Save 10% on Exam Voucher
See Inside

EXAM CRAM

CompTIA® A+®

Core 1 (220-1201)
Core 2 (220-1202)

Flash Cards

Cram Sheet

Practice Tests

DAVID BAYNE
MARK SMITH
JOHN PICKARD

Save 10% on Exam Voucher

See Inside

EXAM CRAM

CompTIA®

A+®

Core 1 (220-1201)

Core 2 (220-1202)



Flash Cards


Cram
Sheet
Practice
Tests
DAVID BAYNE
MARK SMITH
JOHN PICKARD

About This eBook

ePUB is an open, industry-standard format for eBooks. However, support of ePUB and its many features varies across reading devices and applications. Use your device or app settings to customize the presentation to your liking. Settings that you can customize often include font, font size, single or double column, landscape or portrait mode, and figures that you can click or tap to enlarge. For additional information about the settings and features on your reading device or app, visit the device manufacturer's Web site.

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.

CompTIA A+ Core 1 (220-1201) and Core 2 (220-1202) Exam Cram

Companion Website and Pearson Test Prep Access Code

Access interactive study tools on this book's companion website, including practice test software, review exercises, Key Term flash card application, a study planner, and more!

To access the companion website, simply follow these steps by December 31, 2028:

1. Go to **www.pearsonitcertification.com/register**.
2. Enter the **print book ISBN**: 9780135446904.
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.

When you register your book, your Pearson Test Prep practice test access code will automatically be populated with the book listing under the Registered Products tab. You will need this code to access the practice test that comes with this book. You can redeem the code at **PearsonTestPrep.com**. Simply choose Pearson IT Certification as your product group and log into the site with the same credentials you used to register your book. Click the **Activate New Product** button and enter the access code. More detailed instructions on how to redeem your access code for both the online and desktop versions can be found on the companion website.

If you have any issues accessing the companion website or obtaining your Pearson Test Prep practice test access code, you can contact our support

team by going to **informit.com/support**.

Exam ✓ Cram

CompTIA® A+® Core 1 (220-1201) and Core 2 (220-1202)

David Bayne, John Pickard, and Mark Smith



CompTIA® A+® Core 1 (220-1201) and Core 2 (220-1202) Exam Cram

Copyright © 2026 by Pearson Education, Inc.

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit https://www.pearson.com/global-permission-granting.html.

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: 978-0-13-544690-4

ISBN-10: 0-13-544690-2

Library of Congress Control Number: 2025937679

$PrintCode

Trademarks

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

Microsoft and/or its respective suppliers make no representations about the suitability of the information contained in the documents and related graphics published as part of the services for any purpose. All such documents and related graphics are provided “as is” without warranty of any kind. Microsoft and/or its respective suppliers hereby disclaim all

warranties and conditions with regard to this information, including all warranties and conditions of merchantability, whether express, implied or statutory, fitness for a particular purpose, title and non-infringement. In no event shall Microsoft and/or its respective suppliers be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of information available from the services.

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

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

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

Director, ITP Product Management
Julie Phifer

Executive Editor
Nancy Davis

Sponsoring Editor
Malobika Chakraborty

Development Editor
Christopher A. Cleveland

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Chuck Hutchinson

Indexer
Timothy Wright

Proofreader
Jennifer Hinchliffe

Technical Editor
Chris Crayton

Cover Designer
Chuti Prasertsith

Compositor
codeMantra

Contents at a Glance

Introduction

Part I: Introduction to Core 1 (220-1201)

Core 1 (220-1201) Domain 1.0: Mobile Devices

CHAPTER 1 Monitoring, Maintaining, and Replacing Mobile Device Hardware

CHAPTER 2 Mobile Device Accessories and Connectivity Options

CHAPTER 3 Mobile Device Network Connectivity and Application Support

Core 1 (220-1201) Domain 2.0: Networking

CHAPTER 4 TCP and UDP Ports and Protocols

CHAPTER 5 Wireless Technologies

CHAPTER 6 Networked Hosts

CHAPTER 7 Network Configuration Concepts

CHAPTER 8 Network Devices

CHAPTER 9 SOHO Network Configuration

CHAPTER 10 Network Types

CHAPTER 11 Networking Tools

Core 1 (220-1201) Domain 3.0: Hardware

CHAPTER 12 Device Display Components

CHAPTER 13 Cables and Connectors

CHAPTER 14 RAM

CHAPTER 15 Storage Drives

CHAPTER 16 Motherboards and Add-on Cards

CHAPTER 17 CPUs

CHAPTER 18 Power

CHAPTER 19 Multifunction Devices/Printers

CHAPTER 20 Printer Maintenance

Core 1 (220-1201) Domain 4.0: Virtualization and Cloud Computing

CHAPTER 21 Virtualization Concepts

CHAPTER 22 Cloud Computing Concepts

Core 1 (220-1201) Domain 5.0: Hardware and Network Troubleshooting

CHAPTER 23 Troubleshooting Motherboards, CPUs, RAM, and Power

CHAPTER 24 Troubleshooting Storage Drives and RAID Arrays

CHAPTER 25 Troubleshooting Video Issues

CHAPTER 26 Troubleshooting Mobile Devices

CHAPTER 27 Troubleshooting Wired and Wireless Network Problems

CHAPTER 28 Troubleshooting Printers

A+ Core 1 (220-1201) Practice Exam

Part II: Introduction to Core 2 (220-1202)

Core 2 (220-1202) Domain 1.0: Operating Systems

CHAPTER 29 Common Operating Systems

CHAPTER 30 Operating System Installations and Upgrades

CHAPTER 31 Basic Features of Windows Editions

CHAPTER 32 Microsoft Operating System Features and Tools, Part I

CHAPTER 33 Microsoft Operating System Features and Tools, Part II

CHAPTER 34 Microsoft Command-Line Tools, Part I

CHAPTER 35 Microsoft Command-Line Tools, Part II

CHAPTER 36 Windows Control Panel Utilities

CHAPTER 37 Windows Settings

CHAPTER 38 Windows Networking

CHAPTER 39 macOS

CHAPTER 40 Linux

CHAPTER 41 Application Installation and Configuration Concepts

CHAPTER 42 Cloud-Based Productivity Tools

Core 2 (220-1202) Domain 2.0: Security

CHAPTER 43 Physical Security

CHAPTER 44 Logical Security

CHAPTER 45 Windows Security Settings

CHAPTER 46 Wireless Security and Malware

CHAPTER 47 Social Engineering, Threats, and Vulnerabilities

CHAPTER 48 Workstation Best Practices

CHAPTER 49 Mobile Device Security

CHAPTER 50 Data Destruction and Disposal

CHAPTER 51 SOHO Security

CHAPTER 52 Browser Security

Core 2 (220-1202) Domain 3.0: Software Troubleshooting

CHAPTER 53 Troubleshooting Microsoft Windows

CHAPTER 54 Troubleshooting Mobile Operating Systems and Applications

CHAPTER 55 Troubleshooting Mobile Operating Systems' Security Issues

CHAPTER 56 Troubleshooting PC Security Issues

Core 2 (220-1202) Domain 4.0: Operational Procedures

CHAPTER 57 Documentation

CHAPTER 58 Change Management and Backup Methods

CHAPTER 59 Safety Procedures

CHAPTER 60 Environmental Controls

CHAPTER 61 Incident Response, Communication, and Professionalism

CHAPTER 62 Basic Scripting, Part I

CHAPTER 63 Basic Scripting, Part II

CHAPTER 64 Remote Access Technologies

CHAPTER 65 Appropriate Use of Artificial Intelligence

CHAPTER 66 Getting Ready for the Exams, and Farewell

A+ Core 2 (220-1202) Practice Exam

Index

Table of Contents

Introduction

Part I: Introduction to Core 1 (220-1201)

Core 1 (220-1201) Domains
Core 1 (220-1201) Checklist

Core 1 (220-1201) Domain 1.0: Mobile Devices

CHAPTER 1: **Monitoring, Maintaining, and Replacing Mobile Device Hardware**

Introduction to Laptops
Power
Keyboards/Keys
Special Function Keys
Troubleshooting Keyboards
Touchpad
Random-Access Memory (RAM)
Storage Drives
Communications
Camera/Webcam and Microphone
Wi-Fi Antenna Connector and Placement
Physical Privacy and Security Components

CHAPTER 2: **Mobile Device Accessories and Connectivity Options**

Connection Types
Wired Connections

Wireless Connections
Accessories
Docking Stations and Port Replicators
Drawing Pads, Trackpads, and Touch Pens

CHAPTER 3: **Mobile Device Network Connectivity and Application Support**

Enabling Wireless Functions
Bluetooth
Email Configuration
Integrated Commercial Provider Email Configuration
Corporate and ISP Email Configuration
Cellular Radio Technologies
Location Services
GPS
Cellular Location
IMEI and IMSI
Synchronization Methods
Synchronizing to the Cloud
Synchronizing to the Desktop
Synchronizing to the Car
Mobile Device Management (MDM)

Core 1 (220-1201) Domain 2.0: Networking

CHAPTER 4: **TCP and UDP Ports and Protocols**

TCP vs. UDP
Ports and Protocols
HTTP vs. HTTPS
Email Protocols
FTP, SSH, and Telnet
DHCP

DNS
LDAP
RDP
More Protocols and Ports

CHAPTER 5: **Wireless Technologies**

802.11 Wireless
Long-Range Fixed Wireless
RFID

CHAPTER 6: **Networked Hosts**

Server Roles
File Servers/Fileshare
Web Servers
Print Servers
Mail Servers
Database Servers
Proxy Servers
DHCP Servers
DNS Servers
Syslog Servers
Network Time Protocol
AAA Servers
Internet Security Appliances
Network Firewall
UTM
Spam Gateways
Load Balancers
Embedded Systems and IoT
Embedded Systems
IoT

CHAPTER 7: **Network Configuration Concepts**

DNS
Email Authentication Methods
DHCP
DHCP Process
DHCP Exclusions
DHCP Reservations
VLANs
VPNs

CHAPTER 8: **Network Devices**
Switches
Routers
Access Points
Firewalls
Network Interface Cards
Patch Panels
Power over Ethernet
Cable/DSL Modems
Network Interface Devices

CHAPTER 9: **SOHO Network Configuration**
Configuring IPv4
Private vs. Public Addresses
Configuring IPv6

CHAPTER 10: **Network Types**
Network Types
LAN and WAN
MAN
SAN
WLAN
WMN

PAN
Internet Connection Types
Cable Internet
DSL
Fiber
Satellite
Wireless Internet Service Provider
Cellular

CHAPTER 11: **Networking Tools**
Network Cabling Tools
Network Tap
Wi-Fi Analyzers

Core 1 (220-1201) Domain 3.0: Hardware

CHAPTER 12: **Device Display Components**
Display Types
Inverter and Backlight
Damaged Inverter
Worn-Out Backlight
Digitizers and Touchscreens
Attributes

CHAPTER 13: **Cables and Connectors**
Network Cables
Twisted Pair
Coaxial
Optical
Peripheral Cables and Connectors
USB
Lightning and Thunderbolt

Serial
Video Cables and Connectors
Storage Drive Cables and Connectors
Adapters

CHAPTER 14: **RAM**

RAM Types
DDR3
DDR4
DDR5
Installing RAM
RAM Technologies
Single-Channel vs. Multichannel Architectures
ECC vs. Non-ECC

CHAPTER 15: **Storage Drives**

SATA
Magnetic Hard Drives
Solid-State Drives
RAID
Flash
USB Flash Drives
Secure Digital Cards
Optical Drives

CHAPTER 16: **Motherboards and Add-on Cards**

Motherboard Form Factors and Connector Types
ATX
microATX
ITX
Expansion Buses
Expansion Cards

Installing Video Cards
Sound Cards
Other Expansion Cards
More Ports and Connectors
BIOS/UEFI Settings
The POST

CHAPTER 17: **CPUs**
CPU Architecture
Clock Rate
Types of CPUs
Multithreading and Multicore
Cache Memory
CPU Compatibility
Intel and AMD
Sockets
Power Consumption
Cooling Mechanisms
Heat Sinks
Thermal Paste/Pads
Fans
Liquid Cooling Systems
Installing CPUs

CHAPTER 18: **Power**
Planning Which Power Supply to Use
Types of Power Supplies and Compatibility
Wattage and Capacity Requirements
Number and Type of Power Connectors
Energy Efficiency
Modular and Redundant PSUs
Installing the Power Supply

CHAPTER 19: **Multifunction Devices/Printers**

- Setup Considerations
- Firmware
- Printer Configuration Settings
  - Basic Printer Configuration Settings
  - Sharing Printers and Managing Permissions
- Local vs. Network Printers
- Basic Printer Security

CHAPTER 20: **Printer Maintenance**

- Laser Printers
- Inkjet Printers
- Thermal Printers
- Impact Printers

Core 1 (220-1201) Domain 4.0: Virtualization and Cloud Computing

CHAPTER 21: **Virtualization Concepts**

- Purpose of Virtual Machines
- Desktop Virtualization
- Hypervisors
- Examples of Virtual Machine Software
- Virtual Machine Requirements
  - Network Requirements
  - Storage Requirements
  - Security Requirements
- Cross-Platform Virtualization
- Containers and Sandboxes
  - OS-Level Virtualization (Containers)
  - Sandboxes

CHAPTER 22: **Cloud Computing Concepts**

Introduction to Cloud Computing
Common Cloud Models
Cloud Computing Characteristics

Core 1 (220-1201) Domain 5.0: Hardware and Network Troubleshooting

CHAPTER 23: **Troubleshooting Motherboards, CPUs, RAM, and Power**

Troubleshooting Motherboards
Troubleshooting CPUs
Troubleshooting RAM
Troubleshooting Power Supply Issues
Heating and Cooling

CHAPTER 24: **Troubleshooting Storage Drives and RAID Arrays**

Preventive Maintenance and Troubleshooting of Storage Drives
Storage Drive Preventive Maintenance
Storage Drive Troubleshooting
Troubleshooting RAID Arrays

CHAPTER 25: **Troubleshooting Video Issues**

PC Video Troubleshooting
External Laptop Monitors and Projectors
External Laptop Monitors
Projectors

CHAPTER 26: **Troubleshooting Mobile Devices**

Mobile Device Display Troubleshooting
Mobile Device Overheating
More Mobile Device Troubleshooting

Disassembling Processes

CHAPTER 27: **Troubleshooting Wired and Wireless Network Problems**

Troubleshooting Common Symptoms

CHAPTER 28: **Troubleshooting Printers**

Troubleshooting Printers
Print Jobs and the Print Spooler
Managing Printers and Print Jobs
Using the Windows Print Spooler

A+ Core 1 (220-1201) Practice Exam

Part II: Introduction to Core 2 (220-1202)

Core 2 (220-1202) Domains
Core 2 (220-1202) Checklist

Core 2 (220-1202) Domain 1.0: Operating Systems

CHAPTER 29: **Common Operating Systems**

Workstation Operating Systems
Mobile Operating Systems
Android
iOS
iPadOS
File System Types and Formatting
Windows File System Basics
Linux File System Basics
macOS File System Basics
Hard Drive Formatting Comparison
Vendor Life-Cycle Limitations
Compatibility Concerns Between Operating Systems

CHAPTER 30: **Operating System Installations and Upgrades**

- Boot Methods
- Types of Installations
- Partitioning
  - Primary and Extended Partitions and Logical Drives
  - Basic and Dynamic Drives
  - GPT vs. MBR
- More OS Installation and Upgrade Considerations

CHAPTER 31: **Basic Features of Windows Editions**

- Windows 10 Editions and Feature Differences
- Windows 11 Editions and Feature Differences
- Windows Desktop/User Interface and Components
- Windows Upgrade Paths
- Windows 11
- Windows N
- Windows 10 End of Support

CHAPTER 32: **Microsoft Operating System Features and Tools, Part I**

- Task Manager
- The MMC and Administrative Windows Tools
  - The MMC
  - Event Viewer
  - Task Scheduler
  - Device Manager
  - Certificate Manager
  - Local Users and Groups
  - Performance Monitor
  - Group Policy Editor and Local Security Policy

Services
Bonus Tool: Computer Management

CHAPTER 33: **Microsoft Operating System Features and Tools, Part II**

Disk Management
The Disk Management Utility
Mount Points and Mounting a Drive
Disk Cleanup
Optimize Drives/Disk Defragmenter
Additional Windows Tools
System Information/msinfo32
Resource Monitor
System Configuration/MSConfig
The Windows Registry Editor

CHAPTER 34: **Microsoft Command-Line Tools, Part I**

Microsoft Command-Line Basics
Command Prompt
PowerShell
Windows Terminal
Ask for Help!
Navigating in the Command Line
Working with Folders/Directories and Files
Partitioning and File System–Based Commands
chkdsk and sfc
chkdsk
sfc
winver
Advanced Commands: gpupdate and gpresult

CHAPTER 35: **Microsoft Command-Line Tools, Part II**

Networking Commands

ipconfig
ping
tracert and pathping
hostname
netstat
nslookup
net
whoami

CHAPTER 36: **Windows Control Panel Utilities**
Opening and Viewing the Control Panel Utilities
Internet Options
Devices and Printers
Programs and Features
Microsoft Defender Firewall
Mail
Sound
User Accounts
Indexing Options
File Explorer Options
Power Management
Ease of Access Center
Bonus: Storage Sense

CHAPTER 37: **Windows Settings**
How to Access Windows Settings
Internet Options
Network & Internet
Bluetooth & Devices
Apps
System
About

Sound
For Developers
Power & Battery
Accessibility
Time & Language
Windows Update & Security
Windows Update
Privacy & Security
Personalization
Gaming
Accounts
Control Panel Operations
System and Security
Device Manager

CHAPTER 38: **Windows Networking**
Domain Joined vs. Workgroup Setup
Sharing Resources and Making Network Connections
Printer Sharing and Access
How to Establish Networking Connections
Proxy Settings

CHAPTER 39: **macOS**
macOS Basics
System Preferences
macOS Features
iCloud and Continuity
macOS System Folders
Managing and Maintaining macOS
Installation and Uninstallation of Applications
Apple ID

