing, but now the software products listed here are used to perform both tasks. Numerous products help organizations share communication and screens, and each has a place in the market. Some are very familiar, such as Zoom, Microsoft Teams, Google Meet, and Webex by Cisco Systems. Costs, features, and support options vary widely.

## **File Transfer Software**

Several protocols use SSH as a way of making a secure connection. One of these is Secure File Transfer Protocol (SFTP). Regular FTP, which was designed decades ago, before security was a major concern, can be insecure. SFTP combats this by providing file access over a reliable data stream, generated and protected by SSH over port 22.

FTP uses two ports during a file transfer session: port 21 to initiate a connection and port 20 to establish a connection to transfer files.

Many large companies use FTP to manage large documents and files that need to be shared to a distributed workforce. Serv-U ([www.serv-u.com](http://www.serv-u.com)), by SolarWinds, is a commercial provider of FTP, and FileZilla (<https://sourceforge.net/projects/filezilla/>) is an open source FTP application that works for Windows, macOS, and Linux.

Cloud file management is now doing much of the work FTP has performed in the past. Examples of cloud storage providers are Dropbox, Google Drive, Microsoft OneDrive, and Amazon Drive. There is also widening acceptance of cloud-based document sharing, such as Google Docs, in which documents are created and edited in a shared cloud environment. Most cloud-based file transfers are faster and easier than with FTP, but FTP is in wide use and easy to manage, so technicians will encounter it for the foreseeable future.

## Desktop Management Software

Desktop Management Software is designed to allow network administrators to manage the software and software updates on machines, either local or remote. This can mean managing licenses, remote installations, and security patches on machines under their control. Some products facilitate the management of one software product across different OS platforms.

## Security Considerations of Each Access Method

Security has become the most prominent concern in the information technology field. Weaknesses that have existed for years are being discovered—and exploited—on a regular basis. No product or system discussed in this section is immune to the ever-increasing sophistication of private and government-sponsored hackers.

The technologies mentioned here do have associated concerns, but they are closely related.

A famous example from the COVID-19 pandemic provides a valuable lesson. During the pandemic, when Zoom became the most popular remote meeting software in a matter of days or weeks, users were focused on connecting cheaply and easily, and Zoom accomplished both. After a few weeks, however, *Zoom bombing* became an issue when uninvited outsiders were able to join and disrupt meetings. Zoom scrambled to create security systems for the product. Eventually, updates were created that required the sound authentication practices discussed in [Chapter 7, “Security.”](#)

What could have been done to mitigate the security threats? In hindsight, the most important would have been to make security concerns paramount over “cheap and easy” when selecting software.

Another common security practice that improves the safety of these remote technologies is using them over a VPN whenever possible. Remember that VPNs encrypt communication. Along with strong authentication practices, this can help organizations remotely connect and work in a safe environment.

## Exam Preparation Tasks

As mentioned in the Introduction, you have several choices for exam preparation: the exercises here; [Chapter 10, “Final Preparation”](#); and the exam simulation questions in the Pearson Test Prep practice test software.

## Review All the Key Topics

Review the most important topics in the chapter, noted with the Key Topic icon in the outer margin of the page. [Table 9-7](#) lists these key topics and the page number on which each is found.



**Table 9-7** Key Topics for Chapter 9

<b>Key Topic Element</b>	<b>Description</b>	<b>Page Number</b>
Section	Change Management	693
List	Backup and Recovery	697
Section	Onsite vs. Offsite Backups	700
Section	Equipment Grounding/Proper Power Handling	705
Section	Proper Component Handling and Storage	707
Figure 9-10	Using an ESD Strap to Prevent Damaging ESD When Working on Electronics	710
Section	Personal Safety	713
Section	Material Safety Data Sheet (MSDS)	715
Section	Toxic Waste Handling/Disposal	717
List	Proper methods for recycling batteries	717
Section	Battery Backup Units	720
Table 9-4	Electrical Conditions and Protective Measures	721
Section	Incident Response	722
Section	Licensing/Digital Rights Management (DRM)/End-User License Agreement (EULA)	723
List	Regulated data	726
Section	Communication Techniques and Professionalism	727

---

<b>Key Topic Element</b>	<b>Description</b>	<b>Page Number</b>
Table 9-5	Basic Scripting Languages	731
Table 9-6	Use Cases for Scripting	733

---

## Complete the Tables and Lists from Memory

Print a copy of [Appendix C, “Memory Tables”](#) (found online), or at least the section for this chapter, and complete the tables and lists from memory. [Appendix D, “Memory Tables Answer Key,”](#) also online, includes completed tables and lists to check your work.

## Define Key Terms

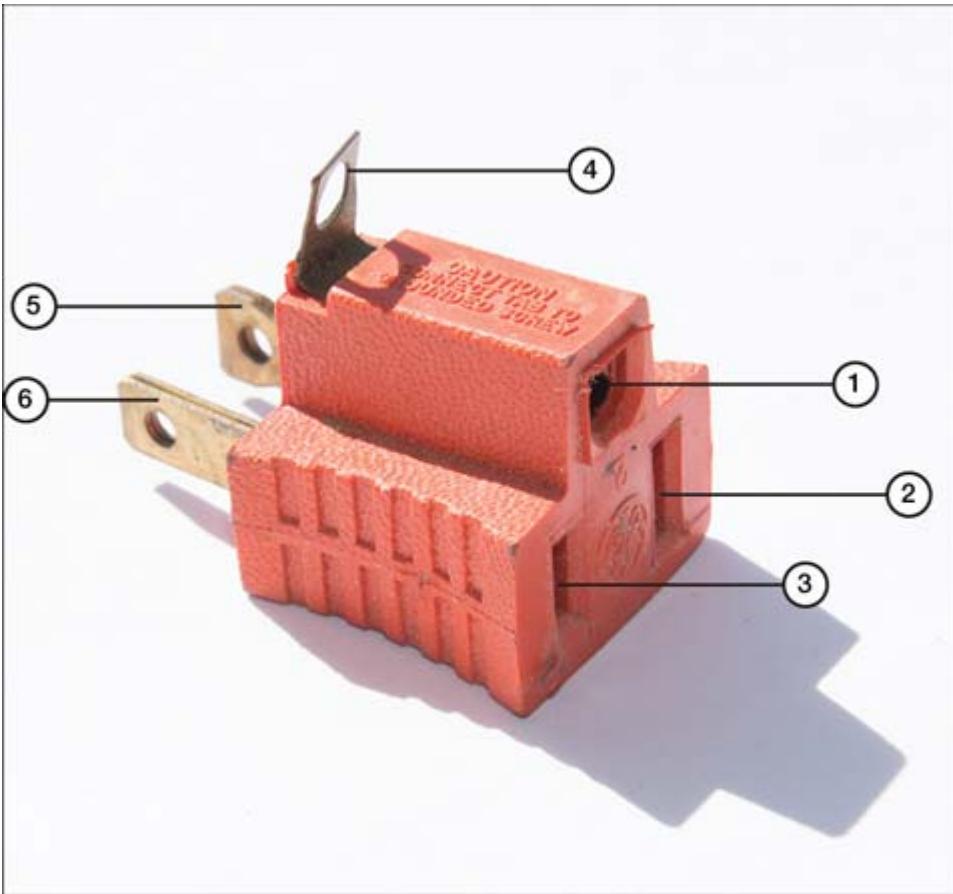
Define the following key terms from this chapter and check your answers in the glossary:

- ticketing systems
- acceptable use policy (AUP)
- network topology diagram
- splash screens
- incident reports
- change management
- rollback plan
- risk analysis
- full backup
- incremental backup
- differential backup
- synthetic backup
- grandfather-father-son (GFS)
- 3-2-1 backup rule
- electrostatic discharge (ESD)

material safety data sheet (MSDS)  
power surges  
chain of custody  
digital rights management (DRM)  
end-user license agreement (EULA)  
open-source licenses  
personal use licenses  
corporate use licenses  
PII  
.bat script files  
.ps1 script files  
.vbs script files  
.sh script files  
.py script files  
.js script files  
Remote Desktop Protocol (RDP)  
virtual private network (VPN)  
virtual network computing (VNC)  
Secure Shell (SSH)  
remote monitoring and management (RMM)  
Microsoft Remote Assistance (MSRA)

## **Answer Review Questions**

- 1.** Identify the parts of the plug in the following figure.



- a. Hot prong
  - b. Hot connector
  - c. Neutral prong
  - d. Neutral connector
  - e. Ground loop
  - f. Ground connector
- 2.** The object in the following figure is an electrical outlet tester. What does this outlet tester tell you about the outlet into which it is currently plugged?



- a. The ground wire is faulty.
  - b. The hot wire is faulty.
  - c. The neutral wire is faulty.
  - d. All of the wires are correct.
3. Which of the following statements best defines ESD?
  - a. Electronic shutdown device
  - b. Electrostatic discharge
  - c. Environmentally sustainable development
  - d. Energy sensitive differential
4. Which of the following can be used as protection against ESD?  
(Choose all that apply.)
  - a. An antistatic bag
  - b. A 3-wire-to-2-wire adapter
  - c. An ESD mat
  - d. An ESD strap
5. Which of the following increases the likelihood of ESD?

- a. Carpet on the floor
  - b. Increasing the humidity of the room
  - c. Increasing the room temperature
  - d. Rubber-soled shoes
- 6. Which of the following best describes how to dispose of used batteries?
  - a. Open the batteries and very carefully remove their lead cores before recycling.
  - b. Recycle batteries in the recycling bin.
  - c. Recycle NiMH and Li-Ion in the recycling bin; NiCad batteries can be disposed of in the trash.
  - d. Return the batteries to an electronics store for recycling.
- 7. Which of the following is considered an environmental hazard?
  - a. Mobile phones and tablets
  - b. UPS batteries
  - c. Toner cartridges
  - d. All of these
- 8. Which class of fire extinguisher should be used on an electrical fire?
  - a. Class A
  - b. Class B
  - c. Class C
  - d. Class D
- 9. When selecting an air filter mask, which category provides the highest level of protection?
  - a. A
  - b. N
  - c. P

**d.** R

- 10.** Which of the following statements best describes an MSDS (also known as SDS)?
- a.** An MSDS provides simultaneous accessibility to multiple data sources.
  - b.** An MSDS provides safety information concerning storage, spills, and accidental exposure to dangerous chemicals.
  - c.** An MSDS helps protect computer components from damage due to ESD.
  - d.** An MSDS is a legal document used to establish chain of custody in legal cases.
- 11.** Which hazardous material is used to make UPS batteries?
- a.** Ni-Cad
  - b.** NiMH
  - c.** Li-Ion
  - d.** Lead-acid
- 12.** Which of the following best describes the function of a UPS in a technology environment?
- a.** A UPS is a battery backup.
  - b.** A UPS is a rating for system performance.
  - c.** A UPS is a security program.
  - d.** A UPS is a package delivery company.
- 13.** Which of the following best describes chain of custody?
- a.** Chain of custody is documentation of the ownership of a computer or computer components.
  - b.** Chain of custody is documentation of who was in possession of evidence relative to an investigation.
  - c.** Chain of custody is documentation of how a computer was repaired, such as what was done and who did it.

- d. Chain of custody is documentation of the possession of a computer and is not related to ownership.
- 14.** Which of the following best describes open source software? (Choose all that apply.)
- a. Open source software can be used for free.
  - b. Open source software can be used for commercial purposes.
  - c. Open source software can be sold.
  - d. Open source software can be modified.
- 15.** As a computer technician, what can you do to help your clients protect their personal information? (Choose all that apply.)
- a. You can advise them to store their sensitive information using cloud storage instead of local storage.
  - b. You can advise them to use BitLocker encryption.
  - c. You can advise them to store sensitive information on a PC's hard drive instead of storing it with the backup files.
  - d. You can advise them to use firewalls to prevent hacker intrusions.
- 16.** Which of the following statements describes the best way to explain a problem to a customer?
- a. Use as much technical vocabulary as possible because this makes you sound knowledgeable and will impress the customer.
  - b. Explain as little as possible because the customer probably would not understand the explanation, and it would only create confusion.
  - c. Explain the problem in nontechnical terms and offer to show the customer what the problem was and how you fixed it.
  - d. Ask the customer not to be concerned about the details and assure the customer that you will take care of the

problem.

- 17.** Ellen is working on a workstation in the Accounting department. In an open browser tab, she notices a meme with racist comments and graphic pictures. What is the next step Ellen should take?
- a.** Finish fixing the problem and warn the user that this content is against the AUP
  - b.** Call corporate security
  - c.** Contact her supervisor
  - d.** Contact the user's supervisor
- 18.** Fatima was helping Mark, a new employee who was having trouble accessing the network folders he needed for his new assignments. When she asked him to describe the problems, she took notes, did not interrupt, and restated his problem in her own words to make sure she understood. Which customer service skill was Fatima demonstrating?
- a.** Presumptive listening
  - b.** Cultural sensitivity
  - c.** Active listening
  - d.** Dealing with a difficult customer
- 19.** Martin, a tech support worker on a macOS help desk, took a support call from Sarah and soon determined that Sarah's laptop needed to have a few settings changed. He had Sarah allow him secure access to her desktop, and he was able to control her mouse and make the necessary changes. Which protocol were Martin and Sarah's computers likely using during that help session?
- a.** Telnet
  - b.** RTP
  - c.** RDP
  - d.** FTP

**20.** Jess and Hiroko have to update several computers, and their lab manager has written a basic script to speed up the process. They are given a flash drive with four files on it, but the one they want is written in a shell for Linux machines. Which file extension is likely the one they want to use?

- a.** update.js
- b.** update.sh
- c.** update.py
- d.** update.bat

**21.** When Josh is unable to answer a question about a new type of software coming onto the market and how his customer might implement it, what action should he take?

- a.** Give the best answer possible with the knowledge he has
- b.** Look for a whitepaper online
- c.** Send the client to the software developer's web page
- d.** Refer the question to his boss

**22.** Carla, who works in payroll, got to work one day and realized that she no longer had access to employee wellness bonus pay information that was key to her job. Later she found out that the health care provider implemented a new reporting system that separated accounting reports from private wellness records. What is this most likely an example of?

- a.** Not getting stakeholder feedback
- b.** Poor password management
- c.** Domain failure
- d.** The knowledge base not being updated

# **Part III: Final Preparation**

# Chapter 10

## Final Preparation

This chapter demystifies the certification preparation process and shares some helpful ideas to ensure that you are ready for the exams. Many people feel anxious about taking exams; our hope is that this chapter will give you the tools to build confidence for exam day. One important way to do that is to take a detailed look at the actual certification exams.

The first nine chapters of this book cover the technologies, protocols, design concepts, and considerations required to pass the CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) exams. Despite having this detailed information, most people need more preparation than just reading the first nine chapters of this book. This chapter provides a set of tools and a study plan to help you complete your preparation for the exams.

This short chapter has four main sections. The first section lists the CompTIA A+ 220-1101 and 220-1102 exam information and breakdown. The second section shares some important tips to keep in mind to ensure that you are ready for these exams. The third section discusses exam preparation tools that might be useful at this point in the study process. The final section of this chapter lists a suggested study plan to follow after you have completed all the earlier chapters in this book.

### Note

[Appendix C, “Memory Tables,”](#) and [Appendix D, “Answer Key to Memory Tables,”](#) exist as digital appendixes on the website for this

book. You can access this website by going to [www.pearsonITcertification.com/register](http://www.pearsonITcertification.com/register), registering your book, and entering this book's ISBN: 9780137675944.

## Exam Information

These details are important to know for the two exams that map to this text:

- **Exam ID codes:** A+ Core 1 (220-1101) and A+ Core 2 (220-1102)
- **Question types:** Multiple-choice and performance-based questions
- **Number of questions:** Maximum of 90 per exam
- **Time limit:** 90 minutes per exam
- **Required passing score:** 220-1101: 675 (on a scale of 100–900); 220-1102: 700 (on a scale of 100–900)
- **Available languages (subject to change):** English, German, Japanese, Portuguese, Simplified Chinese, and Spanish
- **Exam fee (subject to change):** US\$239 per exam

CompTIA A+ 220-1101 covers PC hardware and peripherals, mobile device hardware, and networking and troubleshooting of hardware and network connectivity issues.

CompTIA A+ 220-1102 covers installing and configuring operating systems, including Windows, iOS, Android, macOS, and Linux. It also addresses security, the fundamentals of cloud computing, and operational procedures.

CompTIA A+ is the preferred qualifying credential for technical support and IT operational roles. It is about much more than PC

repair:

- Candidates are better prepared to troubleshoot and solve problems.
- Technicians understand a wide variety of issues, ranging from networking and operating systems to mobile devices and security.
- A+ supports the capability to connect users to the data they need to do their jobs, regardless of the devices being used.

Successful candidates have the knowledge required to do the following:

- Assemble components based on customer requirements
- Install, configure, and maintain PCs, mobile devices, and software for end users
- Understand the basics of networking and security forensics
- Properly and safely diagnose, resolve, and document common hardware and software issues
- Apply troubleshooting skills
- Provide appropriate customer support
- Understand the basics of scripting, virtualization, desktop imaging, and deployment

For a complete breakdown of the exam objectives for these domains of each exam, download the PDF of the exam objectives from the CompTIA site ([www.comptia.org/certifications/a#examdetails](http://www.comptia.org/certifications/a#examdetails)) by filling out the Get Practice Questions and Exam Objectives box, shown in [Figure 10-1](#).

Get Practice Questions and Exam Objectives

First Name  Last Name

Email  Job Description

Select Exam  Country

I'm interested in receiving:

Exam Objectives  Practice Questions

Training Status

I plan on taking the exam...

I agree to the [Terms of Use & Privacy statement](#).

**SUBMIT**

**Figure 10-1** Downloading CompTIA A+ Exam Objectives and Practice Questions

## Core 1 (220-1101) Exam Domains and Objectives

The 220-1101 exam is divided into five different domains. Here are those domains and the percentage of the exam for each one:

- **1.0 Mobile Devices:** 15 percent
- **2.0 Networking:** 20 percent
- **3.0 Hardware:** 25 percent
- **4.0 Virtualization and Cloud Computing:** 11 percent
- **5.0 Hardware and Network Troubleshooting:** 29 percent

## **Core 2 (220-1102) Exam Domains and Objectives**

The 220-1102 exam is divided into four different domains. Here are those domains and the percentage of the exam for each one:

- **1.0 Operating Systems:** 31 percent
- **2.0 Security:** 25 percent
- **3.0 Software Troubleshooting:** 22 percent
- **4.0 Operational Procedures:** 22 percent

## **Getting Ready**

Keep some important tips in mind to ensure that you are ready for this rewarding exam:

- **Build and use a study tracker:** Consider using the exam objectives detailed in this chapter to build a study tracker. In its simplest form, this can be a notebook outlining the objectives, with your notes written out. Using pencil and paper and taking time to think out your answers can improve your concentration. A study tracker also helps you ensure that you have not missed anything and that you are confident in planning for your exams. You can create a study tracker in other ways as well, including creating a sample Study Planner as a website supplement to this book. Whatever method works best for you is the right option to use.
- **Think about your time budget for questions during the exam:** When you do the math, you can see that you have 1 minute per question. This does not sound like enough time, but realize that many of the questions will be very straightforward; you will spend only 15 to 30 seconds on those questions. This leaves additional time for other questions as you take your exam.

- **Watch the clock:** Periodically check on the time remaining as you take the exam. You might find that you can slow down pretty dramatically if you have built up a nice block of extra time.
- **Consider ear plugs:** Some people are sensitive to noise when concentrating. If you are one of them, ear plugs might help minimize distractions from other test takers in the room.
- **Plan your travel time:** Give yourself extra time to find the center and get checked in. Be sure to arrive early for your first exams. As you test more at that center, you can start to decrease your lead time.
- **Get rest:** Most students who report success get plenty of rest the night before the exam. All-night cram sessions do not typically result in success.
- **Be ready to lock up your valuables:** The testing center will provide a secure place to stow your phone, smart watch, wallet, and other such items.
- **Use the restroom before entering the exam room:** If you think you will need a break during the test, clarify the rules with the test proctor before the exam starts.
- **Take your time getting settled:** When you are seated, take a breath and organize your thoughts. Remind yourself that you have worked hard for this opportunity and expect to do well. After a brief tutorial, you start the 90-minute timer. The timer starts when you agree to see the first question.
- **Take notes:** You will be given note-taking materials; take advantage of them. Sketch out lists and mnemonics that you have memorized. You can use the note paper for any calculations that you need during the exam, but it is also okay to write notes to yourself before you begin.
- **Practice exam questions are great—use them:** This text provides many practice exam questions. Be sure to go through

them thoroughly. Remember, you shouldn't blindly memorize answers; instead, let the questions really demonstrate where you are weak in your knowledge so that you can study up on those areas.

## **Tools for Final Preparation**

This section lists some information about the available tools and how to access them.

### **Pearson Cert Practice Test Engine and Questions on the Website**

Register this book to get access to the Pearson IT Certification test engine (software that displays and grades a set of exam-realistic multiple-choice questions). Using the Pearson Cert Practice Test Engine, you can either study by going through the questions in Study mode or take a simulated (timed) A+ exam.

The Pearson Test Prep practice test software comes with two full practice exams. These practice tests are available either online or as an offline Windows application. To access the practice exams that were developed with this book, see the instructions in the card inserted in the sleeve at the back of the book. This card includes a unique access code that enables you to activate your exams in the Pearson Test Prep software.

### **Accessing the Pearson Test Prep Software Online**

The online version of the Pearson Test Prep software can be used on any device with a browser and connectivity to the Internet, including desktop machines, tablets, and smartphones. To start using your practice exams online, simply follow these steps:

**Step 1.** Go to [www.PearsonTestPrep.com](http://www.PearsonTestPrep.com).

**Step 2.** Select **Pearson IT Certification** as your product group.

**Step 3.** Enter the email and password for your account. If you don't have an account on PearsonITCertification.com or CiscoPress.com, you need to establish one by going to PearsonITCertification.com/join.

**Step 4.** In the My Products tab, click the **Activate New Product** button.

**Step 5.** To activate your product, enter the access code printed on the insert card in the back of your book. The product is now listed in your My Products page.

**Step 6.** Click the **Exams** button to launch the exam settings screen and start the exam.

## **Accessing the Pearson Test Prep Software Offline**

If you want to study offline, you can download and install the Windows version of the Pearson Test Prep software. The book's companion website includes a download link for this software, or you can just enter this link in your browser:

[www.pearsonitcertification.com/content/downloads/pcpt/engine.zip](http://www.pearsonitcertification.com/content/downloads/pcpt/engine.zip)

To access the book's companion website and the software, simply follow these steps:

**Step 1.** Register your book by going to PearsonITCertification.com/register and entering the ISBN **9780137675944**.

**Step 2.** Respond to the challenge questions.

**Step 3.** Go to your account page and select the **Registered Products** tab.

**Step 4.** Click the **Access Bonus Content** link under the product listing.

**Step 5.** To download the software, click the **Install Pearson Test Prep Desktop Version** link under the Practice Exams section of the page.

**Step 6.** When the software finishes downloading, unzip all the files on your computer.

**Step 7.** Double-click the application file to start the installation and follow the onscreen instructions to complete the registration.

**Step 8.** When the installation is complete, launch the application and click the **Activate Exam** button on the My Products tab.

**Step 9.** Click the **Activate a Product** button in the Activate Product Wizard.

**Step 10.** Enter the unique access code found on the card in the sleeve in the back of your book; click the **Activate** button.

**Step 11.** Click **Next** and then click the **Finish** button to download the exam data to your application.

**Step 12.** You can now start using the practice exams by selecting the product and clicking the **Open Exam** button to open the exam settings screen.

Note that the offline and online versions will sync together, so saved exams and grade results recorded on one version will be available to you on the other as well.

## Customizing Your Exams

When you are at the exam settings screen, you can choose to take exams in one of three modes:

- Study mode
- Practice Exam mode
- Flash Card mode

Study mode enables you to fully customize your exams and review answers as you are taking the exam. This is typically the mode you use first to assess your knowledge and identify information gaps. Practice Exam mode locks certain customization options and presents a realistic exam experience. Use this mode when you are preparing to test your exam readiness. Flash Card mode strips out the answers and presents you with only the question stem. This mode is great for late-stage preparation, when you really want to challenge yourself to provide answers without the benefit of seeing multiple-choice options. This mode does not provide the detailed score reports that the other two modes do, so do not use this one if you are trying to identify knowledge gaps.

In addition to these three modes, you can select the source of your questions. You can choose to take exams that cover all chapters in this book, or you can narrow your selection to just a single chapter or the chapters that make up specific parts in the book. By default, all chapters are selected. If you want to narrow your focus to individual chapters, simply deselect all the chapters and then select only those you want to focus on in the objectives area.

You can also select the exam banks to focus on. Each exam bank comes complete with a full exam of questions that cover topics in every chapter. You can have the test engine serve up exams from all four banks or just one individual bank by selecting the desired banks in the exam bank area.

You can make several other customizations to your exam from the exam settings screen, including the time of the exam, the number of questions served up, whether to randomize questions and answers, whether to show the number of correct answers for multiple-answer questions, and whether to serve up only specific types of questions.

You can also create custom test banks by selecting only questions that you have marked or questions on which you have added notes.

## **Updating Your Exams**

If you are using the online version of the Pearson Test Prep software, you should always have access to the latest version of the software and exam data. If you are using the Windows desktop version, every time you launch the software, it checks to see if any updates affect your exam data and, if so, automatically downloads any changes that have been made since the last time you used the software. You must be connected to the Internet when you launch the software.

For many reasons, the exam data sometimes does not fully download when you activate your exam. If figures or exhibits are missing, you might need to manually update your exams. To update a particular exam that you have already activated and downloaded, simply select the Tools tab and click the Update Products button. Again, this is an issue only with the desktop Windows application. If you want to check for updates to the Pearson Test Prep exam engine software, Windows desktop version, simply select the Tools tab and click the Update Application button. This ensures that you are running the latest version of the software engine.

## **Premium Edition**

In addition to the free practice exam provided on the website, you can purchase additional exams with expanded functionality directly from Pearson IT Certification. The Premium Edition of this title contains an additional two full practice exams and an eBook (in both PDF and ePUB format). In addition, the Premium Edition title has remediation for each question to the specific part of the eBook that relates to that question.

Because you have purchased the print version of this title, you can purchase the Premium Edition at a deep discount. A coupon code in the book sleeve contains a one-time-use code and instructions for where you can purchase the Premium Edition.

To view the premium edition product page, go to [www.informit.com/title/9780137675944](http://www.informit.com/title/9780137675944).

## Memory Tables

As with most other Exam Cert Guides, this book purposely organizes information into tables and lists, for easier study and review.

Rereading these tables and lists can be useful before exam day. However, be careful not to skim over the tables without paying attention to every detail, especially when you remember having seen the table's contents when reading the chapter.

Instead of just reading the tables in the various chapters, this book's Appendixes C and D give you another review tool. [Appendix C](#) lists partially completed versions of many of the tables from the book. You can open [Appendix C](#) (a PDF available on the book website after you register) and print the appendix. For review, you can attempt to complete the tables. This exercises the memory connectors in your brain and prompts you to think about the information from context clues, which forces a little more contemplation about the facts.

[Appendix D](#), which is also a PDF located on the book website, lists the completed tables so that you can check yourself. You can also just refer to the tables as printed in the book.

## Chapter-Ending Review Tools

[Chapters 1–9](#) offer several features in the “Exam Preparation Tasks” section at the end of each chapter. You might have already worked through these, but looking over them again can be useful as you make your final preparations for the exams.

# Suggested Plan for Final Review/Study

This section lists a suggested study plan from the point at which you finish reading through [Chapter 9](#) until you take the CompTIA A+ 220-1101 and 220-1102 exams. You can ignore this plan, use it as is, or merely take suggestions from it.

The plan involves four steps:

**Step 1. Review key topics and “Do I Know This Already?”**

**questions:** You can use the table that lists the key topics in each chapter or just flip the pages while looking for key topics. Reviewing the “Do I Know This Already?” questions from the beginning of the chapter also can be helpful for review.

**Step 2. Complete memory tables:** Open [Appendix C](#) from the book website, and either print the entire appendix or print the tables by major part. Then complete the tables.

**Step 3. Review the Review sections:** Go through the review questions at the end of each chapter to identify areas where you need more study.

**Step 4. Use the Pearson Cert Practice Test engine to practice:** The test engine offers a bank of unique exam-realistic questions that are available only with this book.

## Summary

The tools and suggestions listed in this chapter have been designed with one goal in mind: to help you develop the skills required to pass the CompTIA A+ 220-1101 and 220-1102 exams. From the beginning, this book was developed to not just tell you the facts, but also help you learn how to apply those facts. No matter what your experience level is leading up to the exams, it is our hope that the broad range of preparation tools, and even the structure of the book, help you pass the exams with ease. We hope you do well!

# Appendix A

## **Answers to the “Do I Know This Already?” Quizzes and Review Questions**

### **Chapter 1**

#### **“Do I Know This Already?” Quiz**

**1.** c

**2.** a, b, c, d

**3.** b

**4.** a

**5.** c

**6.** c

**7.** c

**8.** b, c

**9.** d

**10.** b, c

## Review Questions

- 1. c.** SODIMM stands for small outline DIMM, which is a smaller RAM form factor developed for laptops. DDRSD4 is a fictitious term. DIMM is a form factor used in desktops. SDR SDRAM is a RAM description.
- 2. b.** Tethering is the sharing of a cellular data connection from a smartphone to a laptop, tablet, or other device. Pairing occurs when two Bluetooth devices are connected or synchronized together. NFC is a short-range wireless technology typically used for peer-to-peer payments and other transactions. A hotspot is wireless tethering; no USB cable is involved.
- 3. c.** An SSD (solid-state drive) is faster than an HDD or an SSHD. Adding RAM might be part of the solution, but DIMM is a RAM form factor for desktops, not laptops.
- 4. a, d.** Memory speed and timing must match the existing RAM when adding RAM to a machine.
- 5. b.** An inverter is a power converter that changes DC power into AC power. A transformer converts a higher voltage to a lower voltage, or a lower voltage to a higher voltage. A wireless card and PCIe card are hardware devices that connect to a laptop and provide additional functions.
- 6. b.** The PRL contains a priority list of radio frequencies and service providers the device should use in various geographical areas. This information tells the phone what towers to connect to, what radio frequency to use, and what service provider to use. MAM allows companies to control the software and data used on its devices, no matter where the users are located. OLED is a display screen. NFC is a short-range wireless technology.

- 7. b, c.** Tethering allows two devices to share an Internet connection via a USB cable. A hotspot sets up a smartphone as a temporary SSID that other devices can connect to. *Twisted nematic (TN)* refers to transparent liquid crystals that, when energized, cause light to polarize. This technology was important in the growth of LCDs because high quality could come with very low voltage usage. A port replicator is a device that allows a laptop to expand the number of ports so that additional devices can be attached.
- 8. a.** Airplane mode turns off the antennas in mobile devices so that they cannot transmit or receive cellular and GPS data while in flight. Bluetooth and Wi-Fi can still be enabled.
- 9. d.** In two-factor authentication (2FA), two different authentication factors are used to verify an identity. In this case, the user is providing a password (something the user knows) and a biometric fingerprint (something the user is). Organizations that have many mobile devices need to administer them so that all devices and users comply with the security practices in place. This is usually done with a suite of software known as *mobile device management (MDM)*. The purpose of mobile application management (MAM) is to allow companies to control the software and data used on its devices, no matter where the users are located. Pairing occurs when two Bluetooth devices are connected or synchronized together.
- 10. a, b, c, d.** Bluetooth creates a short-range, low-speed, peer-to-peer network populated by dissimilar devices. This type of network is called a PAN (personal area network).
- 11. d.** A digitizer detects and transmits touch. If the screen is damaged, it will not respond to touch. An inverter converts

DC power to AC power. Touch pen and battery are least likely to be the cause of an unresponsive touchscreen.

- 12. b.** MDM allows companies to push updates to devices and ensure that all devices comply with the security practices that are in place. MAM allows companies to control the software and data used on its devices. PRL is a priority list of radio frequencies and service providers that a mobile device should use in various geographical areas. NFC is a short-range wireless technology.
- 13. d.** NFC is a short-range wireless technology that has a range of about 10cm or 4 inches. Wi-Fi and cellular both cover areas much larger than 10cm. Bluetooth has a range of up to 10m.
- 14. a.** NFC is most commonly used for payments and transactions. Wi-Fi is a wireless technology that allows mobile and other devices to connect to a wireless network and also connect to the Internet. Biometrics are physical characteristics such as fingerprints. Bluetooth is used to pair or link two devices, such as a computer and a wireless keyboard.
- 15. c.** Biometrics is not a file type. It refers to physical characteristics such as fingerprints. Email, calendars, and contacts can all be synchronized between two devices.

## Chapter 2

### “Do I Know This Already?” Quiz

- 1.** b
- 2.** c, d
- 3.** a

**4.** b

**5.** d

**6.** c

**7.** b, c, e

**8.** b

**9.** b

**10.** d

**11.** a

**12.** d

**13.** b

**14.** c

**15.** c

**16.** d

**17.** d

**18.** b

## Review Questions

**1.**

<b>Wired</b>	Fiber	Cable	DSL
← Fastest ----- Slowest →			
<b>Wireless</b>	Cellular	Wireless Internet service provider (WISP)	Satellite

- 2. a, c, d.** Video, voice, and gaming require real-time streaming. Resending data would interrupt the stream. For both email and SMS, data would be re-sent if a message failed.
- 3. c.** The browser is likely using HTTPS to transport on port 443. Port 80 is the less secure HTTP. Port 68 is a DHCP port, and port 53 is used for DNS.
- 4. a.** The router connects the LAN to other LANs. All other devices work with traffic within the LAN.
- 5. b.** VLANs are created in a LAN using advanced switches that allow configuration management.

**6.**

<b>Device</b>	<b>Definition</b>
Wireless access point	Extends wired LANs into wireless connected space
Router	Allows networks to communicate with each other
Switch	Uses a MAC address to direct data to a specific computer
Modem	Converts digital signals to analog, and analog signals to digital
Firewall	Prevents unwanted intrusion from outside the network
Hub	Broadcasts data to all attached computers
Patch panel	Acts as a junction point for network cabling

- 7. c.** An administrator uses WLAN controllers to remotely manage a wireless LAN.