CHAPTER 40: **Linux**

- Linux Basics
- Linux Desktop Distributions
- Linux Partition Scheme and File System
- Linux Command Line
- Recovery Mode
- Common Configuration Files
- Linux Best Practices
  - Updates and Patches
  - OS Components
  - Root Account
  - Linux Permissions
  - In Closing

CHAPTER 41: **Application Installation and Configuration Concepts**

- 32-Bit vs. 64-Bit
- System and OS Requirements for Applications
  - Scenario 1: Video Editing Program
  - Scenario 2: Developer Program
- Distribution Methods
- Other Considerations for New Applications
  - Application Impact
  - User Permissions
  - Security Considerations

CHAPTER 42: **Cloud-Based Productivity Tools**

- Email Systems
- Online Storage
- Collaboration Tools
  - Videoconferencing
  - Instant Messaging

Spreadsheets
Presentation Tools
Word Processing Tools
Identity Synchronization
Licensing Assignment

Core 2 (220-1202) Domain 2.0: Security

CHAPTER 43: **Physical Security**
Physical Locks
Entry Systems
Biometrics
Other Physical Security Precautions
Protecting Data Physically

CHAPTER 44: **Logical Security**
Authentication
Just-in-Time Access
Principle of Least Privilege
MDM Policies
More Logical Security Concepts
Authenticator Applications
Hard Tokens vs. Soft Tokens
Access Control Lists
SAML and Single Sign-On (SSO)
IAM and DLP
SMS
Email Security

CHAPTER 45: **Windows Security Settings**
The CIA of Computer Security
Microsoft Defender Antivirus

Microsoft Defender Firewall
Users and Groups
Permissions
Permission Inheritance and Propagation
Moving and Copying Folders and Files
File Security
Administrative Shares
Encrypting File System
BitLocker Encryption
Active Directory
User Profiles
Logon Script
Home Folder
Group Policy
Security Groups

CHAPTER 46: **Wireless Security and Malware**

Comparing and Contrasting Wireless Security Protocols and Authentication Methods
Wireless and Encryption Protocols
RADIUS and TACACS+
Kerberos
Detecting, Removing, and Preventing Malware Using the Appropriate Tools and Methods
Malicious Software Types
Preventing Malicious Software

CHAPTER 47: **Social Engineering, Threats, and Vulnerabilities**

Social Engineering
Phishing
Shoulder Surfing
Piggybacking/Tailgating

Dumpster Diving
Impersonation
Threats and Vulnerabilities
Network-Based Attacks
Password Cracking
Evil Twin
Additional Security Threats
Vulnerabilities and Security Best Practices

CHAPTER 48: **Workstation Best Practices**
Usernames and Passwords
Password Vaults/Managers
BIOS/UEFI Passwords
Password Policies
Account Management and End-User Best Practices
Disabling Unused Services
Disabling AutoPlay/AutoRun

CHAPTER 49: **Mobile Device Security**
Hardening Techniques
Screen Locks
Authenticator Applications
Theft and Loss of Mobile Devices
Compromised and Damaged Devices
Backups
Updates
Antivirus/Antimalware/Firewalls
MDM and MAM
Full Device Encryption
IoT Security
Policies and Procedures
Profile Security Requirements

CHAPTER 50: **Data Destruction and Disposal**

- Data Security 101
- Formatting Drives
- Overwriting Drives
- Physical Destruction
- Regulatory and Environmental Requirements

CHAPTER 51: **SOHO Security**

- Removing SOHO Malware
- Applying Security Settings on SOHO Wireless and Wired Networks
  - Changing Default Passwords
  - Using Wireless-Specific Security Settings
  - Enabling MAC Filtering and IP Filtering
  - Assigning Static IP Addresses
  - Adjusting Firewall Settings and Additional Configurations
  - Using Content Filtering/Parental Controls
  - Disabling Physical Ports and More Physical Security
  - A Final Word on SOHO Routers

CHAPTER 52: **Browser Security**

- Browser Download/Installation
- Settings
- Extensions and Plug-ins
- Password Managers
- Secure Connections
  - TLS
  - Secure Sites and Tracking
- More Settings

Core 2 (220-1202) Domain 3.0: Software Troubleshooting

CHAPTER 53: **Troubleshooting Microsoft Windows**

- Windows Recovery
  - Windows Recovery Environment (Windows RE)
  - Startup Settings
- System Restore
- Improper, Spontaneous, and Frequent Shutdowns
- Blue Screen of Death (BSOD) Stop Errors
- How to Restore Windows
- Common Windows Symptoms and Solutions

CHAPTER 54: **Troubleshooting Mobile Operating Systems and Applications**

- Wireless Troubleshooting
  - Wi-Fi Troubleshooting
  - Bluetooth Troubleshooting
  - NFC Troubleshooting
- Troubleshooting and Stopping Applications
- Initiating Resets
- More Mobile Application and OS Troubleshooting
  - Updates: The Good and the Bad
  - Application Issues
  - Random Reboots
  - Poor Battery Life Issues
- Addressing Video Issues

CHAPTER 55: **Troubleshooting Mobile Operating Systems' Security Issues**

- Mobile Device Security Concerns and Symptoms

CHAPTER 56: **Troubleshooting PC Security Issues**

- Symptoms of Viruses
- Symptoms of Spyware

More Symptoms of PC Security Issues and Potential Solutions

Core 2 (220-1202) Domain 4.0: Operational Procedures

CHAPTER 57: Documentation

Types of Documents

Incident Report Documentation

Standard Operating Procedures

Custom Installation Procedure for Software

User Checklists (Onboarding and Offboarding)

Service-Level Agreements

Knowledge Base/Articles

Ticketing Systems

Elements of a Help Desk Ticket

Asset Management

CHAPTER 58: Change Management and Backup Methods

Understanding Basic Change Management Best Practices

Implementing Workstation Backup and Recovery Methods

Using Windows Backup

Backup Methods

Recovery

Backup Testing

Backup Rotation Schemes

CHAPTER 59: Safety Procedures

ESD Prevention and Equipment Grounding

Electrical Safety

Electrical Fire Safety
Physical Safety

CHAPTER 60: **Environmental Controls**

Temperature, Humidity, and Air
MSDS and Disposal
Power Devices
Surge Protectors
Uninterruptible Power Supplies

CHAPTER 61: **Incident Response, Communication, and Professionalism**

Understanding the Importance of Prohibited Content/Activity and Privacy, Licensing, and Policy Concepts
Incident Response
Licensing/DRM/EULA
NDA/MNDA
Regulated Data
AUP
Using Proper Communication Techniques and Professionalism
Communication Techniques and Professionalism

CHAPTER 62: **Basic Scripting, Part I**

Programming 101
Basic Data Types
Basic Script Constructs
Environment Variables
Comment Syntax
When to Use Scripts
Other Considerations When Using Scripts

Unintentionally Introducing Malware
Inadvertently Changing System Settings
Browser or System Crashes Due to Mishandling of Resources

CHAPTER 63: **Basic Scripting, Part II**

PowerShell and .ps1
Bash and .sh
Use Cases and Other Considerations for PowerShell and Bash
Mapping a Drive in PowerShell
Remapping a Drive
Script Security
Python and .py
JavaScript and .js
Visual Basic Script and .vbs

CHAPTER 64: **Remote Access Technologies**

Remote Desktop
Remote Assistance
Remote Desktop Connection
How to Connect with Remote Desktop
SSH
Simple Protocol for Independent Computing Environments (SPICE)
Windows Remote Management (WinRM)
More Third-Party Tools
VPN

CHAPTER 65: **Appropriate Use of Artificial Intelligence**

Application Integration
Policy and Privacy

Privacy Concerns with Productivity Tools
Appropriate Use
Limitations of AI
Bias
Hallucinations
Accuracy

CHAPTER 66: **Getting Ready for the Exams, and Farewell**

Getting Ready for the Exams
Tips for Taking the Real Exams
General Practices for Taking Exams
Smart Methods for Difficult Questions
Wrapping Up the Exam
Beyond the CompTIA A+ Certification

A+ Core 2 (220-1202) Practice Exam

The CompTIA A+ Cram Sheet

Index

About the Authors

David Bayne has spent almost 35 years teaching IT, both at the high school and community college levels, and has prepared hundreds of students for careers in IT. He currently works for the State of California as an IT specialist where he oversees technical training and special projects, and is an adjunct professor in the Business department at Woodland Community College. He holds CCNA and CompTIA A+ certifications, as well as a Master's degree in educational technology. When David is not working, he reads (mostly mysteries and sci-fi) and spends time with family. He lives near Sacramento, California, with his wife and daughters and their three cats.

John Pickard is an associate professor at East Carolina University in the College of Engineering and Technology, with more than 21 years of experience teaching information and cybersecurity technology. He also works as a subject matter expert and content developer in support of the Cisco Networking Academy.

Through his career he has held various IT certifications, including Cisco Certified Network Professional, Microsoft Certified Professional, IPv6 Forum Certified Trainer, CompTIA Network +, and CompTIA A+. John is also a Cisco Certified Academy Instructor.

John received his PhD in technology management at Indiana State University.

Mark Smith has been teaching for the past 24 years. He has been computing since 1986 when he first started with his Commodore 128. He started his IT business in 1997, which is still going strong today. Ten years ago, he started a CTE IT Pathway at the high school in his district offering Python programming, IT Essentials, CCNA 1, CCNA 2, and Red Hat Linux. In addition, he runs a top-ranking regional cybersecurity club. Additionally, he is an adjunct at a local community college in the CIS department. He also sits on the Red Hat Academy Advisory Board as well

as California State University, San Bernardino's IDT Advisory Board. Mark earned his master's in instructional design and technology and has CompTIA ITF+, CompTIA A+, CompTIA Network+, CCST: IT Support, CCST: Networking, and CCST: Cybersecurity certifications. When not working, he enjoys traveling domestically and internationally.

Acknowledgments

David Bayne:

Thanks to Chris Cleveland and Chris Crayton, our editors, who ensured that all of the content was both correct and made sense and guided us through this whole project. Thanks to Nancy Davis who got us started and to Malobika Chakraborty who finished us up as executive editor. Without them, this wouldn't have gotten off the ground as a project. For my cowriters Mark and John, it's great working with you as a team again, and I wouldn't want it any other way. And thanks to my wife for putting up with my long nights and weekends writing!

John Pickard:

I sincerely appreciate the support and mentorship I've received from colleagues at Pearson and East Carolina University throughout this endeavor. I'm especially thankful to my friends and family for all their encouragement during the many evenings and weekends dedicated to writing. I'm also grateful to our editors Chris Cleveland and Chris Crayton for helping shape the content with clarity and accuracy. Special recognition goes to Nancy Davis for initiating the project and to Malobika Chakraborty for guiding it to completion. Lastly, working once again alongside my co-authors, Mark and David, has been a true privilege.

Mark Smith:

I would also like to thank Chris Cleveland for his incredible dedication and help in getting this book published—you're amazing! Chris Crayton, thank you for your timely and helpful edits. Thank you to Nancy Davis for bringing us all in for this book, and thank you to Malobika Chakraborty for taking the reins and getting the book out! Thank you to the entire Pearson editing team and Tonya Simpson—it's great to work with you again! Another thanks goes out to my students over the past two decades. While you have been learning from me, I have been learning from you as well.

Last but not least, David and John, it's been great to get the book-writing gang back together for this book! It's been an honor to write another book with the two of you.

I would also like to make a special dedication to those around me who inspire me and push me to accomplish great feats like this. First, my incredible and talented wife, Michelle, who is an inspiration and put up with my absence many evenings and weekends while I toiled away on this book. Thank you, and I love you. Also, my three incredible children—Cheyenne, Sage, and Skyler—who are extraordinary human beings that I am so immensely proud of and love dearly. However, all three of you still don't call or visit enough. Also, my most incredible, amazing sister, Tami. You're a rock star, Tami!

About the Technical Reviewer

Chris Crayton is a technical consultant, trainer, author, and industry-leading technical editor. He has worked as a computer technology and networking instructor, information security director, network administrator, network engineer, and PC specialist. Chris has authored several print and online books on PC repair, CompTIA A+, CompTIA Security+, and Microsoft Windows. He has also served as technical editor and content contributor on numerous technical titles for several of the leading publishing companies. He holds numerous industry certifications, has been recognized with many professional and teaching awards, and has served as a state-level SkillsUSA final competition judge. Chris tech edited and contributed to this book to make it better for students and those wishing to better their lives.

We Want to Hear from You!

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

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

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

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

Email: community@informit.com

Reader Services

Register your copy of *CompTIA A+ Core 1 (220-1201) and Core 2 (220-1202) Exam Cram* for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonITcertification.com/register and log in or create an account*. Enter the product ISBN 9780135446904 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

Introduction

Welcome to the *CompTIA A+ Core 1 (220-1201) and Core 2 (220-1202) Exam Cram*. This book prepares you for the CompTIA A+ Core 1 (220-1201) and Core 2 (220-1202) certification exams. Imagine that you are at a testing center and have just been handed the passing scores for these exams. The goal of this book is to make that scenario a reality. Our names are David Bayne, John Pickard, and Mark Smith, and we are happy to have the opportunity to serve you in this endeavor. Together, we can accomplish your goal to attain the CompTIA A+ certification.

Target Audience

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

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

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

- Attend a hands-on A+ class with a knowledgeable instructor.

- Consider purchasing the CompTIA A+ Core 1 (220-1201) and Core 2 (220-1202) Video Course, which goes into a bit more depth than this text and shows technology concepts from a hands-on perspective.

Essentially, we have written this book for three types of people: those who want a job in the IT field, those who want to keep their job in the IT field, and those who simply want a basic knowledge of computers and want to validate that knowledge. For those of you in the first group, the latest version of the CompTIA A+ certification can have a positive career impact, increasing the chances of securing a position in the IT world. It also acts as a stepping stone to more advanced certifications. For those in the second group, preparing for the exams serves to keep your skills sharp and your knowledge up to date, helping you to remain a well-sought-after technician. For those of you in the third group, the knowledge within this book can be helpful in any career path you decide to take, and it can be beneficial to just about any organization you might work for—as long as that organization uses computers!

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

About the CompTIA A+ Certification

This book covers the CompTIA A+ 220-1201 and 220-1202 exams, also known as Core 1 and Core 2, respectively. To obtain the CompTIA A+ certification, you must pass *both* exams. These exams are administered by Pearson Vue and can be taken at a local test center or online.

Passing the certification exams proves that you are an experienced problem solver and can support today's IT technologies.

Before doing anything else, we recommend that you download the official CompTIA A+ objectives from CompTIA's website. The objectives are a comprehensive bulleted list of the concepts you should know for the exams.

This book directly aligns with those objectives, and each chapter specifies the objective covered in the pages that follow.

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

About This Book

This book covers what you need to know to pass both CompTIA A+ exams. It does so in a concise way that allows you to memorize the facts quickly and efficiently.

We have organized this book into two parts, together comprising 66 chapters, all pertaining to the objectives covered on the exams. The first part of the book—Chapters 1 through 28—applies to the Core 1 (220-1201) exam. The second part of the book—Chapters 29 through 65—applies to the Core 2 (220-1202) exam. At the beginning of each of those parts, you will find a handy checklist you can use as you prepare for the exams. Chapter 66 discusses how to get ready for the real exams and gives some tips and techniques for passing the exams.

For this edition of the book, we decided to organize the content based on the order of the official CompTIA objectives. Typically, you will find one objective per chapter. Less commonly, a chapter will cover two objectives, and in a couple of instances, an objective will stretch across two chapters. The corresponding CompTIA objective or objectives are listed verbatim at the beginning of each chapter. Organizing the book this way enables you to easily locate whatever objective you want to learn more about. In addition, you can use the index to quickly find the concepts you are after.

Regardless of your experience level, we don't recommend skipping content. This book is designed to be read completely. The best way to study is to read the entire book. Then, go back and review the 220-1201 portion and take the real CompTIA 220-1201 exam. Afterward, review the 220-1202 portion and take that exam. The two exams are inextricably linked. It's a good idea to get the whole picture first and then break it down by the exam.

While this might not be possible based on time constraints, we still strongly recommend it as the best study method.

Note

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

Chapter Format and Conventions

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

- **Opening topics list:** This defines the CompTIA A+ objective(s) to be covered in the chapter.
- **Topical coverage:** The heart of the chapter, this text explains the topics from a hands-on and a theory-based standpoint. The text includes in-depth descriptions, tables, and figures geared to build your knowledge so that you can pass the exams.
- **Cram Quiz questions:** At the end of each chapter is a quiz. The quizzes, and ensuing explanations, are meant to help you gauge your knowledge of the subjects you have just studied. If the answers to the questions don't come readily to you, consider reviewing individual topics or the entire chapter. In addition to being in the chapters, you can find the Cram Quiz questions at the book's companion web page, at www.pearsonitcertification.com. The questions are separated into their respective 220-1201 and 220-1202 categories for easier studying when you approach each exam.
- **Exam Alerts, Sidebars, and Notes:** These are interspersed throughout the book. Watch out for them!

ExamAlert

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

- **Challenges:** We've also added skill challenges that are designed to build your hands-on skills for the IT field. Note that these challenges are optional, but we strongly suggest that you attempt them if you have the time.

Additional Elements

Beyond the chapters, there are a few more elements that we've thrown in for you:

- **Practice exams:** These are located at the end of Part I and Part II. There is one practice exam for each CompTIA A+ exam. These practice exams (and additional exams) are available as part of the custom practice test engine at the companion web page also. They are designed to prepare you for the multiple-choice questions that you will find on the real CompTIA A+ exams.
- **Real-world scenarios:** These are located on the companion web page as PDFs. They describe actual situations with questions that you must answer and potential solutions with supporting videos and simulations. These scenarios are designed to help prepare you for the performance-based questions within the real CompTIA A+ exams.
- **Cram Sheet:** The Cram Sheet located near the end of the book is designed to jam some of the most important facts you need to know for each exam into one short section, allowing for easy memorization. It is also available in PDF format on the companion web page. If you have an e-book version, this might be located elsewhere in the e-book; run a search for the term "cram sheet," and you should be able to find it.

The Hands-On Approach

It is incredibly important that you apply what you learn in this book to real hardware and software. This is the kinesthetic approach that we have recommended for years. It works! Practice as much as you can on Windows, mobile devices, computer hardware, network devices…whatever you can get your hands on.

In this book, we give as many use cases and actual technology examples as possible, including command usage, operating system navigation, troubleshooting techniques, and so on. We also will reference our real systems along with scenarios we have really experienced throughout the text. By referencing computer technology in actual scenarios, we hope to infuse some real-world knowledge and to solidify the concepts you need to learn for the exams. This hands-on approach can help you to visualize concepts better. We recommend that every computer technician build their own computer at some point (if you haven't already). This can help to reinforce the ideas and concepts expressed in the book.

You should also work with multiple operating systems while going through this book: primarily Windows but also Linux, macOS, Android, iOS, and Chrome OS. Consider dual-boots, virtual machines, and emulators to learn more about these systems. However, if at all possible, the best way to learn is to run individual computers. This will ensure that you discover as much as possible about the hardware and software of each computer system and how they interact with each other.

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

Goals for This Book

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

Our first goal is to help you understand A+ topics and concepts quickly and efficiently. To do this, we try to get right to the facts necessary for the exam. To drive these facts home, the book incorporates figures, tables, real-world scenarios, and simple, to-the-point explanations. Also, in the introductions

for the Core 1 and Core 2 sections, you will find preparation checklists that give you an orderly step-by-step approach to taking the exams. Be sure to complete all items on the checklists! For students of ours who truly complete every item, there is an extremely high passing rate. Finally, in Chapter 66, you will find some important test-taking tips that we've developed over the years.

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

Our final goal is to provide support for this and all our titles, completing the life cycle of learning. We do this through our website (https://greencurtaintraining.com), which provides additional resources for you, including an errata page (which you should check as soon as possible) and is set up to take questions from you about this book. We'll try our best to get to your questions ASAP. All personal information is kept strictly confidential.

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

Sincerely,

David Bayne

John Pickard

Mark Smith

https://greencurtaintraining.com

Figure Credits

Figures 3-1 through Figure 3-4, Figure 49-1, Figure 49-2, Figure 54-1, Figure 54-2 © 2025 Google Inc

Figure 11-2 © 2025 Wifi Analyzer

Figure 21-3 © 2005-2025 Broadcom

Figure 21-4 © 2025 Oracle

Figure 24-1 © Intel Corporation

Figure 39-1, Figure 39-2 © 2025 Apple Inc.

Figure 40-1 © 2025 Canonical Ltd.

Figure 57-1 © 2023 Yuba Community College District

Figure 4-2, Figure 9-1, Figure 9-2, Figure 14-4, Figure 16-5, Figure 21-1, Figure 21-2, Figure 24-2, Figures 28-1 through 28-3, Figure 29-1, Figures 30-1 through 30-3, Figures 31-1 through 31-3, Figures 32-1 through 32-9, Figures 33-1 through 33-7, Figure 34-2, Figures 36-1 through 36-3, Figures 37-1 through 37-9, Figures 38-1 through 38-6, Figures 42-1 through 42-3, Figures 45-1 through 45-8, Figure 46-1, Figure 46-2, Figures 48-1 through 48-3, Figures 51-1 through 51-3, Figures 53-1 through 53-4, Figure 58-1, Figure 58-2, Figure 63-1, Figure 64-1, Figure 64-2 © 2025 Microsoft Corporation

Part I

Introduction to Core 1 (220-1201)

Welcome to the Core 1 (220-1201) section of this book. This portion of the CompTIA A+ certification focuses on computers such as laptops, smartphones, tablets, and PCs; computer networking; virtualization and cloud computing; and troubleshooting of hardware and networks. That's a great deal of things to know, but you can do this. Take it slow, study hard, and stay positive. Do these things, and you will succeed.

The Core 1 content of this book comprises Chapters 1 through 28. For the most part, we've written the content to match the order of the objectives. This way, you can follow along with the official CompTIA A+ objectives and mark them up as you wish while you progress through the book. After Chapter 28, you will find a practice exam that is designed to test your knowledge of the 220-1201 objectives.

Core 1 (220-1201) Domains

The CompTIA A+ Core 1 exam objectives are broken down into five domains:

- 1.0—Mobile Devices
- 2.0—Networking
- 3.0—Hardware
- 4.0—Virtualization and Cloud Computing
- 5.0—Hardware and Network Troubleshooting

After this introduction, we'll address these objectives in order, starting with Chapter 1, "Monitoring, Maintaining, and Replacing Mobile Device Hardware." Be sure to study each of the domains! To do this properly, we suggest that you get your hands on as much technology gear as you can: PCs, laptops, mobile devices, printers, SOHO routers, and so on. Work with as much of this technology as possible so that you can learn how the hardware and devices really work. Then apply that knowledge to the objectives and the content in this book.

Core 1 (220-1201) Checklist

You must be fully prepared for the exam, so we created a checklist that you can use to make sure you are covering all the bases as you study. Take a look at the following table and make sure you check off each item before attempting the 220-1201 exam. Historically, our readers and students have benefited greatly from this type of checklist. Use the table as a guide for ordering your studies. We suggest you bookmark this page and refer back to it as you complete each item.

Exam Preparation Checklist

Step	Item	Details	220-1201 Status
1.	Read the Core 1 (220-1201) content.	Thoroughly read Chapters 1 through 28.	
2.	Review the Exam Alerts.	The little boxes with Exam Alerts are interspersed throughout the book. Review them and make sure you understand every one.	
3.	Review the Cram Quizzes.	Cram Quizzes are categorized by exam. You can review them in the text or on the companion website.*	

Step	Item	Details	220-1201 Status
4.	Complete the practice exam in the book.	Directly after Chapter 28 is a 220-1201 practice exam. Your goal should be to get at least 90 percent correct on the exam on the first try. (100 percent would be preferable!) If you score less than 90 percent, go back and study more!	
5.	Study the Core 1 Real-World Scenarios.	These can be found on the companion website. Complete them by reading and answering the scenarios and questions within the PDFs and accessing the corresponding videos and simulations.	
6.	Create your own cheat sheet.	Although there is a Cram Sheet at the beginning of this book, you should also create your own. The act of writing down important details helps commit them to memory. Keep in mind that you will not be allowed to take your own cheat sheet or the Cram Sheet into the actual testing room.	
7.	Register for the exam.	Do not register until you have completed the previous steps; you shouldn't register until you are fully prepared. When you are ready, schedule the exam to commence within a couple of days so that you won't forget what you have learned! Registration can be done online. Register at Pearson VUE (https://home.pearsonvue.com). It accepts payment by major credit cards for the exam fee. You need to create an account to sign up for exams.	
8.	Read the test-taking tips.	You can find these tips in the last chapter of the book and on the companion website.	

Step	Item	Details	220-1201 Status
9.	Study the Cram Sheet and cheat sheet.	The Cram Sheet is a fold-out at the beginning of this book. It is also on the companion website. Study from the Core 1 portion of the Cram Sheet and your cheat sheet during the last 24 hours before the exam. (If your exam is delayed for any reason, go back to step 3 and retake the Cram Quizzes and practice exam 24 hours prior to your test date.)	
10.	Take the exam!	When you pass, place that final check mark in the box! Good luck!	

* Some electronic editions of this book do not have access to the practice test software.

ExamAlert

Do not register for the exam until you are thoroughly prepared. Meticulously complete items 1 through 6 in the checklist before you register.

Note

Remember: It's not mandatory, but we recommend going through the entire book (Core 1 and Core 2). Then, return to the Core 1 portion and review it carefully, going through the steps in the checklist. Although this approach takes more time, it is a proven method that we have used with CompTIA A+ exams since the turn of the millennium!

Core 1 (220-1201)

Domain 1.0: Mobile Devices

CHAPTER 1 Monitoring, Maintaining, and Replacing Mobile Device Hardware

CHAPTER 2 Mobile Device Accessories and Connectivity Options

CHAPTER 3 Mobile Device Network Connectivity and Application Support

Chapter 1

Monitoring, Maintaining, and Replacing Mobile Device Hardware

This chapter covers the following A+ 220-1201 exam objective:

- **1.1** – Given a scenario, monitor mobile device hardware and use appropriate replacement techniques.

Welcome to the first chapter of this book! In this chapter, we focus on laptop hardware only. Software will be covered later in the book. The core of this chapter deals with laptop hardware and device replacement. By that we mean laptop power and batteries, keyboards, memory, storage drives, and so on. You might come into contact with laptops old and new that need to be repaired and/or upgraded. Finally, be sure to know how other components are installed that might be located in the display area of a laptop—for instance, webcams, microphones, and Wi-Fi antennas.

This chapter addresses many of those scenarios. Let's get to it.

ExamAlert

Objective 1.1 focuses on the following concepts: battery, keyboard/keys, random-access memory (RAM), hard disk drives (HDDs)/solid-state drives (SDDs), wireless cards, physical privacy and security components (including biometrics and near-field

scanner features), Wi-Fi antenna connector/placement, camera/webcam, and microphone.

Note

Don't forget, a complete list of the Core 1 (220-1201) objectives can be found on the companion website for this book (see the Introduction for details) and on CompTIA's website: https://www.comptia.org/certifications/a.

Introduction to Laptops

Laptops have come a long way over the years—from the Osborne 1 in 1981 to the slick, slim devices of today. The beauty of laptops is that they are portable, and all the connections are right at your fingertips. However, quite often there is a trade-off in performance and in price—that is, in comparison to PCs. This chapter assumes a basic knowledge of laptops and jumps straight into how to install and configure laptop devices.

Laptops were originally designed for niche markets but today are often used in businesses, schools, and at home. Laptops (also known as notebooks, Chromebooks, or portable computers) have integrated displays, keyboards, and pointing devices, making them easy to transport and easy to use in confined spaces. What makes them work when they are not plugged in? The battery, of course! Let's dive right in to laptop power and batteries.

Power

Laptops are designed to run on battery power, but laptops can run only several hours on these batteries. So, a laptop comes with an AC power adapter to plug into an AC outlet; this adapter should always be carried with the laptop. How many times have we heard users say they've forgotten their AC adapter! Recommend to users that they always put the AC adapter back in the laptop case—or use two: one for the workplace and one for "going mobile." Luckily, there is a shift in the marketplace for lower-powered

laptops to use USB-C. Hopefully, this will bring about a more universal power adapter across brands.

The worst-case scenario is when a laptop won't turn on! Without power, a user can't do anything. When troubleshooting power problems, envision the entire chain of power in your mind (or write it on paper)—from the AC outlet to the AC adapter to the DC jack and all the way to the power button. There are a few things you can check if it appears that a laptop is not getting any power.

- **Consult laptop manufacturer instructions:** First and foremost, always check the laptop manufacturer's instructions on how to power your laptop and explore power management features before troubleshooting.
- **Check the power LED:** Check the power light on the AC adapter. If this light is off, not only will the laptop not get power but the battery won't charge. Most laptops also have a power LED on the front of the case or just above the keyboard. If this lights up, then maybe it isn't a power problem at all. For example, the user might start the laptop, see nothing on the display, and determine that the laptop has no power—when, in reality, it is a display issue.

> **Note**
>
> Many laptops also have a storage drive and wireless LEDs, which can tell you more about the status of the laptop when you can't see anything on the screen. Use them!

- **Check connections:** Verify that the laptop is firmly connected to the AC adapter and that the AC adapter is firmly connected to the AC outlet. Sometimes a user presses the power button, expecting the laptop to start, without realizing that the battery is discharged and that the AC adapter is not connected. Also, check for damage. Inspect the DC jack that is on the side of the laptop; it is soldered onto the motherboard of the laptop. Make sure it isn't loose or damaged. Sometimes the battery charges only if the output cord of the AC adapter is held at an angle—probably because the laptop was transported while the output cord was

plugged into the laptop, causing damage to the DC jack. Also make sure that the user is attempting to connect to the actual DC jack, and not an audio port, security port, or something else. The DC jack is sometimes labeled. For example, it might show that it requires 19-V DC. This must be exact, which is covered by using the correct adapter—as explained in the following bullet.

- **Make sure the user uses the right power adapter:** Swapping power adapters between two different laptops is not recommended, but users try to do it all the time. Two different laptop models made by the same manufacturer might use what appear to be similar power adapters, with only 1 or 2 volts separating them; however, the laptop usually won't power on with that "slightly" different power adapter. Laptop AC adapters are known as fixed-input power supplies, meaning they work at a specific voltage. An adapter is not meant to be used on another model laptop. Unfortunately, a user might have plugged in the incorrect power adapter; the laptop then worked fine for 4 or 5 hours because it was actually running on battery power, but the user might not have noticed the laptop wasn't charging, even though the system should have notified the user when the battery was low (and critical). Another power adapter–related issue could be that the user is trying to work in another country. To do this, the user needs an auto-switching AC adapter, meaning that it can switch from 120 to 240 VAC automatically. Some laptops do not come with auto-switching AC adapters, but after-market versions can be purchased for many models of laptops. Remember that an additional adapter might be necessary to connect to AC outlets in foreign countries.
- **Check the battery and voltage:** This advice might sound silly, but check if the battery has been removed for some odd reason. Also, check if the battery is fully inserted into the battery compartment. There is usually a locking mechanism that should hold the battery in place. Finally, test the battery's voltage. Batteries last a finite amount of time. They can be recharged by the laptop only so many times (known as cycles) before failure. After several years, the battery won't hold a charge any longer or will lose charge quickly. In some cases, you can try discharging and recharging the battery a few times to "stimulate" it, but in most scenarios, an extremely short battery life means that the battery

must be replaced. An old or failing battery can cause the system to overheat or could cause operating system freeze-ups or slow performance. In general, lithium-ion batteries last longer when the laptop is operated and stored at the right temperature ranges. Acceptable operating range for laptops is 50 to 95°F (10 to 35°C), and acceptable storage range is –4 to 140°F (–20 to 60°C). Watch out for swollen batteries, which could be caused by age, overcharging, or manufacturer defect. If a battery is user-removable, it will often require the removal of a couple of screws. Use caution in attempting to remove it and be sure not to puncture it. Store it in a dark, cool container until you can recycle it. If it is a non-user-serviceable battery, bring/send the device to the nearest authorized repair center and, as before, keep the entire device within a cool container that light cannot get to.

- **Check whether standby, sleep/suspend, or hibernate mode has failed:** If users regularly put their laptops into standby or hibernate modes, they could encounter issues once in a while. In some cases, the power button needs to be held down for several seconds to reboot the machine out of a failed power-down state. This might have to be done with the battery removed. If either of these modes failed, check within the OS for any relevant information and possibly turn off hibernation and/or standby mode until the situation has been rectified. (On a slightly different note, sometimes laptops take a long time to come out of standby mode, and it's not necessarily an issue with standby but a case of the lid switch being stuck. It looks like a power issue, but it's a simple hardware fix.)
- **Reconnect the power button:** In rare cases, the power button might have been disconnected from the system board, or a new one may be required because the button mechanism failed. To fix this, you must open the laptop, but often the power button is easily accessible once you do so.
- **Discharge the motherboard:** Another uncommon scenario is when there is a charge stored in some capacitance somewhere in the laptop—most likely the motherboard. This can cause the laptop to fail to turn on. LEDs do not light, even when the laptop is plugged in. The problem could be due to a power surge or other irregularity, or it may be an issue with the laptop's power system. You can discharge the motherboard by

disconnecting the power, removing the battery, and then pressing and holding the power button for 30 seconds or so. This will remove any residual voltage from the motherboard and, depending on the laptop, might reset some BIOS/UEFI settings, which would have to be reconfigured later. Some people call this the *30-second trick* (although it could take less time or more), or a laptop *hard reset*, though that is not really an accurate term. What you are really doing here is discharging the motherboard, but be ready for other terms used by various technicians in the field.

- **Check the AC outlet:** Make sure the AC outlet that the user has plugged the laptop into is supplying power. A simple test would be to plug a lamp, clock, or other device into the outlet, but a more discerning and safer test would be to use a receptacle tester or circuit analyzer. For more information on testing AC outlets, see Chapter 18, "Power."

ExamAlert

Power is crucial! When troubleshooting, go through the entire power system step by step, including the power button, battery, DC jack, AC adapter, and AC outlet.

Keyboards/Keys

The keyboard is the most important input device on a laptop (or a PC). One of the great things about the keyboard is that you can use it exclusively, even if you don't have a pointing device or a touchpad available (or functional). You can do just about anything within the system with the keyboard.

Figure 1.1 shows an example of a typical laptop keyboard. Take a close look at the keyboard on your laptop and identify the various keys. Also, look for similarities and differences between the keyboard in the figure and yours. If you don't have a keyboard, go to the Internet and search for images of current laptop keyboards.



FIGURE 1.1 **A Typical Laptop Keyboard**

Special Function Keys

Some laptops have keyboards similar to the 101-key keyboard found on a PC and include a numeric keypad; these laptops are larger than most and are known as *desktop replacements*. However, most laptops are designed with a small form factor in mind, and this means a smaller keyboard. For example, the keyboard shown in Figure 1.1 has 86 keys. But, as shown in Figure 1.2, a user has the option of using the Fn key (Function key). The Fn key is a modifier key used on most laptops. It is designed to activate secondary, or *special*, functions of other keys. For example, in Figure 1.2, the F12 key has the secondary function of turning the wireless connection on or off—but only if you press the Fn key at the same time that you press the F12 key. To make it easier to read, Figure 1.2 breaks up the Fn key and

the F1–F12 function keys, so you can see each of them better. But remember that the Fn key is usually toward the lower-left corner of the keyboard, and the function keys (F1–F12) are situated at the top of the keyboard.