**8. d.** TCP/IP is a suite of protocols used to manage traffic on the Internet. It is the accepted standard used by all major operating systems.

**9. c.** This is an IPv4 address.

**10. b.** The 255s in the subnet mask indicate the network portion of the address. Therefore, the first two octets identify the network portion of the address, and the last two octets are the host portion.

**11. b.** 255.255.255.0 is the subnet mask for a network with 255 addresses in the last octet.

**12. b, e.** 127.0.0.1 is a diagnostic tool known as the IPv4 loopback address, which is used to test connectivity between a computer and its network. ::1 is the IPv6 counterpart.

**13. b.** This is an example of a Class A private IP address.

**14. d.** APIPA addresses are automatically assigned, in case the DHCP system cannot provide IP addresses. As a technician, anytime you see an IP address that begins with 169.254.x.x, you should look for problems with DHCP. APIPA is supported by Microsoft, macOS, and Linux.

**15. d.** Every device that accesses the Internet (every PC, laptop, tablet, smartphone, and so on) must have its own IP address, and no two addresses may be the same. A single family might need a dozen addresses; the world is simply running out of IPv4 addresses. IPv6 provides a huge increase in the number of available IP addresses.

**16. b.** DHCP automatically assigns IP addresses to computers on a network.

**17. c.** DNS resolves domain names to their IP addresses. TCP is an Ethernet protocol, and DHCP assigns addresses to

devices on a network. UPnP is an access setting on SOHO routers.

**18.**

Protocol	IMAP	FTP	HTTP	HTTPS	SMTP	DNS	SSH	POP3
Port	143	21	80	443	25	53	22	110

As an IT technician, you might be called upon to configure ports for a network. The ports in this chart are only a few of the ones you might need to know.

- 19. a.** Simple Mail Transfer Protocol (SMTP) is used to send email.
- 20. b.** 802.11 includes 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax wireless network standards.
- 21. d.** This is an Internet of Things (IoT) device. The number of IoT devices talking to each other and sharing data numbers is in the many billions, and that number is expected to grow exponentially.
- 22. b.** A crimper is used to attach an RJ-45 or RJ-11 connector to a TP cable.

## Chapter 3

### “Do I Know This Already?” Quiz

**1.** c

**2.** b

**3.** b

**4.** c

**5.** c

**6.** a

**7.** a

**8.** d

**9.** a

**10.** c

**11.** d

**12.** b, d

**13.** a, c

**14.** c

**15.** a

**16.** b

**17.** c

**18.** b

**19.** a

**20.** c

**21.** c

**22.** d

## Review Questions

**1. a.** The ATX 24-pin power cable and connector provides primary power to the motherboard and connected devices.

**2. a.** SPDIF audio is not selected as the default output. Computers use analog speakers as the default output. You

must select SPDIF as the output if you are now connecting to a receiver via the SPDIF (digital audio) port. VGA and microphone cables have no effect on audio output. Smart card readers do not cause interference.

- 3. c.** Random access memory (RAM) loses its contents when the computer shuts down. Hard disk drives, USB flash drives, and read-only memory (ROM) are designed to retain their contents even when they are not receiving power.
- 4. c.** DDR3. The label identifies this module as PC3, which indicates that it contains DDR3 type RAM.
- 5. b.** Dual-channel support requires that the paired memory slots both use memory with identical specifications.
- 6. a, c.** Parity memory and ECC have an additional memory chip added for parity. They are both methods used to protect the reliability of memory.
- 7. a.** Unbuffered, non-ECC memory is used in most common desktop computers sold. This kind of memory is also used in some servers and workstations.
- 8. a.** ECC memory enables the system to correct single-bit errors and notify the user of larger errors.
- 9. a.** Thermal paste or thermal pads need to be applied to a CPU before applying a heat sink. Filament is a plastic material used in 3D printing. Resin is used in thermal printing. A paper separation pad is used in laser printers.
- 10. a, b, c.** To correctly insert the memory modules, you should follow all the steps listed. You might also have to use a fair amount of pressure to securely lock these modules in place.
- 11. a.** For best results, you should always install identical modules in the same channel. The two 4GB modules should

be the same size, speed, latency, and so on, and should be installed in the same channel (in this case, in the two blue slots). The same is true for the two 2GB modules, which should be installed in the two blue slots. The slots on this motherboard are color coded to indicate the channels. Always check your documentation for the correct orientation of the channels and the type of RAM your motherboard will accept.

**12. c.** DDR3-800 is also known as PC3-6400 (6400MBps peak transfer rate). DDR3-1066 is also known as PC3-8500 (8500MBps peak transfer rate). DDR3-1333 is also known as PC3-10600 (10667MBps peak transfer rate). DDR3-1600 is also known as PC3-12800 (12800MBps peak transfer rate).

**13.** The storage media types (optical drive, magnetic drive, or flash drive) correspond to the descriptions as follows:

Description	Storage Media
Records information in tracks and sectors containing 512 bytes	Magnetic drive
Stores data in a continuous spiral	Optical drive
Used on memory cards	Flash drive
Records information in a series of lands and pits	Optical drive
Uses laser light to read data	Optical drive
Records information in concentric circles	Magnetic drive
Records information from the center outward	Optical drive
Stores data on double-sided platters	Magnetic drive

Description	Storage Media
Records information from the outer edge inward	Magnetic drive
Used in solid-state drives	Flash drive

- 14. d.** The tablet will have slower data access than if it used an SSD. eMMC memory is slower than memory used in SSDs. It is built into tablets and, therefore, is not removable. A tablet's capability to use USB devices is a function of whether it has USB ports, not its built-in storage.
- 15. c.** 3D printers are the only printer type to create objects by layering filament.
- 16. b, d.** 5400RPM drives are slower but require less energy to run than faster drives. Laptop computers use 2.5-inch or smaller form factor drives.
- 17. b.** RAID 10 includes striping across two drives, for faster performance, and mirroring of the striped array, for data safety.
- 18. a.** The ATX form factor has been the most frequently used motherboard in desktop computers for the past 20 years.
- 19. d.** Mini-ITX is the smallest form factor motherboard, measuring  $6.7 \times 6.7$  inches. For comparison, microATX is  $9.6 \times 9.6$  inches.
- 20. 1. b; 2. c; 3. a**
- 21. 5, 6.** 5 is the 8-pin EPS12V power connector, and 6 is the 24-pin ATX power connector.

**22.** **7** and **8** are RAM slots, as noted by the white tabs that lock them in place. 1 and 4 are PCIe slots. 2 and 3 are PCI slots.

**23. False.** DDR4 and DDR5 DIMMs both have 288-pin designs, but the arrangement and keying of the pins differ. Thus, they are not interchangeable.

**24. c.** The CPU fan connector usually has four pins, and the system fan connector usually has three pins. The extra pin in a CPU fan connector is used to control fan speed.

**25. c.** Make any desired changes to the BIOS startup program and then save those changes to the CMOS chip. The BIOS chip is ROM and cannot be edited; the CMOS chip is RAM and can be edited.

**26. d.** The figure displays a USB 3.0 cable and header.

**27. a.** CMOS is RAM, and RAM is volatile. This means that the CMOS chip must have power to maintain its memory. There are two ways to erase the CMOS settings and revert to the default settings in the BIOS: You can remove the CMOS battery, or you can place the jumper block over the CMOS jumper pins.

**28. b.** When the computer's clock begins to lose time, the fault frequently lies in a weak CMOS battery.

**29. e.** In a high-end customized system, one or all of these components must be upgraded. The CPU needs as many cores as possible for the fastest processing. More and faster RAM, high-end sound cards, multiple displays, and HDMI might be required for peak performance in some systems. In a gaming computer where overclocking is used, you might choose to use a liquid cooling system. A customized system will probably be comparable in cost to a new system.

**30. c.** The computer's power supply is really a power converter. It converts AC power from the wall outlet to DC power that the computer can use.

**31.**

	Total Watts (W)	Number of +12V Amp Output from Rails (R)	+12V Amps (Amp)
Power Supply A	650	4	80
Power Supply B	700	1	52

Power Supply A produces 650 Watts of power and uses four +12V rails that produce 20 amps each, for a total of 80 amps. Power Supply B produces 700 Watts, but it has a single +12V rail that produces only 52 amps. Power Supply A has more usable amperage available to components, so it is the better value. Notice also that Power Supply A was tested at 50° Celsius (122° Fahrenheit) at full load. The Power Supply B label does not tell you how it was tested.

**32. d.** The keyboard, mouse, and touchpad options are incorrect because all use standard input device drivers incorporated into the operating system. A scanner driver is likely not included in the operating system.

**33.** Step 1: Processing

Step 2: Charging

Step 3: Exposing

Step 4: Developing

Step 5: Transferring

Step 6: Fusing

## Step 7: Cleaning

- 34. True.** As long as the drum is kept in the dark, it will retain its charge. During the exposing phase, when the laser writes an image onto the drum, the areas where the laser strikes the drum lose their strong negative charge and become charged at only  $-100V$ . This lesser charge allows the toner—also charged at  $-600V$  —to stick to only the lower-voltage areas, which contain the image to be printed.
- 35. d.** A laser printer stores an entire page in its memory and then prints the entire page at one time. An inkjet printer prints one line at a time. Thermal printers do not use impact printing. A dot-matrix printer is an impact printer; it creates characters by pressing each character onto an inked ribbon and then onto the paper.
- 36. a.** Inkjet printers use closely grouped nozzles of ink to spray tiny dots of color onto the paper to form letters, numbers, and graphics.
- 37. b.** CMYK refers to cyan, magenta, yellow, and black.
- 38. d.** The diagram shows the result of a nozzle check for an inkjet printer. If the print head nozzles are clean and are working properly, the test pattern should look like the left half of the screen. If they are clogged and in need of cleaning, the pattern can look similar to the right side of the screen.
- 39. a.** Thermal printers use either a dot-matrix or a dye-sublimation mechanism. The dot-matrix mechanism has a print head that uses a series of raised dots that can be used to create an image. These dots are heated and used in conjunction with special heat-sensitive paper or a ribbon to transfer the image to the paper.

- 40. b.** Multipart forms require an impact printer to transfer the image through multiple layers of paper. Laser, inkjet, and thermal printers print only on the top layer of a multipart form.
- 41. a, d.** PostScript and Printer Control Language (PCL) are common print drivers. ECC, short for error-correction code, is a special type of memory that enables the system to correct single-bit errors. PCI, short for Peripheral Component Interconnect, is a slot on a motherboard that is used for add-on cards.
- 42. c.** The vendor's website has the most updated drivers available. The disc that ships with the printer will contain the vendor's drivers, but they might not be the most updated versions. The drivers included in Windows might not support recent printers, and Windows Update does not update printer drivers.
- 43. c.** Choosing a cover page is a function of the current application (such as a word processor), not part of the printing process.
- 44. a.** Ad hoc mode supports only WEP encryption. This type of encryption is not as secure as WPA2 or WPA3 and is not generally recommended for secure networking. WPA3 is the recommended wireless encryption today. A NIC is a network interface card, not a type of encryption.

## Chapter 4

### "Do I Know This Already?" Quiz

**1.** c

**2.** a

**3.** c

**4.** a

**5.** a

**6.** a, b

**7.** c

**8.** e

**9.** c

**10.** b

## Review Questions

**1.**

---

### Model Description

- |                   |  |
|-------------------|--|
| <b>a.</b><br>SaaS | <b>3.</b> Enables software to be hosted on remote servers and accessed through web browsers                  |
| <b>b.</b><br>IaaS | <b>1.</b> Provides access to storage, network services, virtualization, and servers                          |
| <b>c.</b><br>PaaS | <b>2.</b> Gives application developers the opportunity to develop and deploy software in a cloud environment |
- 

**2. a, b, c.** Virtualization allows a single machine to act as though it were several machines. A single operating system can host several virtual guest operating systems and can switch between them without being rebooted. These virtual machines can be both 32- and 64-bit systems. A virtual machine uses the same hardware as the host machine, which enables considerable reduction of capital investment.

**3. a, c, d.** Rapid elasticity is the capability of users to quickly increase or decrease the resources they use. Resource

pooling allows a cloud provider's resources to be allocated, divided, and used by many clients simultaneously. Metered service means that the user pays only for the resources used. DHCP is a network service that automatically assigns IP addresses to client computers and is not a service provided by cloud computing.

- 4. b.** A virtual machine manager (VMM) manages the interaction of the virtual environment with the host environment.
- 5. c.** 6144MB (6GB) is the amount of RAM available to the system after starting a 2GB VM. 2048MB (2GB) is the size of the VM itself. 4096MB (4GB) is incorrect. 128MB is the size of the video memory assigned to the display.
- 6. d.** Sandboxing is a security procedure that involves isolating a program, separating it from the main system. A VMM that enables sandboxing (isolation) of each VM and provides physical partitioning of resources provides better security against attacks.
- 7. a.** A hypervisor VMM runs directly on the hardware. It is faster and uses fewer resources than host/guest virtualization. Because the hypervisor uses few computer resources (such as memory and CPU), more computer resources can be made available to each VM.
- 8. c.** *Desktop virtualization* refers to creating a user interface to a computer that is hosted on a central server on-premises or perhaps in the cloud. Either way, the user experience with the virtual desktop is the same. Community cloud computing is a type of hybrid cloud computing that is used by different organizations that are working together. The organizations work together to build the community cloud and share its costs. Cloud providers have designed file synchronization services to make replicating on-

premises data synching to multiple sites automated and reliable. VMMs and hypervisors include a feature known as *virtual machine checkpoints* (or virtual machine snapshots). A checkpoint saves the state, data, and hardware configuration of a VM while it is running.

- 9. d.** Cross-platform virtualization is a type of application virtualization that can involve different underlying virtualization technologies. For example, the virtual software Microsoft 365 is running across platforms as well as operating systems, so users on iPads, Linux devices, and macOS can have the same application software experience. A VMM (virtual machine manager), also called the *hypervisor*, is software that creates and manages virtual machines. Legacy software and operating systems can be used in application virtualization. Support specialists can run several legacy operating systems on one machine without rebooting their systems. On-demand self-services from SaaS providers such as Salesforce.com, Gmail, and others are available to customers when they need them, but they do not need to be maintained by the customer when they are not needed.
- 10. a, b, d.** A workstation that will be used for virtualization needs to be designed with fast multicore processors and as much RAM as possible. Processors selected for a virtualization system should also feature hardware-assisted virtualization. The system BIOS/UEFI firmware must support this feature and be enabled in the system BIOS/UEFI firmware. Answer C is incorrect because the virtual machine manager (VMM)—for example, Hyper-V—runs inside the host operating system. The virtual machines (VMs) themselves are considered the guest operating systems.

## Chapter 5

## **“Do I Know This Already?” Quiz**

- 1.** b
- 2.** a
- 3.** d
- 4.** b, c
- 5.** b, d
- 6.** b, d
- 7.** b, c
- 8.** c
- 9.** d
- 10.** d
- 11.** c
- 12.** c
- 13.** d
- 14.** b
- 15.** b
- 16.** c
- 17.** d
- 18.** d
- 19.** c
- 20.** b

**21.** a, c

**22.** b

**23.** c

## Review Questions

- 1. d.** Reboot the computer and open the BIOS/UEFI menu. Check the BIOS settings for the CPU temperature. As a technician, you should be very familiar with all the diagnostic information that is available in the BIOS.
- 2. a.** A checksum error is generated when the CMOS settings have failed, either because they have been erased or because the CMOS battery has failed. If you see a checksum error message, acknowledge it and allow startup to continue. The system then loads using the default BIOS settings.
- 3. a, b, d.** POST checks the memory, keyboard, hard drives, and other essential hardware. The mouse is not considered to be essential to the operation of the computer and is not checked by POST. If POST finds any problems, it reports them as error messages during startup.
- 4. d.** When the clock and calendar on a computer no longer can keep accurate time, this is an indication of a failing CMOS battery.
- 5. b.** This is a CMOS battery, which provides a constant source of electricity to the CMOS chip to maintain the CMOS programming.
- 6. a.** The Automatic Reboot option is configured in System Properties on the Advanced tab, under Startup and Recovery.

- 7. a.** North America uses 115 volts. Europe and Asia use 230 volts.
- 8. d.** These components are capacitors. Capacitors store an electrical charge and can deliver a painful and even dangerous shock if they are accidentally discharged.
- 9. c.** Having identified the problem as network connectivity and established a theory that a cable is broken, you are testing the theory with a known-good cable.
- 10. a.** These questions are being asked to determine what problem the user's computer has. These questions are part of step 1. Identify the problem in the best practice methodology to resolve problems.
- 11. d.** This jumper forces the SATA drive to run at a slower rate, to make it compatible with older host adapters.
- 12. a.** Reboot the computer and access the BIOS startup program. Reorder the boot sequence and save the changes. Changes made to the BIOS configurations are saved on the CMOS chip.
- 13. c.** S.M.A.R.T. refers to Self-Monitoring, Analysis, and Reporting Technology, which is used to detect problems with an internal magnetic hard drives and warns of failure.
- 14. d.** Had there been proper documentation of a cable map left by a previous technician, the current technician would have saved time.
- 15. a, d.** If an LCD display is flickering, the most likely cause is a failing backlight or inverter.
- 16. c.** Burn-in, the persistent display onscreen of a "ghost" image that was displayed previously, even after the current screen contents changed, can affect both LCD and plasma

displays. On an LCD display, it is frequently caused by stuck pixels.

- 17. b.** Step 2 of the best practice methodology to resolve problems is to establish a theory of probable cause. A DHCP server is responsible for assigning IP addresses on a network. If valid IP addresses are not available, APIPA (169.254.x.x) addresses are assigned. If a network is using APIPA addresses, you should add valid IP addresses to the DHCP server.
- 18. b.** Establishing a plan of action should come after testing the theory to determine the cause (choice C).
- 19. d.** Documenting outcomes is the sixth step of the best practice methodology.
- 20. a, b.** Some cellular connections do not work well if Wi-Fi is enabled, so if you are having problems getting a clear cellular signal, you should disable your Wi-Fi connection. You should also try rotating your screen because the antenna is located around the periphery of the screen casing. 802.11 is a Wi-Fi specification. The iOS slider switch does not affect reception.
- 21. a, c.** You can increase battery life by not overcharging and by shutting down an iOS device weekly with the slider switch.
- 22. d.** Vertical streaks that show up on every page printed by a laser printer usually indicate damage to the imaging drum. Low toner might cause uneven printing. A dirty print ribbon could create problems on a thermal printer or an impact printer. Damaged ink nozzles are a problem on an inkjet printer.
- 23. a.** Clogged or dirty printheads and rollers on an inkjet printer can cause smudging of the printed page. Fusers,

photosensitive drums, and toner cartridges are components of a laser printer, not an inkjet printer.

- 24. b.** The fuser is responsible for heating the toner and pressing it into the paper. Brittle or flaking toner indicates a failing fuser.
- 25. c.** Compressing the data in a print job takes time, which can make the print job slower.
- 26. a.** The print spooler stores print jobs in a queue and releases the computer to perform other tasks while the spooler manages the print job.

## Chapter 6

### "Do I Know This Already?" Quiz

- 1.** d
- 2.** b, c
- 3.** c
- 4.** b
- 5.** b
- 6.** a, b, c, d
- 7.** c
- 8.** a, b
- 9.** b, c
- 10.** c

# Review Questions

- 1. a, b, d.** All computers in a workgroup must be part of the same local network or subnet. If they are to share resources, they must use file and printer sharing. In addition, each user must have a local user account on each computer in the workgroup. However, the workgroup does not have a password.
- 2. a.** Each computer on the network must have a unique name. This name is usually given automatically during installation, but if you want to check your computer's name or if you want to change it, you should open the System Properties. You can do this in several ways. You can open the Control Panel, select System, and select Change Settings. In Windows 10, you can search for rename and find View Your PC's Name in Settings. It is also possible to see the name by right-clicking Start and selecting System. The PC name then is in the top center, and you have the option to rename.

**3.**

Task	Command
a. Open a command prompt	<b>2.</b> cmd or command
b. View all the directories in a specified location	<b>5.</b> dir
c. Create a new folder	<b>8.</b> md or mkdir
d. Remove an empty folder	<b>9.</b> rd or rmdir
e. Remove one or more files	<b>4.</b> del
f. Stop running a specified task	<b>10.</b> taskkill
g. Copy single or multiple files	<b>11.</b> xcopy or robocopy

<b>Task</b>	<b>Command</b>
<b>h.</b> Scan for errors and repair the hard drive	<b>1.</b> chkdsk
<b>i.</b> Close a command prompt	<b>7.</b> exit
<b>j.</b> Create new partitions	<b>6.</b> diskpart
<b>k.</b> Display the help files for a specific command	<b>3.</b> command /?
<b>l.</b> Utility for writing and printing text files	<b>12. cat</b>
<b>4. a.</b> Network discovery and print sharing can be manually configured in the Network and Sharing Center in the Control Panel. These are normally turned off for Guest and Public network settings.	
<b>5. c.</b> Device Manager contains a list of hardware devices and reports on their condition. From Device Manager, you can update drives and disable or enable or uninstall devices. A disabled device in Device Manager displays a downward-pointing arrow over the device icon.	
<b>6. d.</b> System Configuration allows you to select the programs and services that run automatically at startup. Devices and Printers provides centralized management of the computer and most of the hardware connected to it. Programs and Features is used to manage programs installed and Windows features available on the computer. System protection is used to configure System Restore.	
<b>7. c.</b> Open the Network and Sharing Center. In Windows 10, click Change Advanced Sharing Settings, select the type of network you want to configure, and then select Turn on File and Printer Sharing.	
<b>8. c.</b> You have created a mapped network drive. A mapped network drive is a shared folder or drive on a networked	

computer that has been assigned a drive letter and mapped to a location on another computer on the network. That share appears to the user as though it is located on the user's own computer.

**9.**

<b>Utility</b>	<b>Command</b>
a. Registry	4. regedit
b. System Information	3. msinfo32
c. System Configuration	2. msconfig
d. Microsoft Management Console	1. mmc

**10. a.** A VPN is created in the Network and Sharing Center, under Set Up a New Connection or Network. In newer Windows versions, VPNs can also be created in Settings.

**11. a.** Use the Task Scheduler to schedule and view tasks run at regularly scheduled intervals.

**12. a, b, c, d.** All of these features are unavailable when you configure a computer for a public network. When on a public network, you do not want other computers that might be using the network at the same time to be able to see or interact with your computer.

**13. d.** A firewall blocks information from flowing into your computer or, alternatively, allows in that information from the Internet or from another network by closing and opening ports. A firewall can prevent hackers and malware from entering your computer, and it can also prevent your computer from sending malware to other computers.

**14. a, b.** Specific applications that are to be allowed through the firewall and specific ports that are to be opened can be

configured as exceptions in Windows Defender Firewall.

- 15. c.** An IP address has bits that refer to a network and other bits that refer to the host on the network. The number of host and network bits can vary, so a subnet mask is used to define which bits of the IP address refer to the network and which bits refer to the host.
- 16. c.** Time Machine is the backup utility for macOS. **tar** and **crontab** are commands used to schedule and back up a Linux machine. YUM is a utility used in Linux.
- 17. a.** Disk Utility can be used to create blank disk images for use as containers for other files, including image backups. It can also be used to erase non-macOS drives and prepare them for use with macOS. Use **System Preferences > Network** to manage the network connection. Drag the disk icon on the desktop to the trash, wait for it to change into an Eject symbol, and then after the symbol disappears, remove the disk. Use iCloud to manage cloud storage.
- 18. a.** To force quit an app from the Terminal in either macOS or Linux, enter **top** to see a list of process IDs (PIDs) and the apps they represent. Press **q** to quit. To kill an app by specifying its PID, enter the command **kill xxx** (where **xxx** is the PID). Ctrl+Alt+Del is used in Windows to display options, including the Task Manager. **end** and **fq** are not valid terminal commands.
- 19. d.** Linux includes several utilities that can be used for backups. These include the command-line tar and rsync utilities. grsync (GUI for rsync), duplicity (command line and a GUI available as Déjà Dup), and other commands are available from the repository for a Linux distribution or from the vendors. The **compress** command is used to compress files. The **ifconfig** command is used to view IP address information. The **gpg** command is used to encrypt files.

**20. b.** In macOS, screen sharing, file sharing, printer sharing, Internet, Bluetooth, and remote apps are configured through Sharing in System Preferences. Control Panel is a Windows configuration utility. macOS does not have a Sharing app. Display is used to configure display resolution and multiple-monitor settings.

**21. a.** Mission Control allows a user to open and manage applications across multiple displays. Mission Control displays all apps that are open on the desktop so that you can copy or move them between different desktops. This is very helpful when working with multiple displays.

**22. b.** iCloud allows users to store, share, and back up music, video, picture, and document files in a cloud environment. Time Machine is the macOS backup utility. Many utilities for macOS contain the word *assist* or *assistant* (for example, Migration Assistant). Spotlight is the macOS search tool.

**23. c.** The file manager and graphical user interface in the macOS operating systems is known as Finder. In Windows 10 and 11, it is File Explorer. Search is a Windows search utility.

**24. d.** The Dock is the utility that macOS uses to display the icons of all the currently running apps. The taskbar and menu bar are used by Windows. Finder is the file manager for macOS.

**25.**

---

**a. su      9.** Run commands as a different user (usually root)

---

**b. apt-get    5.** Install or manage Advanced Packaging Tools

---

**c. cd      2.** Change folders

---

**d. ls      10.** Show contents of directory or folder

---

a. su	<b>9.</b> Run commands as a different user (usually root)
e. chmod	<b>3.</b> Change permissions
f. ps	<b>6.</b> List currently running processes
g. rm	<b>4.</b> Delete files or folders
h. grep	<b>7.</b> Perform text/word searches
i. pwd	<b>8.</b> Print (display) working directory
j. yum	<b>11.</b> Open-source utility for automatic updates in Linux
k. chown	<b>1.</b> Change file ownership

---

## Chapter 7

### “Do I Know This Already?” Quiz

**1.** b

**2.** c

**3.** d

**4.** b

**5.** d

**6.** a

**7.** c

**8.** a

**9.** b

**10.** d

**11.** c, d

## Review Questions

- 1. b, c.** Andre tailgated into the first door, but the mantrap stopped him from fully entering the building.
- 2. b.** Rack-level security can isolate a single server, to prevent unauthorized access.
- 3.**

Description	Type of Malware
<b>1.</b> Infects and rewrites files. Replicates automatically, with no user intervention.	<b>c.</b> Worm
<b>2.</b> A method of hiding malware from detection programs.	<b>d.</b> Rootkit
<b>3.</b> Tracks web browsing. Uses pop-ups to attract a user's attention.	<b>a.</b> Spyware
<b>4.</b> Encrypts target files and then demands payment to unencrypt files.	<b>e.</b> Ransomware
<b>5.</b> Infects and rewrites files. Replicates itself if a user executes the file.	<b>b.</b> Virus

- 4. d.** WEP is considered insecure and should not be used. Options a, b, and c are all considered important security measures.
- 5. d.** A physical lock and key might be the most difficult form of security to overcome because it cannot be bypassed electronically and cannot be done remotely. An intruder must possess a physical key and must be physically present at the site.
- 6. a, c.** A fingerprint scan, a retinal or iris scan, facial recognition, and voice recognition are all types of biometric

security methods.

- 7. b.** A cable lock is used to secure a laptop to an immovable object, such as a post. A token is any physical object used to gain access to a secure system. Key fobs, RFID cards, and smart cards are all types of tokens.
- 8. c.** A firewall examines data packets that a network is receiving, to determine whether it should deliver the packets to a network location or whether it should block delivery. Data packets can be allowed or blocked, depending on the threat level that is determined by the firewall programming.
- 9. c, d.** A strong password should consist of eight or more characters and a combination of upper- and lowercase letters, symbols, and numbers. In addition, a strong password should not use real names or real words.
- 10. c.** Phishing is a technique that involves tricking a user into revealing confidential information, such as a social security number or credit card information. The technique might involve a bogus security alert in the form of an email or a telephone warning that includes an offer of assistance. In social engineering, the hacker pretends to be a coworker or an IT professional to gain network access. Tailgating is getting through a secure door based on the credentials of the person in front. Dumpster diving involves searching a workstation or the trash for physical clues to passwords or personal information. Shoulder surfing is attempting to physically view confidential information (such as passwords or PINs) by looking over a user's shoulder.
- 11. c.** BitLocker To Go can be used to encrypt a flash drive.
- 12. b, c.** By changing the network name and disabling the SSID broadcast, Ellen can ensure that her neighbors can't

see her network. MAC address filtering allows her to control who has access to the network.

**13. d.** Drive wiping is the most secure formatting technique.

Using standard format and overwriting would work, but recovery software can reconstruct the data. Low-level formatting is done by the manufacturer and is not done in the field.

**14. a.** Share permissions allow group access to folders.

Password attempts do not impact user permissions. Options b and d cannot be true because Hiro could access his account.

**15. b.** File hashing verifies that the contents of files are unaltered. A hash is often created on a file before it is downloaded and then hashed again after the download; the two values are compared to make sure the contents are the same. Trusted sources are sources that you know are legitimate (for example, Microsoft.com, Google.com, Mozilla.org, Apple.com, and so on). Trusted Internet sources can be identified by the *HTTPS* used in the URL. Pop-up blockers are used to prevent pop-ups from appearing when visiting a website. Most newer browsers, such as Google Chrome and Microsoft Edge, have pop-up blocker capabilities built in. Private browsing mode is a feature of web browsers that does not store web browsing data or information. In fact, when you close private browsing mode, all browsing data and information is removed or destroyed.

## Chapter 8

### “Do I Know This Already?” Quiz

**1. c**

- 2.** a
- 3.** a, b, c, d
- 4.** b
- 5.** a
- 6.** b
- 7.** c
- 8.** d
- 9.** b
- 10.** d

## Review Questions

- 1. b.** This is an error message from Windows 10.
- 2. b.** Free space on the system partition is used as a swap file when sufficient RAM is not available. If lack of space is the reason your system has become unresponsive, you should clear space from the system partition by rebooting the computer to free up temporary files, emptying the Trash, or removing files and storing them either on another drive or in the cloud. Upgrading to a newer macOS version can also improve responsiveness.
- 3. a.** Use the System Recovery options and either select the Startup Repair option or open a command prompt and enter **bootrec /fixboot**. In Windows 10, use WinRE. Advanced Boot options are used to start Windows in Safe Mode and other troubleshooting modes. Although a change in the BIOS/UEFI startup settings to a different startup drive could cause this problem, it isn't likely. bootmgr cannot be downloaded from the Internet.

- 4. b.** Ctrl+Alt+Delete is the most common method of accessing the Task Manager in Windows 10.
- 5. a, b, c, d.** The drive containing the paging and temporary files should have at least 10–20 percent free space to process temporary files. If dust and dirt build up around internal components, the CPU and system fans might not be capable of adequately circulating the air and dissipating the heat that builds up, so the CPU might overheat. If your system is performing at a low level, you can try increasing the amount of RAM. Generally, more RAM equals better performance. Too many programs and services at startup will slow the startup process and also slow system performance.

**6.**

---

### **Step Description**

---

- 1. g.** Investigate and verify malware symptoms.
  - 2. d.** Quarantine the infected systems.
  - 3. b.** Disable System Restore (in Windows).
  - 4a. c.** Update the anti-malware software.
  - 4b. h.** Scan and use removal techniques (Safe Mode, preinstallation environment).
  - 5. a.** Schedule scans and run updates.
  - 6. f.** Enable System Restore and create a restore point (in Windows).
  - 7. e.** Educate the end user.
- 
- 7. b.** The Event Viewer contains the log files that Windows creates to record problems in the system. The Device Manager stores information regarding hardware devices and their drivers. Recovery Environment is used in Windows

to diagnose and repair system failures. Finder is the file manager program used in macOS.

- 8. d.** Use the System Restore utility to create restore points before making major changes to your system. If your system has a problem, you can then revert to a restore point, and your computer will be configured as it was when the restore point was created.
- 9. b.** msconfig is a troubleshooting tool that is used to configure system startup. You can use it to disable or enable any programs or services that run automatically when the system boots. You can also use it to configure a normal, diagnostic, or selective startup and to configure the order in which multiple operating systems boot. regedit can be used to change all Windows settings, but it is not the preferred tool for doing so. sfc, the System File Checker, is used to replace damaged Windows system files. msinfo32 is used to display Windows and hardware configuration.
- 10. a, b, and c** can all be causes of a system failure and halt to operations. The cloud connection (d) is not part of the desktop system and should not cause a system failure.
- 11. b.** Selecting Forget This Device clears the old Bluetooth connection data from the device and enables a new pairing connection.
- 12. a, b, c, d.** All these problems can be caused by malicious software that was not downloaded from Google Play or the App Store.

## Chapter 9

### “Do I Know This Already?” Quiz

- 1. b**

**2.** c

**3.** d

**4.** b

**5.** d

**6.** a

**7.** a

**8.** d

**9.** a, c

**10.** c

**11.** a

**12.** a, c

**13.** a

**14.** d

**15.** b

**16.** b

## Review Questions

**a.** 6

**b.** 3

**c.** 5

**d.** 2

**e.** 4

**f. 1**

The object in this diagram is a 3-wire-to-2-wire (grounded-to-ungrounded) adapter. You should use it only when the ground loop is to be connected to a metal grounding device, such as a water pipe.

- 2. c.** In this diagram, the outlet is wired incorrectly. The left light is on, and the center and right lights are off. According to the legend, this indicates that the outlet has an open neutral wire.
- 3. b.** ESD (electrostatic discharge) is the sudden release of static electricity from one object to another. We are not usually aware of the fact that static electricity has built up in our bodies and on the objects around us. When we come in contact with electronic computer components and the static electricity in our bodies discharges into them, those components can be seriously damaged.
- 4. a, c, d.** Electronic components come packaged in antistatic bags and should be stored in them when they are not installed in a computer. Technicians can use electrostatic mats and straps to safely handle computer components.
- 5. a.** Carpet on the floor increases the likelihood of ESD, and a linoleum floor decreases it. Low humidity and low room temperature increase the likelihood of ESD, and increasing them lowers ESD. Rubber-soled shoes help insulate the technician against ESD.
- 6. d.** You should take all batteries to a recycling center. Many electronics stores also accept batteries for recycling. Never put batteries into the trash or even into a recycling bin.
- 7. d.** All of these contain toxic e-waste that should be treated as hazardous material and properly disposed of or recycled.

- 8. c.** Use a Class C fire extinguisher for an electrical fire.
- 9. c.** P = oil proof, R = oil resistant, N = not resistant to oil. A P100 mask is best, giving nearly 100 percent protection against oil and non-oil particulate aerosols. An R95 mask is next, with 95 percent protection against oil and non-oil particulate aerosols. Last is an N95 mask, with 95 percent protection against non-oil particulate aerosols. No class A mask exists.
- 10. b.** An MSDS contains information about dangerous chemicals. It describes how to store them, how to clean up spills, and which type of treatment to follow when you are exposed to them.
- 11. d.** UPS batteries are made from lead-acid cells and are thus much heavier than the other batteries listed. All battery types listed are made of hazardous materials and require proper disposal.
- 12. a.** UPS stands for *uninterruptible power supply*. A UPS is a battery backup that is used to power a system when the main AC power fails. A UPS is not designed to replace the AC power for a long period of time; it is only a backup battery. A UPS is designed to keep a computer running long enough for you to shut down in an orderly manner so that your system does not crash.
- 13. b.** The chain of custody documents who had possession of evidence relative to a legal investigation.
- 14. a, b, c, d.** All of the options apply to open source software. Open source software may be freely used and may be modified. It may be sold and also may be used for commercial purposes.
- 15. a, b, d.** Storing sensitive information in cloud storage is more secure than storing it locally. BitLocker encryption

encrypts the entire hard drive, not just selected files. You should install hardware and software firewalls to prevent intrusion. Files saved to a PC's hard drive, a laptop, or a backup file are all much more vulnerable to hackers than the other methods listed.

- 16. c.** Much of the success of your business (and your employer's business) depends on your customer skills. This is one of the most valuable assets that you bring to the job. You should always treat your customers with respect, listen carefully to what they have to say, and explain what you are doing in clear, easy-to-understand terms. Do not use a lot of technical jargon that the customer might not understand, and do not act aloof.
- 17. d.** The appropriate first response is to contact the violator's supervisor and get instructions on how to proceed. This is considered an incident and needs to be documented.
- 18. c.** Active listening includes all three parts of Fatima's approach. Cultural sensitivity and dealing with difficult customers are important soft skills but are not demonstrated here. Presumptive listening is not a skill in good customer service.
- 19. c.** RDP, or Remote Desktop Protocol, was likely used. Telnet is not secure. FTP is a protocol for transferring files. RDP is available in macOS.
- 20. b.** .sh is the extension for Linux shell script. BASH is the most common shell in Linux. The other extensions listed are .js for JavaScript, .py for Python, and .bat for Windows batch file.
- 21. b.** A whitepaper is a technical paper written to explain complex technical information to nontechnical people. All

three other answers demonstrate poor customer service skills.

- 22. a.** The changes made by the healthcare provider unwittingly left Carla unable to do her job. When a major change is being implemented, an important step in change management is to get feedback from stakeholders who might be affected. The other answers do not involve change management practices.

## Appendix B

# ***CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide Exam Updates***

Over time, reader feedback allows Pearson to gauge which topics give our readers the most problems when taking the exams. To assist readers with those topics, the authors create new materials clarifying and expanding on those troublesome exam topics. As mentioned in the Introduction, the additional content about the exam is contained in a PDF on this book's companion website, at [www.pearsonitcertification.com/title/9780137675944](http://www.pearsonitcertification.com/title/9780137675944).

This appendix is intended to provide you with updated information if CompTIA makes minor modifications to the exams upon which this book is based. When CompTIA releases an entirely new exam, the changes are usually too extensive to provide in a simple update appendix. In those cases, you might need to consult the new edition of the book for the updated content. This appendix attempts to fill the void that occurs with any print book. In particular, this appendix does the following:

- Mentions technical items that might not have been covered elsewhere in the book
- Covers new topics if CompTIA adds new content to the exam over time

- Provides a way to get up-to-the-minute current information about content for the exam

## Always Get the Latest at the Book's Product Page

You are reading the version of this appendix that was available when your book was printed. However, the main purpose of this appendix is to be a living, changing document; be sure to look for the latest version online at the book's companion website. To do so, follow these steps:

**Step 1.** Browse to

[www.pearsonitcertification.com/title/9780137675944](http://www.pearsonitcertification.com/title/9780137675944).

**Step 2.** Click the **Updates** tab.

**Step 3.** If a new Appendix B document is available on this tab, download that document.

### Note

The downloaded document has a version number. Compare the version of the print Appendix B (Version 1.0) with the latest online version of this appendix and do the following:

- **Same version:** Ignore the PDF that you downloaded from the companion website.
- **Website has a later version:** Ignore this Appendix B in your book and read only the latest version that you downloaded from the companion website.

## Technical Content

The current Version 1.0 of this appendix does not contain additional technical coverage.

# Glossary

## Numerics

**3-2-1 backup rule** The 3-2-1 backup rule/scheme is an easy way to define the practice of keeping: (3) 1 primary plus 2 backup copies of data; (2) 2 methods of storage for the data (for example, local and cloud); (1): 1 local backup offsite, in case of fire or storm damage to a facility.

**3D printer** Commonly known as additive manufacturing (AM), a 3D printer comes in two flavors: fused deposition modeling (FDM), which is 3D printing in a tabletop environment, and stereolithography (SLA), which is a newer 3D tabletop process that involves photopolymer resins and lasers. The most common material used with 3D printers is a strand of plastic filament that is fed from a spool to a moving printer head. The printer head heats the plastic and thinly layers it on the printing platform in cross-sections that eventually build up into the 3D object that has been designed on the computer.

**802.11a** A wireless Ethernet standard that uses 5GHz radio signals and provides performance at rates from 6Mbps up to 54Mbps. It is not compatible with other 802.11-based wireless networks unless dual-band access points are used.

**802.11ac (Wi-Fi 5)** A wireless Ethernet standard that uses 5GHz radio signaling for performance up to 1300Mbps. It uses MU-MIMO antenna technology.

**802.11ax (Wi-Fi 6)** A wireless Ethernet standard that uses both 2.4GHz and 5GHz bands, with increased speeds up to 9.6Gbps. Wi-Fi

6E improves upon Wi-Fi 6 by supporting the 6GHz band.

**802.11b** A wireless Ethernet standard that uses 2.4GHz radio signaling for performance from 2Mbps to 11Mbps. It is compatible with 802.11g-based wireless networks but not with 802.11a-based networks unless dual-band access points are used.

**802.11g** A wireless Ethernet standard that uses 2.4GHz radio signaling for performance up to 54Mbps. It is compatible with 802.11b-based wireless networks but not with 802.11a-based networks unless dual-band access points are used.

**802.11n (Wi-Fi 4)** A wireless Ethernet standard that uses 2.4GHz and 5GHz radio signaling for performance up to 600Mbps. It uses MIMO antenna technology.

## A

**A records** DNS stores 32-bit IPv4 address data in A records, and DNS accesses A records when resolving IPv4 address requests.

**AAAA records** DNS stores 128-bit IPv6 address data in AAAA records, and DNS accesses AAAA records when resolving IPv6 address requests.

**acceptable use policy (AUP)** A company's policy for employees that pertains to user safety, security procedures, and computer best practices within a company. The policy is designed to keep the network safe.

**access control list (ACL)** A list of permissions or restriction rules for access to an object such as a file or folder.

**access control vestibule** Formerly known as a mantrap, an access control vestibule is an area with two locking doors that is used to enforce physical security and monitor for unauthorized access to a building entrance.

**access point** A piece of hardware that extends a wired network to wireless connections.

**Active Directory** A Microsoft solution for managing users, computers, and information access in a network.

**ad blocker** A tool that integrates with a web browser and uses filtering to block specific advertisements. Ad blockers assist with online privacy and help to avoid spyware-infected ads.

**Advanced Encryption Standard (AES)** A protocol that is similar to TKIP. AES is more secure and is used with the WPA2 wireless encryption standard.

**Advanced RISC Machine (ARM)** A processor architecture that is based on Reduced Instruction Set Computer (RISC). ARM is the most widely used instruction set architecture. ARM processors are low cost, have minimal power consumption, and generate lower heat, making them ideal for devices such as smartphones, tablets, laptops, and other embedded systems.

**Advanced Technology eXtended (ATX)** A family of motherboards that has dominated desktop computer designs since the late 1990s. An ATX motherboard has the following characteristics: a rear port cluster for I/O ports, expansion slots that run parallel to the short side of the motherboard, and a left-side case opening (as viewed from the front of a tower PC).

**Android** An open-source operating system based on the Linux kernel and used mostly on smartphones and tablet computers. Android is developed by the Open Handset Alliance, a group directed by Google.

**Android Package (APK) source** Format for applications to run on the Android OS.

**anti-malware software** Software that scans for infections that antivirus software might have missed.

**antivirus software** Software that provides real-time protection against threats from local files, websites, and email.

**.app files** In macOS, the application bundle files that contain all the files and folders that make up the application.

**Apple File System (APFS)** The Apple file allocation system designed to work with SSD and flash drives.

**application spoofing** The act of a malicious application imitating a legitimate application and tricking the user into revealing passwords or other sensitive information as they interact with the false app. This process is very similar to a phishing attack.

**application virtualization** Allows users to access applications from a different computer than the one where the application is installed.

**apt-get** A Linux command used to install or manage APT (Advanced Packaging Tool) software packages. It is common in Debian-based distributions such as Ubuntu.

**authentication** The process of verifying user identity.

**authentication, authorization, and accounting (AAA) server** An AAA server is used to examine and either verify or deny credentials to a user who is attempting to log into secured networks.

**automatic document feeder (ADF)** A feature found in printers, photocopiers, and scanners that automatically feeds a single sheet of paper from a stack of paper into the machine. This allows the user to print, scan, or copy without needing to manually feed paper into the machine one sheet at a time.

**Automatic Private IP Addressing (APIPA)** Most IP networks use addresses provided automatically by DHCP; however, if the DHCP server becomes unavailable and an alternate IP address has not been set up, devices on the network assign themselves APIPA/link local addresses. These addresses are in the IPv4 address range 169.254.0.1 to 169.254.255.254 (with the subnet mask 255.255.0.0). The IPv6 version is called a link local address and has the FE80::/64 prefix. A device with an APIPA address cannot connect to the Internet.

## B

**.bat script files** .bat files are script files that are strictly Windows based. They are text files that contain commands or instructions for the command-line interpreter to execute.

**biometrics** The use of a person's biological information, such as fingerprints, retina scans, or facial recognition, to authenticate a potential user of a secure area.

**BitLocker** Full disk encryption software by Microsoft that can encrypt the entire disk. After encryption is completed, authentication is required to access the drive.

**BitLocker To Go** BitLocker functionality that is extended to removable drives.

**black screen** The absence of video output during the boot sequence. It can indicate cable or software issues.

**blue screen of death (BSOD)** An error in which the screen background is blue (or sometimes black), with the error message in white text. Such errors can occur either during startup or after a system is running, and they halt a system by default.

**Bluetooth** A short-range wireless network used primarily by mobile devices.

**bollards** Short wood, metal, or concrete posts installed in sidewalks and driveways to allow pedestrian and bike traffic to pass, while keeping larger vehicles away.

**boot methods** The methods used to load OS files into RAM. Examples are using HD, a thumb drive, a CD, or a network boot.

**boot sector virus** Similar to a root kit virus, in that the virus is embedded deep into the computer. In this case, the virus embeds itself into the initial code of the boot sector on a hard drive.

**bootleg** Unauthorized copies of software; also files with unauthorized changes.

**brute-force attack** A method of cracking passwords by calculating and using every possible combination of characters until the correct password is discovered.

## C

**cable** Broadband Internet service that is provided by a cable TV company. Broadband can deliver voice, data, and video at one time.

**cable modem** A device that encodes and decodes cable Internet network signals. It can be connected to a single computer or to a wired or wireless router.

**cable stripper** A tool used to strip a portion of the plastic jacket off a cable to expose the individual wires.

**cable tester** A tool that tests each wire in a cable and makes sure each one is wired properly.

**capacitor swelling** Capacitors are used as part of the voltage step-down circuits that provide power to the processor. From 2002 to 2007, many motherboards were built using faulty capacitors that became swollen and leaked, causing system failure and sometimes physical damage to the motherboard.

**capture card** A video capture card is equipped to receive HDTV or higher-quality signs via HDMI, DVI, or component. Video capture cards have built-in hardware support for MPEG-4 recording and can be used to capture video for training, game recording, YouTube, or broadcast purposes. Some video capture devices connect to a USB port.

**cat** A Linux utility command for writing text into files and printing file content.

**Cat 5** Category 5 TP cable. Supports Fast Ethernet (up to 100Mbps) and uses 24-gauge wires.

**Cat 5e** Category 5e TP cable. Supports Gigabit Ethernet (10/100/1000Mbps).

**Cat 6** Category 6 TP cable. Supports 10G Ethernet (10/100/1000/10000Mbps) and reduces crosstalk for more reliable connections at gigabit speeds.

**Cat 6a** Category 6a TP cable. Supports 10BASE-T, 100BASE-T, 1000BASE-T, and 10GBASE-T (10Gbps Ethernet).

**cd** A Linux command used to change directories (folders).

**cellular** A data network that enables mobile devices to offer many ways to connect to other devices, including sharing their Wi-Fi or cellular connections with one or more computers.

**Certificate Manager (certmgr.msc)** Allows the import, export, modification, or deletion of root certificates that manage authentication when sending and receiving information in Windows.

**certification of destruction/recycling** Offered by a certified third-party material destruction company that verifies the destruction and recycling of material.

**chain of custody** Chronological documentation or paper trail of evidence.

**change management** The process of preparing for changes in a network, including planning, staffing, organizing, and getting feedback from impacted stakeholders.

**channel** The wireless spectrum is divided into 11 channels. Part of installing a router on a 2.4GHz wireless network is selecting an appropriate channel for the signal.

**charging** Step 2 of the laser printing process, in which the cylinder-shape imaging drum receives an electrostatic charge of -600Vdc (DC voltage) from a conditioning roller.

**chkdsk** A Windows command that scans a specified drive for errors and repairs them.

**chmod** A Linux command used to change permissions on files and directories.

**chown** A Linux command used to change file ownership.

**Chrome OS** Google open-source mobile operating system, which is chiefly designed to run on web-based applications and is installed on Chromebooks, which are an inexpensive laptop option.

**CIFS** Common Internet File System, an early standard method for sharing files across corporate intranets and the Internet. It has largely been replaced by updated versions of Server Message Block (SMB).

**clean install** A fresh installation of the Windows OS as an upgrade or to free up space on the disk.

**cleaning** Step 7 of the laser printing process, which involves preparing the drum for a new page by removing the preceding page from the drum by using a discharge lamp. Toner that is not adhering to the surface of the drum is scraped from the drum's surface for reuse.

**coaxial** A type of cable that consists of a solid center copper core, insulation, a metal braided jacket for grounding, and a vinyl or plastic outer jacket. It is commonly used for cable TV, cable Internet, and satellite Internet.

**[command name] /?** A Windows command that displays help for the specified command.

**community cloud computing** A type of cloud computing in which organizations with common concerns or goals share a cloud infrastructure.

**connection oriented** Transmission Control Protocol (TCP) sessions are known as connection-oriented sessions. This means that every packet that is sent is checked for delivery. If the receiving computer does not receive a packet, it cannot assemble the message and must ask the sending computer to transmit the missing packet again. No packet is left behind.

**connectionless** User Datagram Protocol (UDP) sessions are known as connectionless sessions. This means the messages are sent without an expectation of communication from the receiver. UDP does its best to send a message, but errors are not accounted for.

**content filtering** Blocking content into a local network or group of users, filtering by web address or inappropriate terms in the content.

**copy** A Windows command that copies one or more files to another folder or drive.

**corporate use license** A license that covers the use of software by workers in a company or another organization.

**cp** A Linux command used to copy files to a specified location.

**crimper** A tool used to attach a connector to the end of a raw twisted pair (TP) or coaxial cable.

**cross-platform virtualization** A type of application virtualization that can involve different underlying virtualization technologies.

**cross-site scripting (XSS)** Involves tricking a user, often with a link in an email or some other ruse. When an unsuspecting user clicks, the attacker can inject malicious code into a web-based app.

**cryptominers** Viruses that take over resources of an infected computer for the purpose of mining cryptocurrency (usually Bitcoin). This practice is also known as cryptojacking.

**cursor drift** When a screen cursor unintentionally moves across the screen, typically caused by accidentally swiping or pressing on the device's touchpad, or by a problem with the device's integrated pointing stick.

## D

**data-at-rest encryption** Encryption of backup data that is "at rest," usually archived in data centers and not in current use.

**DB9** A nine-pin D-shell connector.

**Defender Antivirus** The antivirus application built into Windows Defender. This can work in place of or along with third-party antivirus applications.

**degaussing** The process of removing magnetic content from hard drives, magnetic tapes, or other magnetic digital storage.

**denial of service (DoS)** An attack in which one computer sends an overwhelming number of service requests to a specific target.

**desktop virtualization** The creation of a user interface to a computer that is hosted on a central server on the premises or in the cloud.

**Device Manager (devmgmt.msc)** A Microsoft Windows utility that displays detailed information about the computer hardware in a system, including status and driver information.

**df** Linux command used to display used and free space on disks.

**DHCP** Dynamic Host Configuration Protocol; a protocol used to automatically assign IP addresses to hosts. DHCP uses ports 67 and 68.

**DHCP lease** A device is leased an IP address for a certain amount of time and can renew a leased IP address before the lease expires. If the lease expires, the device must request an IP address again.

**DHCP reservation** A permanent lease that is assigned to a DHCP client.

**DHCP scope** A pool or range of IP addresses that the DHCP server can assign or lease to devices.

**dictionary attack** An attempt to crack passwords by trying all the words in a list, such as a dictionary. A simple list might include commonly used passwords such as 12345678 and password.

**differential backup** These backups record data that has changed since the last full backup. They can be done often to ensure that data backups are very current.

**dig** Domain Information Grouper; a Linux command that provides information on DNS servers for troubleshooting DNS issues.

**digital rights management (DRM)** The general term for software or service mechanisms that limit the end user's rights to copy, transfer, or use software or digital media.

**Digital Visual Interface (DVI)** A standard that replaced DFP for the support of LCD displays on desktop computers. DVI-D is for digital displays only, DVI-I supports digital and analog displays, and DVI-A supports analog displays only.

**digitizer** A touchscreen display differs from a standard laptop display, in that it has a digitizer layer on top of the display panel. The digitizer detects and transmits touches to the laptop processor. Digitizers are also used on touchscreen smartphones, tablets, fitness monitors, smart watches, phablets, e-readers, and smart cameras.

**dir** A Windows command that displays a list of a folder's files and subfolders.

**direct burial** Versions of UTP and STP cables designed with enough protection on the outer jacket, commonly known as a CMX jacket, to withstand weather, ground moisture, and even direct placement in water.

**Disk Cleanup (cleanmgr.exe)** A Windows command-line command that brings up disk cleanup and management utilities.

**Disk Defragment (dfsgui.exe)** A Windows command-line utility for defragmenting a drive.

**Disk Management (diskmgmt.msc)** A snap-in of the Computer Management Console that is a GUI-based application for analyzing and configuring hard drives.

**Disk Utility** Utility in macOS for managing disk images.

**diskpart** A Windows command that creates, removes, and manages disk partitions.

**DisplayPort** A cable and port that is primarily used to transmit video that can also send audio and USB signals. It was designed as a replacement for VGA and DVI.

**distributed denial of service (DDoS)** An attack in which the perpetrator uses multiple computers to disrupt the target computer's access to the Internet.

**.dmg files** Disk Image files in the macOS. Similar to ISO files in Windows.

**DNS** Domain Name System; a service that translates domain names into IP addresses. DNS uses port 53.

**Dock** A macOS feature for launching and switching applications that displays app icons across the bottom of the desktop.

**docking station** A device where laptops, smartphones, tablets, or other mobile devices can be placed to be charged and connected to various peripherals.

**domain** A computer network or group of computer networks under the same administration.

**domain access** Accessing the domain to manage computers on the domain.

**Domain Name System (DNS)** Domain Name System; a service that translates domain names into IP addresses. DNS uses port 53.

**Domain-based Message Authentication, Reporting, and Conformance (DMARC)** A mail authentication process that builds on DKIM and SPF to further enhance security from fraudulent spam.

**DomainKeys Identified Mail (DKIM)** A process that enables a receiving mail system to check that the message was authorized by the sending party and was not used for spam or phishing.

**Double Data Rate 3 (DDR3)** DDR3 SDRAM; the successor to DDR2 SDRAM, which runs its external data bus at twice the speed of

DDR2 SDRAM, enabling faster performance. DDR3 SDRAM also uses lower voltages than DDR2 and supports higher memory capacities.

**Double Data Rate 4 (DDR4)** DDR4 SDRAM; the successor to DDR3 SDRAM, which runs its external data bus at twice the speed of DDR3 SDRAM, enabling faster performance. DDR4 SDRAM also uses lower voltages than DDR3 and supports higher memory capacities.

**Double Data Rate 5 (DDR5)** DDR5 SDRAM was released in 2020 and is the fifth generation of DDR memory. Although DDR5 DIMMs has the same number of pins as DDR4 (288 pins), they are not compatible because the alignment key is located in a different area on the RAM stick. Compared to DDR4, DDR5 reduces power consumption (1.1V vs. 1.2V), offers twice the data transfer rate (6.4Gbps vs. 3.2Gbps), and has four times the memory density per chip (64GB vs. 16GB). DDR5 can include an onboard voltage regulator to gain higher speeds. In addition, the burst length in DDR5 is increased from DDR4's 8 to 16.

**DSL** Digital Subscriber Line; a type of broadband Internet service that uses telephone lines to carry Internet traffic at speeds up to 1.5Mbps or more while allowing you to use your phone for normal functions at the same time. Two major types of DSL are ADSL and SDSL.

**dual channel** A motherboard feature in which two identical memory modules are treated as a single logical unit for faster access.

**dumpster diving** The process of going through the trash, seeking information about a network or a person with access to the network.

**duplexing assembly** A printer component that switches paper from the front to the back side so that the printer can print on both sides of the paper.

**Dynamic Host Configuration Protocol (DHCP) reservations** A protocol that allows a computer, router, or other DHCP-enabled device to assign IP addresses to hosts on a local network.

**dynamic IP addresses** Addresses that are assigned by a DHCP server and that will likely change each time a device leaves and then rejoins the network or when the address is used beyond its lease time and expires.

## E

**Ease of Access** Windows app for configuring settings to the user's needs and tastes.

**electrostatic discharge (ESD)** Static electricity that discharges to something that has a different electric potential, especially metallic items such as circuit boards. Casually picking up an expensive video card can possibly damage it. This damage can cause a complete failure or can cause intermittent issues that might be difficult to troubleshoot.

**embedded system** Dedicated computing devices used for specific tasks such as machine control, point-of-sale systems, or ATMs. Embedded systems are often legacy systems.

**Encrypting File System (EFS)** A feature used to protect sensitive data files and temporary files through encryption that can be applied to individual files or folders.

**end-user license agreement (EULA)** An agreement that restricts how an app can be used and what the transfer rights are.

**error-correction code (ECC)** Advanced memory that can correct errors and requires special chipsets. ECC is used primarily in servers.

**Event Viewer (eventvwr.msc)** A Windows tool that allows an administrator to track all the logs of events logins, security actions, crashes, and so on that have happened in the computer.

**evil twin** A type of network attack that involves setting up a fake access point to gather access information from legitimate users.

**expansion cards** Onboarded video, audio, and graphics cards that have dedicated memory space to enhance video, audio, and graphics

capabilities beyond what most CPUs can do inherently.

**exposing** Step 3 of the laser printing process, in which a moving mirror moves the laser beam across the surface of the drum. As it moves, the laser beam temporarily records the image of the page to be printed on the surface of the drum by reducing the voltage of the charge applied by the charger corona to -100VDC.

**Extensible File Allocation Table (exFAT)** Also known as FAT64; a file system designed to enable mobile personal storage media to be used seamlessly on mobile and desktop computers.

**External SATA (eSATA)** External SATA cables enable external drives to be mounted at the same data rate. eSATA has better shielding to protect the cable and the data than regular SATA.

## F

**F type** A connector used for cable, satellite, and fixed wireless Internet and TV service. It can be crimped or attached via compression to the coaxial cable.

**fiber** Abbreviation for *fiber optic*. Network cable that uses glass fibers to transmit photons to carry data.

**fiber-optic cabling** Network cable that uses glass fibers to transmit photons to carry data.

**filament** The (usually) plastic material that is fed from a spool, which is basically the "ink" for a 3D printer. The two most common types of filament are polylactic acid (PLA) and acrylonitrile butadiene styrene (ABS).

**File Allocation Table 32 (FAT32)** The Windows file system introduced in 1995 that has a 32-bit file allocation table, which allows for 268,435,456 entries (2<sup>32</sup>) per drive.

**file server** Typically a computer with a single large drive or a RAID array for shared storage on a network.

**file synchronization** The process of ensuring that one or more files that are stored in different locations are updated and identical.

**FileVault** A disk encryption app in macOS.

**find** A Linux command for searching for files and folders.

**Finder** Application on Apple computers for searching for files or apps.

**firewall** A hardware appliance or software application that protects a computer from unwanted intrusion.

**firmware update** Solves operational problems and adds features that enhance Wi-Fi interoperability, security, and ease of use on devices.

**flash drive** A small electronic device (typically a USB drive) that contains flash memory that is used for storing data or transferring it to or from a computer, digital camera, or similar device.

**Force Quit** A Linux and macOS option to shut down an unresponsive app or program.

**format** A Windows command-line command that prepares a hard drive with a file system in order to install an operating system.

**Fourth Extended Filesystem (ext4)** Linux OS journaling system of events to minimize the impact of a system failure. It is the replacement for ext3.

**frequencies** The frequency ranges in the wireless spectrum that carry the 2.4GHz and 5GHz Wi-Fi bands.

**FTP** File Transfer Protocol; a protocol that both web browsers and specialized FTP programs use to access dedicated file transfer servers for file downloads and uploads. FTP uses port 21.

**full backup** A backup of the entire contents of the computer or selected drive to another local or network location. Because every file is copied, a full backup takes the longest and uses the most storage of the backup types.

**fuser assembly** A laser printer component that fuses the page image to the paper.

**fusing** Step 6 of the laser printing process, in which the printed sheet of paper is pulled through fuser rollers, using high temperatures (approximately 350° Fahrenheit) to heat the toner and press it into the paper. The printed image is slightly raised above the surface of the paper.

## G

**gateway** Identifies the IP address of a device that connects the computer to the Internet or another network.

**gestures** Finger movements made across a macOS trackpad or Magic Mouse surface, or across a touchscreen on another OS to perform specific tasks.

**gpedit.msc** *See Group Policy Editor.*

**gpresult** A Windows command that displays the resultant set of policy for the specified computer and user.

**gpupdate** A Windows command that refreshes the Group Policy on local or Active Directory systems.

**grandfather-father-son (GFS)** A backup rotation method that describes keeping three different generations, or types of backups, in various places. The name is simply an easy way to remember that full backups (grandfather—perhaps a monthly backup stored redundantly offsite) can be combined with a weekly backup (father—also sent offsite) and a daily incremental backup (son).

**grep** A Linux command used to perform text searches.

**Group Policy Editor (gpedit.msc)** Utility in Windows that is a graphic interface for editing items in the Registry.

**GUID [globally unique identifier] Partition Table (GPT)** The table that describes the partitions on a physical HD so that they are

recognized by the OS.

## H

**hard disk drive (HDD)** A mass storage device. This term can also refer to a hybrid drive or a solid-state drive (SSD).

**hard token** Any physical device that a user must carry to gain access to a specific system. Examples are smart cards, RFID cards, USB tokens, and key fobs.

**hardware security module (HSM)** A module or external device that can be added to store security keys for general use.

**hashing** Method of verifying that the contents of files are unaltered. A hash is often created on a file before it is downloaded and then hashed after the download; the two values then are compared to make sure that the contents are the same.

**headers** Refers to the pin headers that the connectors plug into on a motherboard.

**heat sink** A finned metal device that radiates heat away from the processor.

**high availability** Ensuring that resources are always up and available to users.

**high latency** An escalated amount of data delay between sender and receiver, which can be caused by router overloads or high demand on a key bottleneck of a network.

**High-Definition Multimedia Interface (HDMI)** A compact audio/video interface for transmitting uncompressed digital data.

**hostname** The name given to a device on the network, making it distinguishable from other devices.

**hotspot** A method for sharing a smartphone's Internet access via Wi-Fi.

**HTTP** Hypertext Transfer Protocol; a protocol used by web browsers, such as Internet Explorer, Microsoft Edge, Firefox, and Chrome, to access websites and content. HTTP uses port 80.

**HTTPS** Hypertext Transfer Protocol over Secure Sockets Layer; a protocol that is often used for payment transactions on the World Wide Web and for sensitive transactions in corporate information systems. HTTPS uses port 443.

**hub** A simple device used on an Ethernet network for connecting devices to each other.

**hybrid cloud computing** A type of computing that shares characteristics of both private and public clouds. A hard disk drive with a small solid-state drive (SSD) onboard is used to improve disk access time.

## I

**IaaS** Infrastructure as a Service; a type of cloud computing in which users can lease cloud-based network services, servers, storage space, and other resources.

**iCloud** The iOS cloud backup service.

**image deployment** The process of installing Microsoft Windows from an image. It is also known as disk cloning.

**imaging drum** A printer component that applies the page image to the transfer belt or roller. It is frequently combined with the toner supply in a toner cartridge.

**IMAP** Internet Message Access Protocol; an email protocol that enables messages to remain on the email server so that they can be retrieved from any location. IMAP uses port 143.

**impact printer** A printer that uses a mechanical print head that presses against an inked ribbon to print characters and graphics. Impact printers are the oldest printer technology, and they are primarily used today in industrial and point-of-sale applications.

**impersonation** A type of social engineering similar to phishing, in which a hacker sends an email pretending to be someone the victim trusts.

**Incident reports** When a rule or law has been broken, an incident report is necessary so that the company can track its legal responsibilities. This allows the company to plan for training and to comply with laws as necessary.

**incremental backup** These backups copy only data that has changed since the last backup. If a full backup is performed every Saturday, an incremental backup could be run each day of the week, recording one day of activity each time. This way, backups are current but a full backup does not have to be run each day.

**Information Technology eXtended (ITX)** A family of motherboards that was originally developed by VIA Technologies in 2001 for use with its low-power x86 C3 processors.

**injectors** Power over Ethernet (PoE) devices installed between a standard Ethernet switch and a PoE device to provide power only.

**inkjet printer** A print technology that sprays fine droplets of ink onto the page.

**in-place upgrade** A type of upgrade that involves updating an installation to the new version with the existing configuration. It is another name for a repair installation in Windows.

**in-plane switching (IPS)** An active matrix LCD technology that holds liquid crystal cells horizontally between two glass layers. When electric current is applied, the cells rotate, allowing light and color to display on the screen.

**input/output operations per second (IOPS)** The standard way to measure the performance of hard disk drives (HDDs) and solid-state drives (SSDs) in a computer.

**Integrated Drive Electronics (IDE)** The interface that connects the motherboard to drives such as a CD-ROM/DVD or a hard drive.

**Internet appliances** A single-purpose device used to perform specific tasks on an IP network.

**Internet of Things (IoT)** A catch-all term referring to devices that have embedded Internet communication capabilities. These devices include phones, cars, home appliances, door locks, wall outlets, lights, and video-enabled doorbells, among many others. IoT devices communicate data without human interaction.

**Internet Protocol (IP) addressing scheme** Refers to the pattern of IP addresses for hosts on a local network or subnetworks.

**iOS** The closed source mobile OS for Apple devices, used by iPod Touch, iPad, and iPhone devices.

**IP** Internet Protocol; the common protocol for communications on networks and over the Internet.

**IP addresses** Changeable, logical addresses that are assigned to devices for communicating outside their local networks.

**IP filtering** Method of controlling which Internet Protocol (IP) traffic will be allowed into and out of your network.

**iPadOS** Mobile OS developed by Apple for tablets.

**ipconfig** Command that returns IP configurations on local network adapters (virtual and physical) on a computer.

**IPv4** An IP version 4 (IPv4) address consists of a group of four numbers that each range from 0 to 255 (for example, 192.168.5.1). An IP address is divided into two sections: the network portion, which is the number of the network the computer is on, and the host portion, which is the individual number of the computer.

**IPv6** IP version 6 (IPv6) greatly increases the number of available IP addresses for computers, smartphones, and other mobile devices. IPv6 uses 128-bit source and destination IP addresses (compared to 32-bit addresses for IPv4), theoretically enabling up to 340 undecillion addresses ( $3.4 \times 10^{38}$ ).

## J–L

**jailbreaking** “Breaking into” the root access of a phone to change settings or portability.

**jitter** The presence of variations of a network’s latency, which can cause problems for end users on a network.

**.js script files** JavaScript is a programming language that has many uses today. It is valuable for creating scripts because it can be run on any operating system. It is usually written into web pages to create client interactions; JavaScript is read by the browser. Creating and running command-line JavaScript requires installing Node.js.

**Kerberos** An open standard authentication protocol that is used between two clients (or a client and a server) and a third-party Kerberos Key Distribution Center server. The clients acquire a Kerberos key and can mutually authenticate across an unsecure network or the Internet.

**keyboard** An alphanumeric data entry device with a typewriter-style keyboard and additional functional, numeric, directional, and text-editing keys. It connects via a USB or PS/2 keyboard port. The keyboard also includes Fn keys for special functions.

**Keychain** A macOS password-management system.

**keylogger** A hardware device or software program (often a virus) that can track keystrokes and capture the usernames and passwords of unwitting users.

**LAN** Local area network; a group of computers and other devices that are usually located in a small area such as a house, a small office, or a single building.