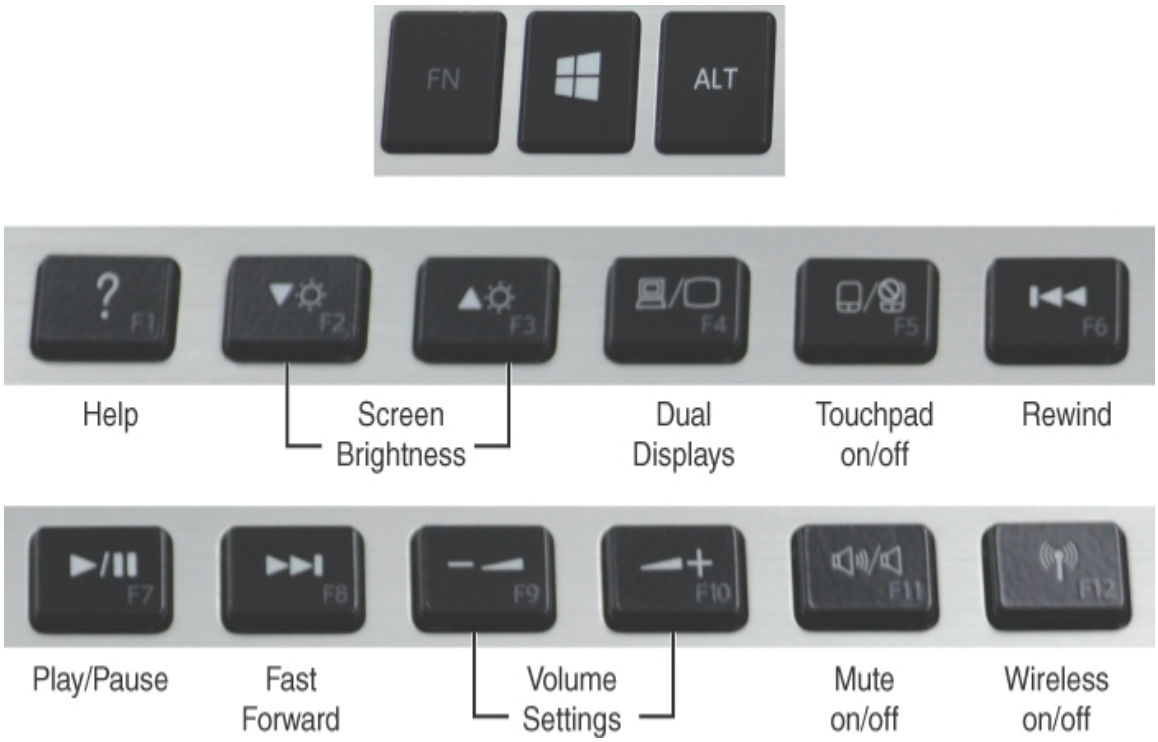


FIGURE 1.2 **Typical Function Keys and Their Tasks**

Thanks to the Fn key and the F1–F12 function keys, much more functionality can be incorporated into the keyboard without the need for additional keys. This idea has since grown to include all kinds of controls; for example, controls for using the media player (play/pause/fast forward/rewind); putting the computer to sleep; enabling wireless, the keyboard backlight, and the touchpad; adjusting screen orientation; and a variety of other functions, including enabling an external monitor. On the laptop shown in this example, the F4 key seconds as a display toggle between the built-in display and an external monitor. Take a look at Figure 1.2 and attempt to identify what each of the function key images represents.

ExamAlert

Use the Fn key in combination with the F1–F12 function keys to configure many things, including media options, Wi-Fi access, brightness, the touchpad, and an external monitor.

All this key configuration is up to the manufacturer, and any key can be given a secondary function. This secondary function enables things like the numeric keypad and the number lock key, which might be abbreviated as Num Lock, or num lk. (This could also be an individual key.) Sometimes, users forget about the Num Lock key, and when they try to type, strange garbled code comes out! The reason is that the numbers are sharing keys used by letters and symbols. Simply press the Num Lock key once to fix the problem. This issue is also common if the user works with an external keyboard at the office and disconnects it when leaving the office. However, today's operating systems and programs are pretty good at sensing things such as an enabled Num Lock or Caps Lock key.

ExamAlert

If it is available, press the Num Lock key to enable/disable the numeric keypad on a laptop. If the Num Lock indicator light is on, then the numeric key is enabled.

Troubleshooting Keyboards

We have had many people tell us that their laptop's keyboard isn't working properly. Over time we've noticed several culprits: overuse, loose ribbon cables, spilled coffee, or users simply pounding the tar out of the keyboard! It happens. The telltale signs include bent or warped keyboards and missing keycaps. Whatever the cause, here are a couple of actual problems you might encounter:

- **Stuck keys:** Sticking keys could be a result of overuse, damage to an individual key's switch, or liquid spilled on the keyboard. (If a stuck key is the worst that happens due to a liquid spill, consider yourself

lucky!) A stuck key can be identified by the key failing to work in the operating system or the BIOS/UEFI reporting an error. Use an external keyboard to troubleshoot further. By removing the keycap and cleaning the keyswitch underneath, you can usually fix the problem. If not, the entire keyboard will probably have to be replaced.

> **Note**
>
> The Basic Input/Output System (BIOS) is the underlying setup system for a laptop or PC. We'll discuss that and the Unified Extensible Firmware Interface (UEFI) more in Chapter 16, "Motherboards and Add-on Cards."

- **Loose connection:** If a laptop is moved around and jostled a lot, as many laptops are, it could possibly cause loose connections. One of these is the ribbon cable that connects the keyboard to the motherboard. To fix this issue, you must lift the keyboard away from the laptop and attach the ribbon cable securely.
- **Damaged keyboard:** Users who inadvertently drop heavy items onto the keyboard or operate the keyboard with a heavy hand might cause a warped or bent keyboard. Some brands of laptops suffer from this more than others. This issue is usually impossible to repair; the keyboard often needs to be replaced.

When replacing a keyboard, be sure to shut down the laptop, unplug it, and disconnect the battery. Then employ electrostatic discharge (ESD) prevention measures. Among other things, that means using an antistatic strap and antistatic mat. We speak more to this in Chapter 59, "Safety Procedures." You'll need a very small Phillips-head screwdriver and/or small Torx screwdriver—as low as T8 or even T6—some things to add to your computer repair toolkit!

> **Note**

ESD can occur when two objects with different voltages come into contact with each other.

Try to document the process as you go. Write down what you see and how and where cables and screws were attached. Also make note of how devices were oriented before they were removed. Label any parts that you remove for easier identification later on. Take pictures with your smartphone or another camera as you go through the disassembly process. If it is available, refer to the manufacturer's documentation that came with the laptop.

When you are done with the repair, verify that the new keyboard works by testing every key using Notepad or another text editor or word processor and by testing Fn-enabled keys as well.

If a user needs access to a laptop right away (before it can be repaired), a temporary solution would be to connect a USB or wireless keyboard. This *should* be recognized automatically by the operating system, though a BIOS/UEFI configuration might be necessary.

Touchpad

Whereas a PC uses a mouse, a laptop uses a built-in pointing device. The bulk of laptops come with a pointing device known as a touchpad. By gliding a finger across the touchpad surface, a user can move the cursor on the screen. Touchpads might also come with two buttons that take the place of a mouse's buttons. In portable computing lingo, the word *click* is replaced with the word *tap*. In addition to using the buttons, many touchpad surfaces can also be tapped or double-tapped upon, just by tapping with the finger. Touchpads can be replaced, though it is uncommon to do so; they are often connected by two cables similar to the flex cable that connects the keyboard. However, you might have to remove other devices first to get at the touchpad. You might also have to work from the bottom and from the top of the laptop; it depends on the brand of laptop.

Now and again you will encounter users reporting that when they type on the keyboard, the mouse pointer scrolls across the screen. This is sometimes referred to as a *ghost cursor*, *cursor drift*, or *pointer drift*. It could occur

because a part of the user's hand, or even the user's sleeve, is brushing against the touchpad or touchscreen. It could also be caused by paired Bluetooth devices such as an external mouse or mouse/keyboard combination, especially if the person is moving about and the external device is in a backpack. To remedy this, you can turn off pointing devices within the operating system, usually through the laptop manufacturer's software. Watch out for situations in which the entire device might have been disabled or perhaps just the pad portion of the touchpad was disabled. It can be disabled in the OS and with a function key on some laptops. It's also possible to disable the tapping capability of the touchpad while still allowing movement of the cursor. In rarer cases, a ghost cursor occurring while working in the operating system or in an application can be caused by an incorrect or bad device driver. (A device driver is a small program that controls the device and acts as a software interface between the device and the OS.) If you suspect a driver issue, then reinstall or update the mouse/touchpad driver and the video driver and update the OS as well.

Of course, external mice can be connected to a laptop or its docking station as well. These would be connected to USB ports or could be wireless devices. Chapter 2, "Mobile Device Accessories and Connectivity Options," provides more information about docking stations, port replicators, and accessories.

Random-Access Memory (RAM)

Laptops use double data rate (DDR) memory. But in laptops it's miniaturized and is known as a small outline dual inline memory module (SODIMM). Two common types of SODIMMs in laptops are DDR4 (which has 260 pins) and DDR5 (which has 262 pins). Different versions of SODIMM memory are not compatible. For example, normally you can't put a DDR5 SODIMM into a DDR4 SODIMM slot. SODIMM DDR speeds are similar to their PC equivalents. We'll discuss the different types of DDR and their speeds and data transfer rates in Chapter 14, "RAM."

ExamAlert

Know that SODIMM DDR4 has 260 pins and SODIMM DDR5 has 262 pins. Understand the pin format differences between them and standard DIMMs (used in PCs).

Random-access memory (RAM) has a center notch that helps to orient the RAM during installation. This notch will usually be in a different location depending on the SODIMM version.

Before installing any new RAM, check compatibility. Remember to consult the laptop's documentation to find out exactly how much RAM and which type of RAM the laptop will accept. When you have purchased compatible RAM, installing it to a laptop is usually quite simple. RAM is often located on the bottom of the laptop, underneath an access cover. In other laptops, it might be underneath the keyboard, or there could be one stick of RAM under the keyboard and a second (usually for add-ons) under an access cover underneath the laptop. Consult your laptop's documentation for the exact location of the RAM compartment. Table 1.1 shows the steps involved in adding RAM to a laptop. Keep in mind that SODIMMs and their corresponding memory boards are more delicate than their counterparts in a desktop computer.

TABLE 1.1 **Installing a SODIMM in a Laptop**

Step	Procedure
1. Prepare the laptop for surgery!	Shut down the laptop, unplug it, and disconnect the battery. Then employ ESD prevention measures.
2. Review your documentation.	Review your documentation to find out where RAM is located. For this step, assume that the RAM can be added to an area underneath the laptop.

Step	Procedure
3. Locate the memory.	Quite often, you will need to remove the bottom cover of the laptop. Be ready to document and store the many screws somewhere safe. Older laptops might have two screws that you need to remove to open a memory compartment door. Often, these are captive screws and will stay in the door. But if they are not, label them and store them in a safe place.
4. Remove the old RAM.	If you are upgrading, remove the current RAM by pushing both of the clips out. The RAM should pop up. If it does not, lift the RAM at a 45-degree angle. Gently remove the RAM, holding it by the edges.
5. Insert the RAM.	There could be one or two slots for RAM. One of them might already be in use. Many laptops support multichannel memory. If this is the case and you install a second memory module, the best option is to select one that is identical to the first, though that is not always necessary. Insert the memory module at a 45-degree angle into the memory slot, aligning the notch with the keyed area of the memory slot. Press the module into the slot; then press the module down toward the circuit board until it snaps into place (GENTLY!). Two clips (one on either side) lock into the notches in the side of the memory module. Press down again to make sure it is in place. See Figure 1.3 for an example of an installed SODIMM. Note the locking clips holding the memory module into place.

Step	Procedure
6. Close the laptop and then test.	Attach the cover (or compartment). You might want to wait on screwing it in until you test the laptop. Then boot the computer into the BIOS/UEFI and make sure it sees the new memory module(s). Finally, boot into the operating system, make sure that it sees the new total amount of RAM, and then verify whether applications work properly.



FIGURE 1.3 **Installed SODIMM**

Sometimes upgraded memory fails to be identified by the BIOS/UEFI. This usually means that the memory was not installed properly. Turn off the computer, reseat the RAM modules, and then reboot. This technique usually fixes the problem.

Occasionally a laptop fails to boot and emits a series of continuous beeps. This failure could be due to faulty memory. However, it could simply be that the memory contacts are dirty. As mentioned before, laptops are often mistreated and are used in a variety of environments. Pop the memory hatch

and inspect the RAM modules. If they require cleaning, use compressed air or try using a RAM cleaner. Plug the modules back in and verify functionality by rebooting the system several times. If they still don't work, try swapping out the RAM with known good modules.

Note

Some laptop manufacturers solder their RAM to the motherboard to save space. If this is the case, you will not be able to upgrade the RAM without risking serious damage to the motherboard. You will need to send the entire laptop back to the factory for repair.

Storage Drives

While RAM excels at storing data temporarily, a laptop needs something to store data permanently (that is, until it is erased). Storage drives allow for this "permanent" storage of data.

Note

Storage drives are often referred to as *hard drives*. While this term is probably not accurate for a drive being used in a laptop today, it is still a commonly used term that you should be ready for.

Storage drives *will* fail; it's just a matter of when. Laptop storage drives are even more susceptible to failure than those in desktop computers due to their mobility and the bumps and bruises that laptops regularly sustain.

Many laptops come with Serial ATA (SATA) drives, which incorporate two connectors: a 7-pin data connector and a 15-pin power connector. The bulk of the storage drives in laptops are 2.5 inches wide, though ultra-small laptops and other small portable devices might use a drive as small as 1.8 inches. See Figure 1.4 for an example of a 2.5-inch SATA solid-state drive (SSD). Note the smaller data connector and larger power connector.



FIGURE 1.4 **A Typical 2.5-Inch SSD**

SATA drives are broken down into three categories:

- **SSD:** Has no moving parts and generally uses NAND-based flash memory to store data. These are the most common storage drives today. SSDs are smaller and faster than hard disk drives (HDDs); SSDs are noiseless and allow PCs to be thinner and more lightweight.
- **Magnetic disk:** Also known as a hard disk drive (HDD), a magnetic-based drive that uses an actual mechanical disk and an arm with a read/write head to store data to the disk. They are more common in older devices.
- **Hybrid:** A hybrid drive that uses a magnetic disk as well as SSD cache memory—so it combines the capacity of a magnetic disk with the performance of an SSD.

We'll discuss the various types of storage drives in Chapter 15, "Storage Drives."

ExamAlert

Know that laptop storage drive types include SSD, magnetic disk, and hybrid. Also, be aware that they have either 2.5- or 1.8-inch form factors. In addition, M.2 form factor storage drives have become more popular in modern laptops.

One of the ways to make an older laptop run faster is to replace the storage drive. For example, if a laptop contains a SATA magnetic disk, you might opt to replace it with an SSD or perhaps a hybrid drive, or perhaps even an M.2 drive, if the laptop has an M.2-compatible slot on its motherboard. These options can offer greater data transfer rates as well as improvements in overall system efficiency. Upgrades such as these might also need to be performed if the original drive fails. At that point, you'll probably need to rescue some data from the original drive.

Note

Be careful with M.2 drives. They create a lot of heat, and in a laptop's tight environment, overheating is a possibility. That being said, many modern laptops are opting for M.2 for their quick performance and smaller footprint.

Of course, to rescue data from a drive, you must first remove it. Laptop drives can be accessed from one of three places. The first, and maybe the most common, is from the bottom; this requires removing either the entire bottom cover or an access panel. The second is from underneath the keyboard. And the third is from the side of the laptop where the drive is located, in some kind of caddy. These last two options are much less common than the first. In any of the three scenarios, some kind of rubber molding or bracket usually has to be removed or unscrewed from the drive

when replacing it. Hold on to this item for the new drive. In any case, employ antistatic measures and *use care* when working around any connections inside the laptop; they are more fragile than their PC counterparts.

Communications

Communicating quickly and efficiently with other computers and wireless devices is key in business and home environments. To do so, laptops use a variety of different devices, including the following:

- **Wired and wireless networking:** Most laptops today come equipped with wired Ethernet and Wi-Fi to connect to a local area network (LAN) or a wireless local area network (WLAN). The wired connection has an RJ-45 port and can typically transfer data at 1000 Mbps or greater, auto-negotiating its speed to the network it is connected to. Wireless networking connections are made with an internal Mini PCIe card that can potentially connect to 802.11a, b, g, n, ac, ax, and be networks. It is also possible to connect wired or wireless network adapters to USB ports. There is often a WLAN button (or Wi-Fi button) that can enable/disable a laptop's built-in wireless adapter. It usually shares a function key. Keep this in mind when troubleshooting. If this adapter is disabled, the laptop cannot connect wirelessly, even if the device is enabled in the operating system. Many laptops use proprietary software for the configuration of wireless network connections instead of using the built-in Windows WLAN AutoConfig service. In some cases, it might be easier to disable the proprietary application and use Windows instead.

> **ExamAlert**
>
> If a laptop can't connect to a wireless network, try pressing the Wi-Fi button—either a button associated with a function key or a standalone button near the keyboard.

- **Bluetooth:** Bluetooth modules enable a laptop to connect to other Bluetooth devices, such as headsets and phones, over short distances, thus joining or creating a personal area network (PAN). A Bluetooth module might be included inside the laptop as an individual card or as a combo Bluetooth/WLAN card. External USB and remote controls are also available. For more information on Bluetooth, see Chapter 3, "Mobile Device Network Connectivity and Application Support." Many laptops come with WLAN and Bluetooth capabilities; however, the two technologies can possibly compete over frequencies. If the WLAN connection runs at 2.4 GHz, you might need to recommend that a user make use of only one technology at a time, if possible. Function keys or individual buttons are often available on a laptop for enabling/disabling Wi-Fi and Bluetooth. If not, it can be done within the operating system (for example, in the Notification Area in Windows).
- **Cellular:** Wireless wide area network (WWAN) cellular connections can be made in a variety of ways. Some laptops are designed with built-in Mini PCIe or M.2 cellular modules. Some telecommunications providers offer cellular connections via USB-based devices as well.