**laser printer** A page printer that stores the entire contents of a page to be printed in its memory before printing it. By contrast, inkjet, thermal, and impact printers print a page as a series of narrow bands.

**LDAP** Lightweight Directory Access Protocol; a protocol used to access and maintain distributed directories of information, such as the kind involved with Microsoft domains. LDAP uses port 389.

**legacy software and operating systems** An outdated operating system, programming language, application, or hardware.

**light-emitting diode (LED) status indicators** LED lights that technicians use to evaluate a computer's health at a glance. Computers, NICs, switches, routers, and other devices all use LEDs to visually communicate their activity status or problems with communication.

**Lightning** The proprietary, reversible Apple iOS sync/charging USB 2.0 connector and port. It is used on older iOS devices.

**Linux** An open-source operating system derived from the UNIX OS.

**liquid crystal display (LCD)** A flat-panel screen that applies electrical currents to a layer of liquid crystal cells to modulate its optical properties.

**load balancer** Increases redundancy and performance by distributing the load to multiple servers. Network load balancers are often reverse proxy servers configured in a cluster to provide scalability and high availability.

**Local Users and Groups (lusrmgr.msc)** The lusrmgr.msc command opens the Local Users and Groups Manager on Windows 10/11 for user/group configuration.

**long-range fixed wireless** A solution for providing Internet connectivity where physical access to an Internet service provider (ISP) is not possible, such as in rural areas. Fixed wireless providers send a signal from a wireless tower to customers who have a small antenna in their home or business.

**loopback plug** A plug that routes output to input wires, to enable a port to be tested for proper send/receive functions. Loopback plugs are widely available for testing Ethernet ports as well as legacy COM

and LPT ports. Some BIOS/UEFI and third-party vendors also offer USB loopback plugs.

**Lucent connector (LC)** A square connector type used in fiber-optic devices and cables.

## M

**M.2** A solid-state drive (SSD) that can mount directly onto a motherboard or an expansion card, giving the drive more direct access to the CPU, for much faster reading than with an SSD.

**macOS** The operating system on Apple computers.

**magnetometers** Another name for a metal detector, common in all airports and many public areas.

**mail exchanger (MX) records** A DNS record that efficiently maps email addresses to the destination email servers.

**mail servers** A server that sends or receives email.

**malware** Malicious software; software designed to infiltrate a computer system and possibly damage it without the user's knowledge or consent. *Malware* is a broad term that includes viruses, worms, Trojan horses, spyware, rootkits, adware, and other types of unwanted software.

**MAN** Metropolitan area network; a type of network that results when a company has two offices in the same city and makes a high-speed connection between them.

**man** Linux command to view the distribution's manual (manpages).

**managed switch** Switch that is common in corporate and enterprise networks. Managed switches also support SNMP, for diagnostics and performance measurement; virtual LANs (VLANs), to enable multiple workgroups to use the same physical switch but keep their traffic separate; and redundancy.

**master boot record (MBR)** Partition supported by BIOS/UEFI with boot settings.

**material safety data sheet (MSDS)** Also known as a safety data sheet (SDS), a document that provides information about a particular substance or device, such as the toner in a laser printer's toner cartridge.

**md** Windows command-line tool for making a directory, used for creating folders and subfolders.

**metered connections/metered utilization** Terms describing cloud services that are priced by the time or capacity used. The client pays only for what is used.

**metered utilization** A term describing cloud services that are priced by the time or capacity used. The client pays only for what is used.

**MicroATX (mATX)** A smaller version (24cm × 24cm) of the ATX motherboard commonly used in mini tower computers.

**Microsoft Management Console (MMC) snap-in** A blank console that uses various snap-in console windows. The MMC saves the consoles you snap in and remembers the last place you were working, which makes it a valuable, time-saving tool.

**Microsoft Remote Assistance (MSRA)** The Windows utility for offering or accepting remote assistance.

**micro-USB** Smallest of the USB connector types. This is the USB type for many non-Apple phones.

**mini-USB** A Type B USB cable (USB 1). It is used in cameras, phones, and similar devices.

**Mission Control** A visual setting in macOS that allows for simultaneous viewing of all open apps.

**mobile application management (MAM)** Software that enables an organization to manage software on devices across its enterprise

network.

**mobile device management (MDM)** A way to manage the mobile devices within an enterprise—for example, to ensure that all mobile users on the network have updated security files.

**modular power supply** A power supply that uses modular connections so that you can customize the power supply connections needed for your hardware. An advantage of such a power supply is that the cables can detach from the power supply. Cable management also is much easier.

**Molex** A four-pin power connector used for desktop PATA drives and some add-on cards. Molex connectors can be adapted to SATA drives, case fans, and Bern connectors (used for floppy drive power).

**mSATA** A miniPCIe form factor used by some high-performance laptops and desktops.

**multicore** A processor with two or more cores; some desktop processors have as many as eight cores.

**multifactor authentication** A security system that uses two or more authentication methods and is far more secure than single-factor authentication. An example is a person using a digital code from a fob and typing a username and password to gain access to a system.

**multithreading** As CPUs developed and added cores, multithreading was developed as a method to allow multiple threads on each core. This works differently from hyperthreading because multithreading breaks each core into logically smaller CPUs to handle more sets of operating instructions, resulting in higher CPU performance.

**mv** A Linux command used to move files to a specified location.

## N

**nano** A command-line text editor with keyboard shortcuts and functions for editing files.

**near-field communication (NFC)** A feature included in many mobile devices, such as tablets, for data transfer and shopping. When NFC is enabled and a suitable payment system (such as Apple Pay or Android Pay) is installed on a mobile device, it can be used for secure payments at any retailer that supports NFC payments.

**net use** A Windows command that connects to shared folders; it works similarly to mapping a network drive.

**net user** A Windows command used to manage user accounts (for adding, removing, or changing).

**NetBIOS/NetBIOS over TCP/IP (NetBT)** Also known as NetBT (RFC 1001), this protocol allows some legacy applications that were developed in the 1980s, before the TCP/IP environment had become the standard, to work on larger networks and the Internet. NetBIOS/NetBT uses ports 137–139.

**netstat** A Windows command that displays a list of active TCP connections on a local network.

**network tap** A device that is inserted into the network cable and makes an exact duplicate of network traffic, allowing network managers to “tap” into the data flowing through a network.

**network topology diagram** A map of a network that shows how equipment is physically arranged in the building and logically connected as a network.

**New Technology File System (NTFS)** The native secure file system of Windows 10 and 11, as well as some previous versions.

**NFC** Near-field communication; a feature included in many mobile devices such as tablets for data transfer and shopping. When NFC is enabled and a suitable payment system (such as Apple Pay or Android Pay) is installed on a mobile device, it can be used for secure payments at any retailer that supports NFC payments.

**NIC** Network interface card; an interface on a computer (or other device) that connects to a LAN.

**Non-Volatile Memory Express (NVMe)** A protocol designed to allow solid-state drives (SSDs) to transfer data between the motherboard and the SSDs at staggeringly high rates.

**nslookup** A Windows command that gathers a network's Domain Name System (DNS) information.

**NTFS** New Technology File System; the native secure file system of Windows 10.

## O

**on-demand** A characteristic of cloud computing in which users can purchase access to additional resources as needed.

**on-path attack** Involves the attacker intercepting a connection while fooling the endpoints into thinking that they are communicating directly with each other.

**open-source license** License for software that can be freely accessed, used, changed, and shared (in modified or unmodified form) by anyone.

**optical drive** Drive that stores data in a continuous spiral of indentations called pits and lands that are burned into the nonlabel side of a disc from the middle outward to the edge. Optical drives use a laser to read the data.

**optical network terminal (ONT)** An optical network device similar to a modem in purpose: It connects the end user to the ISP, but because the communication is light pulses instead of electrical signals, no modulating/demodulating takes place. Therefore, an ONT is technically different than a modem.

**organic LED (OLED)** A type of display that uses organic compounds that emit light.

## P

**PaaS** Platform as a Service; a cloud computing category designed for developing and deploying apps.

**PAN** Personal area network; a network that is larger than a LAN and smaller than a WAN.

**partitioning** The process of creating separate portions on a hard disk. These can be assigned drive letters and can be bootable sectors.

**patch panel** A box designed as a junction point for twisted pair (TP) cable and fiber cable used in networks.

**pathping** Command-line command that returns latency data for the path across the network or Internet.

**Performance Monitor (perfmon.msc)** A Windows Computer Management node that enables the customized logging of system performance factors, including processor performance, memory transfers, and network performance.

**Peripheral Component Interconnect (PCI)** (1) A 32-bit I/O bus that provides a shared 33MHz or 66MHz data path between the CPU and peripheral controllers. (2) Payment Card Industry; standards that protect a cardholder's data.

**Peripheral Component Interconnect Express (PCIe)** A high-speed set of serial bus communication channels used by adapter cards.

**personal license** A software license provided for a computer purchased at a retail or online store, and for downloaded or packaged apps designed for use by individuals.

**phishing** The process of creating bogus websites or sending fraudulent emails in an attempt to trick users into providing personal, bank, or credit card information.

**pickup rollers** Printer component that picks up paper.

**PII** Personally identifiable information; information such as a person's name and social security number.

**ping** A Windows command that sends IP packets to check network connectivity.

**pinwheel** A macOS spinning icon that is caused by an application failing, but that can also indicate that the system is locked up and needs a hard reboot. It is also referred to as the "spinning rainbow" or "beachball of death."

**.pkg files** In macOS, these are compressed application files.

**plenum** An air space in a building, such as HVAC ductwork or a suspended ceiling. Plenum cable, which produces very little smoke when burned, is required when a plenum is being used for cabling.

**PoE** Power over Ethernet; a switch with added capability (a built-in end span) to send power out a port using Cat 5 or better grades of twisted pair cable.

**pointing device** A general term for any mouse-type device.

**POP3** Post Office Protocol version 3; an email protocol used by client computers to download or receive email. POP3 uses port 110.

**port** A number or range of numbers assigned to a particular connection session or connection type.

**port flapping** Condition that occurs when the physical port on a device turns on and off intermittently, usually very rapidly.

**port forwarding/mapping** A method of allowing inbound traffic on a particular TCP or UDP port or range to go to a particular IP address instead of to all devices on a network. It is used to forward external visitors through the router to a specific computer. Instead of opening up the entire LAN, port forwarding directs particular traffic where you want it to go.

**port replicator** A device that allows a laptop to expand the number of ports so that additional devices can be attached.

**PostScript** A printer driver that does not depend on the printer for processing the print job, so the printing might be slower than with PCL printers. However, the advantage is that the print jobs will be consistent, no matter where they are printed in the network.

**power surges** Overvoltage events that last no more than 50ms and that can reach voltage levels as high as 6000V and 3000A.

**power-on self-test (POST) beeps** Sounds used by many BIOS versions to indicate either fatal or serious errors.

**Preferred Roaming List (PRL)** A database created by the mobile service provider that contains a priority list of radio frequencies and service provider IDs that the device needs to connect to the right tower in various geographical areas.

**principle of least privilege** Giving a user access to only what is required to do his or her job.

**print bed** With 3D printing, the platform on which the object is created.

**print server** A device that manages the printing tasks for multiple users who share one or more printers in an office.

**Printer Control Language (PCL)** A common printer driver language used by many different printer companies that works with many different operating systems. PCL uses the printer hardware to process the print job data. This can take work off the computer and speed up the printing process; however, because the printer does the processing work, the print job output can vary, depending on the brand of printer.

**private cloud computing** Use of a privately owned cloud that is accessible only to authorized users. Private cloud services are more secure than public cloud services.

**product life cycle** Expected time for a product such as a CPU to be considered standard before it is replaced with a newer version.

**protocol** A set of rules used to enable communication between network devices.

**proxy server** A server that caches Internet page requests, enabling a single page to be viewed by all the devices requesting it. A proxy server reduces outbound traffic to the Internet and can also be used for filtering content.

**proxy settings** Specific settings for the types of content using a proxy server and its IP address and port numbers.

**ps** A Linux command used to list current processes.

**.ps1 script files** Windows PowerShell is a tool to help technicians and network administrators automate support functions through the use of scripts and snippets. Windows 10 and 11 ship with PowerShell.

**public cloud computing** Use of cloud services provided over the public Internet.

**punchdown tool** A tool that punches down the individual wires into the 110 IDC clips of an RJ-45 jack and a patch panel.

**pwd** A Linux command used to display the name of the current/working directory.

**.py script files** Python is often a good choice for those beginning to learn programming. It is relatively easy to learn, and Python scripts can run on most operating systems. For example, Windows Shell is known as Python Interactive Shell.

## Q–R

**quad-channel** A type of RAM designed to quadruple the speed of the RAM bandwidth using two sets of four sockets.

**RAID Level 0 (RAID 0)** A type of RAID in which two drives are treated as a single drive, with both drives used to simultaneously store different portions of the same file.

**RAID Level 1 (RAID 1)** A type of RAID in which two drives are treated as mirrors of each other; changes to the contents of one drive are immediately reflected on the other drive.

**RAID Level 1+0 (RAID 10)** A type of RAID in which four drives combine striping plus mirroring, for extra speed plus better reliability. RAID 10 is suitable for use with program and data drives. RAID 10 is a striped set of mirrors.

**RAID Level 5 (RAID 5)** A type of RAID in which three or more drives are treated as a logical array, and parity information (used to recover data in case a drive fails) is spread across all drives in the array. RAID 5 is suitable for use with program and data drives.

**RAM** Random Access Memory; the main memory in a computer, where the operating system (OS), application programs, and data reside so that they can be quickly reached by the device's processor.

**ransomware** A virus that takes over a computer or network until a ransom is paid.

**rapid elasticity** A characteristic of cloud computing that refers to how quickly and easily more or fewer cloud resources can be used or set aside, as needed.

**RDP** Remote Desktop Protocol; a protocol used by Remote Desktop Services (RDS), which is the Windows Server-based companion of Remote Desktop Connection. RDP uses port 3389.

**read/write failure** A hard drive error caused by a failure to read data on the drive or write new data to the drive.

**recovery mode** The mode of a computer (or other device) that provides access to core functions of the computer for repair or reset purposes after a system failure.

**recovery partition** A space on the hard drive that holds the Windows Recovery Environment (WinRE) during a clean install.

**Redundant Array of Independent (or Inexpensive) Disks** A method for creating a faster or safer single logical hard disk drive

from two or more physical drives.

**Registry Editor (regedit.exe)** The Windows Registry Editor.

**Remote Authentication Dial-In User Service (RADIUS)**

Software and a protocol that allows remote authentication via a central server.

**Remote Desktop Protocol (RDP)** A protocol used by Remote Desktop Services (RDS), which is the Windows Server-based companion of Remote Desktop Connection. RDP uses port 3389 and enables a user to securely connect to a remote computer in order to perform services or support another user.

**Remote Disc** A feature that enables a macOS computer that lacks an optical disc drive to use another computer's optical disc drive.

**Remote Monitoring and Management (RMM)** Tools that allow technicians to monitor and manage remote networks. This usually involves installing special tools called agents that collect data and report it back to the management team for data analysis.

**remote network installation** Installing software via a network connection instead of a physical disk.

**remote wipes** A program that can be initiated from a desktop computer to delete all the contents of a remote mobile device that has been lost or stolen.

**repair installation** A Windows installation option in which the OS is installed over the same version to fix problems with the previous installation. It is also known as an in-place upgrade.

**resin** The liquid medium in 3D printers that is heated and fused to form thin layers of plastic to print an object.

**Resource Monitor (resmon.exe)** Utility that tracks CPU usage and performance.

**RFID** Radio-frequency identification; a technology that consists of an RFID tag that can broadcast information about an item, plus an

RFID reader to accept the broadcast information and deliver it to a computer system for use.

**risk analysis** A method of identifying risks to a network performed using either qualitative or quantitative analysis methods, with the end goal being a plan to mitigate the impact of risks.

**RJ-11** A standard phone jack.

**RJ-45** Registered jack function 45; the most common Ethernet cable, which connects network interface cards on PCs to network switches and SOHO routers.

**rm** A Linux command used to remove (delete) files from a system.

**rmdir** Command-line command that removes a directory and the subdirectories within it.

**robocopy** A Windows command that is used as a highly configurable file/folder copy-and-move app. It can be configured with various optional GUIs.

**rollback plan** A document that lets the change administrators restore the network to the service level that was present before the change.

**root access** Accessing root files of an OS to change settings or allow portability between cell providers.

**rootkit** A set of hacking tools that finds its way deep into a computer's operating system or applications and sets up shop to take over the computer.

**router** A device that routes data from one network to another. It is often integrated with wireless access points and switches.

## S

**SaaS** Software as a Service; software programs that can be run from the cloud without downloading an app. Examples include Google Docs, Microsoft Word Online, and Excel Online.

**Safe Mode** A mode that loads minimal Windows features, such as low-resolution graphics and minimal networking. It is helpful in troubleshooting Windows features.

**Samba** A utility that allows Linux to operate in a Windows environment.

**sandboxing** Creating an isolated machine (or network of machines) where experiments can be run or software can be securely tested without risk to machines on the production network.

**SATA (Serial Advanced Technology Attachment)** A version of ATA that uses thin data and power cables to transmit data serially at rates of 1.5Gbps, 3.0Gbps, 6.0Gbps, and 16Gbps (SATA Express).

**satellite** An Internet provider option that uses dish antennas similar to satellite TV antennas to receive and transmit signals between geosynchronous satellites and computers.

**screened subnet** Formerly known by CompTIA as a demilitarized zone (DMZ). A screened subnet allows outside traffic through to a particular IP address on a LAN.

**Secure Boot** A setting that blocks the installation of untrusted software during the boot process.

**Secure Shell (SSH)** A protocol that allows data to be exchanged between computers on a secured channel. SSH is a more secure replacement for FTP and Telnet.

**Self-Monitoring, Analysis, and Reporting Technology (S.M.A.R.T.)** A technology that monitors internal hard disks and warns of impending failure.

**Sender Policy Framework (SPF)** A tool that lets domain owners list the IP addresses that are authorized to send mail, to control spam.

**serial** A serial communication physical interface (also known as a COM port) through which information transfers in or out 1 bit at a

time. The RS-232 standard is commonly used to transmit data through DB-9 ports.

**sfc** A Windows command that scans system files and replaces damaged or missing files.

**.sh script files** A shell script is a text file that contains a sequence of commands for a Linux- or UNIX-based system. Shell scripts might not run correctly on a Windows system. Linux has had several shells; BASH (Bourne-Again Shell) is the most common of them.

**share permissions** A set of rules that determine a user's level of access to a file or folder.

**shared resources** Resources such as data files and devices that can be used by multiple users in a cloud environment.

**Shell** A macOS or Linux command-line environment.

**shielded twisted pair** Ethernet cable with added shielding to protect against electromagnetic interference.

**shoulder surfing** Attempting to view physical documents on a user's desk or electronic documents displayed on a monitor by looking over the user's shoulder.

**shutdown** A Windows command that shuts down a computer.

**single channel** A single RAM slot on an earlier motherboard.

**single core** An early CPU with only a single processing thread running.

**single sign-on (SSO)** The use of a single password to authenticate multiple apps in an organization that require authentication.

**Small Computer System Interface (SCSI)** A flexible interface that can be used for hard drives and optical drives, scanners, and other devices. Narrow SCSI interfaces enable the daisy chaining of seven devices to a single port. Wide SCSI enables the daisy chaining of up to 15 devices to a single port.

**Small Outline Dual Inline Memory Module (SODIMM)** A compact version of the standard DIMM module, available in various pinouts for use in notebook and laptop computers and laser printers.

**smart card** A credit card-size card that contains stored information and might also contain a simple microprocessor or an RFID chip.

**SMB** Server Message Block; a protocol that provides access to shared items such as files and printers. SMB uses ports 137–139 for SMB traffic using NetBIOS over TCP (NetBT) and port 445 for SMB hosted on TCP.

**SMTP** Simple Mail Transfer Protocol; a protocol that is used to send email from a client system to an email server, which also uses SMTP to relay the message to the receiving email server. SMTP uses port 25.

**SNMP** Simple Network Management Protocol; a protocol that is used as the standard for managing and monitoring devices on a network. SNMP uses ports 161 and 162.

**social engineering** A type of attack in which hackers trick users into providing passwords or other sensitive information.

**soft token** Part of a multifactor authentication process. Software (soft) tokens exist in software and are commonly stored on devices.

**software-defined networking (SDN)** A network in which a virtual layer created in software controls the data flow over the physical network devices.

**software firewalls** A program that examines data packets on a network to determine whether to forward them to their destination or block them.

**solid-state drive (SSD)** A hard drive that uses flash memory instead of magnetic storage platters.

**spam gateways** Email filters that can detect almost all spam coming into a system, which increases email efficiency and network security as well.

**splash screens** Display of logos or policies that “welcome” a user at startup or login. These might come with a checkbox requiring the acknowledgment of rules before the user can access the company resources.

**spoofing** A general term for malware attacks that purport to come from a trustworthy source. Phishing, spear phishing, and rogue antivirus programs are three examples of spoofing.

**Spotlight** A macOS search tool.

**spyware** Software that spies on system activities and transmits the details of web searches or other activities to remote computers.

**SSH** Secure Shell; a protocol that allows data to be exchanged between computers on a secured channel. It is a more secure replacement for FTP and Telnet. SSH uses port 22.

**static IP addresses** Assigned to a device by the administrator and not subject to change until reconfigured by the administrator.

**static wide area network (WAN) IP** Provided by the ISP and applied (usually automatically) to the “Internet” port on the router. The address is “static” because it does not change and does not expire like a leased dynamic address.

**storage area network (SAN)** A special network made of computers storing vast amounts of information in blocks of data. The SAN storage servers reside in data centers both near and far; to the user, however, it can appear to be attached to the local computer.

**straight tip (ST)** A round connector type used in fiber-optic devices and cables.

**Structured Query Language (SQL) injection** Malicious code inserted into strings that are later passed to a database server.

**su** A Linux command used to switch between accounts.

**subnet mask** An IPv4 network-addressing feature used to specify how much of an IP address is the host address and what part is the

extended network address.

**subscriber connector (SC)** A square connector type used in fiber-optic devices and cables.

**sudo** A Linux command used to run a command as another user.

**supervisory control and data acquisition (SCADA)** SCADA systems are designed to provide centralized control to manage industrial equipment, such as in manufacturing or water and waste treatment plants.

**switch** A network device that sets a direct path for data to run from one system to another; it can be combined with a router or a wireless access point. A switch is faster than a hub because it supports the full bandwidth of the network at each port instead of subdividing the bandwidth among active ports, as a hub does.

**synthetic backup** These backups are similar to full backups, except they are actually reconstructed in software from a full backup in the past and modified with the incremental backups that have occurred since the full backup. The benefit is reduced storage needs for backup data.

**syslog server** A server that tracks events, such as user logins and crashes, that happen on devices on a network.

**System Configuration (msconfig.exe)** The MSConfig utility in Windows, which configures startup, boot settings, services, and startup apps, and also provides access to tools.

**System Information (msinfo32.exe)** The Microsoft System Information utility, which displays information about Windows, the computer, peripherals, and installed applications.

**System Restore** A Windows feature that enables a system to be returned to a previous condition using restore points.

T

**T568A** A TP wiring standard that uses the following wires from pins 1 to 8: green stripe, green, orange stripe, blue, blue stripe, orange, brown stripe, brown.

**T568B** A TP wiring standard that uses the following wires from pins 1 to 8: orange stripe, orange, green stripe, blue, blue stripe, green, brown stripe, brown.

**tailgating** A process in which an unauthorized person attempts to accompany an authorized person into a secure area by following closely and grabbing the door before it shuts.

**Task Manager** A utility that provides a useful real-time look into the inner workings of Windows and the programs that are running.

**Task Scheduler (taskschd.msc)** A Windows utility used to run a task on a specified schedule.

**Telnet** A protocol that enables a user to make a text-based connection to a remote computer or networking device and then use it as if he or she were a regular user sitting in front of it instead of simply downloading pages and files as the user would with an http:// or ftp:// connection. Telnet uses port 23.

**Temporal Key Integrity Protocol (TKIP)** An encryption protocol for wireless LANs. TKIP replaced WEP, which had security vulnerabilities.

**Terminal** A command-line environment available in macOS, Linux, and Windows for managing computer settings and files.

**Terminal Access Controller Access-Control System Plus (TACACS+)** An authentication protocol that allows a remote access server to verify a user by communicating with an authentication server.

**test development** The process of testing software in various ways to see how the code runs and operates.

**tethering** The sharing of a cellular data connection from a smartphone to a laptop, tablet, or other device.

**text (TXT) records** Records that enable administrators to enter common text explanations into DNS, usually describing domain ownership or other information. TXT records are also used to counter email spam.

**thermal paste/pads** Adhesive used to reapply a heat sink, typically applied with a syringe.

**thermal printer** A printer that uses heat transfer to create text and graphics on the paper.

**Third Extended Filesystem (ext3)** Linux feature that journals changes to minimize damage in case of a system failure.

**Thunderbolt** A high-speed interface capable of supporting hard disk drives, SSDs, HDTVs up to 4K resolution, and other types of I/O devices.

**ticketing systems** A system that enables technical processes to run smoothly and helps the clients, whether customers or coworkers, feel that their needs were addressed and their problems were resolved in a professional manner.

**Time Machine** The macOS backup app.

**toner probe** A reliable communication protocol that ensures reliable delivery of data to the destination computer.

**top** A Linux command that provides summary information on resource use for tasks and processes in the form of a dashboard.

**tracert** A Windows command that is similar to **ping** but returns path information to an IP address destination. **traceroute** is a similar command used in macOS and Linux.

**tractor feed** A printer mechanism used to pull or push the paper past the print head.

**transfer belt/roller** A printer component that transfers a page image from the drum to the page.

**Transmission Control Protocol (TCP)** A communication protocol that is considered reliable; the delivery of network packets to the destination computer is guaranteed.

**triple channel** A motherboard technique used to triple RAM speed.

**Trivial File Transfer Protocol (TFTP)** A protocol used for transporting file packets that do not need a response.

**Trojan** A malware program disguised as a “gift” (such as a popular video or website link), to trick the user into downloading the virus.

**Trusted Platform Module (TPM)** A chip residing on a motherboard that stores encrypted keys.

**twisted nematic (TN)** An LCD screen technology that uses nematic liquid crystal cells between two glass layers that align in a twisted form when no electric current is applied.

**two-factor authentication** An authentication method that requires the user to provide two different forms of verification. Most forms of two-factor authentication are based on something the user knows and something the user possesses, such as a password and a biometric scan or security token.

## U

**UDP** User Datagram Protocol; a communication protocol that is considered unreliable and does not guarantee delivery of network packets of information to the destination computer.

**Universal Plug and Play (UPnP)** Designed to allow devices on a home or SOHO local area network (LAN) to easily connect and cooperate with other devices on the LAN.

**unmanaged switch** Low-cost switches used in small office/home office (SOHO) networks that cannot be configured to perform complex switching functions.

**unshielded twisted pair** Ethernet cables with four pairs of twisted wires inside a sheath.

**USB 2.0** Universal Serial Bus version 2; a version of USB with a peak speed of 480Mbps that is compatible with USB 1.

**USB 3.0** Universal Serial Bus version 2; it works at 5Gbps. This version of USB supports older USB devices at the native speeds of those devices.

**USB-C** The newest reversible USB connector; it should replace other USB types.

**User Account Control (UAC)** Allows the end user to select a level of notifications concerning changes being made to the computer. The purpose of this tool is to prevent unauthorized changes to the computer.

**UTM** Unified threat management; a device that provides firewall, remote access, and virtual private network (VPN) support, as well as web traffic filtering with anti-malware software and network intrusion prevention.

## V

**.vbs script files** VBScript, a scripting language developed by Microsoft, is considered a subset of the Visual Basic programming language. It was designed specifically for use with Microsoft Internet Explorer and gives web pages a level of interactivity.

**Vertical Alignment (VA)** An LCD screen technology that holds liquid crystal cells between two glass layers and aligns them vertically when no electric current is applied.

**Video Graphics Array (VGA)** The first popular analog video standard, and the basis for all current video cards.

**video random access memory (VRAM)** RAM dedicated to processing graphic displays.

**Virtual desktop infrastructure (VDI)** IT infrastructure that allows organizations to offer users remote access to enterprise computer systems.

**virtual network computing (VNC)** A common desktop support model that allows a support agent to remotely control mouse and keyboard inputs to a client's computer.

**virtual private network (VPN)** A private and secure network connection that is carried by an insecure public network, such as the Internet.

**virtual RAM** Virtual memory, also known as the paging file, that uses part of the hard drive to expand the RAM. This allows users to run more apps than the RAM could otherwise handle.

**virus** A generic term for any malicious software that can spread to other computers and cause trouble.

**vishing** Involves leaving deceptive voice messages that appear to come from an internal source or other authority. These messages request providing confidential information, such as payroll or tax information.

**VLAN** Virtual local area network; a grouping of some computers on a local area network (LAN) that are configured to behave as if they have their own separate LAN. A VLAN allows users to create an encrypted connection to their home or business network via the Internet when accessing the network remotely.

**VPN** A private and secure network connection that is carried by an insecure public network, such as the Internet.

## W

**WAN** Wide area network; a group of one or more LANs over a large geographic area.

**wattage rating** A power measurement used to determine the appropriate size of a UPS or a power supply. It is also used to

measure the thermal design power of a CPU so that an adequate cooling solution can be used.

**web server** A specialized computer that hosts websites and provides various types of content to clients via the Internet. A web server uses HTTPS to communicate with computers on other networks that are requesting information.

**whaling** A specific type of phishing attack that goes after high-level employees (the big fish, or whale) in an organization, especially the CEO.

**Wi-Fi analyzer** A device or app that detects Wi-Fi signals and determines signal strength.

**Wi-Fi Protected Access 2 (WPA2)** Released in 2004 and uses Advanced Encryption Standard (AES) encryption. WPA2's AES encryption is much stronger than the previous version.

**Windows** The commercial OS from Microsoft; currently, Windows versions 10 and 11 are in use.

**Windows Defender Firewall** Windows built-in network security program.

**winver** A text command that displays the version of Windows OS.

**wireless card** A Wi-Fi adapter or a USB-based wireless adapter.

**wireless Internet service provider (WISP)** An Internet service provider that offers Internet access through a wireless connection to customers in areas where other options are unavailable.

**wireless wide area network (WWAN)** A wireless network based on cellular connections. A WWAN requires a SIM card activated by the mobile provider.

**WLAN** A network made up of wireless computers and other devices communicating via wireless transmissions, not cables and wires. A common type of WLAN is a Wi-Fi network in a home or office. A group of network access points that make up the WLAN can be

configured to work together and can be managed with a specialized device called a WLAN controller.

**WLAN controller** A configurable device used to manage connectivity between devices in a WLAN.

**workgroup** A network that does not use a domain controller. Each computer can share or not share folders or printers with others. Unless password-protected sharing is disabled, anyone who wants to use a different computer's resources must have an account on that system.

**WPA3** Released in January 2018, uses 128-bit encryption (192-bit in an enterprise version), and has a different method for sharing security keys than the other types of encryption. WPA3 is designed to add better privacy and protection against attacks on public Wi-Fi networks.

## X–Z

**xcopy** A Windows command that copies one or more files and folders to another folder or drive.

**yum** An open-source utility for automatic updates and package management in Linux.

**zero-day attack** Attack in which hackers exploit software vulnerabilities discovered as a result of notifications put out by users of that software before the company has a chance to create a security patch.

# Index

## Numerics

- 3-2-1 backup rotational scheme, [704](#)
- 3D printers, [302](#)
  - FDM (fused deposition modeling), [302–303](#)
  - maintenance, [304](#)
  - SLA (stereolithography), [302, 303–304](#)
- 4G, [34](#)
- 10BASE2, [143](#)
- 10BASE5, [143](#)
- 32-bit versus [64-bit](#) file systems, [501](#)

## A

- AAA (authentication, authorization, and accounting) server, [84](#)
- access control, [600](#)
  - permissions, [602](#)
    - Allow vs. Deny, [602](#)
    - file and folder attributes, [602–603](#)
    - inheritance, [602](#)
    - propagation, [603](#)
    - shared files and folders, [603](#)
  - UAC (User Account Control), [604](#)
  - users and groups, [600](#)
    - local vs. Microsoft account, [600–601](#)
    - standard vs. administrator account, [601–602](#)

vestibule, 573

accessories

- drawing pad, 31
- headsets, 30
- speakers, 30
- touch pens, 31
- trackpad, 31
- webcam, 31

accounts

- Group Policy, 612–614
- recovery, 698–699
- Windows, 600
  - local vs. Microsoft, 600–601
  - standard vs. administrator, 601–602

ACLs (access control lists), 579

Active Directory, 581

ad blockers, 638

adapters

- DVI to HDMI, 163
- DVI-I to VGA, 163–164
- power supply, 265
- USB, 159–160, 232–233
  - USB to Ethernet, 163

add-on cards, USB, 155

administrative shares, 487

Administrative Tools, 474

AES (Advanced Encryption Standard), 582

agent, 65

air filter masks, 715

airflow problems, troubleshooting, 366–368

alarm systems, 574

AMD. *See also* CPU (central processing unit)

CPUs, 210–211, 214–217

GPUs, 253

Android, 512. *See also* mobile devices

- factory reset/clean install, 674
- hotspots, enabling/disabling, 34
- Location Services, disabling, 44–45
- mobile hotspot feature, 110–111
- tethering, 39, 110
- wired connections, micro-USB/mini-USB, 27

antenna

- MIMO (multiple input multiple output), 74–75
- Wi-Fi, 25

antistatic bags, 709

antivirus/antimalware, 587. *See also* social engineering

- Defender Antivirus, 597
- macOS, 539
- mobile device, 618
- tools
  - anti-phishing training, 589
  - OS reinstallation, 585–590
  - Recovery Mode, 587–588
  - user education, 588–589

APIPA (Automatic Private IP Addressing), 96

app scanner, 673

App Store, 535

Apple ID, 536

apps/application(s)

- 32-bit versus 64-bit dependent, 503–504
- cloud printing, 278
- CPU requirements, 505
- crashes, troubleshooting, 376–377, 657
- distribution methods, 507
- locator, 617
- macOS, installation and uninstallation, 534–536

operating system requirements, 506  
    32-bit versus 64-bit, 507  
    application-to-OS compatibility, 506  
RAM requirements, 505  
remote backup, 617–618  
security, 599–600  
spoofing, 671–672  
storage requirements, 506  
virtualization, 337  
VRAM requirements, 504–505  
apt-get command, 551  
architecture, CPU  
    ARM (Advanced RISC Machine), 238  
    x64/x86, 237–238  
ARM (Advanced RISC Machine), 238  
articles, 692  
asset management  
    database system, 688–689  
    inventory list, 688  
    licensing agreements, 689  
    procurement lifecycle, 689  
attacks. *See also* vulnerabilities  
brute force, 594  
DDoS (distributed denial of service), 593  
dictionary, 594–595  
DoS (denial of service), 593  
evil twin, 593  
insider threat, 595  
on-path, 594  
spoofing, 594  
SQL injection, 595  
XSS (cross-site scripting), 595  
zero-day, 594

ATX (Advanced Technology eXtended) motherboards, 202  
audio  
    ports, 233  
    troubleshooting, 398  
AUP (acceptable use policy), 689–690  
authentication, 580. *See also* password(s)  
    Apple ID, 536  
    biometric, 22, 619  
    Kerberos, 584  
    multifactor, 505–506, 579, 583  
    operating system, 604–605  
    RADIUS (Remote Authentication Dial-In User Service), 583  
    single-factor, 583  
    TACACS+ (Terminal Access Controller Access Control System), 583  
AutoPlay, disabling, 612–614  
autoswitching power supplies, 264

## B

backup(s). *See also* recovery  
    critical application, 700  
    differential, 698  
    file-level, 700  
    full, 697  
    incremental, 697  
    Linux, 553–555  
    macOS, 536–539  
    rotation schemes, 700  
        3–2–1, 704  
        GFS (grandfather-father-son), 704  
        onsite vs. offsite, 701–704  
    synthetic, 698  
    system image, 699–700

testing, 698

badge reader, 573–574

baseband transmission, 136

battery(ies), 20

- backup units, 720–721
- CMOS, 234–235
- improper charging, troubleshooting, 399–400
- recycling, 718–719
- replacing, 21–22
- swollen, 400

beep codes, troubleshooting, 355–356

best practices

- disassembling laptops, 6–7
- macOS, 536
  - antivirus/anti-malware updates, 539
  - backups, 536–539
  - updates/patches, 539
- for passwords, 609–610
  - BIOS/UEFI, 609
  - expiration policy, 609
  - log off when not in use, 611
  - screensavers, 609
  - secure PII, 611
  - use screensaver locks, 611
- biometric authentication, 22, 619

BIOS (Basic Input/Output System), 218–225. *See also* motherboards

- boot sequence and settings, 225–226
  - audio and Ethernet ports, 233–234
  - fan settings, 230–231
  - firmware updates, 225–226
  - SATA configuration, 231–232
  - security features, 229–230
- USB host adapters and charging support, 232–233

CMOS battery, 234–235  
HSM (hardware security module), 236–237  
passwords, 609  
POST beep codes, troubleshooting, 355–356  
TPM (Trusted Platform Module), 235–236  
video card configuration, 247

BitLocker, 230, 437, 605–606  
BitLocker To Go, 606  
black screen, troubleshooting, 361–363  
Bluetooth, 29–30, 40–41, 76–77  
    classes, 77  
    headset  
        configuring on an Android device, 41  
        configuring on an iOS device, 43–44  
    multifunction device sharing, 275  
    pairing, 77  
Blu-ray, 179–181  
BNC connectors, 144  
bollards, 576  
boot process, 518–520  
    No OS found, troubleshooting, 660  
    troubleshooting, 653–654  
boot sector virus, 586  
browsers  
    certificates, 633  
    clearing browsing data, 635–636  
    clearing the cache, 636  
    data synchronizations, 637  
    downloading and installation, 630–631  
        hashing, 631–632  
        untrusted sources, 632  
    extensions and plug-ins, 632  
    HTTPS (Hypertext Transfer Protocol Secure), 634

malware symptoms, 666  
password managers, 633  
settings  
    ad blockers, 638  
    pop-up blocker, 635  
    private browsing mode, 636–637  
TLS (Transport Layer Security), 633–634  
brute force attack, 594  
BSOD (blue screen of death), 357  
    causes of, 358–360, 651  
    STOP errors, troubleshooting, 358  
    troubleshooting, 652  
bus topology, 142  
BYOD (bring your own device), 596–597, 620

## C

cable Internet, 105–106  
cable modem, 72, 101  
cable stripper, 115  
cable tester, 118  
cabling. *See also* connectors; TP (twisted pair) cable  
    coaxial, 142  
        10BASE5, 143  
        RG-6, 144  
        RG-58, 143  
        RG-59, 143  
        splitters, 145  
    direct burial, 139  
    Ethernet  
        STP (shielded twisted pair) cabling, 138–139  
        TP (twisted pair), categories, 136–137  
        UTP (unshielded twisted pair) cabling, 138–139

fiber-optic, 140–141  
connectors, 141–142  
multi-mode, 141  
single-mode, 141

hard drive  
IDE (Integrated Drive Electronics), 162  
SATA (Serial Advanced Technology Attachment), 161  
SCSI (Small Computer System Interface), 162–163

patch panel, 70

safety, 715

serial, 160–161

UTP (unshielded twisted pair)  
T568A (EIA-568A) standard, 139–140  
T568B (EIA-568B) standard, 139

cache, 190

capacitor swelling, 378–379

cards  
dedicated graphics, 504  
integrated graphics, 504  
smart, 576–577

cat command, 553

CD, 179

cd command, 548

CDMA (Code Division Multiple Access), 39

CD-ROM/CD-RW, 179–180

cellphones and cellular networks, 109–110. *See also* mobile devices; smartphones  
first generation, 34  
hotspots, 110–111  
PRL (Preferred Roaming List), 39–40  
recycling, 718–719  
SIM cards, 39  
tethering, 110

Cellular Data Options, iPhone, 34  
Certificate Manager, 461–462  
certificates, 633  
chain of custody, 724  
change management, 507–508, 693–694  
    advisory board, 696  
    affected systems/impact, 695  
    date and time of change, 695  
    end user acceptance, 696–697  
    request forms, 694–695  
    risk analysis, 696  
    rollback plan, 694  
    sandboxing, 694  
    scoping, 695  
channels, 75–76  
charging, USB, 232–233  
chkdsk command, 449–450  
chmod command, 550  
chown command, 550  
Chrome OS, 511  
CIFS (Common Internet File System (CIFS), 66  
CL (CAS latency) values, 167  
ClamAV, 539  
clean install, Windows, 521–523  
cleaning  
    laser printers, 287–288  
    PC internals, 368–369  
client-side virtualization, 334–335  
cloud computing. *See also* virtualization  
    backup and recovery, 703–704  
characteristics  
    on-demand, 332  
    file synchronization, 332

- high availability, 331
- metered utilization, 332–333
- rapid elasticity, 331
- shared resources, 330–331
- community, 330
- desktop virtualization, 333–334
- hybrid, 330
- models, 327
  - IaaS (Infrastructure as a Service), 327
  - PaaS (Platform as a Service), 329
  - SaaS (Software as a Service), 327–328
- pricing schedules, 332
- printing, 277–278, 279
- private, 330
- public, 329–330
- servers, 322
- virtualization, 323
- coaxial cable, 142
  - 10BASE5, 143
  - RG-6, 144
  - RG-58, 143
  - RG-59, 143
  - splitters, 145
- color laser printers, 284–285
- commands. *See also* PowerShell
  - ftp, 61–62
  - ipconfig, 93–94
  - ipconfig/all, 35
- Linux
  - apt-get, 551
  - cat, 553
  - cd, 548
  - chmod, 550

chown, 550  
cp, 549  
df, 201, 552  
DIG, 553  
find, 553  
grep, 547–548  
ip, 551  
ipconfig -a, 35, 94–95  
ls, 547  
man, 550  
mv, 549  
nano, 553  
pwd, 549  
rm, 549  
shutdown, 548–549  
su/sudo, 550  
top, 552  
YUM, 551  
perfmon, 390  
ping, 92  
PowerShell, 440–443  
    chkdsk, 449–450  
    copy, 445–446  
    diskpart, 447–448  
    findstr, 449  
    format, 443–445  
    gpupdate, 450  
    pathping, 450–451  
    robocopy, 446–447  
    sfc, 448–449  
    xcopy, 446  
telnet, 62  
commercial licenses, 725

communication

- cultural sensitivity, [730](#)
- listening, [728–730](#)
- meeting customer expectations, [730–731](#)
- projecting confidence, [728–730](#)
- proper language, [729](#)
- community cloud computing, [330](#)
- compatibility, [532–533](#)
- compliance policy, [691–692](#)
- compressed air and vacuum systems, [720](#)
- CompTIA troubleshooting methodology, [353–354](#)
- confidentiality, [730](#)
- connectors, [165–166](#). *See also* port(s)
  - adapters
    - DVI to HDMI, [163](#)
    - DVI-I to VGA, [163–164](#)
    - USB to Ethernet, [163](#)
  - BNC, [144](#)
  - F type, [144](#)
  - fiber-optic, [141–142](#)
  - power supply, [265–267](#)
  - video, [145–146](#)
    - DisplayPort, [149–150](#)
    - DVI (Digital Visual Interface), [150–151](#)
    - HDMI (High-Definition Multimedia Interface), [147–148](#)
    - VGA (Video Graphics Array), [146–147](#)
- content filtering, [624–625](#)
- Control Panel, [471](#)
  - Administrative Tools, [474](#)
  - Ease of Access settings, [479–480](#)
  - File Explorer Options, [474–475](#)
  - Indexing Options, [474](#)
  - Internet options, [471–472](#)

## Power Options

- Hibernate option, [476](#)
- Power Plans, [476](#)–[477](#)
- Sleep/Suspend, [478](#)
- Standby, Lid, and Fast Startup options, [478](#)
- Universal Serial Bus (USB) Selective Suspend, [478](#)–[479](#)
- starting, [471](#)
- User Accounts, [473](#)
- utilities, [473](#)
- copy command, [445](#)–[446](#)
- corporate use licenses, [726](#)
- cp command, [549](#)
- CPU (central processing unit). *See also* GPU (graphics processing unit)
  - application requirements, [505](#)
  - architecture
    - ARM (Advanced RISC Machine), [238](#)
    - x64/x86, [237](#)–[238](#)
  - cooling mechanisms, [255](#)
    - fanless/pассивный heat sink, [256](#)–[257](#)
    - fans, [255](#)–[256](#)
    - heat sink, [256](#)
    - liquid-based cooling, [259](#)–[260](#)
    - thermal paste, [257](#)–[259](#)
  - integrated video, [241](#)
  - LGA (Land Grid Array) sockets, [213](#)–[214](#)
  - motherboard compatibility, [210](#)–[211](#)
  - mPGA (micro Pin Grid Array) sockets, [213](#)–[216](#)
  - multicore, [238](#)–[239](#)
  - multithreading, [239](#)
  - server, [217](#)
  - single-core, [238](#)
  - sockets, [212](#)–[213](#)

- speeds, 240–242
- virtualization support, 240

crimper, 115–116

critical application backup, 700

cross-platform virtualization, 337

cursor drift, troubleshooting, 404

cutting tool, 114

## D

- data destruction and disposal, 621
  - outsourcing, 623
  - physical destruction methods, 621–622
  - recycling or repurposing best practices, 622
- data-at-rest encryption, 608
- database system, 688–689
- DDoS (distributed denial of service) attack, 593
- DDR SDRAM (double data rate SDRAM), 14, 170–171. *See also* memory
  - DDR4 SDRAM, 170
  - DDR5 SDRAM, 170
- DD-WRT, 68
- dedicated graphics card, 504
- Defender Antivirus, 597
- desktop
  - management software, 737
  - virtualization, 333–334
- Device Manager, 456–461
- devices
  - disabling, 461
  - drivers, 526
  - gateway, 494
  - troubleshooting, 460

df command, 201, 552  
DHCP (Dynamic Host Configuration Protocol), 63–64, 98, 102–103  
    reservations, 625  
    server, 82  
dictionary attack, 594–595  
differential backup, 698  
DIG command, 553  
digitizer, 26, 403  
DIMM (dual in-line memory module), 14, 175–178. *See also* memory  
direct burial cables, 139  
directory services, 65  
dirt and dust, removing from inside a PC, 368–369  
disabling  
    AutoPlay, 612–614  
    devices, 461  
    ports, 630  
disassembling laptops, best practices, 6–7  
Disk Cleanup, 468  
disk cloning, 524–525  
Disk Defragment/Optimize Drives, 469  
Disk Management snap-in, 453–454  
Disk Utility, macOS, 544  
diskpart command, 447–448  
display burn-in, troubleshooting, 397  
DisplayPort, 149–150  
DNS (Domain Name System), 63, 101–102  
    email, 102  
    server, 82  
docking station, 31–33  
documentation, 6–7  
    articles, 692  
    asset management  
        database system, 688–689

inventory list, 688  
licensing agreements, 689  
procurement lifecycle, 689  
AUP (acceptable use policy), 689–690  
chain of custody, 724  
change, 694  
    purpose of the change, 695  
    request forms, 694–695  
    risk analysis, 696  
incident report, 692, 723  
MSDS (material safety data sheet), 715–717  
network topology diagram, 690–691  
regulatory and compliance policies, 691–692  
rollback plan, 694  
SOP (standard operating procedure) manual, 692  
ticketing systems, 686, 688  
    category of problem, 687  
    description of problem, 687  
    device information, 686  
    escalation levels, 687–688  
    severity of problem, 687  
    user information, 686  
whitepaper, 693  
domains, 436, 485–486  
door locks, 575  
DoS (denial of service) attack, 593  
DOS (Disk Operating System), 509  
dot-matrix printers, 298–299. *See also* impact printers  
drawing pad, 31  
drivers, 526  
    printer, 272  
video card  
    installing, 251

removing, 247  
DRM (digital rights management), 725  
DSL (Digital Subscriber Line), 101, 106–107  
dual-channel RAM, 172  
dual-voltage power supplies, 263  
dumpster diving, 593  
DVD disks, 179–180  
DVI (Digital Visual Interface), 150–151  
dynamic disks, 529–530  
dynamic IP addressing, 96–98, 494

## E

Ease of Access settings, 479–480  
ECC (error correction code), 174–175  
EFS (Encrypting File System), 606–608  
ejecting a drive  
    in Linux, 201  
    in Windows, 199–200  
electrical fire safety, 714–715  
email  
    DNS (Domain Name System), 102  
    IMAP (Internet Message Access Protocol), 65  
    mobile device synchronization, 47  
    POP3 (Post Office Protocol version 3), 64  
    security, 579  
    server, 83  
    spam gateway, 84  
embedded systems, 86–87  
emulation, 335  
encryption  
    BitLocker, 437, 605–606  
    BitLocker To Go, 606

data-at-rest, 608  
EFS (Encrypting File System), 606–608  
full-device, 619  
protocols, 582  
wireless networking, 627  
end-of-life operating systems, 596  
environmental impacts. *See also* safety  
MSDS (material safety data sheet), 715–717  
toxic waste handling/disposal, 717  
    cellphone and tablet recycling, 718–719  
    recycling batteries, 718–719  
    toner, 718–719  
EOL (end of life), 517  
equipment locks, 575  
error messages  
    accessing, 377–378  
    POST, troubleshooting, 355–356  
    STOP, troubleshooting, 358  
eSATA (external SATA), 161, 210  
ESD, 713  
    mats, 711  
    straps, 709–711  
Ethernet, 136. *See also* connectors; TP (twisted pair) cable  
    ports, 233–234  
    Thick, 143  
    Thin, 143  
    TP (twisted pair) cable, categories, 136–137  
    UTP (unshielded twisted pair) cabling  
        T568A (EIA-568A) standard, 139–140  
        T568B (EIA-568B) standard, 139  
EULA (end-user license agreement), 725  
Event Viewer, 453  
evil twin attack, 593

exFAT (FAT64), 502–503  
expiration policy, password, 609  
extended partition, 528  
extensions, browser, 632

## F

F type connectors, 144  
failed login attempts restrictions, 618  
fan, 255–256  
    replacing, 370  
    settings, 230–231  
FAT32, 501–502  
FCC (US Federal Communications Commission), 75, 81  
FDM (fused deposition modeling), 302–303  
feature updates, 533  
fences, 576  
fiber connections, 108  
fiber-optic cabling, 140–141  
    connectors, 141–142  
    multi-mode, 141  
    single-mode, 141  
File Explorer  
    navigation, 499  
    options property sheet, 474–475  
file server, 82  
file systems, 514–515  
    32-bit versus 64-bit, 501  
    comparison, 516–517  
EFS (Encrypting File System), 606–608  
exFAT (FAT64), 502–503  
FAT32, 501–502  
NTFS (New Technology File System), 515–516

file-level backup, 700  
fileshare, 82  
FileVault, 545  
FileZilla, 62  
final preparation, 747  
    chapter-ending review tools, 756  
    Core 1 (220–1101) exam domains and objectives, 750  
    Core 2 (220–1102) exam domains and objectives, 750  
    customizing your exams, 753–754  
    exam information, 748–749  
    getting ready, 750–751  
    memory tables, 755  
    tools for final preparation, 751–753  
    updating your exams, 754–755  
find command, 553  
findstr command, 449  
fire safety, 714–715  
firewall(s), 70, 597–598, 628–629. *See also* security  
    physical, 598  
    software, 597–598  
SOHO network  
    disabling ports, 630  
    port forwarding/mapping, 629–630  
Windows Defender, 489–491, 598–599  
firmware, 67  
    DD-WRT, 68  
    home router, 624  
    updates, 225–226  
first generation cellphones, 34  
fixed wireless providers, 80  
flash drives, 190–192, 193–194  
folders  
    attributes, 602–603

mapping, 487–489  
sharing, 487, 603  
Force Quit feature, macOS, 545–546  
form factor  
    magnetic hard disk drives, 189  
    memory, 14  
    motherboard, 201  
    SSD (solid-state drive), 184–185  
format command, 443–445  
formatting a hard drive, 530  
frequency bands, wireless router, 73  
frequent shutdowns, troubleshooting, 654–655  
FTP (File Transfer Protocol), 61–62  
ftp command, 61–62  
full backup, 697  
full-device encryption, 619

## G

gateway, 494  
geosynchronous satellites, 108  
GFS (grandfather-father-son) backup rotational scheme, 704  
Gmail, 328  
GPS (Global Positioning System), 44  
GPT (globally unique ID partition table), 529  
GPU (graphics processing unit), 251–252  
    AMD, 253  
    Intel, 252  
gpupdate command, 450  
graphics cards, 504  
grep command, 547–548  
grinding noise, troubleshooting, 378  
grounding, 705–708, 711–712

## Group Policy

- account management, [612–614](#)
- Editor, [437](#)
- GSM (Global System for Mobile Communications), [39](#)
- guards, [574](#)
- guest access, wireless networks, [628](#)

## H

- hand tools, [7](#). *See also* tools
  - cable stripper, [115](#)
  - crimper, [115–116](#)
  - cutting tool, [114](#)
  - punchdown tool, [116](#)
- hard disk drives, [11](#), [182](#), [188](#)
  - bootable device not found, troubleshooting, [385–387](#)
  - cabling
    - IDE (Integrated Drive Electronics), [162](#)
    - SATA (Serial Advanced Technology Attachment), [161](#)
    - SCSI (Small Computer System Interface), [162–163](#)
  - cache size and performance, [190](#)
  - comparison, [11](#), [187](#)
  - data loss/corruption, troubleshooting, [387–388](#)
  - defragging, [469](#)
  - ejecting
    - in Linux, [201](#)
    - in Windows, [199–200](#)
  - extended read/write times, troubleshooting, [389–390](#)
  - failure to boot, troubleshooting, [385](#)
  - formatting, [444](#), [530](#)
  - grinding and clicking noises, troubleshooting, [384–385](#)
  - HDD/SDD migration, [14](#)
  - hot-swappable, [199](#)

hybrid, 190

IOPS (input/output operations per second), 390

LED status indicators, 381–382

magnetic, 188

- form factors, 189
- speed/spin rate, 188–189

migration, 14

missing drives in OS, troubleshooting, 390–392

partition(ing), 447–448, 527

- dynamic disks, 529
- extended, 528
- GPT (globally unique ID partition table), 529
- MBR (master boot record), 528–529
- primary, 527–528
- during Windows installation, 529–530

RAID (Redundant Array of Inexpensive Disks), 194–196

- SATA, 196–199
- troubleshooting, 388

read/write failure, troubleshooting, 382

recovery partition, 525

replacing, 12–13

SATA

- 2.5, 187–188
- S.M.A.R.T. failure, troubleshooting, 388–389
- slow performance, troubleshooting, 382–384

SSD (solid-state drive), 11, 182–183

- flash memory, 186
- form factors, 184–185
- installing, 183–184

SSHD (solid-state hybrid drive), 11, 186

hard tokens, 580

hashing, 631–632

HDMI (High-Definition Multimedia Interface), 147–148

headers, motherboard, 210  
headsets, 30  
    Bluetooth  
        configuring on an Android device, 41  
        configuring on an iOS device, 43–44  
heat sink, 256  
high availability, cloud computing, 331  
host/guest virtualization, 335–336  
hotspots, 20, 30, 34–38, 110–111  
HSM (hardware security module), 236–237  
HTTP (Hypertext Transfer Protocol), 64  
HTTPS (Hypertext Transfer Protocol Secure), 60, 64, 634  
hubs, 71, 155  
hybrid cloud, 330  
hybrid drives, 190  
hypervisor, 334–335

## I

IaaS (Infrastructure as a Service), 327  
IDE (Integrated Drive Electronics) cable, 162  
IDS (intrusion detection system), 84–85  
IEEE (Institute of Electrical and Electronics Engineers), 73  
image deployment, Windows, 524–525  
IMAP (Internet Message Access Protocol), 65  
impact printers, 298–299. *See also* printers and printing  
    heads, 300  
    maintenance, 301  
        replacing paper, 302  
        replacing the print head, 301  
        replacing the ribbon, 301  
    paper types, 301  
    print process, 299

ribbons, 300

impersonation, 592

incident response and reporting, 692, 722

- chain of custody, 724
- documentation, 723
- first response, 723

incremental backup, 697

Indexing Options, Windows, 474

inheritance, permission, 602

inkjet printers, 288. *See also* printers and printing

- components, 288–289
- maintenance, 291
  - calibration, 292–293
  - nozzle check and head cleaning, 293–295
  - replacing ink cartridges, 291–292
- media types, 291
- printing process, 289–291

insider threat, 595

installation

- DIMM memory, 175–178
- memory, 175
- NIC, 254–255
- sound card, 241–244
- SSD (solid-state drive), 183–184
- video capture card, 253
- video cards, 245–246, 250–251
- web browser, 630–631
  - hashing, 631–632
  - untrusted sources, 632

Windows, 520–521

- clean install, 521–523
- image deployment, 524–525
- remote network installation, 523

repair installation, 523  
unattended, 521

integrated graphics card, 504

Intel

- CPUs, 210–211, 216–217. *See also* CPU (central processing unit)
- GPUs, 252

intermittent shutdown, troubleshooting, 375–376

Internet

- appliances
  - IDS (intrusion detection system), 84–85
  - IPS (intrusion prevention system), 85
  - load balancer, 85
  - proxy server, 85
  - spam gateway, 84
  - UTM (unified threat management) devices, 84
- connection types, 104
  - cable, 105–106
  - cellular, 109
  - DSL (Digital Subscriber Line), 106–107
  - fiber, 108
  - metered connections and limitations, 500
  - satellite, 108–109
- WISP (wireless Internet service provider), 112

interprocess communication mechanisms, 65

inventory list, 688

inverter, 26

IOPS (input/output operations per second), 390

iOS, 512–514. *See also* mobile devices

- Bluetooth headset, configuring, 43–44
- factory reset/clean install, 674
- Lightning connector, 28
- Location Services, disabling, 44

IoT (Internet of Things), 22–23, 40, 87–89, 620–621

IP addressing, 89, 491–493  
APIPA (Automatic Private IP Addressing), 96  
converting between numbering systems, 90  
DHCP (Dynamic Host Configuration Protocol), 98, 102–103  
DNS settings, 493–494  
IPv4, 89–90  
IPv6, 91–93  
NAT (network address translation), 91  
octet, 90, 493  
private IP addresses, 90–91  
public, 90  
reserved, 91  
static versus dynamic, 96–98, 494  
subnet mask, 493  
unicast addresses, 92–93  
viewing information, 93–95  
ip command, 551  
ipconfig -a command, 35, 94–95  
ipconfig command, 93–94  
ipconfig/all command, 35  
iPhone  
    Cellular Data Options, 34  
    hotspots, enabling/disabling, 36–38  
IPS (in-plane switching), 24  
IPS (intrusion prevention system), 85  
ITU-R (International Telecommunication Union Radiocommunication Sector), 75  
ITX (Information Technology eXtended)  
    on mobile devices, 217–218  
    motherboards, 201–204

## J-K

jailbreaking, 671

jitter, 419

Kerberos, 584

key fobs, 576

keyboard, replacing, 10

keylogger, 586

keys, 577

## L+3

LAN (local area network), 103, 112

laptops. *See also* memory; mobile devices

access panels, 8

battery, 20–22

Bluetooth, 29–30

connectivity, troubleshooting, 401

disassembling, best practices, 6–7

display, 23

docking station, 31–32

hard drive storage, 11

comparison, 11

HDD (hard disk drive), 11

HDD/SDD migration, 14

replacing, 12–13

SSD (solid-state drive), 11

SSHD (solid-state hybrid drive), 11

keyboard, replacing, 10

LCD display, inverter, 26

LoJack, 230

memory, upgrading, 14–17

mPCIe (mini PCI Express), 17–18

pointing sticks, 9

port replicator, 33  
proprietary vendor-specific ports, 28–29  
removing from all power sources, 20–21  
replacement components, power sources, 6  
screen/screen assembly  
    LCD (liquid crystal display), 23–24  
    microphone, 26  
    OLED (organic light-emitting diode), 24–25  
    webcam, 25–26  
serial interfaces, 28  
SODIMM (small outline DIMM), features, 15  
touchpads, 9  
touchscreen, 26  
underside, 7–8  
Wi-Fi antenna, 25  
wireless card, 18  
laser printers, 280–281. *See also* printers and printing  
    cleaning, 287–288  
    color, 284–285  
    imaging process, 281–284  
    maintenance, 285  
        applying maintenance kits, 286  
        performing calibration, 286–287  
        replacing toner cartridges, 286  
    media types, 285  
    toner cartridges, 281  
latency, 419  
LC (Lucent connector), 141  
LCD (liquid crystal display) displays, 23–24  
    display burn-in, troubleshooting, 397  
inverter, 26  
IPS (in-plane switching), 24  
TN (twisted nematic), 24

VA (vertical alignment), 24

LDAP (Lightweight Directory Access Protocol), 65

legacy systems, 86–87

LGA (Land Grid Array) sockets, 213–214

license(s)

- agreements, 689, 725
- commercial, 725
- corporate use, 726
- DRM (digital rights management), 725
- non-expiring, 726
- open-source, 726
- personal use, 726
- valid, 726–727

lifting techniques, 713–714

lighting, 577–578

Lightning connector, 28

Linux, 510–511. *See also* commands

- backup utilities, 703
- best practices
  - scheduled backups, 553–555
  - updates and patches, 555
- commands
  - apt-get, 551
  - cat, 553
  - cd, 548
  - chmod, 550
  - chown, 550
  - cp, 549
  - df, 201, 552
  - DIG, 553
  - find, 553
  - ftp, 61–62
  - grep, 547–548

ip, 551  
ipconfig -a, 35, 94–95  
ls, 547  
man, 550  
mv, 549  
nano, 553  
pwd, 549  
rm, 549  
shutdown, 548–549  
su/sudo, 550  
top, 552  
YUM, 551  
firmware, DD-WRT, 68  
IP configuration, 98  
safely ejecting a drive in, 201  
Samba, 556  
scripts, 94–95  
shell, 556  
sound card, configuring, 245  
terminal, 556  
liquid cooling system, 259–260  
liquid damage, mitigating, 401–402  
load balancing, 85  
Local Users and Groups, 462–463  
Location Services, disabling  
    on Android devices, 44–45  
    on iOS devices, 44  
locator applications, 617  
locks, 575, 611  
logical security, 578  
    ACLs (access control lists), 579  
    authentication, 580  
    email, 579

hard tokens, 580  
MFA (multifactor authentication), 579  
principle of least privilege, 578  
soft tokens, 580  
logs, 377–378, 415–417  
LoJack, 230  
loopback address, 92  
loopback plug, 119  
low memory warnings, troubleshooting, 657–659  
ls command, 547  
LTE (Long Term Evolution), 34

## M

M.2, 210  
MAC address, viewing, 35  
macOS, 510  
    App Store, 535  
    apps, uninstallation process, 535–536  
    best practices, 536  
        antivirus/anti-malware updates, 539  
        backups, 536–539  
    Disk Utility, 544  
    dynamic IP addressing, 97  
    FileVault, 545  
    Force Quit feature, 545–546  
    install file types, 534  
    pinwheel/unresponsiveness, troubleshooting, 360  
    sound card, configuring, 244–245  
    System Preferences, 540–544  
    Terminal, 545  
    Time Machine, 701–703  
    updates/patches, 539

magnetic hard disk drives, 188  
    form factors, 189  
    speed/spin rate, 188–189

magnetometers, 578

mail server, 83

maintenance  
    3D printers, 304  
    impact printers, 301  
        replacing the print head, 301–302  
        replacing the ribbon, 301

inkjet printers  
    calibration, 292–293  
    nozzle check and head cleaning, 293–295  
    replacing ink cartridges, 291–292

laser printer, 285  
    applying maintenance kits, 286  
    cleaning, 287–288  
    performing calibration, 286–287  
    replacing toner cartridges, 286

thermal printers, 298  
    cleaning heating elements, 298  
    removing debris, 298

malware, 584. *See also* attacks; social engineering  
    protecting against, 404

ransomware, 586

spyware, 585

Trojan, 584

troubleshooting  
    best practices, 667–668  
    browser-related symptoms, 666

virus, 585  
    boot sector, 586  
    cryptominers, 586–587

keylogger, 586

MAM (mobile application management), 45

MAN (metropolitan area network), 113

man command, 550

managed devices, 65

managed switch, 69

mapped drives and folders, 487–489

MBR (master boot record) partitions, 528–529

MDM (mobile device management), 45, 580–581

memory. *See also* hard disk drives

- cards, 190–192
- DDR SDRAM (double data rate SDRAM), 170–171
- DDR4 SDRAM, 170
- DDR5 SDRAM, 170
- DIMM (dual in-line memory module), installing, 175–178
- ECC (error correction code), 174–175
- flash drives/memory cards, 190–192
- form factor, 14
- installing, 175
- low, troubleshooting, 657–659
- parity checking, 173–174
- RAM, 14, 166–168
  - CL (CAS latency) values, 167
  - dual-channel, 172
  - quad-channel, 173
  - single channel RAM, 172
  - triple-channel, 173
- SODIMM, 15, 169
- speed, 14
- timing, 15
- upgrading, 14–17

methodology, 353

MFA (multifactor authentication), 505–506, 579, 583

microphone, 26

Microsoft account, 600–601

micro-USB/mini-USB, 27

migration, hard drive, 14

MIMO (multiple input multiple output), 74–75

mini-HDMI, 148

MMC (Microsoft Management Console) snap-in, 452

- Certificate Manager, 461–462
- Device Manager, 456–461
- Disk Management snap-in, 453–454
- Event Viewer, 453
- Local Users and Groups, 462–463
- Performance Monitor, 463
- Task Scheduler, 454–456

mobile devices

- accessories
  - drawing pad, 31
  - headsets, 30
  - speakers, 30
  - touch pens, 31
  - trackpad, 31
  - webcam, 31
- antivirus/antimalware, 618
- biometric authentication, 22, 619
- Bluetooth headset, configuring, 41
- broken screen, 400–401
- factory reset/clean install, 674
- failed login attempts restrictions, 618
- firewalls, 619
- first generation, 34
- full-device encryption, 619
- GPS (Global Positioning System), 44
- hotspots, 20, 30, 34–38, 110–111

improper battery charging, troubleshooting, 399–400  
ITX dimensions, 217–218  
locator applications, 617  
MAM (mobile application management), 45  
MDM (mobile device management), 45  
NFC (near-field communication), 22–23  
overheating, troubleshooting, 402–403  
patches and updates, 618–619  
policies and procedures  
    BYOD (bring your own device), 620  
    IoT, 620–621  
    profile security requirements, 620  
proprietary vendor-specific, 28–29  
recycling, 718–719  
remote backup applications, 617–618  
remote wipes, 617  
screen locks, 615–616  
security issues  
    APK (Android Package) source, 670  
    application spoofing, 671–672  
    Developer mode, 671  
    jailbreaking, 671  
    root access, 671  
    symptoms, 672–673  
synchronization, 45–46  
    email, 47  
    methods, 46–47  
tethering, 28, 36, 39  
troubleshooting common OS and application issues, 668  
    security-related, 670–674  
    symptoms, 668–670  
wired connections  
    Lightning, 28

micro-USB/mini-USB, [27](#)  
USB-C, [27](#)–[28](#)

wireless connections  
Bluetooth, [29](#)–[30](#)  
NFC (near-field communication), [29](#)

modems, [71](#)–[72](#)  
satellite, [109](#)  
setting up, [101](#)

motherboards. *See also* CPU (central processing unit)  
ATX (Advanced Technology eXtended) family, [202](#)–[204](#)  
BIOS (Basic Input/Output System)/UEFI (Unified Extensible Firmware Interface) settings, [218](#)–[225](#)  
audio and Ethernet ports, [233](#)–[234](#)  
boot sequence and settings, [225](#)–[226](#)  
CMOS battery, [234](#)–[235](#)  
fan settings, [230](#)–[231](#)  
firmware updates, [226](#)–[229](#)  
HSM (hardware security module), [236](#)–[237](#)  
inaccurate system date/time, troubleshooting, [379](#)–[380](#)  
SATA configuration, [231](#)–[232](#)  
security features, [229](#)–[230](#)  
TPM (Trusted Platform Module), [235](#)–[236](#)  
USB host adapters and charging support, [232](#)  
video cards, [247](#)

capacitor swelling, [378](#)–[379](#)

comparison, [204](#)–[206](#)