Laptop wireless cards can be added to laptops or upgraded if needed. You will find combination cards that offer Wi-Fi and Bluetooth. These often use the M.2 form factor. Such a card has one antenna for each technology. After employing antistatic methods and opening the laptop, you'll find that the M.2 card is connected with a single screw. The connector edge of the card will often have two divots—showing you how it should be oriented. After installation, be sure to use insulating tape to cover the antenna leads and to wrap around the antenna wires if they come into close contact with any power wires/connections. Finally, route the wires carefully. Often, they will terminate in the laptop's hinge or similar endpoint.

If there is no option for upgrade, meaning there is no M.2 slot for wireless, then a laptop can still access Wi-Fi and Bluetooth by way of an external, low-profile mini-USB device.

ExamAlert

Know the various ways that a laptop could communicate with other computers, including wired and wireless Ethernet, Bluetooth, and cellular WAN connections.

Camera/Webcam and Microphone

Most webcams have a built in camera, microphone, and speaker. Camera/webcams are great for communication, but sometimes they fail, and in some cases they are considered security vulnerabilities. In the event that a webcam has to be replaced, or just removed altogether, you can follow a few simple steps. First, employ antistatic measures. Then, remove the bezel from the display. The camera/webcam module should then be visible above the display screen. Often, it is just connected with a small plug and no screws or attachment of any kind. Next, *carefully* disconnect it with your shim or other thin prying tool (non-metal), place it in an antistatic bag, and label the bag for later use. Hold on to any tape or sticky material that keeps the webcam in place. Next, replace it with an identical part. Be very careful when connecting the power for the new webcam; the plug is often delicate. Use (or reuse) tape to fasten the webcam in the right spot (if necessary). Then, attach the bezel to the display once again. Finally, test the camera/webcam's video and audio with an application such as the built-in Windows Camera program.

Some people use tape to cover their webcams for security or privacy purposes, but depending on the policies of your organization, this solution might not be enough, and you will have to remove webcams altogether. Some companies offer filler items to fill the gap where the camera lens normally goes.

A laptop might have a function key that can disable the camera/webcam. It can also be disabled in the operating system, so be sure to check those options before replacing a webcam.

The microphone on a laptop is often part of the camera/webcam module (for example, to the left of the lens). In such a case, removing the webcam module removes the microphone. The microphone could also be disabled in the operating system. For example, in Windows, you would do this in the

Recording tab of the Sound dialog box. As mentioned, some people use tape to cover their webcams, and they also use tape to cover the microphone openings; however, depending on the type of tape, it might muffle the recorded sound but not eliminate it. Once again, for security purposes, you might need to disable the webcam altogether or remove it.

ExamAlert

Know where to find the camera/webcam and microphone within a laptop display and know how to disable them.

Some companies opt to disable webcams (and associated microphones) and instead use external USB-based webcams to achieve better security as well as better performance so that the users can physically disconnect webcams when they are not in use.

Here are some things you can try if your webcam isn't working:

- **Check the connection:** Make sure the webcam is fully inserted into a USB port on your computer. You can also try plugging it into a different USB port.
- **Update drivers:** You can update your webcam's drivers in Device Manager:

  1. Open Device Manager.
  2. Find your webcam in the list of devices.
  3. Right-click your camera and select **Update Driver Software**.
  4. Follow the instructions, and select **Search Automatically for Updated Driver Software**.
  5. Restart your computer to complete the installation.

Wi-Fi Antenna Connector and Placement

A Wi-Fi antenna is used to connect to a wireless network, also known as a wireless local area network (WLAN). Wi-Fi antennas can be found inside a laptop as well as externally. If an antenna is inside the laptop, it is usually some type of module—either an M.2 card (as shown in Figure 1.5) or a PCI Express Mini Card (also known as a Mini PCIe card).



FIGURE 1.5 **A Typical Internal Wi-Fi Module Using the M.2 Form Factor**

ExamAlert

Be able to identify M.2 and Mini PCIe cards by name and by sight.

Usually, this module can be identified quickly by removing the bottom cover of the laptop. It is connected to a slot and is attached with either one screw (for M.2) or two screws (for Mini PCIe). M.2-based cards have up to 67 pins and might use the 2230 standard (22×30 mm) or the 1216 standard (12×16 mm), among others. The one in Figure 1.5 uses the 2230 standard. Full-size Mini PCIe cards are 30×50.95 mm and use a 52-pin edge connector.

Be careful when installing an M.2 or Mini PCIe card; the contacts can be easily damaged. Place even pressure on both sides and press the card into the slot evenly so it goes in straight, without any side-to-side movement. If a Wi-Fi antenna cable already exists in the laptop, reuse it by connecting the wire ends to the contacts on the card. Usually, there are two: one for Wi-Fi and one for Bluetooth (BT). If there is no antenna, install a new one and route it through the laptop hinge and around the display as far as it can go. The longer the antenna, the better the reception.

Of course, external Wi-Fi adapters can be used, connecting to USB or an RJ-45 port. With external adapters, antennas (if there are any) can be pointed in the direction that you desire. However, it is important to note that the signal coming out of those antennas comes out in a perpendicular, umbrella-like wave. Therefore, it is often useful to point your antenna vertically for single-story homes or horizontally or angled for multistoried homes to help the signal travel upward. Or, the adapter can be moved from a USB port on one side of the laptop to a USB port on the other side. Just remember to consider using USB 3.0 or higher; blue ports or better. Also, keep the module away from any sources of interference. If it has actual antennas that you can move, first attempt a 90-degree angle, and if that doesn’t work, experiment! However, many external Wi-Fi modules that connect via USB are small, self-contained devices with the antenna embedded inside. So, the choice of USB port is really your only option in that scenario when it comes to antenna placement.

Wi-Fi transmissions rely on the IEEE 802.11 standards, including 802.11be, ax, ac, n, g, and b (listed here from fastest to slowest).

Every Wi-Fi adapter has its own unique media access control (MAC) address, also known as a MAC ID. This identification number is usually printed on a sticker on the Wi-Fi adapter, and it is programmed into the ROM of the adapter. It differentiates the Wi-Fi adapter from all other network adapters on your network and around the world. Regardless of the type of network adapter, the MAC address is a 48-bit number, described using hexadecimal numbering (for example, 68-05-CA-2D-A4-B3). The number is also referred to as a physical address in the Windows command-line interface. If you have an internal Wi-Fi adapter, you can find out the MAC address in Windows by typing **ipconfig /all** in the Command Prompt or the PowerShell. (In macOS or Linux, you can use **ip a** or **ifconfig**.) We'll discuss the MAC address more in Chapter 8, "Network Devices."

Physical Privacy and Security Components

A laptop can be secured through the use of cable locks, biometrics, and by disabling NFC. Let's briefly discuss each of those.

One way to physically secure a laptop is to use a cable lock. This lock works in a similar fashion to a bicycle theft prevention lock. It consists of a very strong cable that is difficult to cut through—often galvanized, multistranded steel—with a lock on one end and a loop on the other. This allows the user to secure the laptop in a variety of ways, such as to a table, desk, and so on. Some companies incorporate metal loops or eye bolts near workstations to use with the cable lock for increased security. The lock itself will often adhere to lock-picking protection standards and is usually a tubular cam lock. Many laptops come with a security slot to be used with cable locks; the tubular lock is inserted into the slot and turned 90 degrees to lock it or unlock it. This, of course, is only one anti-theft solution for laptops, but it is one that is commonly used by organizations, corporations, and individuals.

Biometrics is the science of identifying human beings based on their physical characteristics, such as a thumbprint, retina scan, voice pattern, or facial recognition. A USB-based biometric reader can be connected to a laptop, which then requires an additional form of identification from the user before the user can log in—for instance, a thumbprint. This requirement secures the laptop further through what is known as multifactor

authentication (MFA); the user must provide a thumbprint, as well as a username and password to gain access to the computer. For more information on biometrics, see Chapters 43, "Physical Security," and 44, "Logical Security."

ExamAlert

Know that multifactor authentication requires users to verify their identity using two or more authentication factors such as password and fingerprint. MFA increases security by adding an extra layer of protection if one factor is compromised.

Near-field communication (NFC) is a technology that allows two mobile devices to "beam" information to each other wirelessly if they are in close proximity. It has gained in popularity for use with smartphones and electronic payment systems. A device such as a laptop that is equipped with NFC will employ near-field scanning techniques in order to communicate with other NFC-enabled devices. Because NFC is a two-way, short-range communications technology, it opens the door for an attacker to attempt to gain access to the laptop's data with a third-party app/scanner. If NFC is deemed too great a security risk (and for many organizations it is), then it can be individually disabled in the operating system's settings, or you could set the laptop to operate in airplane mode to turn off all wireless transmissions. See Chapter 2 for more information about NFC.

Here are some ways to secure NFC transactions:

- **Encryption:** Use encryption protocols like Transport Layer Security (TLS) to keep data secure.
- **Update regularly:** Keep your device's software up to date to fix vulnerabilities.
- **Use security software:** Use a reputable security software to detect and block threats.
- **Use tokenization:** Many NFC payment systems use tokenization to maintain security.

- **Use device authentication:** Many devices require authentication to complete an NFC payment.
- **Set transaction limits:** Some banks limit NFC transactions to reduce the risk of fraud.

ExamAlert

Turning on airplane mode will disable wireless transmissions such as NFC; however, it can also disable your ability to connect to Wi-Fi or send/receive calls. Remember this for troubleshooting purposes!

Note

Know that you can increase the security for your laptop, but there is never a 100 percent secure solution because any security technique can be bypassed given time, persistence, and ingenuity. So, for example, a cable lock can help, but don't rely solely on that—or on any other single security precaution.

Wrap-up of Chapter 1

That wraps up this first chapter. We recommend you review the ExamAlerts and any notes that you have taken before you continue to the Cram Quiz. Do this for the rest of the book as well.

What follows is your first cram quiz. This will help to reinforce the concepts you have learned. Good luck!

Cram Quiz

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

1. What is the module format for a stick of SODIMM DDR4 RAM?

- **A.** 1.8-inch
- **B.** 262-pin
- **C.** 260-pin
- **D.** 2.5-inch

2. You just added a second memory module to a laptop. However, after you reboot the system, the OS reports the same amount of memory as before. What should you do next?

- **A.** Replace both memory modules.
- **B.** Run Windows Update.
- **C.** Replace the motherboard.
- **D.** Reseat the laptop memory.

3. Which of the following are ways that a laptop can communicate with other computers? (Select all that apply.)

- **A.** Bluetooth
- **B.** WLAN
- **C.** DC jack
- **D.** Cellular WAN

4. Which of the following are possible reasons that a laptop's keyboard might fail completely? (Select the two best answers.)

- **A.** A key is stuck.
- **B.** A ribbon cable is disconnected.
- **C.** The user spilled coffee on the laptop.
- **D.** The keyboard was disabled in the Device Manager.

5. A user doesn't see anything on his laptop's screen. He tries to use AC power and thinks that the laptop is not receiving any. Which of

the following are two possible reasons for this? (Select the two best answers.)

- ○ **A.** He is using an incorrect AC adapter.
- ○ **B.** The AC adapter is not connected to the laptop.
- ○ **C.** Windows won't boot.
- ○ **D.** The battery is dead.

6. One of your customers reports that she walked away from her laptop for 30 minutes, and when she returned, the display was very dim. She increased the brightness setting and moved the mouse but to no effect. What should you do first?

- ○ **A.** Replace the LCD screen.
- ○ **B.** Check the operating system for corruption.
- ○ **C.** Connect an external monitor to verify that the video card works.
- ○ **D.** Check whether the laptop is now on battery power.

7. You are helping a customer with a laptop issue. The customer says that two days ago the laptop was accidentally dropped while it was charging. You observe that the laptop will not turn on and that it is connected to the correct power adapter. Which of the following is the most likely cause?

- ○ **A.** The battery
- ○ **B.** The power adapter
- ○ **C.** The storage drive
- ○ **D.** The DC jack
- ○ **E.** The BIOS/UEFI

8. You want to reduce the risk of your laptop being stolen. Which of the following is the best option?

- ○ **A.** Incorporate biometrics

- ○ **B.** Disable NFC
- ○ **C.** Use a cable lock
- ○ **D.** Enable MFA

9. A user cannot make contactless payments using NFC, connect to the Internet, or send/receive calls from a mobile device. The user is able to boot the device and sign on. Which of the following is most likely the cause of the problem?

- ○ **A.** Failed power-down state
- ○ **B.** Airplane mode
- ○ **C.** Biometric authentication
- ○ **D.** ESD has occurred

10. Which of the following allows you to access a WLAN?

- ○ **A.** LED
- ○ **B.** Webcam
- ○ **C.** Digitizer
- ○ **D.** Stylus
- ○ **E.** Wi-Fi card

11. You have been tasked with replacing a Wi-Fi/Bluetooth card in a laptop. You open the laptop and find a card that uses the 2230 standard. What type of card is this?

- ○ **A.** Mini PCI
- ○ **B.** M.2
- ○ **C.** Digitizer
- ○ **D.** RJ-45

12. What would you most likely need to do to replace a Wi-Fi card antenna cable in a laptop?

- **A.** Remove the current module by pushing both of the clips out.
- **B.** Insert the new module at a 45-degree angle into the slot.
- **C.** Press down again to make sure the module is in place.
- **D.** Open the display to replace the cable.

13. Which of the following are storage drive form factors for laptops? (Choose three.)
    - **A.** 2.5
    - **B.** 1.8
    - **C.** M.2
    - **D.** SODIMM

Cram Quiz Answers

1. **C.** DDR4 SODIMM modules have 260 pins. DDR5 is 262-pin. 1.8-inch is the size associated with smaller storage drives used in some laptops. 2.5-inch is the standard size for SSD storage drives.

2. **D.** The next step you should take is to reseat the memory. SODIMMs can be a bit tricky to install. They must be firmly installed, but you don't want to press too hard and damage any components. If the laptop worked fine before the upgrade, you shouldn't have to replace the modules or the motherboard. Windows Update will not find additional RAM.

3. **A, B, and D.** Some of the methods that laptops use to communicate with other computers include Bluetooth, WLAN, and cellular WAN wireless connections, plus wired connections like Ethernet (RJ-45) and, for older laptops, dial-up (RJ-11). The DC jack is the input on the laptop that accepts power from the AC adapter.

4. **B and C.** A laptop's keyboard could fail due to a disconnected or loose keyboard ribbon cable. It could also fail if a user spilled

coffee on the laptop, dropped it on the ground, and so on. One stuck key will not cause the entire keyboard to fail, and on most laptops, the keyboard cannot be disabled in the Device Manager. It can be uninstalled but not disabled.

5. **A and B.** An incorrect adapter will usually not power a laptop. The adapter used must be exact. And, of course, if the laptop is not properly plugged into the adapter, it won't get power. Windows doesn't play into this scenario. And if the battery were dead, it could cause the laptop to fail to power up, but only if the AC adapter were also disconnected; the scenario states that the user is trying to use AC power.

6. **D.** It could be that the laptop is now on battery power and is set to a dimmer display and shorter sleep configuration while on battery. The laptop may not be getting AC power from the AC outlet for some reason. The battery power setting is the first thing you should check; afterward, start troubleshooting the AC adapter, cable, AC outlet, and so on. It's too early to try replacing the display; try not to replace something until you have ruled out all other possibilities. A dim screen is not caused by OS corruption. There's no need to plug in an external monitor. You know the video adapter is working; it's just dim.

7. **D.** The DC jack was probably damaged when the laptop was dropped. It may have been plugged in (charging) and fallen on the plug that connects to the DC jack (which is easily damaged on many laptops). The customer probably used the laptop until the battery became discharged before noticing that the laptop wouldn't take a charge anymore—and now it won't turn on at all. So the battery is probably not the issue. A power adapter can be damaged, but the DC-in jack is more easily damaged. The storage drive and the BIOS/UEFI normally will not affect whether the laptop will turn on.

8. **C.** To best reduce the chance of theft, use a cable lock. This physical cable can be wrapped around a sturdy object and locked to the laptop, keeping it *relatively* secure from theft. Incorporating

biometrics means implementing a thumbprint scan or other physical characteristic scan into the authentication process. Disabling NFC means that near-field communications will be turned off, and data can't be "beamed" to other devices. Enabling MFA means that you are implementing multifactor authentication—for example, combining a password and biometrics. While none of the incorrect answers can reduce the risk of a laptop being stolen, they do decrease the chance of *data* being stolen. As you can guess, computer security can be incredibly deep. That's why we dedicate Chapters 43 through 52 of this book to it!

9. **B.** Turning on airplane mode (the most likely cause of the problem) will disable wireless transmissions, including NFC. This is great for security purposes, but it can also disable the ability to connect to Wi-Fi networks or send/receive calls. A failed power state would render the entire device unusable; however, the question says the user was able to boot and sign on to the device. Biometric authentication is most likely not the cause of the problem in this scenario because the user is not having problems signing on to the device. Electrostatic discharge (ESD) can occur when two objects with different voltages come into contact with each other. ESD can wreak havoc with electronic components, but it is not the most likely problem here because the device appears to be working normally in all other regards; plus it's somewhat uncommon for mobile devices.

   The real issue here is *user error*: The user did not remember that the device was in airplane mode. When you troubleshoot problems, remember that they are often user-related!

10. **E.** A Wi-Fi card, also known as a Wi-Fi network adapter, allows you to connect to a wireless local area network (WLAN), which is essentially another name for a Wi-Fi network. LED is a type of display. A webcam is used to communicate visually and audibly with others or to record oneself. A digitizer is a device that converts tapped or written impulses on a screen into digital information that the operating system can use. A stylus is a writing device used with a digitizer or touchscreen.

11. **B.** The 2230 standard is a kind of M.2 size measuring 22×30 mm. It is common in laptops for use with Wi-Fi and Bluetooth. In comparison, a PC often uses a 2280 M.2 card. Mini PCI is an older type of card slot that might be used for Wi-Fi cards, but it does not use measurements such as 2230 or 2280 the way that M.2 does. A digitizer is not a port at all but a device that converts tapped impulses into digital information. An RJ-45 port is a networking port that allows a laptop to communicate with the rest of the network in a wired fashion—that is, if the laptop has such a port!

12. **D.** Most often in laptops, the antenna is located in the display area of the laptop. You will most likely need to separate the display from the laptop's motherboard section to open it and replace the antenna cable. The other answer options have to do with installing a SODIMM in a laptop.

13. **A, B, and C.** Laptop storage drive types include SSD, magnetic disk, and hybrid. Also, be aware that they have either 2.5- or 1.8-inch form factors. In addition, M.2 form factor storage drives have become more popular in modern laptops. Laptop RAM uses a small outline dual inline memory module (SODIMM). Two common types of SODIMMs in laptops are DDR4 (which has 260 pins) and DDR5 (which has 262 pins).

Chapter 2

Mobile Device Accessories and Connectivity Options

This chapter covers the following A+ 220-1201 exam objective:

- **1.2** – Compare and contrast accessories and connectivity options for mobile devices.

Mobile device connectivity is imperative. For the exam, you need to know the physical ports used for charging and synchronizing and for communicating with external devices. People love to deck out their devices! From headphones to extra storage, the options are endless. Brace yourself for the inevitable tech support requests for those ports and gadgets!

ExamAlert

Objective 1.2 focuses on the following concepts: connection methods such as Universal Serial Bus (USB), USB-C, microUSB, miniUSB, Lightning, near-field communication (NFC), Bluetooth, and tethering/hotspots; accessories such as stylus, headsets, speakers, and webcams; docking stations; port replicators; and trackpads/drawing pads/track points.

Connection Types

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

Wired Connections

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

The most common wired connection is USB. USB has been around for a long time and has gone through several versions and port changes. USB is used by devices that run Android and Windows (among others). However, aside from USB-C, older iOS-based devices from Apple use the proprietary Lightning connector. Fortunately, new iOS-based devices have transitioned over to USB-C. Figure 2.1 shows examples of the ports and connectors that you should know for the exam, including miniUSB, microUSB, USB-C, and Lightning.

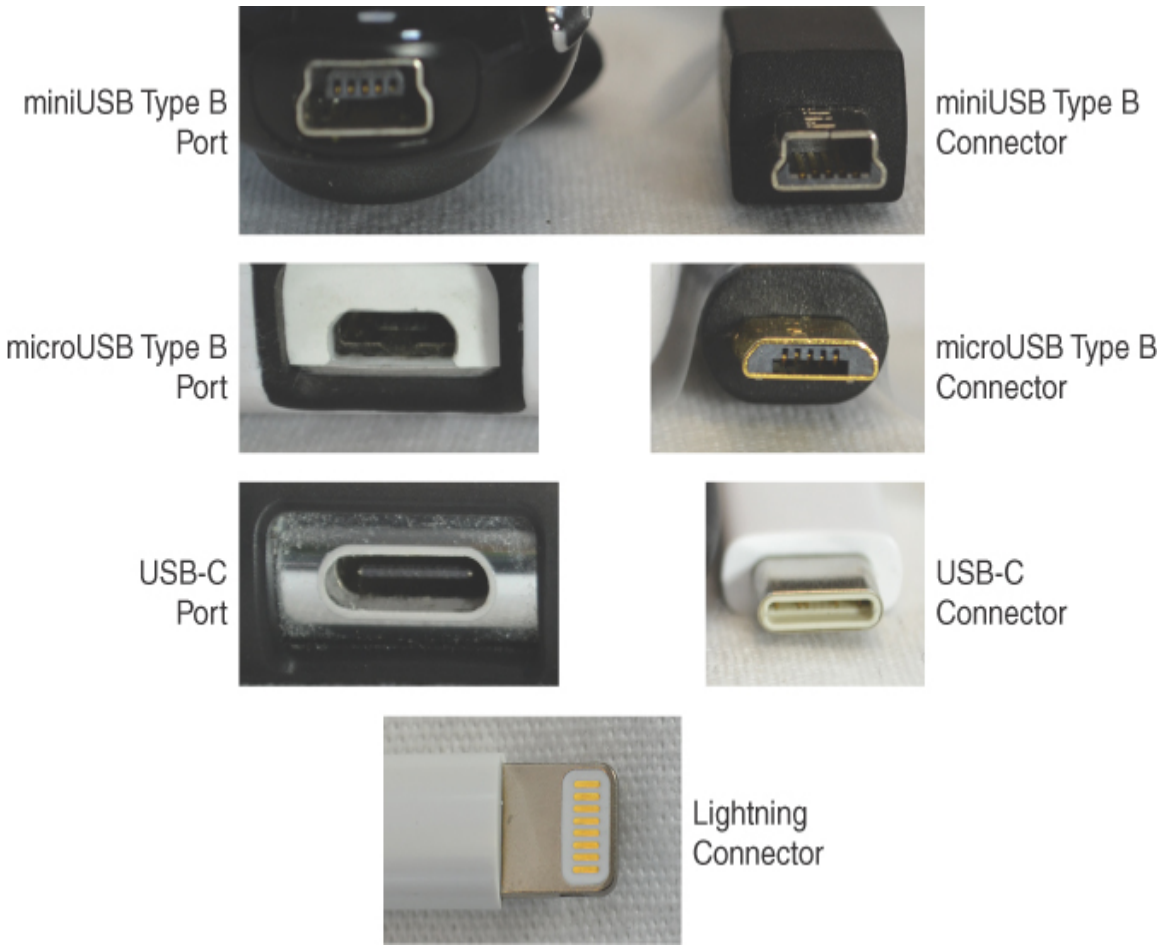


FIGURE 2.1 **USB and Lightning Ports and Connectors**

Almost all device charging cables use a standard Type A USB port on the other end, regardless of the connector type that is used to attach to the device. This allows connectivity to the majority of charging plugs and PCs and laptops in the world. However, a lot of adapters are available out there, so be ready.

As of the writing of this book (2025), USB-C is common for many Android-based smartphones and tablets. Previously, and for many years, Android devices used microUSB, but USB-C has been the dominant port on new devices since at least 2019. Even some Apple devices started using it in 2019. On the other hand, miniUSB is quite uncommon, but you might see it on older devices, such as accessories for smartphones.

ExamAlert

Know your mobile device ports and connectors. Remember that Android devices generally use USB-C (with older ones using microUSB), and iOS-based devices use USB-C or Lightning.

Note

We'll cover more about ports and connectors in Chapter 13, "Cables and Connectors."

Another purpose of a wired port is to make it possible to tether the mobile device to a desktop or laptop computer (usually via the computer's USB port). This tethering can allow a desktop computer or laptop to share the mobile device's Internet connection. Tethering functionality can be very useful in areas where a smartphone has cellular access but the PC/laptop cannot connect to the Internet. Once the physical USB connection is made, USB tethering can be turned on in the OS settings (where you will usually find the Mobile Hotspot option as well). Keep in mind that Wi-Fi capability on a smartphone is usually disabled when USB tethering is enabled and that the user must have hotspot service with their cellular provider for USB tethering to work. This being said, most modern mobile devices rely on Wi-Fi hotspotting to "tether" the data rather than the older method of physical tethering to share data. This requires the user to turn on their mobile hotspot in the OS settings on the mobile device and have their other device connect to the Wi-Fi hotspot name via the Wi-Fi given in the OS settings. You can change the default hotspot name by going to the OS settings.

Some mobile devices can also be equipped with serial interfaces (RS-232) or adapters from USB to serial. This allows for testing of devices and connectivity to various networking equipment and industrial devices. We will discuss serial interfaces and RS-232 in Chapter 13.

Wireless Connections

Wireless technologies are what really make a smartphone attractive to users. Most people would rather do without cables, and technologies such as Bluetooth, near-field communication (NFC), and hotspots make a smartphone functional and easier to use.

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

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

Another commonly used wireless technology is the mobile hotspot. When enabled on a properly equipped smartphone or tablet (with 4G or 5G connection), a hotspot allows a user to connect desktops, laptops, and other mobile devices (wirelessly, of course) through the device running the hotspot, ultimately allowing access to the Internet. This can be a great way to connect your laptop or other computer if Wi-Fi goes down, often with speeds rivaling wired Internet speeds. But remember, there's usually a catch! Many providers charge for data usage (unless you have a corporate plan). Because of this, a hotspot is often used as a secondary connection or as a backup plan. In addition, the further the hotspot-enabled mobile device is from a cell tower, the lower the data transfer rate. So know the pros and cons of running a hotspot on a mobile device.

ExamAlert

Understand the difference between configuring USB tethering (which is wired) and creating a mobile hotspot (which is wireless).

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

ExamAlert

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

Accessories

Adding a little bling or accessorizing your mobile device seems to almost be a requirement in today's society. Probably the number one thing that people do to augment their device is to protect it—using protective covers or cases, plastic or glass-based screen protectors, waterproofing, car mounts, and so on.

Then there's add-on storage. You can never have enough memory, right? Adding long-term storage is usually accomplished with the addition of a microSD card (for example 62, 128, or 256 GB). It is common for people who shoot a lot of videos (or a whole lot of photos) to need more memory than the mobile device comes with when purchased. Some older devices

allowed for add-on storage via a slide-out tray on the side of the device. Today, most don't allow upgrades unless you buy a new device.

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

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

IP Code

Many smartphones and other handheld computers are certified as being ingress protection (IP) compliant. Ingress protection means protection against dust and water, which are tested separately. There are a lot of different IP ratings, but let's use IP68 as an example. The first digit, 6, deals with dust and means that the device is dust tight and that no ingress of dust can occur. The second digit, 8, means that the device can be immersed in water up to and beyond 1 meter, generally for 30 minutes, though this can vary. The exact depth and length of time are up to the manufacturer, so IP68 could be slightly different from one device to the next. Regardless, the manufacturer must

test the device and prove that it is IP compliant before the rating can be applied to that particular model.

Docking Stations and Port Replicators

A docking station expands a laptop so that it can behave more like a desktop computer. By connecting a laptop to a docking station and adding a full-size keyboard, mouse, and monitor, the user doesn't actually touch the laptop except perhaps to turn it on. Some laptops can *hot dock*, meaning they can connect to a docking station while powered on. The docking station recharges the laptop's battery, and possibly a second battery, and has connections for video, audio, networking, and expansion cards. Docking stations might even have an optical disc drive, an additional hard drive, and additional display and USB ports; it all depends on the brand and model. If all these extras aren't necessary, a user might require only a *port replicator*, which is a similar device but has only ports (for example, video, sound, and network). Sometimes these are just referred to as docking stations as well. You will also hear the term *multiport adapter dongle*. This is becoming more common because many laptops will have only a limited number of USB-C ports and nothing else. Consequently, the user buys a USB-C dongle that allows other connections. It is essentially a port replicator.

ExamAlert

Note the difference: A laptop is placed, or "docked," into a docking station. Docking stations basically turn a laptop into a desktop computer. They replicate the ports on the back of a laptop so that peripherals like displays, mice, keyboards, and even printers, that don't travel with the laptop, can stay connected to the dock and don't have to be disconnected every time the laptop is taken away. In contrast, a port replicator is connected to a laptop simply to provide additional ports. Its main function is to allow the user to connect several devices at one time and doesn't require the laptop to be connected to offer connectivity between the devices. Also, a port replicator doesn't commonly supply power to charge a laptop, while

a laptop docking station many times will often charge a laptop while in use.

Drawing Pads, Trackpads, and Touch Pens

A mobile device's screen is often small, and it can be difficult to manipulate with your fingers. Sometimes a mobile device is not entirely accessible to your hands, perhaps because it is being used as a desktop replacement. And so, necessity breeds invention—in this case, easier manipulation in the form of drawing pads, touchpads, and touch pens.

A drawing pad is a flat tablet that allows you to use a stylus to "draw" on the screen of a mobile device. It can be used in illustration programs, slideshows, teaching utilities, and complex programs that have very tight interfaces where the tip of a stylus will work much better than your finger.

A stylus is often referred to as a touch pen or stylus pen. A touch pen can be used by itself with a mobile device to increase the accuracy of input to the screen.

A trackpad (or touchpad) is used to take the place of a laptop's touchpad; it is much larger and easier to manipulate. It is usually connected via USB or Bluetooth.

A *track point* refers to a small, pressure-sensitive nub, typically found on Lenovo ThinkPad keyboards, which acts as a pointing device allowing users to control the cursor on the screen without lifting their hands from the keyboard, essentially functioning like a mini joystick between the G, H, and B keys. A *trackpad* is a flat surface on a laptop where users can slide their fingers to move the cursor on the screen, similar to a traditional mouse pad.

Always check whether a mobile device's operating system will support any of these devices before purchasing and installing them. Installing such accessories is usually very easy because they are typically either plug and play or configured within the Bluetooth properties.

We could go on for days about the accessories available for mobile devices, and we'll discuss the concepts more later in the book, but that should be

enough for the exam for now. Remember, protecting a mobile device and protecting its memory capacity are crucial. The rest of the things we have discussed enable a user to increase functionality or just plain make it more fun, but these things are usually not essential to the device performing its job. Plus, in a bring your own device (BYOD) or choose your own device (CYOD) environment, the users are often quite limited when it comes to accessorizing to prevent compatibility issues and to avoid security vulnerabilities.

ExamAlert

Mobile accessories you need to be familiar with for Exam Objective 1.2 are stylus, headset, speakers, and webcam. Docking stations, port replicators, and trackpad/drawing pad/track points are also listed. Be sure you are familiar with them all!

Cram Quiz

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

1. Which type of charging connector would you find on an iPad? (Select all that apply.)

   - ○ **A.** microUSB
   - ○ **B.** Lightning
   - ○ **C.** USB-C
   - ○ **D.** IP68

2. You are required to add long-term storage to a smartphone. Which type would you most likely add?

   - ○ **A.** DDR4

- **B.** microSD
- **C.** LPDDR4
- **D.** SSD
- **E.** SIM

3. Which of the following can be useful in areas where a smartphone has cellular access but a PC (or laptop) cannot connect to the Internet?

- **A.** Proprietary vendor-specific connector
- **B.** Accessories
- **C.** IP codes
- **D.** Tethering/hotspotting

4. A user has asked you to provide a more accurate way of manipulating their smartphone screen. This user is part of a mobile salesforce and needs to be able to work quickly and efficiently. Which of the following is the easiest and best solution?

- **A.** Connect an external monitor so that the images on the screen will be bigger.
- **B.** Configure a drawing pad to work with the smartphone.
- **C.** Set up a touch pen to access the screen directly.
- **D.** Add an external touchpad to the device.

5. Which of the following refers to a small, pressure-sensitive nub typically found on Lenovo ThinkPad keyboards, which acts as a pointing device allowing users to control the cursor on the screen without lifting their hands from the keyboard?

- **A.** Trackpad
- **B.** Touchpad
- **C.** Mini joystick

- **D.** Track point

6 What device replicates the ports on the back of a laptop so that peripherals like displays, mice, keyboards, and even printers, that don't travel with the laptop, can stay connected and don't have to be disconnected every time the laptop is taken away?

- **A.** Drawing pad
- **B.** Stylus
- **C.** Docking station
- **D.** Port replicator

Cram Quiz Answers

1. **B and C.** The Lightning connector is one of Apple's proprietary charging and synchronization connectors used by older iPads and iPhones. Today, Apple uses USB-C. microUSB is used by older Android-based mobile devices, and USB-C is more common on newer Android-based devices. IP68 deals with ingress protection against dust and water.

2. **B.** You would most likely add a microSD card (if the smartphone has a slot available for add-ons or upgrading). This is the most common method for adding long-term storage. DDR4 is a type of RAM; it is not used for adding long-term memory storage. Some smartphones use LPDDR4 or LPDDR5 as their main memory, but this is part of the system on a chip (SoC) and not accessible to the typical user. An SSD is a solid-state drive, which generally means a hard drive that is installed to a PC or laptop, connected either as SATA or M.2. SSDs are too large for smartphones and tablets. A SIM is a subscriber identity module, usually represented as a small card (mini-SIM) used in smartphones that securely stores authentication information about the user and device, such as the International Mobile Subscriber Identity (IMSI), which we will discuss more in the following chapter.

3. **D.** Tethering and hotspotting can allow a desktop computer or laptop to share the mobile device's Internet connection. Tethering and hotspotting functionality can be very useful in areas where a smartphone has cellular access but a PC/laptop cannot connect to the Internet. Mobile device accessories such as headsets, speakers, game pads, extra battery packs, and protective covers are useful, but they are not used to connect to the Internet. IP codes (for example, IP68) are used to classify and rate the degree of protection against dust and water.

4. **C.** The best option is to set up a touch pen to access the smartphone's screen directly. A smartphone may come with a touch pen (also known as a stylus pen or simply a stylus); or it may be able to have a touch pen added later. A touch pen enables a person to input information to the screen more accurately. The other devices listed will make mobility more difficult (if not impossible). The next best answer would be an external touchpad, but it isn't the easiest solution. If the user needs the touchpad more often, then a better, more permanent solution might be to use a tablet computer instead of a smartphone.

5. **D.** A track point refers to a small, pressure-sensitive nub typically found on Lenovo ThinkPad keyboards, which acts as a pointing device allowing users to control the cursor on the screen without lifting their hands from the keyboard, essentially functioning like a mini joystick between the G, H, and B keys. A trackpad is a flat surface on a laptop where users can slide their fingers to move the cursor on the screen, similar to a traditional mouse pad.

6. **C.** Docking stations basically turn a laptop into a desktop computer. They replicate the ports on the back of a laptop so that peripherals like displays, mice, keyboards, and even printers, that don't travel with the laptop, can stay connected to the dock and don't have to be disconnected every time the laptop is taken away. In contrast, a port replicator is connected to a laptop simply to provide additional ports. A port replicator doesn't commonly supply power to charge a laptop, while a laptop docking station many times will often charge a laptop while in use. A drawing pad

is a flat tablet that allows you to use a stylus to “draw” on the screen of a mobile device. A stylus is often referred to as a touch pen or stylus pen. A touch pen can be used by itself with a mobile device to increase the accuracy of input to the screen.