CPU (central processing unit)  
LGA (Land Grid Array) sockets, [213](#)–[214](#)  
mPGA (micro Pin Grid Array) sockets, [213](#)–[216](#)  
sockets, [212](#)–[213](#)

eSATA (external SATA) connectors, [210](#)

form factor, [201](#)

headers, [210](#)

ITX (Information Technology eXtended) family, 201–204  
M.2 SSD, 210  
PCI (Peripheral Component Interconnect) slots, 206  
PCIe (Peripheral Component Interconnect Express) slots, 206–209  
power connectors, 209  
processor compatibility, 210–211  
SATA (Serial Advanced Technology Attachment) connectors, 209–210  
sound card, 241–245  
video capture card, installing, 253  
video cards, 241  
    installing, 245–246  
    physical installation, 250–251  
    removing, 248–250  
    removing drivers, 247  
motion sensors, 574  
mPCIe (mini PCI Express), 17–18  
mPGA (micro Pin Grid Array) sockets, 213–216  
MSDS (material safety data sheet), 715–717  
MSRA (Microsoft Remote Assistance), 738–739  
multicore CPUs, 238–239  
multifunction devices, 271. *See also* printers and printing  
    configuration settings, 272–273  
    drivers, 272  
    setting up, 272  
    sharing, 273  
        ad hoc, 275–276  
        Bluetooth, 275  
        wired Ethernet, 274–275  
        wireless Ethernet, 275  
        wireless hosted networking, 277  
multimeter, 116–117  
multi-mode fiber, 141

multithreading, 239  
MU-MIMO (multiuser MIMO), 74  
mv command, 549

## N

nano command, 553  
NAS (network-attached storage), 82  
NAT (network address translation), 91  
navigation, File Explorer, 499  
negative pressure, 368  
nested paging, 339  
NetBIOS/NetBT, 64–65  
network tap, 120  
networking. *See also* cabling; connectors; Internet, appliances; IP addressing; wireless networking  
  administrative shares, 487  
  change management, 507–508  
  DNS settings, 493–494  
  domains, 436, 485–486  
  end-user device configuration, 101  
  gateway, 494  
  hardware  
    firewall, 70  
    hub, 71  
    modems, 71–72  
    NIC (network interface card), 72  
    ONT (optical network terminal), 72  
    patch panel, 70  
    PoE (Power over Ethernet) switch, 70–71  
    router, 67–68  
    switch, 68–69  
  WAP (wireless access point), 69–70

## IP addressing, 89

- APIPA (Automatic Private IP Addressing), 96
- converting between numbering systems, 90
- DHCP (Dynamic Host Configuration Protocol), 98, 102–103
- IPv4, 89–90
- IPv6, 91–93
  - NAT (network address translation), 91
  - octet, 90
  - private, 90–91
  - public, 90
  - reserved, 91
  - static versus dynamic addressing, 96–98
  - viewing information, 93–95
- IPv6, unicast addresses, 92–93
- LAN (local area network), 112
- local OS firewall settings, 489–491
- MAN (metropolitan area network), 113
- mapped drives and folders, 487–489
- metered connections, 500
- modems, setting up, 101
- NIC (network interface card), configuration steps, 100–101
- PAN (personal area network), 113
- printer sharing vs. network printer mapping, 489
- protocols, 60, 73
  - associated ports, 61
  - CIFS (Common Internet File System (CIFS), 66
  - DHCP (Dynamic Host Configuration Protocol), 63–64
  - DNS (Domain Name System), 63
  - FTP (File Transfer Protocol), 61
  - HTTPS (Hypertext Transfer Protocol Secure), 60, 64
  - IMAP (Internet Message Access Protocol), 65
  - LDAP (Lightweight Directory Access Protocol), 65
  - NetBIOS/NetBT, 64–65

POP3 (Post Office Protocol version 3), 64  
RDP (Remote Desktop Protocol), 66  
SMB (Server Message Block), 65  
SMTP (Simple Mail Transfer Protocol), 63  
SNMP (Simple Network Management Protocol), 65  
SSH (Secure shell), 62  
TCP (Transmission Control Protocol), 66–67  
Telnet, 62–63  
TFTP (Trivial File Transfer Protocol), 66  
UDP (User Datagram Protocol), 66  
proxy settings, 497–498  
public versus private, 498–499  
SAN (storage area network), 113  
shares, 486–487  
software-defined, 72  
topology, 114  
    bus, 142  
    diagrams, 690–691  
troubleshooting  
    external interference and intermittent wireless connectivity, 417–418  
    latency and jitter, 419  
    limited connectivity, 418–419  
    no connectivity, 417  
    port flapping, 420  
    slow speeds, 418  
    VoIP (Voice over Internet Protocol), 420  
virtual, 339–340. *See also* virtualization  
VLAN (virtual local area network), 103  
VPN (virtual private network), 103–104, 495–496, 737  
WAN (wide area network), 112–113  
WLAN (wireless local area network), 113  
workgroups, 436, 484

NFC (near-field communication), 22–23, 29, 81  
NIC (network interface card), 72, 100  
    configuration steps, 100–101  
    installing, 254–255  
NMS (network management system), 65  
no power, troubleshooting, 364, 370–371  
non-compliant systems, 596  
non-expiring license, 726  
nonresponsive touchscreen, troubleshooting, 403  
NTFS (New Technology File System), 515–516  
    permissions  
        Allow vs. Deny, 602  
        file and folder attributes, 602–603  
        inheritance, 602  
        propagation, 603  
        shared files and folders, 603  
NVMe (Non-Volatile Memory Express), 187

## O

octet, 90, 493  
OEM (original equipment manufacturer) parts, 6  
OLED (organic light-emitting diode), 23–25  
ONT (optical network terminal), 72  
open-source licenses, 726  
operating systems. *See also* Android; file systems; iOS; Linux;  
macOS; Windows  
    authentication, 604–605  
    boot process, 518–520  
    compatibility, 532–533  
    drivers, 526  
    EOL (end of life), 517, 596  
    firewalls, 598

mobile device, 511  
    Android, 512  
    iOS, 512–514  
    troubleshooting, 668–674  
requirements for applications, 506  
    32-bit versus 64-bit, 507  
    application-to-OS compatibility, 506  
update limitations, 517  
vendor-specific limitations, 518  
Windows  
    clean install, 521–523  
    Defender Antivirus, 597  
    feature updates, 533  
    image deployment, 524–525  
    major/minor reset, 525–526  
    remote network installation, 523  
    repair installation, 523  
    types of installations, 520–521  
    unattended installation, 521  
    update life cycle, 534  
    upgrading, 521, 530–531  
workstation, 509  
    Chrome OS, 511  
    Linux, 510–511  
    macOS, 510  
    Windows, 509  
optical drives, 179  
    Blu-ray, 180–181  
    CD-ROM/CD-RW, 179–180  
    drive speed ratings, 181  
    DVD recordable and rewritable, 180  
    recording files to, 181–182  
outsourcing, 623

overheating  
burning smells, causes of, 372  
troubleshooting, 364, 372, 402–403  
overloaded power supply, troubleshooting, 365

## P

PaaS (Platform as a Service), 329  
pairing, Bluetooth, 29–30, 77  
PAN (personal area network), 40, 113  
parity checking, 173–174  
partition(ing), 527  
dynamic disks, 529–530  
extended, 528  
GPT (globally unique ID partition table), 529  
MBR (master boot record), 528–529  
primary, 527–528  
parts  
OEM (original equipment manufacturer), 6  
storage, 7  
passive heat sink, 256–257  
password(s)  
best practices  
log off when not in use, 611  
secure PII, 611  
use screensaver locks, 611  
BIOS/UEFI, 609  
expiration policy, 609  
home router, 623–624  
managers, 633  
requiring, 609–610  
screensaver, 609  
strong, 609

PATA (Parallel ATA), S.M.A.R.T. failure, troubleshooting, 388–389  
patch panel, 70  
patches  
    Linux, 555  
    macOS, 539  
    mobile device, 618–619  
on-path attack, 594  
pathping command, 450–451  
PCI (Peripheral Component Interconnect), 17, 206  
PCIe (Peripheral Component Interconnect Express), 188, 206–209  
.pdf files, 279  
perfmon command, 390  
Performance Monitor, 390, 463  
peripherals  
    cabling, Thunderbolt, 151–153  
    PCI (Peripheral Component Interconnect), 17  
    power supply, 266–267  
permissions, 602  
    NTFS (New Technology File System)  
        Allow vs. Deny, 602  
        file and folder attributes, 602–603  
        inheritance, 602  
        propagation, 603  
        shared files and folders, 603  
personal use licenses, 726  
phishing, 589, 591  
physical security, 573  
    access control vestibule, 573  
    alarm systems, 574  
    badge reader, 573–574  
    bollards, 576  
    door locks, 575  
    equipment locks, 575

- fences, 576
- guards, 574
- motion sensors, 574
- for staff
  - biometrics, 577
  - key fobs, 576
  - keys, 577
  - lighting, 577–578
  - magnetometers, 578
  - smart card, 576–577
- video surveillance, 574

PII (personally identifiable information), 611

ping command, 92

pinwheel/unresponsiveness, troubleshooting on macOS, 360

plug-ins, web browser, 632

PoE (Power over Ethernet)

- standards, 71
- switch, 70

pointing sticks, 9

policy(ies)

- acceptable use, 689–690
- data destruction and disposal, 621–623

mobile device

- BYOD (bring your own device), 620
- IoT, 620–621
- profile security requirements, 620
- regulatory and compliance, 691–692

POP3 (Post Office Protocol version 3), 64

pop-up blocker, 635

portable speakers, 30

port(s), 60

- associated protocols, 61
- audio, 233–234

disabling, 630  
Ethernet, 233–234  
flapping, 420  
proprietary vendor-specific, 28–29  
replicator, 33  
security, 599  
serial, 28  
troubleshooting, 403  
USB, 153  
    2.0, 154–156  
    3.0, 154–156  
    3.1, 154–156  
    3.2, 156–158  
    4, 158  
    adapters, 159–160  
    add-on cards, 155

POST (Power-On Self-Test)  
    beep codes, troubleshooting, 355–356  
    error messages, troubleshooting, 355–356

Power Options  
    Hibernate option, 476  
    Power Plans, 476–477  
    Sleep/Suspend, 478  
    Standby, Lid, and Fast Startup options, 478  
    Universal Serial Bus (USB) Selective Suspend, 478–479

power supply(ies), 259–261  
    adapters, 265  
    autoswitching, 264  
    connectors, 265–267  
    disconnecting, 265  
    dual-rail design, 262  
    dual-voltage, 263–264  
    fan failure, troubleshooting, 365–366

modular, 269–270  
negative pressure, 368  
no power, troubleshooting, 364  
on/off switch, 264  
overloading, 365  
ratings, 261–262  
redundant, 268  
removing, 20–21  
replacements, 6  
safety standards, 263  
surge suppressors, 720  
tester, 372–374  
troubleshooting, 374–375  
voltage, 267  
wattage and amperage, 263, 270–271

PowerShell  
commands, 440–443

- chkdsk, 449–450
- copy, 445–446
- diskpart, 447–448
- findstr, 449
- format, 443–445
- gpupdate, 450
- pathping, 450–451
- robocopy, 446–447
- sfc, 448–449
- xcopy, 446

standard vs. administrative privileges, 439  
starting a command prompt session, 438–439

primary partition, 527–528  
principle of least privilege, 578  
print server, 83  
printers and printing, 271

3D, [302](#)  
    FDM (fused deposition modeling), [302–303](#)  
    maintenance, [304](#)  
    SLA (stereolithography), [302–304](#)

ADF (Automatic Document Feeder), [280](#)

cloud, [277–279](#)

configuration settings, [272–273](#)

drivers, [272](#)

hard drive caching, [278](#)

impact, [298–299](#)  
    heads, [300](#)  
    maintenance, [301–302](#)  
    paper types, [301](#)  
    print process, [299](#)  
    ribbons, [300](#)

inkjet, [288](#)  
    components, [288](#)  
    maintenance, [291–295](#)  
    media types, [291](#)  
    printing process, [289–291](#)

laser, [280–281](#)  
    color, [284–285](#)  
    imaging process, [281–284](#)  
    maintenance, [285–288](#)  
    media types, [285](#)  
    toner cartridges, [281](#)

.pdf files, [279](#)

print logs, [415–417](#)

setting up, [272](#)

sharing, [273, 489](#)  
    ad hoc, [275–276](#)  
    Bluetooth, [275](#)  
    wired Ethernet, [274–275](#)

wireless Ethernet, 275  
wireless hosted networking, 277

thermal, 295  
    maintenance, 298  
    print process, 296–297  
    ribbons, 295–296  
    thermal feed assembly and heating element, 295  
    thermal paper and media, 297

troubleshooting  
    double/echo images on the print, 407  
    faded prints, 406–407  
    finishing issues, 414  
    garbled print, 409  
    grinding noise, 413–414  
    incorrect chroma display, 412–413  
    incorrect page orientation, 414–415  
    incorrect paper size, 407  
    multipage misfeed, 409  
    multiple prints pending in the queue, 410–411  
    paper jams, 408–409  
    paper not feeding, 408  
    smudges and lines, 405–406  
    speckling on printed pages, 411–412  
    toner not fusing to the paper, 407  
    vertical lines on page, 410

user authentication/audit logs, 278  
using apps, 278

privacy screens, 578

private browsing mode, 636–637

private cloud, 330

private IP addresses, 90–91

private network, 498–499

PRL (Preferred Roaming List), 39–40

processors, motherboard compatibility, 210–211

procurement lifecycle, 689

professionalism. *See also* communication

- appearance and attire, 727
- avoid distractions, 729–730
- dealing with difficult customers or situations, 729
- language, 729
- privacy and confidentiality, 730
- punctuality, 729–730

projectors

- bulb issues, troubleshooting, 393–394
- dead pixels, troubleshooting, 394–395
- dim image, troubleshooting, 395–396
- flashing screen, troubleshooting, 396
- fuzzy or distorted image, troubleshooting, 396–397
- incorrect color display, troubleshooting, 395
- incorrect data source, troubleshooting, 392–393
- intermittent shutdown, troubleshooting, 394
- physical cabling issues, troubleshooting, 393

propagation, permission, 603

proprietary vendor-specific ports, 28–29

protocols, 60, 73. *See also* authentication

- associated ports, 61
- CIFS (Common Internet File System (CIFS), 66
- DHCP (Dynamic Host Configuration Protocol), 63–64, 98, 102–103
- DNS (Domain Name System), 63, 101–102
- encryption, 582
- FTP (File Transfer Protocol), 61–62
- HTTPS (Hypertext Transfer Protocol Secure), 60, 64, 634
- IMAP (Internet Message Access Protocol), 65
- LDAP (Lightweight Directory Access Protocol), 65
- NetBIOS/NetBT, 64–65
- POP3 (Post Office Protocol version 3), 64

RDP (Remote Desktop Protocol), 66  
SMB (Server Message Block), 65  
SMTP (Simple Mail Transfer Protocol), 63  
SNMP (Simple Network Management Protocol), 65  
SSH (Secure Shell), 62  
TCP (Transmission Control Protocol), 66–67  
Telnet, 62–63  
TFTP (Trivial File Transfer Protocol), 66  
TLS (Transport Layer Security), 633–634  
UDP (User Datagram Protocol), 66  
proxy server, 85, 497–498  
public cloud, 329–330  
public IP addresses, 90  
public network, 498–499  
punchdown tool, 116  
pwd command, 549

## Q

quad-channel RAM, 173  
qualitative risk analysis, 696  
quantitative risk analysis, 696

## R

RADIUS (Remote Authentication Dial-In User Service), 583  
RAID (Redundant Array of Inexpensive Disks), 194–196  
    SATA, 196–199  
    troubleshooting, 388  
RAM (random access memory), 14, 166–168. *See also* memory  
    application requirements, 505  
    CL (CAS latency) values, 167  
    DDR SDRAM (double data rate SDRAM), 170–171

DDR4 SDRAM, [170](#)  
DDR5 SDRAM, [170](#)  
dual-channel, [172](#)  
quad-channel, [173](#)  
single channel, [172](#)  
SODIMM (small outline DIMM), [169](#)  
triple-channel, [173](#)  
video, [504–505](#)  
virtual, [168](#)  
Windows 10 requirements, [437](#)  
ransomware, [586](#)  
rapid elasticity, cloud computing, [331](#)  
RDP (Remote Desktop Protocol), [66](#), [436](#), [736–737](#)  
rebuilding user profiles, [663–664](#)  
recording, to optical disc, [181–182](#)  
recovery  
    account, [698–699](#)  
    partition, [525](#)  
Recovery Mode, [587–588](#)  
recycling  
    batteries, [718–719](#)  
    cellphones and tablets, [718–719](#)  
    toner, [718–719](#)  
redundant power supplies, [268](#)  
Registry Editor, [469–471](#)  
regulatory policy and compliance, [691–692](#), [713](#), [726–728](#). *See also* policy(ies)  
remote access  
    MSRA (Microsoft Remote Assistance), [738–739](#)  
    RDP (Remote Desktop Protocol), [736–737](#)  
    SSH (Secure Shell), [736](#)  
    VNC (virtual network computing), [737](#)  
    VPN (virtual private network), [737](#)

remote backup applications, 617–618  
remote network installation, Windows, 523  
remote printing, 279  
remote wipes, 617  
removing  
    malware, 667–668  
    wireless card, 18  
repair installation, Windows, 523  
replacement components  
    OEM (original equipment manufacturer) parts, 6  
    power sources, 6  
replacing  
    battery, 21–22  
    case fan, 370  
    hard drive storage, 12–13  
    keyboard, 10  
request forms, 694–695  
reserved IP addresses, 91  
resetting Windows, 525–526  
Resource Monitor, 465–467  
RFID (radio frequency identification), 81  
RG-6, 144  
RG-58, 143  
RG-59, 143  
risk analysis, 696  
rm command, 549  
RMM (Remote Monitoring and Management), 736–738  
robocopy command, 446–447  
rootkit, 584–585  
routers, 67–68  
    SOHO  
        content filtering, 624–625  
        DHCP reservations, 625

firmware, 624  
IP filtering, 624  
password, 623–624  
placement, 625  
screened subnet, 626  
static WAN IP address, 626  
UPnP (Universal Plug and Play), 626  
wireless, frequency bands, 73

## S

SaaS (Software as a Service), 327–328  
Safe Mode, 363  
safety, 705, 713–714  
air filter mask, 715  
battery backup units, 720–721  
cable management, 715  
component handling and storage, 707–708, 713  
antistatic bags, 709  
ESD mats, 711  
ESD straps, 709–711  
self-grounding, 711–712  
compressed air and vacuum systems, 720  
electrical fire, 714–715  
equipment grounding, 705–708  
goggles, 715  
lifting techniques, 713–714  
surge suppressors, 720  
toxic waste handling/disposal, 717–719  
ventilation, 720  
weight limitations, 714  
Samba, 556  
SAN (storage area network), 113

sandboxing, 694

SATA (Serial Advanced Technology Attachment), 161, 209–210. *See also* hard disk drives

- configuration options, 231–232
- slow performance, troubleshooting, 382–384
- S.M.A.R.T. failure, troubleshooting, 388–389

SATA 2.5, 187–188

satellite Internet, 108–109

SC (subscriber connector), 141

scan services, 279–280

screen locks, 615–616

screensaver

- locks, 611
- passwords, 609

screen/screen assembly

- LCD (liquid crystal display), 23–24
  - inverter, 26
  - IPS (in-plane switching), 24
  - TN (twisted nematic), 24
  - VA (vertical alignment), 24
- microphone, 26
- OLED (organic light-emitting diode), 24–25
- webcam, 25–26

screen-sharing and videoconferencing, 737

screws, 7

scripts and scripting, 733–734

- languages, 731–732
- Linux, 94–95
- use cases, 732–734

SCSI (Small Computer System Interface) cable, 162–163

SDN (software-defined network), 72

SDR SDRAM (single data rate SDRAM), 14. *See also* memory

SDRAM (synchronous dynamic RAM), 14

security. *See also* encryption; firewall(s)  
application, 599–600  
BIOS (Basic Input/Output System)/UEFI (Unified Extensible Firmware Interface), 229–230  
browser  
certificates, 633  
extensions and plug-ins, 632  
HTTPS (Hypertext Transfer Protocol Secure), 634  
password managers, 633  
TLS (Transport Layer Security), 633–634  
home router  
content filtering, 624–625  
DHCP reservations, 625  
firmware, 624  
IP filtering, 624  
password, 623–624  
placement, 625  
screened subnet, 626  
static WAN IP address, 626  
UPnP (Universal Plug and Play), 626  
HSM (hardware security module), 236–237  
legacy and embedded systems, 86–87  
logical, 578  
ACLs (access control lists), 579  
authentication, 580  
email, 579  
hard tokens, 580  
MFA (multifactor authentication), 579  
principle of least privilege, 578  
soft tokens, 580  
passwords, 611  
BIOS/UEFI, 609  
expiration policy, 609

requiring, 609–610  
screensaver, 609, 611  
strong, 609

physical, 573  
    access control vestibule, 573  
    alarm systems, 574  
    badge reader, 573–574  
    biometrics, 577  
    bollards, 576  
    door locks, 575  
    equipment locks, 575  
    fences, 576  
    guards, 574  
    key fobs, 576  
    keys, 577  
    lighting, 577–578  
    magnetometers, 578  
    motion sensors, 574  
    privacy screens, 578  
    smart card, 576–577  
    video surveillance, 574

PII (personally identifiable information), 611

port, 599

requirements for virtualization, 339–340

smartphones  
    antivirus/antimalware, 618  
    biometric authentication, 619  
    failed login attempts restrictions, 618  
    firewalls, 619  
    full-device encryption, 619  
    locator applications, 617  
    patches and updates, 618–619  
    remote backup applications, 617–618

- remote wipes, 617
- screen locks, 615–616
- third-party tool, 738
- TPM (Trusted Platform Module), 235–236
- troubleshooting common issues
  - on mobile devices, 670–674
  - PCs, 646–666
- wireless
  - channels, 628
  - encryption settings, 627
  - guest access, 628
  - SSID (service set identifier), 627–628
- self-grounding, 711–712
- serial cable, 160–161
- serial interfaces, 28
- servers
  - AAA (authentication, authorization, and accounting), 84
  - cloud, 322
  - CPUs, 217
  - DHCP (Dynamic Host Configuration Protocol), 82
  - DNS (Domain Name System), 82, 101–102
  - file, 82
  - mail, 83
  - NAS (network-attached storage), 82
  - print, 83
  - proxy, 85, 497–498
  - syslog, 83
  - web, 83
- services not starting, troubleshooting, 655–657
- Settings menu (Windows), 480–481
  - Accounts settings, 484
  - Apps settings, 482
  - Gaming settings, 483–484

Network and Internet settings, 483  
Personalization settings, 481  
Privacy settings, 482  
System settings, 483  
Time and Language settings, 481  
Update and Security settings, 481  
sfc command, 448–449  
SFTP (Secure File Transfer Protocol), 62  
shares, 486–487, 603  
shell, 556  
shoulder surfing, 592  
shutdown command, 548–549  
SIM cards, 39  
single channel RAM, 172  
single-core CPUs, 238  
single-factor authentication, 583  
single-mode fiber, 141  
SLA (stereolithography), 302–304  
SLAT (second-level address translation), 339  
slow profile load, troubleshooting, 660–661  
sluggish performance, troubleshooting, 371–372, 652–653  
smartphones. *See also* Android; iOS; mobile devices  
    4G, 34  
    antivirus/antimalware, 618  
    biometric authentication, 619  
    broken screen, 400–401  
    failed login attempts restrictions, 618  
    firewalls, 619  
    full-device encryption, 619  
    GPS (Global Positioning System), 44  
    hotspots, 30, 34–38, 110–111  
    improper battery charging, troubleshooting, 399–400  
    Location Services, disabling

on Android devices, 44–45  
on iOS devices, 44  
locator applications, 617  
MAM (mobile application management), 45  
MDM (mobile device management), 45  
patches and updates, 618–619  
PRL (Preferred Roaming List), 39–40  
proprietary vendor-specific, 28–29  
remote backup applications, 617–618  
remote wipes, 617  
screen locks, 615–616  
tethering, 28  
vendor-specific limitations, 518  
SMB (Server Message Block), 65  
SMTP (Simple Mail Transfer Protocol), 63  
SNMP (Simple Network Management Protocol), 65  
social engineering, 590–591  
    attacks  
        brute force, 594  
        DDoS (distributed denial of service), 593  
        dictionary, 594–595  
        DoS (denial of service), 594  
        insider threat, 595  
        on-path, 594  
        spoofing, 594  
        SQL injection, 595  
        XSS (cross-site scripting), 595  
        zero-day, 594  
    dumpster diving, 593  
    evil twin attack, 593  
    impersonation, 592  
    phishing, 591  
    shoulder surfing, 592

tailgating, 593  
vishing, 592  
vulnerabilities, 596  
    BYOD (bring your own device), 596–597  
    end-of-life operating systems, 596  
    non-compliant systems, 596  
    unpatched systems, 596  
    unprotected systems, 596  
whaling, 592  
sockets, 212–213  
    LGA (Land Grid Array), 213–214  
    mPGA (micro Pin Grid Array), 213–216  
SODIMM (small outline DIMM), 14–15, 169. *See also* memory  
soft tokens, 580  
software firewall, 597–598  
SOHO networks. *See also* wireless networking  
    APIPA (Automatic Private IP Addressing), 96  
    DHCP (Dynamic Host Configuration Protocol), 98  
    end-user device configuration, 101  
    firewall settings, 628–629  
        disabling ports, 630  
        port forwarding/mapping, 629–630  
    NAT (network address translation), 91  
    private IP addresses, 90–91  
    router settings  
        content filtering, 624–625  
        DHCP reservations, 625  
        firmware, 624  
        IP filtering, 624  
        password, 623–624  
        placement, 625  
        screened subnet, 626  
        static WAN IP address, 626

UPnP (Universal Plug and Play), 626  
static versus dynamic addressing, 96–98  
SOP (standard operating procedure) manual, 692  
sound cards  
    configuring  
        on macOS, 244–245  
        on Windows, 244  
    external USB, 243  
    installing, 241–244  
spam gateway, 84  
speakers, 30  
speed  
    CPU, 240–242  
    magnetic hard disk drive, 188–189  
    memory, 14  
    network, 418  
    optical drive, 181  
spin rate, magnetic hard disk drive, 188–189  
splitters, 145, 267  
spoofing, 594, 671–672  
spyware, 585  
SQL injection, 595  
SSD (solid-state drive), 11, 182–183  
    flash memory, 186  
    form factors, 184–185  
    installing, 183–184  
    M.2, 210  
    NVMe (Non-Volatile Memory Express), 187  
SSH (Secure Shell), 62, 738  
SSHD (solid-state hybrid drive), 11, 14 186  
SSID (service set identifier), 627–628  
ST (straight tip) connector, 141  
standards. *See also* connectors

DVD recordable and rewritable, 180

Ethernet

- 10BASE2, 143
- 10BASE5, 143

T568B (EIA-568B), 139

Wi-Fi, 78–80

static IP addressing, 96–98, 494

STOP errors, 650

storage. *See also* backup(s); hard disk drives; memory; optical drives

- application requirements, 506
- local vs. cloud, 703–704
- RAID (Redundant Array of Inexpensive Disks), 194–196
  - SATA, 196–199
- safety, 707–708

STP (shielded twisted pair) cable, 138–139

strong passwords, 609

subnet mask, 493

SU-MIMO (single-user MIMO), 74

surge suppressors, 720

su/sudo command, 550

switches, 68–70

swollen battery, 400

synchronization

- browser data, 637
- file, 332
- mobile device, 45–47

synthetic backup, 698

syslog server, 83

System Configuration Utility, 467–468

system image, 699–700

System Information (msinfo32), 464–465

System Preferences, macOS, 540–544

# T

- T568A (EIA-568A), [139](#)–140
- T568B (EIA-568B) standard, [139](#)
- TACACS+ (Terminal Access Controller Access Control System), [583](#)
- tailgating, [593](#)
- Task Manager, [451](#)–452
- Task Scheduler, [454](#)–456
- TCP (Transmission Control Protocol), [66](#)–67
- Telnet, [62](#)–63
- telnet command, [62](#)
- terminal, [556](#)
- Terminal, macOS, [545](#)
- testing, backups, [698](#)
- tethering, [28](#), [36](#), [39](#), [110](#)
- TFTP (Trivial File Transfer Protocol), [66](#)
- thermal paste, [257](#)–259
- thermal printers, [295](#). *See also* printers and printing
  - maintenance, [298](#)
    - cleaning heating elements, [298](#)
    - removing debris, [298](#)
  - print process, [296](#)–297
  - ribbons, [295](#)–296
  - thermal feed assembly and heating element, [295](#)
  - thermal paper and media, [297](#)
- Thicknet, [143](#)
- thin client networking, [333](#)
- Thinnet, [143](#)
- third-party tools
  - desktop management software, [737](#)
  - file transfer software, [737](#)–739
  - screen-sharing and videoconferencing, [737](#)
  - security, [738](#)
- ticketing systems, [686](#), [688](#)

category of problem, 687  
description of problem, 687  
device information, 686  
escalation levels, 687–688  
severity of problem, 687  
user information, 686  
time drift, troubleshooting, 661–662  
timing, memory, 15  
TKIP (Temporal Key Integrity Protocol), 582  
TLS (Transport Layer Security), 633–634  
TN (twisted nematic), 24  
toner cartridges, 281, 718–719  
toner probe, 117–118  
tools. *See also* Control Panel; MMC (Microsoft Management Console)  
snap-in  
    antivirus/anti-malware, 587  
    antivirus/antimalware  
        Recovery Mode, 587–588  
        user education, 588–589  
app scanner, 673  
cable tester, 118  
Disk Cleanup, 468  
Disk Defragment/Optimize Drives, 469  
interactive memory upgrade, 15  
Linux  
    Samba, 556  
    shell/terminal, 556  
loopback plug, 119  
multimeter, 116–117  
network tap, 120  
power supply tester, 372–374  
Registry Editor, 469–471  
remote access, 736–738

Resource Monitor, 465–467

RMM (Remote Monitoring and Management), 736–738

rootkit, 584–585

System Configuration Utility, 467–468

System Information (msinfo32), 464–465

third-party

- desktop management software, 737
- file transfer software, 737–739
- screen-sharing and videoconferencing, 737

toner probe, 117–118

Wi-Fi analyzer, 119–120

top command, 552

topology, 114

- bus, 142
- diagrams, 690–691

touch pens, 31

touchpads, 9

touchscreen, 26

- digitizer issues, troubleshooting, 403
- nonresponsive, troubleshooting, 403

toxic waste handling/disposal, 717–719

TP (twisted pair) cable

- categories, 136–137
- shielded and unshielded, 138–139

TPM (Trusted Platform Module), 235–236, 606

trackpad, 31

training, anti-phishing, 589

triple-channel RAM, 173

Trojan horse, 584

troubleshooting. *See also* ticketing systems

- airflow problems
  - external, 366
  - internal, 366–368

application crashes, 657  
audio issues, 398  
black screen, 361–363  
boot problems, 653–654  
BSOD (blue screen of death), 357, 652  
    causes of, 358–360  
    STOP errors, 358  
cursor drift, 404  
damaged ports, 403–404  
devices in Device Manager, 460  
display burn-in  
    on LCD displays, 397  
    on plasma displays, 397  
frequent shutdowns, 654–655  
grinding noise, 378  
hard disk drives  
    bootable device not found, 385–387  
    data loss/corruption, 387–388  
    extended read/write times, 389–390  
    failure to boot, 385  
    grinding and clicking noises, 384–385  
    LED status indicators, 381–382  
    missing drives in OS, 390–392  
    RAID failure, 388  
    read/write failure, 382  
    slow performance, 382–384  
inaccurate system date/time, 379–380  
intermittent shutdown, 375–376  
liquid damage, 401–402  
low memory warnings, 657–659  
macOS, pinwheel/unresponsiveness, 360  
malware  
    best practices, 667–668

browser-related symptoms, [666](#)  
methodology, [353–354](#)  
mobile devices  
    OS and application issue symptoms, [668–670](#)  
    security issues, [670–674](#)  
networks  
    external interference and intermittent wireless connectivity, [417–418](#)  
    latency and jitter, [419](#)  
    limited connectivity, [418–419](#)  
    no connectivity, [417](#)  
    port flapping, [420](#)  
    slow speeds, [418](#)  
    VoIP (Voice over Internet Protocol), [420](#)  
No OS found, [660](#)  
no power, [364, 370–371](#)  
overheating, [364, 372, 402–403](#)  
poor/no connectivity, [401](#)  
POST beep codes, [355–356](#)  
POST error messages, [356–357](#)  
power supply, [365, 374–375](#)  
printers and printing  
    double/echo images on the print, [407](#)  
    faded prints, [406–407](#)  
    finishing issues, [414](#)  
    garbled print, [409](#)  
    grinding noise, [413–414](#)  
    incorrect chroma display, [412–413](#)  
    incorrect page orientation, [414–415](#)  
    incorrect paper size, [407](#)  
    lines down the printed page, [405–406](#)  
    multipage misfeed, [409](#)  
    multiple prints pending in the queue, [410–411](#)