Chapter 2 is done! Let’s keep up the excellent work and head to the next chapter. Onward and upward!

Chapter 3

Mobile Device Network Connectivity and Application Support

This chapter covers the following A+ 220-1201 exam objective:

- **1.3** – Given a scenario, configure basic mobile device network connectivity and provide application support.

Welcome back! This is the last chapter focusing specifically on mobile devices. Here we'll be discussing networking and synchronization. Because those are big topics, this is a relatively big chapter (for this book at least). Take it one step at a time, and you should be fine.

Users need Wi-Fi, Bluetooth, and email. They need cellular connections for voice calls as well as for data. And let's not forget the need to synchronize data to computers, cars, and the cloud. That's what this chapter is all about. Now that you know, it's time to begin.

ExamAlert

Objective 1.3 concentrates on the following concepts: wireless/cellular technologies, Bluetooth setup, location services, mobile device management (MDM), and mobile device synchronization.

Note

For simplicity, most of the time we use the term *cellular* to refer to smartphone connectivity to a telecommunications provider, meaning 3G, 4G, 5G, and so on.

Enabling Wireless Functions

You will most definitely be called upon to enable and disable various wireless and cellular functionality. In this section we'll discuss how to connect to Wi-Fi, set up a mobile hotspot, and turn on airplane mode.

Cellular connections such as 3G, 4G, LTE, 5G, and beyond are commonplace on smartphones. If you purchase a smartphone from a telecommunications provider, then you get cellular access. It is enabled by default, and it functions unless you turn on airplane mode. We'll talk more about cellular technologies later, but for now keep in mind a couple of things:

- Cellular connections can be slow when transmitting data. That could be due to the distance from the nearest cell tower, the connection speed, or a general lack of service availability. While cellular companies are rapidly trying to change this to market their services as an alternative to traditional home-based Internet connections like cable, DSL, and fiber, know that this is still an issue as of this writing.
- Cellular connections can cost the customer money. That's why all mobile devices are equipped with an embedded wireless antenna to connect to wireless LANs (WLANs). This Wi-Fi antenna can potentially allow access to 802.11a, b, g, n, ac, ax, and be networks. The wireless connection works similarly to a wireless connection on a PC, laptop, or tablet. See Chapter 9, "SOHO Network Configuration," for a detailed description of connecting to wireless networks.

In general, a mobile device must search for wireless networks before it can connect. This is done in the wireless settings of the device. Figure 3.1 shows a typical Wi-Fi settings screen.

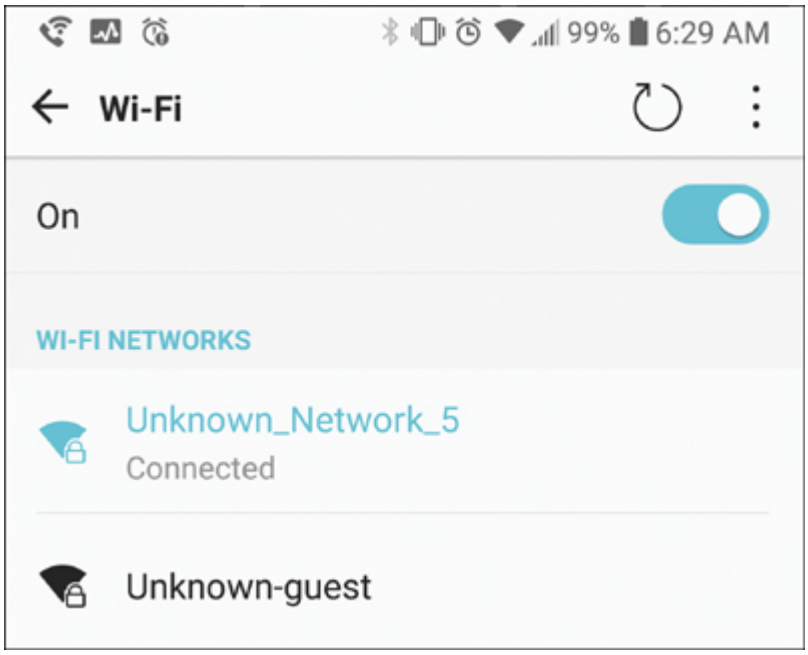


FIGURE 3.1 **Wi-Fi Settings Screen in Android**

In the Wi-Fi settings screen, perform the following general steps:

1. Most devices usually scan for wireless networks automatically and list them for you, or you can tap **Add Wi-Fi Network** (or something similar) to add one manually.
2. When adding a network manually, enter the service set identifier (SSID) of the wireless access point (WAP).
3. Enter the passcode for the network. If the code is correct, then the wireless adapter in the mobile device gets an IP address, allowing it to communicate with the network. Remember to use the latest wireless protocol available to you (such as WPA2 or WPA3). Update the mobile device if it isn't compatible.
4. Check for the universal wireless icon at the top of the screen (in the notification bar) to verify connectivity.

ExamAlert

Understand how to connect to a Wi-Fi network in Android, iOS, and iPadOS.

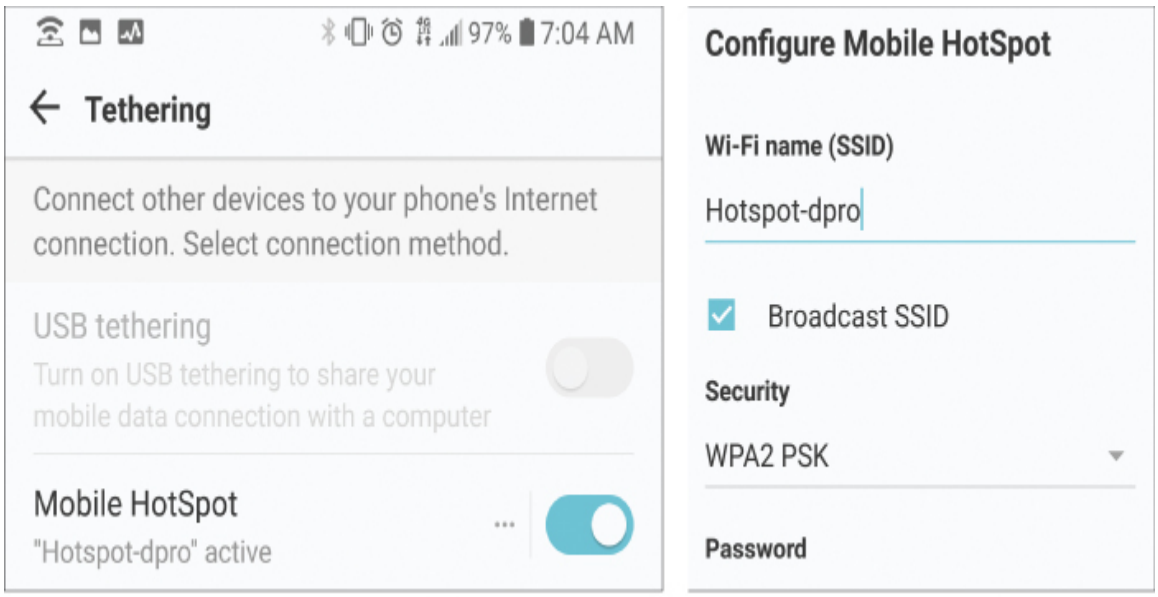
If you bring your mobile device into a secure area or onto an airplane, you will most likely be asked to place the device in *airplane mode*. This mode disables all wireless connectivity, including (but not limited to) cellular, Wi-Fi, and Bluetooth. You can put a device in this mode by pressing and holding the power button and selecting airplane mode or by accessing the quick settings drop-down menu (Android) or Control Center (iOS).

Once in airplane mode, you should see the airplane icon in the notification bar. However, keep in mind that this is primarily designed to disable cellular access. On many devices, a user can still re-enable Wi-Fi, Bluetooth, or NFC even when airplane mode is on. Sometimes a user might complain that there is no wireless connectivity. If so, check if the device has been inadvertently placed into airplane mode and disable it from the same locations mentioned previously.

So, you know how to set up Wi-Fi. But what if you want to share that connection with other computers, such as laptops or tablets? That's where the mobile hotspot comes in. When you configure a *mobile hotspot*, the mobile device shares its Internet connection with other Wi-Fi-capable devices. For example, if a user has a smartphone that can access the Internet through a cellular network, it can be configured to become a portable Wi-Fi hotspot for other mobile devices (or desktops/laptops) that are Wi-Fi-capable but have no cellular option. Beware of the hotspot option; most providers have a fairly low consumer bandwidth threshold for data transferred through the hotspot by default, even if the plan is called "unlimited." This data transmission limit (often referred to as a "data cap") is a service provider–imposed limit on the amount of data that can be sent and received by a customer over the course of a month or other time period. When the customer surpasses the cap, additional fees can be applied to the customer's account. To guard against this, there are Internet usage

monitoring apps available that will give a warning when approaching the cap.

Enabling hotspots is easy and is usually done in the network settings section of the device. Figure 3.2 shows an example of this. The first time you enable the hotspot, you will be asked to supply a password and the wireless protocol to be used, which can be modified later. As of this writing, it is recommended to use WPA2/WPA3 and, of course, set a strong password. An example of the configuration screen is also shown in Figure 3.2.



Enabling a HotSpot Configuring a HotSpot

FIGURE 3.2 **Hotspot Configuration in Android**

When a hotspot is enabled on a smartphone, Wi-Fi is automatically disabled. So, the smartphone will only be able to connect via the cellular network, but it is designed this way on purpose, expecting to be used only when there is no Wi-Fi connection available. Other Wi-Fi-ready systems (laptops, PCs, tablets, and so on) need only look for and connect to the Wi-Fi network that was created (for example, *Hotspot-dpro* in Figure 3.2). Running a mobile hotspot can also be a great backup option in the event that the main Internet connection in a small office or home office fails temporarily.

Bluetooth

Bluetooth is a wireless standard for transmitting data over short distances. It is commonly implemented for multimedia purposes and for connecting to mobile device accessories.

To connect a Bluetooth device to a mobile device, you first must enable Bluetooth, then you must synchronize the Bluetooth device to the mobile device. This process is known as *pairing*, or *linking*. It sometimes requires a PIN code, depending on how the remote device is configured. Once synchronized, the device should automatically connect and should function at that point. Finally, the Bluetooth connection should be tested. Following are the steps involved in connecting a Bluetooth device to a typical mobile device. Before you begin, make sure the Bluetooth device is charged (if applicable). The typical procedure for making a Bluetooth connection is as follows:

1. Turn on Bluetooth in the Settings of the mobile device.
2. Prepare the device by turning it on and pressing (and sometimes holding) the Bluetooth button.
3. Scan for devices on the mobile device.
4. Pair to the desired device.
5. Enter a PIN code if necessary. Some devices come with the default PIN 0000.

When finished, the screen will look similar to Figure 3.3. Note the Bluetooth icon at the top-middle of the screen. It almost looks like an uppercase *B* made of triangles. (Really, it's two runes merged together to form the initials of 10th-century Dane King Harald "Bluetooth" Gormsson, who got the nickname Bluetooth from his dark, dead tooth—but you won't be tested on this!) This icon indicates whether Bluetooth is running on the device. It will remain there even after you disconnect the Bluetooth device but in a grayed-out state. To disconnect or reconnect a Bluetooth device, simply tap the device on the screen. It will remain paired but nonfunctional until a connection is made again. (Typically, devices are listed in bold if they are connected.) You can also unpair and/or forget a Bluetooth device in

the settings for that device. Unpairing removes the link between the smartphone and the Bluetooth device, but the mobile device will remember the Bluetooth device. “Forgetting” removes the connection altogether.

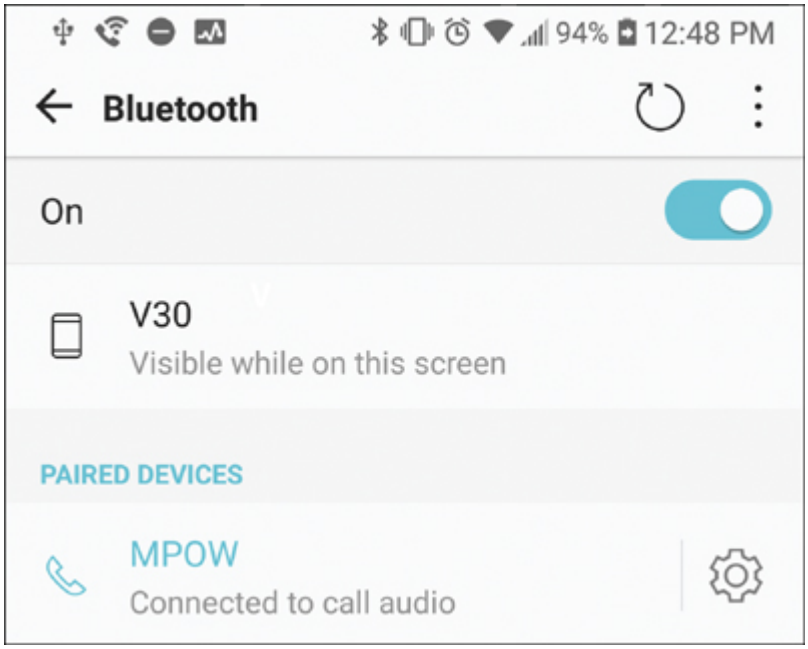


FIGURE 3.3 **Bluetooth Paired Devices Screen in Android**

A Bluetooth device 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 unpair or disconnect it or, going further, “forget” it from the current connection before making a new one.

ExamAlert

Know the CompTIA process for configuring Bluetooth:

1. Enable Bluetooth.
2. Enable pairing.
3. Find a device for pairing.
4. Enter the appropriate personal identification (PIN) code.
5. Test connectivity.

Email Configuration

Although there are many other types of communication available to mobile users, email still accounts for an important percentage. You should know how to configure a mobile device for web-based email services such as Gmail, MSN, and so on. You should also know how to configure Post Office Protocol Version 3 (POP3), Internet Mail Access Protocol (IMAP), and connections to Microsoft Exchange Server.

Integrated Commercial Provider Email Configuration

Mobile devices can access web-based email through a browser, but this is not necessary today because most commercial providers offer integrated email configuration for mobile operating systems. For example, most Android-based devices come with a Gmail application (app) built in, allowing a user to access Gmail directly, without having to use the browser. A device also might have a proprietary email application. Apple iOS devices allow connectivity to Gmail, MSN, and a host of other email providers as well. Apple users might also connect to iCloud for mail features. Users of other devices might use Microsoft's Outlook on the Web (part of a Microsoft 365 subscription), or for more users and for collaboration, a company might opt for Exchange Online. As you can see, there are a lot of options when it comes to mail services for mobile devices.

Note

Software as a Service (SaaS) email examples such as Gmail, MSN, and Outlook enable users to connect to and use cloud-based email apps over the Internet. Other common SaaS examples are calendaring and office tools (such as Microsoft 365). SaaS offers a complete software solution that allows you to purchase apps on a pay-as-you-go basis from a cloud service provider. See Chapter 21,

"Virtualization Concepts," and Chapter 22, "Cloud Computing Concepts," for more information.

Connecting to these services is simple and works in a fashion that is similar to working on a desktop or laptop computer. Choose the type of provider you use, enter a username (the email address) and password (and, on Apple devices, an Apple ID), and the user will have access. In more advanced cases, a user may have to select the protocol and ports to be used. That's where you, as the administrator, come in; we'll discuss those protocols and ports in a little bit.

When troubleshooting user issues with email, make sure that the username and password are typed correctly. Using onscreen keyboards often leads to mistyped passwords. Also make sure that the mobile device is currently connected to the Internet.

Corporate and ISP Email Configuration

Connecting a mobile device to a specific organization's email system gets a little more complicated. You need to know the server that you want to connect to, the port you need to use, and whether security is employed. Look at the following email configuration information and Figure 3.4 for an example:

- **Incoming server name:** secure.dpro42.com
- **POP3 port (SSL/TLS):** 995
- **Outgoing server name:** secure.dpro42.com
- **SMTP port (SSL/TLS):** 465

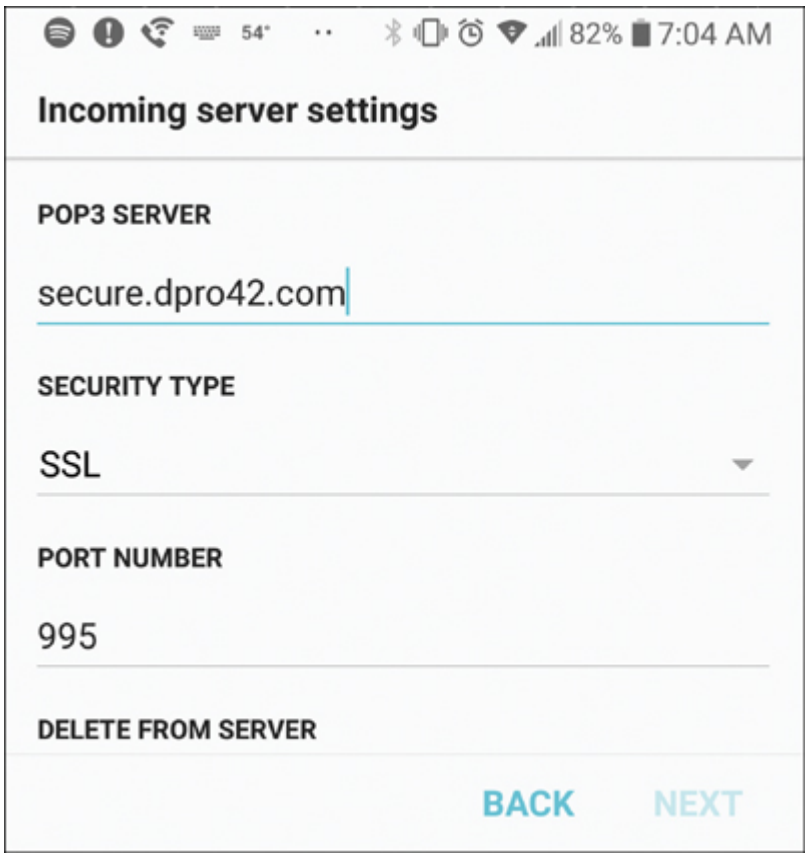


FIGURE 3.4 **Email Server Settings Screen in Android**

The figure shows manual configuration of an email client in Android. At this stage, the email client is asking for the incoming server, meaning the one used for receiving mail. It just so happens that the same server takes care of incoming mail and outgoing mail: secure.dpro42.com; but sometimes it could be two different servers. So, you add the name of the server into the POP3 Server field. Then you specify the security type. In this case, you select Secure Sockets Layer (SSL) instead of "no security," which is important. Most of the time you want to have encrypted email sessions to your email server to prevent eavesdropping and tampering. This could be SSL or Transport Layer Security (TLS), depending on the server configuration. Then you select the port, which, according to the previous documentation, is 995. That is the default secure port for POP3 email connections that make use of SSL/TLS; however, this port number can vary depending on what protocol you are using for email and what type of security you implement. As a technician configuring the client email, you

must go by the documentation provided by the network administrator (or just "admin" for short). When you're the admin, it's generally a good idea to go with the default secure port numbers, but in reality, you can choose which port to use (within reason), and as long as the client configures that port to connect, it should be successful. See Table 3.1 for a list of original and secure ports used by the various email protocols.