- paper jams, 408–409
- paper not feeding, 408
- speckling on printed pages, 411–412
- toner not fusing to the paper, 407
- vertical lines on page, 410

projectors

- bulb issues, 393–394
- dead pixels, 394–395
- dim image, 395–396
- flashing screen, 396
- fuzzy or distorted image, 396–397
- incorrect color display, 395
- incorrect data source, 392–393
- intermittent shutdown, 394
- physical cabling issues, 393

recommended steps, 662–663

security issues, 646–666

services not starting, 655–657

slow profile load, 660–661

sluggish performance, 371–372, 652–653

system instability, 660

touchscreens

- digitizer issues, 403
- nonresponsive, 403

USB problems, 659

## U

UAC (User Account Control), 604

UDP (User Datagram Protocol), 66

UEFI (Unified Extensible Firmware Interface) settings, 218–225, 609.  
*See also* BIOS (Basic Input/Output System)

unattended installation, 521

unicast addresses, 92–93  
unmanaged switch, 69  
unpatched systems, 596  
unprotected systems, 596  
updates  
    Linux, 555  
    macOS, 539  
    Windows, 517  
upgrading/upgrade paths  
    compatibility, 532–533  
    memory, 14–17  
    Windows  
        application and driver support/backward compatibility, 531  
        backup files and user preferences, 530  
        hardware and application prerequisites and compatibility, 531  
    Windows 10, 438, 521, 531  
UPnP (Universal Plug and Play), 626  
USB  
    2.0, 154–156  
    3.0, 154–156  
    3.1, 154–156  
    3.2, 156–158  
    4, 158  
    adapters, 159–160  
    add-on cards, 155  
    -C, 27–28  
    host adapters and charging support, 232–233  
    hubs, 155  
    troubleshooting, 659  
User Accounts, 473. *See also* accounts  
user education, 588–589  
UTM (unified threat management) devices, 84

UTP (unshielded twisted pair) cable, 138–139  
T568A (EIA-568A) standard, 139–140  
T568B (EIA-568B) standard, 139

## V

VA (vertical alignment), 24  
valid license, 726–727  
vendor-specific limitations, 518  
ventilation, 720  
VGA (Video Graphics Array), 146–147  
video  
    application, 337  
    capture cards, 253  
    cards, 241  
        BIOS/UEFI configuration, 247  
        driver installation, 251  
        installing, 245–246  
        physical installation, 250–251  
        removing, 248–250  
        removing drivers, 247  
    connectors, 145–146  
        DisplayPort, 149–150  
        DVI (Digital Visual Interface), 150–151  
        HDMI (High-Definition Multimedia Interface), 147–148  
        VGA (Video Graphics Array), 146–147  
    surveillance, 574  
virtual RAM, 168  
virtualization, 240, 323  
    application, 337  
    client-side, 334–335  
    cross-platform, 337  
    desktop, 333–334

host/guest, 335–336  
hypervisor, 335  
nested paging, 339  
resource requirements, 338–339  
sandboxing, 694  
security requirements, 339–340  
VM (virtual machine), 336  
    sandboxing, 336–337  
    test development, 337  
virus, 585. *See also* antivirus/antimalware  
    boot sector, 586  
    cryptominer, 586–587  
    keylogger, 586  
vishing, 592  
VLAN (virtual local area network), 103  
VM (virtual machine), 334–336, 338  
    sandboxing, 336–337  
    test development, 337  
VMM (virtual machine manager), 334  
VNC (virtual network computing), 737  
VoIP (Voice over Internet Protocol), troubleshooting, 420  
voltage, power supply, 267  
VPN (virtual private network), 103–104, 495–496, 737  
VRAM (video RAM), 504–505  
vulnerabilities, 596  
    BYOD (bring your own device), 596–597  
    end-of-life operating systems, 596  
    non-compliant systems, 596  
    unpatched systems, 596  
    unprotected systems, 596

## W

WAN (wide area network), 112–113  
WAP (wireless access point), 69–70  
web browser. *See* browsers  
web server, 83  
webcam, 25–26, 31  
WEP (Wired Equivalent Privacy), 582  
whaling, 592  
whitepaper, 693  
Wi-Fi, 89  
    analyzer, 119–120  
    antenna, 25  
    hotspot, 30  
    standards, 78–80  
Windows, 509. *See also* NTFS (New Technology File System);  
PowerShell  
    accounts, 600  
        local vs. Microsoft, 600–601  
        standard vs. administrator, 601–602  
    boot process, 518–520  
    BSOD (blue screen of death), 357  
        causes of, 358–360, 651  
        STOP errors, troubleshooting, 358  
        troubleshooting, 652  
    Control Panel  
        Administrative Tools, 474  
        Ease of Access, 479–480  
        File Explorer Options, 474  
        Indexing Options, 474  
        Internet options, 471–472  
        Power Options, 476–479  
        starting, 471  
        User Accounts, 473  
        utilities, 473

Defender Antivirus, 597  
Defender Firewall, 489–491, 598–599  
dynamic IP addressing, 98  
feature updates, 533  
major/minor reset, 525  
MMC (Microsoft Management Console) snap-in, 452  
    Certificate Manager, 461–462  
    Device Manager, 456–461  
    Disk Management snap-in, 453–454  
    Event Viewer, 453  
    Local Users and Groups, 462–463  
    Performance Monitor, 463  
    Task Scheduler, 454–456  
networking  
    administrative shares, 487  
    domains, 485–486  
    mapped drives, 487–489  
    shares, 486–487  
    workgroups, 484  
Performance Monitor, 390  
rebuilding user profiles, 663–664  
Recovery Mode, 587–588  
recovery partition, 525  
Remote Desktop/Remote Assistance, 436  
run as an administrator, 603  
Safe Mode, 363  
safely ejecting a drive in, 199–200  
Settings menu, 480–481  
    Accounts settings, 484  
    Apps settings, 482  
    Gaming settings, 483–484  
    Network and Internet settings, 483  
    Personalization settings, 481

Privacy settings, [482](#)  
System settings, [483](#)  
Time and Language settings, [481](#)  
Update and Security settings, [481](#)  
sharing a folder, [487](#)  
sound card, configuring, [244](#)  
Task Manager, [451](#)–[452](#)  
types of installations, [520](#)–[521](#)  
    clean install, [521](#)–[523](#)  
    image deployment, [524](#)–[525](#)  
    remote network installation, [523](#)  
    repair installation, [523](#)  
    unattended, [521](#)  
UAC (User Account Control), [604](#)  
update life cycle, [534](#)  
upgrading, [521](#)  
    application and driver support/backward compatibility, [531](#)  
    backup files and user preferences, [530](#)  
    hardware and application prerequisites and compatibility,  
        [531](#)  
    wireless hosted networking, [277](#)  
Windows [10](#)  
    BitLocker, [437](#)  
    domain access vs. workgroups, [436](#)  
    editions, [435](#)–[436](#)  
    Group Policy Editor, [437](#)  
    RAM requirements, [437](#)  
    upgrade paths, [438](#)  
    upgrading, [531](#)  
    user interface, [436](#)  
Windows [11](#), requirements, [532](#)  
wired connections  
    configuration settings, [497](#)

mobile device  
    Lightning, 28  
    micro-USB/mini-USB, 27  
    USB-C, 27–28

wireless networking, 18, 43–44, 496. *See also* Internet, appliances  
    Bluetooth, 29–30, 40–41, 76–77  
        classes, 77  
        headset, 41, 43–44  
        pairing, 77  
    channels, 75–76  
    fixed wireless providers, 80  
    guest access, 628  
    MIMO (multiple input multiple output), 74–75  
    multifunction device sharing, 275  
    network card, removing, 18  
    NFC (near-field communication), 29, 81  
    routers, frequency bands, 73  
    security  
        channels, 628  
        encryption settings, 627  
    SSID (service set identifier), 627–628  
    troubleshooting, external interference and intermittent wireless connectivity, 417–418  
    WISP (wireless Internet service provider), 112  
    WWAN (wireless wide area network) connections, 497

WISP (wireless Internet service provider), 112

WLAN (wireless local area network), 113

workgroups, 436, 484

workstation operating systems, 509  
    Chrome OS, 511  
    Linux, 510–511  
    macOS, 510  
    Windows, 509

WPA2 (Wi-Fi Protected Access 2), 582  
WPA3 (Wi-Fi Protected Access 3), 582  
WPT (wireless power transfer), 81  
WWAN (wireless wide area network) connections, 497

## X

x64/x86 CPUs, 237–238  
xcopy command, 446  
XSS (cross-site scripting), 595

## Y-Z

YUM command, 551  
zero compression, 92  
zero-day attack, 594

**Exclusive Offer – 40% OFF**

## Pearson IT Certification Video Training

livelessons®

[pearsonitcertification.com/video](http://pearsonitcertification.com/video)

Use coupon code PITCVIDEO40 during checkout.



### Video Instruction from Technology Experts



#### Advance Your Skills

Get started with fundamentals,  
become an expert,  
or get certified.



#### Train Anywhere

Train anywhere, at your  
own pace, on any device.



#### Learn

Learn from trusted author  
trainers published by  
Pearson IT Certification.

### Try Our Popular Video Training for FREE!

[pearsonitcertification.com/video](http://pearsonitcertification.com/video)

Explore hundreds of **FREE** video lessons from our growing library of Complete Video Courses, LiveLessons, networking talks, and workshops.

**PEARSON  
IT CERTIFICATION**

ALWAYS LEARNING

[pearsonitcertification.com/video](http://pearsonitcertification.com/video)

**PEARSON**



**REGISTER YOUR PRODUCT** at [PearsonITcertification.com/register](http://PearsonITcertification.com/register)  
Access Additional Benefits and **SAVE 35%** on Your Next Purchase

- Download available product updates.
- Access bonus material when applicable.
- Receive exclusive offers on new editions and related products.  
(Just check the box to hear from us when setting up your account.)
- Get a coupon for 35% for your next purchase, valid for 30 days. Your code will be available in your PITC cart. (You will also find it in the Manage Codes section of your account page.)

Registration benefits vary by product. Benefits will be listed on your account page under Registered Products.

---

**PearsonITcertification.com—Learning Solutions for Self-Paced Study, Enterprise, and the Classroom**

Pearson is the official publisher of Cisco Press, IBM Press, VMware Press, Microsoft Press, and is a Platinum CompTIA Publishing Partner—CompTIA's highest partnership accreditation.

At [PearsonITcertification.com](http://PearsonITcertification.com) you can

- Shop our books, eBooks, software, and video training.
- Take advantage of our special offers and promotions ([pearsonitcertification.com/promotions](http://pearsonitcertification.com/promotions)).
- Sign up for special offers and content newsletters ([pearsonitcertification.com/newsletters](http://pearsonitcertification.com/newsletters)).
- Read free articles, exam profiles, and blogs by information technology experts.
- Access thousands of free chapters and video lessons.

**Connect with PITC – Visit [PearsonITcertification.com/community](http://PearsonITcertification.com/community)**

Learn about PITC community events and programs.



## PEARSON IT CERTIFICATION

Addison-Wesley • Cisco Press • IBM Press • Microsoft Press • Pearson IT Certification • Prentice Hall • Que • Sams • VMware Press

ALWAYS LEARNING

PEARSON

To receive your 10% off Exam Voucher, register your product at:

[www.pearsonitcertification.com/register](http://www.pearsonitcertification.com/register)

and follow the instructions.

# Appendix C

## Memory Tables

### Chapter 1

**Table 1-2** Comparison of HDD, SSD, and SSHD

Type of Hard Drive	Cost	Capacity	Speed	Reliability
HDD				
SSD				
SSHD				

**Table 1-4** SODIMM Features

Memory Type	Number of Pins	Notch Location	Notes
DDR3			67.6mm long and 30mm high
DDR4			69.6mm long and 30mm high
DDR5			69.6mm long and 30mm high

### Chapter 2

**Table 2-2** Common Protocols and Their Ports

Port Number(s)	Protocol	Port Type
20/21		
22		
23		
25		
53		
67/68		
80		
110		
137/139		
143		
161/162		
389		
443		

Port Number(s)	Protocol	Port Type
445		
3389		

**Table 2-3** PoE Standards

Name	IEEE Standard	Power Available to Powered Device (PD)	Maximum Power
PoE		____ W	____ W
PoE+		____ W	____ W
PoE++		____ W	____ W
PoE++		____ W	____ W

**Table 2-5** Bluetooth Classes

Class	Power (mW)	Range
Class 1		
Class 2		
Class 3		

**Table 2-6** Wireless Ethernet Standards

Wireless Ethernet Type	Frequency	Maximum Speed	MIMO Support	Estimated Range Indoors/Outdoors	Channel Width/Number of Channels	Interoperable With
802.11a						
802.11b						
802.11g						
802.11n						
802.11n (optional) (Wi-Fi 4)						
802.11ac						

Wireless Type	Ethernet Frequency	Maximum Speed	MIMO Support	Estimated Range Indoors/Outdoors	Channel Width/Number of Channels	Interoperable With
(Wi-Fi 5)						
802.11ax (Wi-Fi 6)						
802.11ax (Wi-Fi 6E)						

\* Non-overlapping channels; exact number varies by country.

\*\* Non-overlapping channels.

\*\*\* Up to four streams supported. Most devices have up to three antennas but can receive/transmit only two streams at a time.

## Chapter 3

**Table 3-5** USB Standards Overview

Version	Marketing Name	Speeds Supported	Maximum Cable Length*	Notes
1.1 (legacy)				
2.0				Also supports USB 1.1 devices and speeds
3.2 Gen 1 (also known as USB 3.0 and USB 3.1 Gen 1)				Also supports USB 1.1 and 2.0 devices and speeds
3.2 Gen 2 (also known as USB 3.1 Gen 2)				Also supports USB 1.1, 2.0, 3.0/3.1 Gen 1 devices and speeds
USB 3.2 Gen 1x2				Uses two lanes of data
3.2 Gen 2x2				Uses two lanes of data USB-C only
USB4 Gen 2x2				
USB4 Gen3x2				

\* To exceed recommended or maximum cable lengths, connect the cable to a USB hub or use an active USB extension cable.

† 3m is the recommended length, but no maximum cable length has been established for these versions of USB.

**Table 3-6** Network Connector Types

Type Description/Application	Status Figure
Standard phone jack. Smaller than RJ-45.	
Standard Ethernet cable connector.	Figures 3-2 and 3-4
Type of coax connector used with satellite boxes, set-top boxes, and CATV.	Figure 3-5
The standard fiber-optic connector with a bayonet-style insert and clip. Usually used in pairs with one fiber of inbound data and one fiber of outbound data. Uses round connectors.	Figure 3-3
Similar to ST, but uses square connectors.	Figure 3-3
Similar to ST, but uses square connectors.	Figure 3-3
Used for Ethernet cable connections to wall jacks and cross-connect racks in telecom closets. (See <a href="#">Chapter 2</a> .)	Figure 2-16
Universal Serial Bus. Most common connector currently in use	Figures 3-15 and 3-16
Smallest of the USB connector types. The USB type for many non-Apple phones.	
About half the size of USB-A. Common for external storage, cameras, and so on.	Figures 3-12 and 3-17
Newest reversible USB connector. Should replace other USB types.	Figure 3-12
Nine-pin serial connector that was once common on PCs. Once used for peripherals such as mouse devices and keyboards. Can be used for serial communications to networking equipment. Also used with a DB9-to-USB adapter to PCs without DB9 ports.	
Apple mobile device connector used for data and power.	
Used internally (hard drives) or externally (printers, storage, and so on).	
Used for connecting external storage. Thicker than internal SATA cables.	Figure 3-20

Type Description/Application	Status Figure
Not a networking connector. Delivers power from the power supply to various drives and the motherboard inside a PC.	

**Table 3-8** RAM Comparison

RAM Type	Pins (DIMM)	Pins (SODIMM)	Common Type and Speed	Defining Characteristic
DDR SDRAM				Double the transfers per clock cycle, compared to regular SDRAM
DDR3 SDRAM				External data bus speed (I/O bus clock) that is 4x faster than DDR SDRAM
DDR4 SDRAM*				External data bus speed (I/O bus clock) that is 2x faster than DDR3 SDRAM (8x faster than DDR SDRAM)
DDR5 SDRAM*				External data bus speed (I/O bus clock) that is 2x faster than DDR4 SDRAM (16x faster than DDR SDRAM)

\*DDR SODIMM keying is closer to the middle of the motherboard than with SDRAM SODIMMs.

†The keying on DDR3 is offset to one side, compared to DDR2.

‡The keying on DDR4 is different from the keying on DDR3, and they are not interchangeable.

**Table 3-9** Comparison of the Three Hard Drive Types

Type	Cost	Capacity	Speed	Reliability
HDD				
SSD				
SSHD				

**Table 3-10** Hard Disk Spin Rate Comparison

Spin Rate (RPM)	Typical Use	Desktop Drive Example	Laptop Drive Example
	"Green" power-saving drives	WD Blue Seagate 4TB Desktop HDD*	WD Blue Seagate Laptop HDD
	Midrange performance	WD Black	WD Black

<b>Spin Rate (RPM)</b>	<b>Typical Use</b>	<b>Desktop Drive Example</b>	<b>Laptop Drive Example</b>
		Seagate Barracuda	Seagate Laptop Thin
High performance		WD VelociRaptor	—
Servers and enterprise	Servers		—

\* Actual spindle speed 5900RPM

**Table 3-12** Comparisons of Common RAID Levels

<b>Minimum RAID Number of Level Drives Required</b>	<b>Data Protection Features</b>	<b>Total Capacity of Array</b>	<b>Major Benefit over Single Drive</b>	<b>Notes</b>
None		Twice the capacity of either drive (if same size) OR twice the capacity of the smaller drive	Improved read/write performance	Also called <i>striping</i>
	Changes to the contents of one drive are immediately performed on the other drive.	Capacity of one drive (if they are same size) OR the capacity of smaller drive	Automatic backup; faster read performance	Also called <i>mirroring</i>
	Parity information is saved across all drives.	Capacity of smallest drive (where x equals the number of drives in the array)	Full data redundancy in all drives; hot swap of the damaged drive supported in most implementations	
	Changes on one two-drive array are immediately performed on the other two-drive array.	Capacity of the smallest drive × the number of drives / 2	Improved read/ write performance and automatic backup	Also called <i>striped and mirrored</i>

**Table 3-13** ATX Motherboard Family Comparison

Motherboard Type	Maximum Width	Maximum Depth	Maximum Number of Expansion Slots	Typical Uses
	12 in. (30.5cm)	9.6 in. (24.4cm)	7	Full tower
	9.6 in. (24.4cm)	9.6 in. (24.4cm)	4	Mini tower

**Table 3-20** Power Levels for Different Connector Types

Connector +5V +12V +3.3V			Notes
Yes	Yes	No	Used today primarily for case fans that do not connect to the motherboard or that can be adapted to SATA drives
Yes	Yes	No	Used for power by some add-on cards
Yes	Yes	Optional	Requires using a Molex-to-SATA power connector if the power supply lacks adequate SATA connectors
No	Yes	No	Midrange PCIe video cards
No	Yes	No	High-performance PCIe video cards
No	Yes	No	Most recent and current motherboards, except those using EPS12V
No	Yes	No	Split into two ATX12V-compatible sections

## Chapter 5

**Table 5-2** The Six-Step CompTIA Troubleshooting Methodology

Step	Description
Step 1	
Step 2	
Step 3	
Step 4	
Step 5	
Step 6	

## Chapter 6

**Table 6-2 Windows 10 Editions and Features**

<b>Windows 10 Edition:</b> -	<b>Home</b>	<b>Pro</b>	<b>Pro for Workstations</b>	<b>Enterprise</b>
<b>Features :</b>				
<b>Domain Access vs. Workgroup</b>				
<b>Desktop Styles/ Control</b>				
<b>RDP</b>				
<b>Minimum RAM</b>				
<b>BitLocker</b>				
<b>gpedit.msc</b>				

**Table 6-3 Windows 10 Editions and Supported Upgrade Methods**

<b>Windows 10 Edition:</b> -	<b>Upgrade Path for:</b> -	<b>Command-Line tools</b>	<b>Product Key</b>	<b>Purchase License from Microsoft Store</b>
<b>Home to Pro</b>				
<b>Pro to Pro for Workstations</b>				
<b>Pro to Enterprise</b>				

**Table 6-4 Windows Command Prompt Commands**

### **Navigation Commands**

Changes the working directory (folder).

Displays a list of the current directory and subdirectories.

Creates a directory on the drive.

Removes an empty directory.

Navigates to the previous directory.

Takes you to the command prompt of the drive letter.

### **Command-Line Tools**

C:\Users>**ipconfig**

Displays TCP/IP network configuration information for each network adapter (both physical and virtual) on the device.

Sends IP packets to check network connectivity:

C:\Users>**ping cisco.com**

(reply follows)

Pinging **cisco.com** [2001:420:1101:1::185] with 32 bytes of data:

Reply from 2001:420:1101:1::185: time=64ms

Reply from 2001:420:1101:1::185: time=65ms

---

## **Navigation Commands**

---

Reply from 2001:420:1101:1::185: time=65ms

Reply from 2001:420:1101:1::185: time=69ms

Ping statistics for 2001:420:1101:1::185:

    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

    Approximate round trip times in milli seconds:

        Minimum = 64ms, Maximum = 69ms, Average = 65ms

---

Returns the computer name of the local device.

C:\Users>**hostname**

PC of RMcD

---

Displays a list of active TCP connections on a local network.

C:\Users>**netstat**

Active Connections

Protocol	Local Address	Foreign Address	State
TCP	10.0.0.34:49554	12.64.180.116:https	ESTABLISHED

(example output. Several lines omitted here)

---

Gathers the network's Domain Name System (DNS) information.

C:\Users>**nslookup**

Default Server: [cdns01.ISPprovider.net](http://cdns01.ISPprovider.net)

Address: 2101:568:feed::1

---

Scans the specified drive for errors and repairs them.

C:\Windows>**chkdsk** (Note: Run as Administrator)

---

The type of the file system is NTFS.

WARNING! /F parameter not specified.

Running CHDKSK in read-only mode.

Stage 1: Examining basic file system structure ...

    895232 file records processed.

File verification completed.

---

Manages user accounts (add, remove, change).

C:\Users>**net user**

User accounts for \\PC-RMcD

admin	Administrator	ctctechs
-------	---------------	----------

DefaultAccount

The command completed successfully.

---

Connects to shared folders, similar to mapping a network drive.

C:\Users>**net use**

New connections will be remembered.

---

## Navigation Commands

---

There are no entries in the list.

Similar to ping, but returns path information to an IP address destination. Similar to the traceroute command in macOS and Linux. Can be used for troubleshooting connectivity across the Web.

C:\Users>**tracert Cisco.com**

Tracing route to [cisco.com](http://cisco.com) [2001:420:1101:1::185]

over a maximum of 30 hops:

1 5 ms 2601:602:cc01:16e0:623d:26ff:feb9:8830  
2 13 ms 12 ms 12 ms 2001:558:4082:c6::1  
3 12 ms 13 ms 13 ms 2001:558:a2:601b::1  
(20 hops in *output omitted*)

---

*(Note: Do not practice this command on an operational computer!)*

Creates or re-creates the specified file system on recordable or rewritable storage (magnetic, flash, or optical media) and overwrites the contents and file table of the drive.

Copies one or more files and folders to another folder or drive.

C:\Users>**XCOPY source [destination] [/A |**

For format and function table, type:

C:\Users>**help xcopy**

---

Copies one or more files to another folder or drive.

Robust File Copy for Windows. Copies or moves files/folders; can be configured with various optional GUIs.

Usage :: **ROBOCOPY** source destination [file [file]...] [options]

source :: Source Directory (drive:\path or \\server\share\path).

destination :: Destination Dir (drive:\path or \\server\share\path).

file :: File(s) to copy (names/wildcards: default is “\*.\*”).

For options table, use : C:\Users>**help robocopy**

---

Refreshes Group Policy on local or Active Directory systems.

C:\Users>**gpupdate**

Updating policy...

Displays the resultant set of policy for the specified computer and user.

For the usage guide, type: C:\Users>**gpresult /?**

---

*(Note: Do not practice this command on an operational computer!)*

Shuts down the computer. For usage, enter: C:\Users>**shutdown /?**

---

Scans system files and replaces damaged or missing files.

C:\Windows>**sfc /scannow** (*run as administrator*)

Beginning system scan. This process will take some time.

Beginning verification phase of system scan.

Verification 4% complete.

---

---

## Navigation Commands

---

Displays help for the specified command name—for example, **xcopy /?**.

---

*(Note: Do not practice this command on an operational computer!)*

Creates, removes, and manages disk partitions.

---

Similar to **traceroute** but provides information on network latency along the path to the destination. **pathping** traces and tests network connections to an IP address.

C:\Users>**pathping cisco.com**

---

Stops specified task(s) on a local or remote computer.

C:\Users>**TASKKILL /IM notepad.exe**

---

Returns version information of the current Windows OS.

C:\Users>**winver**

---

**Table 6-6** Internet Properties Dialog Tabs

---

### Tab Function

---

Set the home page; set tab settings; delete browsing history, cookies, temporary files, and saved passwords; change appearance; and configure accessibility settings

---

Configure security zones

---

Select privacy settings for the current zone, location settings, pop-up blocker, and InPrivate browsing settings

---

Set options for family safety, SSL certificate management, AutoComplete, and feeds

---

Set options for VPNs, dial-up, LAN connections, and proxy servers

---

Select the default web browser, manage add-ons, select the default HTML editor, and set the default apps for email and other Internet services

---

Enable and disable accelerated graphics; configure accessibility settings, browsing settings, HTTP settings, international settings, multimedia settings, and security settings; and reset Internet Explorer to the default settings

---

**Table 6-8** File System Format Comparison

---

System Type	Full Name	Details
		Microsoft file system used for flash drives larger than 32GB and files larger than 4GB.
		Format for USB flash drives that hold files smaller than 4GB, game consoles, and so on. Works with all operating systems.
		Windows default formatting for hard drives. Supports sharing and journaling.
		Apple file system of macOS that is designed to enhance performance with solid state drives (SSDs) and flash storage. It is available on macOS 10.13 and higher.

<b>System Type</b>	<b>Full Name</b>	<b>Details</b>
		Open source system that works independently of the operating system, allowing network user access. It appears local but is a common network drive.
		Linux version of NTFS. Allows journaling of changes, to minimize damage if a crash occurs. Supports a maximum of 32,000 subdirectories.
		Linux system. Supports larger file sizes than ext3. Can disable journaling. Supports a maximum of 64,000 subdirectories.

## Chapter 8

**Table 8-2** Slow/Sluggish System Performance Causes and Solutions

### Windows System Performance Troubleshooting

<b>Problem</b>	<b>Solution</b>
System is not configured for maximum performance	
Drive containing paging file and temporary files is nearly full or badly fragmented	
System is overheating and CPU is running at reduced speed	
Memory is running low	
Sudden performance drop occurs	
Registry error messages appear	

**Table 8-3** Common Symptoms of PC Security Issues

<b>Symptom</b>	<b>Possible Causes</b>
No access to the network	
Desktop alerts	
False alerts regarding antivirus protection	

<b>Symptom</b>	<b>Possible Causes</b>
Altered system or personal files	
Unwanted notifications within the OS	
OS update failures	

**Table 8-4** Browser-Related Symptoms

<b>Symptom</b>	<b>Possible Causes</b>
Random or frequent pop-ups	
Certificate warnings	
Browser redirection	

**Table 8-5** Common Symptoms of Mobile OS and Application Issues

<b>Symptom</b>	<b>Troubleshooting Step(s)</b>
App fails to launch	
App fails to close or crashes	
App fails to update	

Symptom	Troubleshooting Step(s)
App is slow to respond	
OS fails to update	
Battery life issues arise	
Phone or device randomly reboots	
Screen does not autorotate	

### Connectivity Issues

Symptom	Troubleshooting Step(s)
Bluetooth	
Wi-Fi	
Near-field communication (NFC)	
AirDrop	

## Chapter 9

**Table 9-4** Electrical Conditions and Protective Measures

Type of Electrical Condition	Description	Protective Measure
Power surge	Overshoot event lasting less than _____. Up to _____ V and _____ A.	
Under-voltage event	Sustained voltage drop of _____ normal voltage. Can last for _____.	
Power failure	Total loss of power for an extended period of time.	

**Table 9-5** Basic Scripting Languages

Extension Language	Basic Information
Windows batch file	Batch files are script files that are strictly Windows based. They are text files that contain commands or instructions for the command-line interpreter to execute. The instructions in a batch file can be interpreted only by the Windows operating system.
PowerShell	Windows PowerShell is a tool to help technicians and network administrators automate support functions through the use of scripts and snippets. Windows 10 and 11 ship with PowerShell.
VBScript	VBScript, a scripting language developed by Microsoft, is considered a subset of the Visual Basic programming language. It was designed specifically for use with Microsoft Internet Explorer. It gives web pages a level of interactivity.
Linux shell script	A shell script is a text file that contains a sequence of commands for a Linux- or UNIX-based system. Shell scripts might not run correctly on a Windows system. Linux has had several shells; BASH (Bourne-Again Shell) is the most common of them.
Python	Python is often a good choice for those beginning to learn programming. It is relatively easy to learn, and Python scripts can run on most operating systems. For example, Windows Shell is known as Python Interactive Shell.
JavaScript	JavaScript is a programming language that has many uses today. It is valuable for creating scripts because it can be run on any operating system. It is usually written into web pages to create client interactions; JavaScript is read by the browser. Creating and running command-line JavaScript requires installing Node.js.

# Appendix D

## Memory Tables Answer Key

### Chapter 1

**Table 1-2** Comparison of HDD, SSD, and SSHD

Type of Hard Drive	Cost	Capacity	Speed	Reliability
HDD	Least expensive and readily available	Highest capacity	Slowest because of moving parts and magnetic disks	Has moving parts that can wear over time
SSD	Most expensive, but price is dropping	Lowest capacity, but improving	Fastest	Has no moving parts
SSHD	Midrange cost	Blends high HDD capacity with fast solid-state cache for most-used files	Blends fast solid-state cache with slower magnetic storage	Has moving parts that can wear out, but spins less than HDD

**Table 1-4** SODIMM Features

Memory Type	Number of Pins	Notch Location	Notes
DDR3	204	After pin 36	67.6mm long and 30mm high
DDR4	260	After pin 144	69.6mm long and 30mm high
DDR5	262	After pin 116	69.6mm long and 30mm high

### Chapter 2

**Table 2-2** Common Protocols and Their Ports

Port Number(s)	Protocol	Port Type
20/21	File Transfer Protocol (FTP)	TCP, UDP
22	Secure Shell (SSH)	TCP, UDP
23	Telnet	TCP, UDP
25	Simple Mail Transfer Protocol (SMTP)	TCP, UDP
53	Domain Name System (DNS)	TCP, UDP
67/68	Dynamic Host Configuration Protocol (DHCP)	UDP
80	Hypertext Transfer Protocol (HTTP)	TCP, UDP
110	Post Office Protocol 3 (POP3)	TCP, UDP

<b>Port Number(s)</b>	<b>Protocol</b>	<b>Port Type</b>
137/139	Network Basic Input/Output System (NetBIOS)/NetBIOS over TCP/IP (NetBT)	TCP, UDP
143	Internet Message Access Protocol (IMAP)	TCP
161/162	Simple Network Management Protocol (SNMP)	TCP, UDP
389	Lightweight Directory Access Protocol (LDAP)	TCP, UDP
443	Hypertext Transfer Protocol Secure (HTTPS)	TCP, UDP
445	Server Message Block (SMB)/Common Internet File System (CIFS)	TCP
3389	Remote Desktop Protocol (RDP)	TCP, UDP

**Table 2-3** PoE Standards

<b>Name</b>	<b>IEEE Standard</b>	<b>Power Available to Powered Device (PD)</b>	<b>Maximum Power</b>
PoE	IEEE 802.3af	12.95W	15.4W
PoE+	IEEE 802.3at (Type 2)	25.5W	30W
PoE++	IEEE 802.3bt (Type 3)	51W	60W
PoE++	IEEE 802.3bt (Type 4)	71W	100W

**Table 2-5** Bluetooth Classes

<b>Class</b>	<b>Power (mW)</b>	<b>Range</b>
Class 1	100mW	100m (328 feet)
Class 2	2.5mW	10m (33 feet)
Class 3	1mW	1m (3 feet)

**Table 2-6** Wireless Ethernet Standards

<b>Wireless Frequency Ethernet Type</b>	<b>Maximum Speed</b>	<b>MIMO Support</b>	<b>Estimated Range Indoors/Outdoors</b>	<b>Channel Width/Number of Channels</b>	<b>Interoperability With</b>
802.11a 5GHz	54Mbps	No	35m/120m	20MHz/12*	Requires dual-mode (802.11a/b or 802.11a/g) hardware; 802.11n networks that support 5GHz frequency
802.11b 2.4GHz	11Mbps	No	32m/140m	20MHz/3**	802.11g
802.11g 2.4GHz	54Mbps	No	32m/140m	20MHz/3**	802.11b, 802.11n
802.11n 2.4GHz	72Mbps per stream	Yes***	70m/250m	20MHz/3**	802.11b, 802.11g;

Wireless Frequency Type	Maximum MIMO Speed	Estimated Range Support Indoors/Outdoors	Channel Width/Number	Interoperability With Other Standards
	(20MHz channel)			802.11a on networks that also support 5GHz frequency
802.11n 5GHz (optional) (Wi-Fi 4)	150Mbps per stream (40MHz channel)	Yes***	70m/250m 20MHz or 40MHz/12*	802.11a (20MHz-wide channels only)
802.11ac 5GHz (Wi-Fi 5)	433Mbps per stream (80MHz channel)	Yes***	70m/250m 20MHz or 40MHz or 80MHz	802.11a, 802.11n (5GHz); 802.11ac routers that also support previous standards
802.11ax 2.4GHz/5GHz (Wi-Fi 6)	Up to 9.6Gbps, 1Gbps (5GHz channel)	Mu-MIMO	Same, but better throughput at longer ranges	160MHz Supports previous standards
802.11ax 2.4GHz/5GHz/6GHz (Wi-Fi 6E)	Up to 9.6Gbps	Mu-MIMO	Same as Wi-Fi 6, but 6GHz has a shorter range	160MHz Supports previous standards

\* Non-overlapping channels; exact number varies by country.

\*\* Non-overlapping channels.

\*\*\* Up to four streams supported. Most devices have up to three antennas but can receive/transmit only two streams at a time.

## Chapter 3

**Table 3-5** USB Standards Overview

Version	Marketing Name	Speeds Supported	Maximum Cable Length*	Notes
1.1 (legacy)	USB	12Mbps 1.5Mbps	3m	
2.0	Hi-Speed USB	480Mbps	5m	Also supports USB 1.1 devices and speeds
3.2 Gen 1 (also known as USB 3.0 and USB 3.1 Gen 1)	SuperSpeed USB	5Gbps	† 15m	Also supports USB 1.1 and 2.0 devices and speeds
3.2 Gen 2 (also known as USB 3.1 Gen 2)	SuperSpeed+ USB	10Gbps	†	Also supports USB 1.1, 2.0, 3.0/3.1 Gen 1

<b>Version</b>	<b>Marketing Name</b>	<b>Speeds Supported</b>	<b>Maximum Cable Length*</b>	<b>Notes</b>
				devices and speeds
USB 3.2 Gen 1x2	Superspeed +	10Gbps	†	Uses two lanes of data
3.2 Gen 2x2	Superspeed+ USB	20Gbps	†	Uses two lanes of data USB-C only
USB4 Gen 2x2	USB4 20Gbps	20Gbps	2m	
USB4 Gen3x2	USB4 40Gbps	40Gbps	2m	

\* To exceed recommended or maximum cable lengths, connect the cable to a USB hub or use an active USB extension cable.

† 3m is the recommended length, but no maximum cable length has been established for these versions of USB.

**Table 3-6** Network Connector Types

<b>Type</b>	<b>Description/Application</b>	<b>Status</b>	<b>Figure</b>
RJ-11	Standard phone jack. Smaller than RJ-45.	Current	
RJ-45	Standard Ethernet cable connector.	Current	<a href="#">Figures 3-2 and 3-4</a>
F Type	Type of coax connector used with satellite boxes, set-top boxes, and CATV.	Current	<a href="#">Figure 3-5</a>
Straight Tip (ST)	The standard fiber-optic connector with a bayonet-style insert and clip. Usually used in pairs with one fiber of inbound data and one fiber of outbound data. Uses round connectors.	Current and most common in use	<a href="#">Figure 3-3</a>
Subscriber Connector (SC)	Similar to ST, but uses square connectors.	Current	<a href="#">Figure 3-3</a>
Lucent Connector (LC)	Similar to ST, but uses square connectors.	Current	<a href="#">Figure 3-3</a>
Punch-down Block	Used for Ethernet cable connections to wall jacks and cross-connect racks in telecom closets. (See <a href="#">Chapter 2</a> .)	Current	<a href="#">Figure 2-16</a>
USB	Universal Serial Bus. Most common connector currently in use	Current	<a href="#">Figures 3-16 and 3-17</a>
microUSB	Smallest of the USB connector types. The USB type for many non-Apple phones.	Current/to be displaced by USB-C	
miniUSB	About half the size of USB-A. Common for external storage, cameras, and so on.	Legacy, but still in use	<a href="#">Figures 3-12 and 3-18</a>
USB-C	Newest reversible USB connector. Should replace other USB types.	Current	<a href="#">Figure 3-12</a>

Type	Description/Application	Status	Figure
DB9	Nine-pin serial connector that was once common on PCs. Once used for peripherals such as mouse devices and keyboards. Can be used for serial communications to networking equipment. Also used with a DB9-to-USB adapter to PCs without DB9 ports.	Legacy, but still in specialized use	
Lightning	Apple mobile device connector used for data and power.	Current	
SCSI	Used internally (hard drives) or externally (printers, storage, and so on).	Legacy	
eSATA	Used for connecting external storage. Thicker than internal SATA cables.	Current	Figure 3-21
Molex	Not a networking connector. Delivers power from the power supply to various drives and the motherboard inside a PC.	Legacy, but still around; replaced by SATA	

**Table 3-8** RAM Comparison

RAM Type	Pins (DIMM)	Pins (SODIMM)	Common Type and Speed Defining Characteristic
DDR SDRAM	184	200*	PC3200 = 400MHz/3200Mbps Double the transfers per clock cycle, compared to regular SDRAM
DDR3 SDRAM	240†	204	DDR3-1333 (PC3-10600) = 1333MHz/10,600Mbps External data bus speed (I/O bus clock) that is 4x faster than DDR SDRAM
DDR4 SDRAM*	288‡	260	DDR4-2400 (PC4-19200) = 2400MHz/19200Mbps External data bus speed (I/O bus clock) that is 2x faster than DDR3 SDRAM (8x faster than DDR SDRAM)
DDR5 SDRAM*	288	262	DDR5-7200 (PC5-57600) = 7200MHz/57600Mbps External data bus speed (I/O bus clock) that is 2x faster than DDR4 SDRAM (16x faster than DDR SDRAM)

\*DDR SODIMM keying is closer to the middle of the motherboard than with SDRAM SODIMMs.

†The keying on DDR3 is offset to one side, compared to DDR2.

‡The keying on DDR4 is different from the keying on DDR3, and they are not interchangeable.

**Table 3-9** Comparison of the Three Hard Drive Types

Type	Cost	Capacity	Speed	Reliability
HDD	Least expensive and readily available	Highest	Slowest due to moving parts and magnetic storage	Moving parts that can wear over time
SSD	Most expensive, but price is dropping	Lowest, but improving	Fastest	Solid state; no moving parts

Type Cost	Capacity	Speed	Reliability
SSHD Midrange	Blends high HDD capacity with fast SSD cache for most-used files	Blends fast solid-state cache with slower magnetic storage	Moving parts that can wear out, but spins less than HDD

**Table 3-10** Hard Disk Spin Rate Comparison

Spin Rate (RPM)	Typical Use	Desktop Drive Example	Laptop Drive Example
5400	"Green" power-saving drives	WD Blue Seagate 4TB Desktop HDD*	WD Blue Seagate Laptop HDD
7200	Midrange performance	WD Black Seagate Barracuda	WD Black Seagate Laptop Thin
10000	High performance	WD VelociRaptor	—
15000	Servers and enterprise	Servers	—

\* Actual spindle speed 5900RPM

**Table 3-12** Comparisons of Common RAID Levels

RAID Level	Minimum Number of Drives Required	Data Protection Features	Total Capacity of Array	Major Benefit over Single Drive	Notes
0	2	None	Twice the capacity of either drive (if same size) OR twice the capacity of the smaller drive	Improved read/write performance	Also called <i>striping</i>
1	2	Changes to the contents of one drive are immediately performed on the other drive.	Capacity of one drive (if they are same size) OR the capacity of smaller drive	Automatic backup; faster read performance	Also called <i>mirroring</i>
5	3	Parity information is saved across all drives.	Capacity of smallest drive (where x equals the number of drives in the array)	Full data redundancy in all drives; hot swap of the damaged drive supported in most implementations	
10	4	Changes on one two-drive array are immediately performed on the other two-drive array.	Capacity of the smallest drive × the number of drives ÷ 2	Improved read/write performance and automatic backup	Also called <i>striped and mirrored</i>

**Table 3-13** ATX Motherboard Family Comparison

Motherboard Type	Maximum Width	Maximum Depth	Maximum Number of Expansion Slots	Typical Uses
ATX	12 in. (30.5cm)	9.6 in. (24.4cm)	7	Full tower
mATX	9.6 in. (24.4cm)	9.6 in. (24.4cm)	4	Mini tower

**Table 3-20** Power Levels for Different Connector Types

Connector +5V +12V +3.3V Notes			
Molex	Yes	Yes	No
			Used today primarily for case fans that do not connect to the motherboard or that can be adapted to SATA drives
Berg	Yes	Yes	No
			Used for power by some add-on cards
SATA	Yes	Yes	Optional
			Requires using a Molex-to-SATA power connector if the power supply lacks adequate SATA connectors
PCIe 6-pin	No	Yes	No
			Midrange PCIe video cards
PCIe 8-pin	No	Yes	No
			High-performance PCIe video cards
ATX12V	No	Yes	No
			Most recent and current motherboards, except those using EPS12V
EPS12V	No	Yes	No
			Split into two ATX12V-compatible sections

## Chapter 5

**Table 5-2** The Six-Step CompTIA Troubleshooting Methodology

Step	Description
Step 1	<b>Identify the problem.</b> Question the user and identify user changes to the computer. If applicable, perform backups before making further changes. Inquire about environmental or infrastructure changes that might have occurred. Review system application logs for clues to possible system errors.
Step 2	<b>Establish a theory of probable cause (question the obvious).</b> If necessary, conduct external or internal research based on symptoms.
Step 3	<b>Test the theory to determine the cause.</b> When the theory is confirmed, determine the next steps to resolve the problem. If the theory is not confirmed, re-establish a new theory or escalate the issue.
Step 4	<b>Establish a plan of action to resolve the problem and implement the solution.</b> Refer to the vendor's instructions for guidance.
Step 5	<b>Verify full system functionality and, if applicable, implement preventive measures.</b>

---

**Step Description**

---

Step **Document the findings, actions, and outcomes.**

6

---

## Chapter 6

**Table 6-2** Windows 10 Editions and Features

<b>Windows 10 Edition: -</b>	<b>Home</b>	<b>Pro</b>	<b>Pro for Workstations</b>	<b>Enterprise</b>
<b>Features :</b>				
<b>Domain Access vs. Workgroup</b>	Workgroup	Workgroup or domain	Domain	Domain
<b>Desktop Styles/Control</b>	No	No	Yes	Yes
<b>RDP</b>	Client only	Host and client	Host and client	Host and client
<b>Minimum RAM</b>	1GB	2GB	2GB	2GB
<b>BitLocker</b>	No	Yes	Yes	Yes
<b>gpedit.msc</b>	No	Yes	Yes	Yes

**Table 6-3** Windows 10 Editions and Supported Upgrade Methods

<b>Windows 10 Edition: -</b> <b>Upgrade Path for: :</b>	<b>Command-Line tools</b>	<b>Product Key</b>	<b>Purchase License from Microsoft Store</b>
<b>Home to Pro</b>	no	Yes	Yes
<b>Pro to Pro for Workstations</b>	Yes—no reboot	Yes—no reboot	Yes—no reboot
<b>Pro to Enterprise</b>	Yes—no reboot	Yes—no reboot	No

**Table 6-4** Windows Command Prompt Commands

---

**Navigation Commands**

---

**cd (chdir)** Changes the working directory (folder).

**dir** Displays a list of the current directory and subdirectories.

**md (mkdir)** Creates a directory on the drive.

**rmdir** Removes an empty directory.

**cd ..** Navigates to the previous directory.

C:\ or D:\ or X:\ Takes you to the command prompt of the drive letter.

---

**Command-Line Tools**

---

**ipconfig** C:\Users>**ipconfig**

Displays TCP/IP network configuration information for each network adapter (both physical and virtual) on the device.

---

## Navigation Commands

---

<b>ping</b>	Sends IP packets to check network connectivity: C:\Users> <b>ping cisco.com</b> (reply follows) Pinging cisco.com [2001:420:1101:1::185] with 32 bytes of data: Reply from 2001:420:1101:1::185: time=64ms Reply from 2001:420:1101:1::185: time=65ms Reply from 2001:420:1101:1::185: time=65ms Reply from 2001:420:1101:1::185: time=69ms  Ping statistics for 2001:420:1101:1::185: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 64ms, Maximum = 69ms, Average = 65ms
<b>hostname</b>	Returns the computer name of the local device. C:\Users> <b>hostname</b> PC of RMcD
<b>netstat</b>	Displays a list of active TCP connections on a local network. C:\Users> <b>netstat</b>  Active Connections Protocol Local Address   Foreign Address   State TCP 10.0.0.34:49554   12.64.180.116:https ESTABLISHED (example output. Several lines omitted here)
<b>nslookup</b>	Gathers the network's Domain Name System (DNS) information. C:\Users> <b>nslookup</b> Default Server: cdns01.ISPprovider.net Address: 2101:568:feed::1
<b>chkdsk*</b>	Scans the specified drive for errors and repairs them. C:\Windows> <b>chkdsk</b> ( <i>Note: Run as Administrator</i> )  The type of the file system is NTFS. WARNING! /F parameter not specified. Running CHDKSK in read-only mode. Stage 1: Examining basic file system structure ... 895232 file records processed. File verification completed.
<b>net user</b>	Manages user accounts (add, remove, change). C:\Users> <b>net user</b>  User accounts for \\PC-RMcD admin       Administrator    ctctechs DefaultAccount The command completed successfully.
<b>net use</b>	Connects to shared folders, similar to mapping a network drive. C:\Users> <b>net use</b>

---

---

<b>Navigation Commands</b>	
	New connections will be remembered. There are no entries in the list.
<b>tracert</b>	Similar to ping, but returns path information to an IP address destination. Similar to the traceroute command in macOS and Linux. Can be used for troubleshooting connectivity across the Web.  C:\Users> <b>tracert Cisco.com</b>  Tracing route to cisco.com [2001:420:1101:1::185]  over a maximum of 30 hops: 1 5 ms 2601:602:cc01:16e0:623d:26ff:feb9:8830 2 13 ms 12 ms 12 ms 2001:558:4082:c6::1 3 12 ms 13 ms 13 ms 2001:558:a2:601b::1 (20 hops in <i>output omitted</i> )
<b>format</b>	(Note: Do not practice this command on an operational computer!)  Creates or re-creates the specified file system on recordable or rewritable storage (magnetic, flash, or optical media) and overwrites the contents and file table of the drive.
<b>xcopy</b>	Copies one or more files and folders to another folder or drive.  C:\Users> <b>XCOPY source [destination] [/A  </b> For format and function table, type: C:\Users> <b>help xcopy</b>
<b>copy</b>	Copies one or more files to another folder or drive.
<b>robocopy</b>	Robust File Copy for Windows. Copies or moves files/folders; can be configured with various optional GUIs.  Usage :: <b>ROBOCOPY</b> source destination [file [file]...] [options] source :: Source Directory (drive:\path or \\server\share\path). destination :: Destination Dir (drive:\path or \\server\share\path). file :: File(s) to copy (names/wildcards: default is "*.*"). For options table, use : C:\Users> <b>help robocopy</b>
<b>gpupdate</b>	Refreshes Group Policy on local or Active Directory systems. C:\Users> <b>gpupdate</b> Updating policy...
<b>gpresult</b>	Displays the resultant set of policy for the specified computer and user. For the usage guide, type: C:\Users> <b>gpresult /?</b>
<b>shutdown</b>	(Note: Do not practice this command on an operational computer!) Shuts down the computer. For usage, enter: C:\Users> <b>shutdown /?</b>
<b>sfc*</b>	Scans system files and replaces damaged or missing files. C:\Windows> <b>sfc /scannow</b> ( <i>run as administrator</i> )  Beginning system scan. This process will take some time. Beginning verification phase of system scan. Verification 4% complete.

---

<b>Navigation Commands</b>	
[command name]/?	Displays help for the specified command name—for example, <b>xcopy /?</b> .
<b>diskpart*</b>	(Note: Do not practice this command on an operational computer!) Creates, removes, and manages disk partitions.
<b>pathping</b>	Similar to <b>traceroute</b> but provides information on network latency along the path to the destination. <b>pathping</b> traces and tests network connections to an IP address. C:\Users> <b>pathping cisco.com</b>
<b>taskkill</b>	Stops specified task(s) on a local or remote computer. C:\Users> <b>TASKKILL /IM notepad.exe</b>
<b>winver</b>	Returns version information of the current Windows OS. C:\Users> <b>winver</b>

**Table 6-6** Internet Properties Dialog Tabs

<b>Tab</b>	<b>Function</b>
General	Set the home page; set tab settings; delete browsing history, cookies, temporary files, and saved passwords; change appearance; and configure accessibility settings
Security	Configure security zones
Privacy	Select privacy settings for the current zone, location settings, pop-up blocker, and InPrivate browsing settings
Content	Set options for family safety, SSL certificate management, AutoComplete, and feeds
Connections	Set options for VPNs, dial-up, LAN connections, and proxy servers
Programs	Select the default web browser, manage add-ons, select the default HTML editor, and set the default apps for email and other Internet services
Advanced	Enable and disable accelerated graphics; configure accessibility settings, browsing settings, HTTP settings, international settings, multimedia settings, and security settings; and reset Internet Explorer to the default settings

**Table 6-8** File System Format Comparison

<b>System Type</b>	<b>Full Name</b>	<b>Details</b>
exFAT	Extended File Allocation Table	Microsoft file system used for flash drives larger than 32GB and files larger than 4GB.
FAT32	File Allocation Table	Format for USB flash drives that hold files smaller than 4GB, game consoles, and so on. Works with all operating systems.
NTFS	New Technology File System	Windows default formatting for hard drives. Supports sharing and journaling.
APFS	Apple File System	Apple file system of macOS that is designed to enhance performance with solid state drives (SSD) and flash storage. It is available on macOS 10.13 and higher.
NFS	Network File System	Open source system that works independently of the operating system, allowing network user access. It appears local but is a common network drive.

<b>System Type</b>	<b>Full Name</b>	<b>Details</b>
ext3	Third Extended File System	Linux version of NTFS. Allows journaling of changes, to minimize damage if a crash occurs. Supports a maximum of 32,000 subdirectories.
ext4	Fourth Extended File System	Linux system. Supports larger file sizes than ext3. Can disable journaling. Supports a maximum of 64,000 subdirectories.

## Chapter 8

**Table 8-2** Slow/Sluggish System Performance Causes and Solutions

### Windows System Performance Troubleshooting

<b>Problem</b>	<b>Solution</b>
System is not configured for maximum performance	To solve this problem, set the Power setting to High Performance using the Power options icon in the notification area or the Power options in the Control Panel. This option is not available on tablets.
Drive containing paging file and temporary files is nearly full or badly fragmented	Use Disk Cleanup in the drive properties to remove unwanted files, check the drive for errors, and defragment the drive. If you have more available space on a different drive, use the Advanced tab in the system properties to change the location of the paging file and temp files.
System is overheating and CPU is running at reduced speed	Remove dust and dirt on the CPU and system fans. Check for adequate airflow through the system. Change back to the Balanced power setting.
Memory is running low	Add RAM; this fixes many performance problems. For better performance, exceed the minimums recommended for the version of Windows in use.
Sudden performance drop occurs	Check for viruses and malware; this is especially important if performance has suddenly plunged.
Registry error messages appear	The program CCleaner is widely used for this task.

**Table 8-3** Common Symptoms of PC Security Issues

<b>Symptom</b>	<b>Possible Causes</b>
No access to the network	Internet connectivity problems that do not affect all computers and devices on the network could be caused by malware. Run troubleshooters to repair the problem. If the problem continues to occur, scan the systems.
Desktop alerts	The Notifications and Quick Actions center is easily accessed on the taskbar next to the time and date. Notifications can be edited by going to <b>Settings &gt; System &gt; Notifications and Actions</b> . Options include connectivity, VPN, network, and settings notifications, as well as notifications from apps. OS updates also can be sent here. A regular check of the Notifications and Quick Actions center can help keep small problems from turning into big ones.
False alerts regarding	Security alerts from Windows Defender or from your OS might indicate malware infection or other problems. Sometimes alerts that pop up without any notification

Symptom	Possible Causes
antivirus protection	in Defender or the Action Center are attempts to infect your system by tricking you into clicking a phishing link in the pop-up. Scan the system.  Rogue antivirus programs look like legitimate antivirus programs but actually are designed to infect your system or phish users for personal information. Uninstall any such program and scan the computer.
Altered system or personal files	Malware infections might rename system files (such as msconfig, regedit, and taskmgr) that can help block malware.  Files can go missing or be renamed on your storage devices if they are corrupted, infected with malware, unknowingly hidden, or automatically moved by a program without user acknowledgement. Files that have actually disappeared and have not been moved or artificially hidden can often be recovered with undeletion software that scans the hard drive for files that are no longer recorded in the file allocation table, the storage device data that tracks where files start and end. Undeleted malware-infected files can reinfect a system if they are not properly cleaned before use.
Unwanted notifications within the OS	Notifications can be easily managed in Windows 10 by going to <b>Settings &gt; System &gt; Notifications &amp; Actions</b> . From this page, you can customize notifications and alerts from Windows and from individual apps that are installed.
OS update failures	A common reason OS updates fail is lack of disk space. Make sure ample free disk space is available; some updates can be quite large.  Also make sure that automatic updates are not blocked by antivirus protection settings.

**Table 8-4** Browser-Related Symptoms

Symptom	Possible Causes
Random or frequent pop-ups	If the browser has pop-up blocking enabled but pop-ups are still showing up, the system might be infected with malware. If many pop-ups are displayed onscreen rapidly and they keep showing up even as they are closed, the system is almost certainly infected and needs to be scanned immediately.
Certificate warnings	Operating systems and browsers use digital certificates to determine the valid sources of apps and drivers. Certificates that have been obtained fraudulently from a certificate authority can be used to launch malware attacks.
Browser redirection	Browser redirection, also known as browser hijacking, takes place when the home page setting for your browser is changed without your permission. Some free apps offer to change your browser home page during installation, but you can opt in or opt out of the change. If an app changes your browser home page without notifying you, it could be malware. Scan the system.

**Table 8-5** Common Symptoms of Mobile OS and Application Issues

Symptom	Troubleshooting Step(s)
App fails to launch	Delete the app and reinstall it.
App fails to close or crashes	Delete the app and reinstall it. Force-stop the app (methods vary by phone or device). Clear the app's cache and data (Settings menu).

Symptom	Troubleshooting Step(s)
App fails to update	If the app pauses during the update, a file might have been corrupted in transit. Delete the app and repeat the download and install procedures.
App is slow to respond	If rebooting does not fix this problem, check the available storage and delete old or unused data. When a phone nears storage capacity, it can lag.
OS fails to update	This is likely a storage issue. Check for space, and make enough room for the update to download and launch.
Battery life issues arise	<p>Many features that run in the background can limit the battery life of a phone or device. For example:</p> <ul style="list-style-type: none"> <li>▪ Make use of battery optimizing information and settings such as Low Power Mode.</li> <li>▪ Reduce the brightness of the screen.</li> <li>▪ Identify apps that use more power, and manage them.</li> <li>▪ Turn off alert sounds and vibrations.</li> <li>▪ Charge the phone or device before it runs out of power. One strategy is to occasionally run the battery down to 10–15 percent capacity and then charge it fully.</li> </ul>
Phone or device randomly reboots	Close any apps not in use. Determine whether an installed app is the problem by restarting in Safe Mode, removing the most recent app, and then restarting. If problem persists, repeat for other recent apps.
Screen does not autorotate	<p>Access the control center (with an iPhone, swipe down from the upper-right corner; on an Android device, swipe down from the top). Tap the rotation lock icon to toggle the setting.</p> <p>Also check the Display settings and make sure the display is Standard and not Zoomed; the zoom can prevent the screen from rotating.</p>

## Connectivity Issues

Symptom	Troubleshooting Step(s)
Bluetooth	For both iPhone and Android, the most common solution is to “forget” the device that is failing to pair from the cache.
Wi-Fi	<p>Check that signal strength is good. Sometimes walking away from a strong signal activates cellular data and drops the Wi-Fi connection.</p> <p>Verify the networks and authentication.</p> <p>Be aware that crowds at large events can overwhelm Wi-Fi (and cell) data systems.</p>
Near-field communication (NFC)	<p>Make sure NFC is enabled in the Control Center (for iPhone models up to 11—in subsequent models, NFC is always on and no setting is available).</p> <p>NFC is good for only a few inches. To connect, be sure that the reader and the phone are nearly touching.</p>
AirDrop	<p><i>For iPhone/iPad:</i></p> <p>Make sure the receiving device is both compatible and discoverable.</p> <p>AirDrop works only when the receiving device is turned on and its screen is awake.</p>

Symptom	Troubleshooting Step(s)
	AirDrop uses Bluetooth and Wi-Fi; make sure they are enabled. Check that Airplane mode is off.

## Chapter 9

**Table 9-4** Electrical Conditions and Protective Measures

Type of Electrical Condition	Description	Protective Measure
Power surge	Overshoot event lasting less than 50ms. Up to 6000V and 3000A.	Surge suppressor
Under-voltage event	Sustained voltage drop of up to half the normal voltage. Can last for minutes to hours.	UPS
Power failure	Total loss of power for an extended period of time.	UPS or generator

**Table 9-5** Basic Scripting Languages

Extension	Language	Basic Information
.bat	Windows batch file	Batch files are script files that are strictly Windows based. They are text files that contain commands or instructions for the command-line interpreter to execute. The instructions in a batch file can be interpreted only by the Windows operating system.
.ps1	PowerShell	Windows PowerShell is a tool to help technicians and network administrators automate support functions through the use of scripts and snippets. Windows 10 and 11 ship with PowerShell.
.vbs	VBScript	VBScript, a scripting language developed by Microsoft, is considered a subset of the Visual Basic programming language. It was designed specifically for use with Microsoft Internet Explorer. It gives web pages a level of interactivity.
.sh	Linux shell script	A shell script is a text file that contains a sequence of commands for a Linux- or UNIX-based system. Shell scripts might not run correctly on a Windows system. Linux has had several shells; BASH (Bourne-Again Shell) is the most common of them.
.py	Python	Python is often a good choice for those beginning to learn programming. It is relatively easy to learn, and Python scripts can run on most operating systems. For example, Windows Shell is known as Python Interactive Shell.
.js	JavaScript	JavaScript is a programming language that has many uses today. It is valuable for creating scripts because it can be run on any operating system. It is usually written into web pages to create client interactions; JavaScript is read by the browser. Creating and running command-line JavaScript requires installing Node.js.

# Appendix E. Study Planner

Practice Test	Reading	Task			
Element	Task	Goal Date	First Date Completed	Second Date Completed (Optional)	Notes
<b>Core 1 (220-1101) Chapters</b>					
1. Mobile Devices	Read Foundation Topics				
1. Mobile Devices	Review Key Topics				
1. Mobile Devices	Define Key Terms				
1. Mobile Devices	Complete all memory tables in this chapter using <a href="#">Appendix C</a>				

Practice Test	Take practice test in study mode in practice test software for this chapter				
2. Networking	Read Foundation Topics				
2. Networking	Review Key Topics				
2. Networking	Define Key Terms				
2. Networking	Complete all memory tables in this chapter using <a href="#">Appendix C</a>				
Practice Test	Take practice test in study mode in practice test				

	software for this chapter				
3. Hardware	Read Foundation Topics				
3. Hardware	Review Key Topics				
3. Hardware	Define Key Terms				
3. Hardware	Complete all memory tables in this chapter using <a href="#">Appendix C</a>				
Practice Test	Take practice test in study mode in practice test software for this chapter				
4. Virtualization and Cloud Computing	Read Foundation Topics				

4. Virtualization and Cloud Computing	Review Key Topics				
4. Virtualization and Cloud Computing	Define Key Terms				
4. Virtualization and Cloud Computing	Complete all memory tables in this chapter using <a href="#">Appendix C</a>				
Practice Test	Take practice test in study mode in practice test software for this chapter				
5. Hardware and Network Troubleshooting	Read Foundation Topics				
5. Hardware and Network Troubleshooting	Review Key Topics				
5. Hardware and Network	Define Key Terms				

Troubleshooting					
5. Hardware and Network Troubleshooting	Complete all memory tables in this chapter using <a href="#">Appendix C</a>				
Practice Test	Take practice test in study mode in practice test software for this chapter				
Practice Test	Take practice test in study mode for Core 1 exam in practice test software for this chapter				
<b>Core 2 (220-1102)</b>					

<b>Chapters</b>					
6. Operating Systems	Read Foundation Topics				
6. Operating Systems	Review Key Topics				
6. Operating Systems	Define Key Terms				
6. Operating Systems	Complete all memory tables in this chapter using <a href="#">Appendix C</a>				
Practice Test	Take practice test in study mode in practice test software for this chapter				
7. Security	Read Foundation Topics				
7. Security	Review Key Topics				

7. Security	Define Key Terms				
7. Security	Complete all memory tables in this chapter using <a href="#">Appendix C</a>				
Practice Test	Take practice test in study mode in practice test software for this chapter				
8. Software Troubleshooting	Read Foundation Topics				
8. Software Troubleshooting	Review Key Topics				
8. Software Troubleshooting	Define Key Terms				
8. Software Troubleshooting	Complete all memory tables in this				

	chapter using <a href="#">Appendix C</a>				
Practice Test	Take practice test in study mode in practice test software for this chapter				
9. Operational Procedures	Read Foundation Topics				
9. Operational Procedures	Review Key Topics				
9. Operational Procedures	Define Key Terms				
9. Operational Procedures	Complete all memory tables in this chapter using <a href="#">Appendix C</a>				
Practice Test	Take practice test in				

	study mode in practice test software for this chapter				
Practice Test	Take practice test in study mode for Core 2 exam in practice test software for this chapter				
Final Review	Review all Key Topics in all chapters				
Final Review	Review all Key Terms in all chapters or using the Key Terms Flashcards on the companion website				

Final Review	Complete all memory tables for all chapters in <a href="#">Appendix C</a>				
Final Review	Take practice test in practice exam mode using Exam Bank #1 questions for all Core 1 chapters				
Final Review	Take practice test in practice exam mode using Exam Bank #2 questions for all Core 2 chapters				

# CompTIA® A+ **Core 1 (220-1101) and Core 2 (220-1102) Cert Guide**

ISBN: 978-0-13-767594-4

**See inside ▶ ▶ ▶**

**for your Pearson Test Prep activation code and special offers**

## **Complete Video Course**

To enhance your preparation, Pearson IT Certification also sells Complete Video Courses for both streaming and download. Complete Video Courses provide you with hours of expert-level instruction mapped directly to exam objectives.

## **Special Offer—Save 70%**

This single-use coupon code will allow you to purchase a Complete Video Course at a **70% discount**. Simply go to the product URL below, add the Complete Video Course to your cart, and apply the coupon code at checkout.

**[www.pearsonITcertification.com/videostore](http://www.pearsonITcertification.com/videostore)**

Coupon Code:

# CompTIA® A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide

## Premium Edition eBook and Practice Test

To enhance your preparation, Pearson IT Certification also sells a digital Premium Edition of this book. The Premium Edition provides you with three eBook files (PDF, EPUB, and Kindle) as well as an enhanced edition of the Pearson Test Prep practice test software. The Premium Edition includes four additional practice exams with links for every question mapped to the PDF eBook.

## Special Offer—Save 80%

This single-use coupon code will allow you to purchase a copy of the Premium Edition at an **80% discount**. Simply go to the URL below, add the Premium Edition to your cart, and apply the coupon code at checkout.

[www.pearsonITcertification.com/title/9780137675869](http://www.pearsonITcertification.com/title/9780137675869)

Coupon Code:

## DO NOT DISCARD THIS NUMBER

You will need this activation code to activate your practice test in the Pearson Test Prep practice test software.

To access the online version, go to [www.PearsonTestPrep.com](http://www.PearsonTestPrep.com). Select **Pearson IT Certification** as your product group. Enter your email/password for your account. If you don't have an account on PearsonITCertification.com or CiscoPress.com, you will need to establish one by going to PearsonITCertification.com/join. In the My Products tab, click the **Activate New Product** button. Enter the access code printed on this insert card to activate your product. The product will now be listed in your My Products page.

If you wish to use the Windows desktop offline version of the application, simply register your book at [www.pearsonITcertification.com/register](http://www.pearsonITcertification.com/register), select the **Registered Products** tab on your account page, click the **Access Bonus Content** link, and download and install the software from the companion website.

This activation code can be used to register your exam in both the online and the offline versions.

Activation Code:



Pearson

## Where are the companion content files?

Register this digital version of CompTIA® A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide to access important downloads.

Register this eBook to unlock the companion files. Follow these steps:

1. Go to [pearsonITcertification.com/account](https://pearsonITcertification.com/account) and log in or create a new account.
2. Enter the ISBN: **9780137675944** (NOTE: Please enter the print book ISBN provided to register the eBook you purchased.)
3. Answer the challenge question as proof of purchase.
4. Click on the "Access Bonus Content" link in the Registered Products section of your account page, to be taken to the page where your downloadable content is available.

This eBook version of the print title does not contain the practice test software that accompanies the print book.

You May Also Like—Premium Edition eBook and Practice Test. To learn about the Premium Edition eBook and Practice Test series, visit [pearsonITcertification.com/practicetest](http://pearsonITcertification.com/practicetest)

---

The Professional and Personal Technology Brands of Pearson



Cisco Press

informIT

PEARSON IT Certification

QUE'

SAMS

# Special Offer

## Save 80% on Premium Edition eBook and Practice Test

The *CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide Premium Edition eBook and Practice Test* provides three eBook files (PDF, EPUB, and Kindle) to read on your preferred device and an enhanced edition of the Pearson Test Prep practice test software. You also receive four additional practice exams with links for every question mapped to the PDF eBook.

**See the card insert in the back of the book for your Pearson Test Prep activation code and special offers.**

CompTIA®

# A+ Core 1 (220-1101) and Core 2 (220-1102) Cert Guide Companion Website

---

Access interactive study tools on this book's companion website, including practice test software, a Key Term flash card application, study planner, and more!

To access the companion website, simply follow these steps:

- 1.** 1. Go to [www.pearsonITcertification.com/register](http://www.pearsonITcertification.com/register).
- 2.** Enter the print book ISBN: **9780137675944**.
- 3.** Answer the security question to validate your purchase.
- 4.** Go to your account page.
- 5.** Click on the **Registered Products tab**.
- 6.** Under the book listing, click on the Access Bonus Content link.

If you have any issues accessing the companion website, you can contact our support team by going to <http://pearsonitp.echelp.org>.

# Code Snippets

Many titles include programming code or configuration examples. To optimize the presentation of these elements, view the eBook in single-column, landscape mode and adjust the font size to the smallest setting. In addition to presenting code and configurations in the reflowable text format, we have included images of the code that mimic the presentation found in the print book; therefore, where the reflowable format may compromise the presentation of the code listing, you will see a “Click here to view code image” link. Click the link to view the print-fidelity code image. To return to the previous page viewed, click the Back button on your device or app.

```
Wireless LAN adapter Wireless Network Connection:  
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::5cf1:2f98:7351:b3a3%12  
IPv4 Address. . . . . . . . . . . : 192.168.1.155  
Subnet Mask . . . . . . . . . . . : 255.255.255.0  
Default Gateway . . . . . . . . . . : 192.168.1.1
```

The type of the file system is NTFS.  
Cannot lock current drive.  
Chkdsk cannot run because the volume is in use by another  
process. Would you like to schedule this volume to be  
checked the next time the system restarts? (Y/N)

```
Bcdedit /export C:\BCD_Backup  
ren c:\boot\bcd bcd.old  
Bootrec /rebuildbcd
```