ExamAlert

Secure Sockets Layer/Transport Layer Security (SSL/TLS) is a secure communication protocol that encrypts data sent between devices on the Internet to keep it private and secure.

TABLE 3.1 **Email Configuration Example**

Email Protocol	Original Port Number	Secure Port Number
SMTP	25	465 or 587
POP3	110	995
IMAP	143	993

ExamAlert

Know the email protocols/ports: SMTP = 25/465/587; POP3 = 110/995, IMAP = 143/993.

We say Table 3.1 shows the "original" port numbers because these are what we used for many years until encrypted email sessions became necessary. The secure port numbers are defaults, but they can vary, depending on whether you have to select TLS or whether another secure technology is used. In addition, the admin simply might decide to go with a different port number. Here's the thing: Most ports can work in a secure fashion—if configured properly—but you should know the most common defaults in

Table 3.1 for the exam. These are what email server programs and client applications will typically default to.

> **Note**
>
> Another protocol you might implement when setting up secure email is S/MIME (Secure/Multipurpose Internet Mail Extensions). This is used for authentication and message integrity and is built into some email clients.

Cellular Radio Technologies

Without a properly working radio in your smartphone, you won't hear anything. This section is designed to teach you the basics about cellular voice calls and data transmissions. Most people can't live without their phones—and ultimately, phones are radios.

Originally, cellular phones used the Global System for Mobile Communications (GSM) to make voice calls and GSM or the General Packet Radio Service (GPRS) to send data at 2G speeds through the cellular network. Extensions of these standards—the Universal Mobile Telecommunications System (UMTS) and Enhanced Data rates for GSM Evolution (EDGE)—are used to attain 3G speeds. 4G and 4G LTE speeds can be attained only when a mobile device complies with the International Mobile Telecommunications Advanced (IMT-Advanced) requirements, has a 4G antenna, and is in range of a 4G transmitter. LTE builds on 4G by using an updated radio interface/antenna in the mobile device and by utilizing core network infrastructure improvements. The fifth generation of cellular, 5G, is known as the ITU IMT-2020 standard and has data transfer rates of up to 20 gigabits per second (Gbps). It can also offer latency under 5 milliseconds! Additionally, 5G can operate on a new high-frequency spectrum called millimeter wave, or mmWave. This operates on frequencies between 30 GHz and 300 GHz, whereas 4G was under 6 GHz. Higher frequency means much faster speeds, but it also means shorter distance. So, to take advantage of the new mmWave technology in 5G, cellular companies have to set up many new small cell bases. Many large cities have

these, but rural areas don't always have the infrastructure yet for this new technology.

ExamAlert

Know the different cellular standards and that 5G can transmit at 20 Gbps.

Most devices cannot shut off the cellular antenna by themselves (unless you shut down the device itself). However, every device manufactured now is required to have an airplane mode, which turns off any wireless antenna in the device, including disabling the connection to the cellular network and disabling Wi-Fi, and Bluetooth. You will find that some airlines don't consider this to be acceptable and for security purposes will still ask you to turn off your device altogether, either for the duration of the flight or at least during takeoff and landing. Some devices can also limit or disable cellular *data* usage—often known as "mobile data."

Let's get a little more into it and briefly discuss some additional mobile technology and acronyms, such as baseband updates and radio firmware.

When a phone uses Global System for Mobile Communications (GSM), that technology and its radio functions are controlled by a chip and software package that is collectively referred to as "baseband." Baseband updates are necessary to communicate properly with GSM cell towers. If an older phone won't update properly, it must be taken to the provider for a wired, manual update. Baseband is also referred to as radio firmware because it controls network connectivity for GSM. Other wireless antennas, such as Wi-Fi and GPS antennas, are controlled by the operating system's drivers. GSM, while still used, is quickly being replaced by 5G.

Note

Do not attempt a radio firmware (baseband) update if your phone does not require it. A faulty update can easily make the phone inoperable.

You can find the versions of most of these technologies (and the types of radio technology used) in the About (or About device) section on a device. Take a look at your own mobile device's settings, such as the radio technologies you are connecting to, the baseband version, and the IMEI. You might also consider using a cellular analyzer app to see this data—as well as data concerning cellular towers—in a more visual and centralized manner.

Your mobile account number, carrier information, and other important data needed to connect to the cellular network are stored in a SIM card. A SIM, or subscriber identity module, is a small physical card in your phone that holds this information. If you are traveling to another country and want to use another cellular provider's services for cost reasons, you will often buy a SIM card and swap out your existing one for this new one. A word of caution here: Don't lose your existing SIM card, because otherwise, you'd return home without your phone number! While swapping cards can save you money while traveling, it also has its disadvantages. Your original number will not be available while the other SIM card is in your phone. This means traditional texting, SMS/MMS, and calling will be based on your new SIM number and not your original one.

Recently, there has been a rise in a new type of SIM card. It is called an eSIM and stands for embedded SIM. This is a digital version of the original physical SIM card, which means that there is no physical card slot on phones equipped with this new technology. An eSIM is activated remotely by the carrier and means you can switch carriers remotely without swapping out SIM cards. It also has the potential to hold multiple lines simultaneously. Some companies are already dedicated to this service for global travelers, so you can keep your original number with your carrier but also pay for another eSIM line while traveling abroad.

ExamAlert

Know what a SIM is and the difference between a physical SIM and an eSIM.

Location Services

Location services (or location-based services) is a somewhat ambiguous term and can take form as one of two things: GPS and cellular location. It's a generalized term that refers to software services that work with geographic data in order to provide services and information to users—or, to track user location. On a mobile device, location services (or simply "location") can be enabled or disabled in the settings of the mobile device. If enabled, GPS apps and other location-based programs will function. If disabled, the mobile device is "taken off the grid" to a certain extent. This approach can be beneficial if a user wants to prevent particular types of tracking, such as geotagging—which allows location data to be attached to images, videos, SMS messages, and website postings, providing permanent and searchable data about the user (a privacy concern for sure). Most devices allow a user to disable location services but then selectively use individual location features as desired.

Note

Corporate access policies can also be controlled by location data. For example, geofencing, which uses location-based services such as Global Positioning System (GPS), radio-frequency identification (RFID), Wi-Fi, or cellular data to define virtual boundaries or geographical areas around real-world locations, can trigger an action when a mobile device enters or exits a specific geographic area called a geofence.

Let's define GPS and cellular location now.

GPS

The Global Positioning System (GPS) is a satellite-based navigation system that provides geolocation to properly equipped GPS devices, including smartphones and dedicated GPS devices. If you have a smartphone, you probably use some kind of GPS app, but there are also dedicated smart GPS

systems for vehicles that can work independently and possibly integrate with your smartphone and social media via Wi-Fi and Bluetooth. The beauty of these is that the bulk of the CPU in the device is dedicated to GPS. If you have ever run GPS on a smartphone while other apps are running and experienced slow performance, then you can understand why a dedicated GPS system might be a valid option for delivery drivers, those in the transportation industry, or those who simply want more accurate and efficiently presented GPS data.

Many vehicles offer systems with touchscreens that can integrate with a person's smartphone and GPS apps. The most common of these systems are Apple CarPlay and Android Auto. To use such a system, the vehicle must be compatible, and the smartphone must have the correct app installed; often the device must be connected in a wired fashion via USB. In this scenario, a technician should make sure that the vehicle's firmware and software are updated, that the smartphone's vehicle connectivity software and GPS software are updated, and that a *quality* cable is used. This way, the user can be properly "geolocated," and GPS directions will be up to date. Many new vehicles are starting to feature wireless CarPlay and Android Auto through a combination of Wi-Fi and Bluetooth to allow for wire-free operation.

ExamAlert

Know that GPS technology is integrated into mobile devices to help a user navigate while driving (among other things) but that it will be useless if location services is disabled on the mobile device.

Cellular Location

Cellular location is a method of locating a mobile device with the use of cellular technologies. For example, by using GSM or 5G, and a smartphone's signal strength, it is possible to estimate the distance of the smartphone to a cell tower. Going further, it is possible to use multiple towers' radio signals (known as multilateration) to "triangulate" a more

exact location of the smartphone. This is an example of *mobile phone tracking*.

IMEI and IMSI

Another related concept is mobile device identification technology—namely International Mobile Equipment Identity (IMEI) and International Mobile Subscriber Identity (IMSI). IMEI identifies phones used on 3GPP-based networks (GSM, UMTS, and LTE). You can find this ID number in Settings, and on older phones it is printed inside the phone, either on or near the battery. It is used only to identify the device. However, IMSI is used to identify the user. For GSM, UMTS, and LTE networks, this ID is loaded into the subscriber identity module (SIM) card or eSIM.

> **Note**
>
> 3GPP-based networks are networks developed by the 3rd Generation Partnership Project (3GPP), which is an international collaboration of telecommunications standards development organizations. This group is responsible for UMTS 3G, LTE, and 5G technologies. Please see https://www.3gpp.org/ for more information.

Synchronization Methods

A person might want to synchronize a mobile device's data somewhere else to be able to access that data from anywhere. This synchronization also offers peace of mind: If the mobile device is lost or stolen, the data will be available on the other system when a new mobile device is procured. And, of course, even though mobile devices today can store a lot of data, there's always the need for more storage. External systems allow for a much greater amount of storage, as well as redundancy of data.

A person can choose to synchronize data to an individual computer that is physically nearby, or to a car, or to the cloud, which is the most common option.

Synchronizing to the Cloud

For simplicity, we can refer to the cloud as any computer that you synchronize to on the Internet. Generally, this means using some type of service. You might synchronize your mobile device's data to Google Drive, Microsoft OneDrive, Apple iCloud, Dropbox, or one of several other services. Making this happen entails creating an account, installing the appropriate app on the mobile device (if it is not already there), and specifying what folders, files, and other data you would like to synchronize. The first time you synchronize your device's data, the application will copy the data over to the cloud recipient. Subsequent synchronizations will copy new files and append changed files.

> **Note**
>
> You might also opt for a service such as Nextcloud, which you can run locally on your own server, as well as connect to in the cloud. Check it out!

When it comes to popular services such as Gmail, you might question whether you really are "synchronizing" anymore. You are. It's just that the data is all stored on the service's servers, and you are simply accessing it from a mobile device or PC. A person who signs up for a Gmail account allows Google to automatically synchronize mail, contacts, and the calendar so that the information can be viewed on the mobile device or on the PC (when connected to the Google website).

However, because the data is stored on a Google server, security should be a concern. If you choose to use Gmail (or another similar service), you should use an extremely strong password and consider changing it periodically (for example, every 6 to 12 months). Also, if possible, incorporate two-factor authentication (such as using a password and some kind of biometrics or encrypted key technology in conjunction with the password). Beyond this, use a secure browser when connecting to Gmail from a desktop computer. On the mobile device side, make sure the Gmail app is updated often to ensure that any security vulnerabilities are patched.

The same concepts hold true for other similar services. Utilizing the cloud presents many configuration and security concerns, which we will discuss further in the networking chapters of this book.

Note

Keep in mind that you might also *back up* your data, but this is different from synchronization. For example, you might back up an Android-based device's apps, call history, contacts, device settings, SMS text messages, and other items that are normally stored locally. You could back up this data to a server on the cloud owned by the manufacturer of the mobile device, or you could use a separate service, such as Google Drive. Either way, this is done separately from synchronization.

Synchronizing to the Desktop

Today, synchronizing to the desktop is not nearly as common as syncing to the cloud. But it might be necessary, or desired, by some users. When you connect mobile devices to a Windows PC via a USB connection, they are typically seen automatically and are represented as devices in File Explorer under This PC. On the mobile device, you might have to change the USB options from Charging to File Transfer or another similar option in order to see the device in Windows. At this point, you can copy files back and forth between the mobile device and the PC manually or rely on automatic synchronization software from the manufacturer of the mobile device or from a third party.

Windows devices can be synchronized together with the Sync Center. This allows you to choose individual synchronize settings such as Theme, Passwords, Language preferences, Ease of Access, and other Windows settings, but a user would have to sign in with a Microsoft account in order to synchronize.

Note

Exchange ActiveSync can be used to synchronize email, contacts, and calendars between a variety of devices (iOS-based devices, Windows devices, etc.) with Microsoft Exchange Server.

To synchronize data—contacts, calendars, and so on—from Apple devices to a PC requires the use of iTunes for Windows. From iTunes, a user selects Sync Contacts or Sync Calendars, for example. Calendar items can also be synced from the Apple-based device (such as an iPad) by going to **Settings > Mail**, **Contacts, Calendars**. Then scroll down and select **Sync**. iCloud can also be downloaded for Windows. You can also now use the Apple Device app to sync from an iPad to a PC instead of iTunes. It is quite similar in use but doesn't require the music-centered app that is iTunes.

Synchronizing to the Car

It had to happen—computers in cars. People want to harness the power of their smartphone in conjunction with their car's computer and display. It's easy with tools such as Android Auto and Apple CarPlay. These apps can be used independently on a mobile device or can be synchronized to a car's computer if it has the proper firmware/software installed. Then, the user can make use of the car's larger screen for easier accessibility, better viewing, and increased safety. For integration of these platforms, the mobile device usually has to be plugged in via USB, and a high-quality cable should be used to avoid interruptions unless your car is capable of wireless CarPlay and/or Android Auto.

In reality, this isn't as much "synchronizing" as it is screen sharing. The larger screen in the car is used to display, and control, the common apps you might need: phone, maps, music player, and so on. Apple CarPlay and Android Auto both limit the number and types of apps you can use in the car for safety reasons.

Figure 3.5 shows an example of Android Auto running on a smartphone connected to a car via USB. Of course, most smartphones can multitask, so you can potentially use both screens at the same time with different apps running on each—when parked, of course!



FIGURE 3.5 **Example of Android Auto**

If a vehicle does not support Android Auto or Apple CarPlay, it might support Bluetooth (BT). If that is the case, then a smartphone or tablet can be synchronized to the vehicle via BT by pairing the car to the device in the same manner described earlier in the chapter. Then the user can operate voice calling and texting hands-free. If the vehicle is not equipped with any computer or BT integration, then a replacement head unit (stereo) can be purchased to allow BT and USB integration as well as Apple CarPlay or Android Auto.

Mobile Device Management (MDM)

For networks with a lot of users, consider third-party offerings from companies that make use of mobile device management (MDM) platforms.

These centralized software solutions allow admins to control, configure, update, and secure remote mobile devices (Android, iOS, and so on), all from one administrative console. The MDM software can be run from a server within an organization or administered within the cloud. MDM makes the job of a mobile IT administrator at least manageable. From the central location, the administrator can carry out the tasks of application management, content management, and patch management. The admin can also set up more secure levels of mobile device access control. *Access control* is the methodology used to allow access to computer systems.

For larger organizations, MDM software makes it easy for an admin to view inventory control, such as how many devices are active for each of the mobile operating systems used. It also makes it simpler to track assets, such as the devices themselves, and the types of data each contains. In addition, MDM software makes it less complicated to disable unused features on multiple devices at once, thereby increasing the efficiency of the devices, reducing their footprint, and ultimately making them more secure. For instance, an employee who happens to have both a smartphone and a tablet capable of making cellular calls doesn't necessarily need the latter. The admin could disable the tablet's cellular capability, which would increase battery efficiency as well as security for that device. Insecure user configurations such as rooting and jailbreaking can be blocked from MDM, as can sideloading—the art of loading third-party apps from a location outside the official application store for that device.

Finally, application control becomes easier thanks to *mobile application management (MAM)*. With MAM, applications can be installed, uninstalled, updated, and secured from a central location. Even devices' removable storage (often USB based) can be manipulated—as long as the removable storage is currently connected to the device. We'll discuss MDM more in Chapter 49, "Mobile Device Security."

Note

Remember that bring your own device (BYOD) is a policy governing employees bringing personally owned devices (laptops, smartphones, and the like) to the workplace and the use of those devices to access company data. Choose your own device (CYOD)

is policy where an organization allows employees to select the mobile devices they would like to use, typically from a limited number of company-approved options. With a COPE policy, or corporate-owned personally enabled policy, the business owns and pays for the mobile devices. This model allows employees to use company-owned devices for both work and personal use. The BYOD, CYOD, or COPE policies should address how data and corporate-owned applications will be handled when employees are hired, terminated, quit, or retire.

ExamAlert

Understand that MDM is software that is used to update and secure mobile devices from a central location. MAM focuses on managing specific corporate mobile applications.

Cram Quiz

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

1. Which of the following connections require a username, password, and SMTP server? (Select the two best answers.)

   - ○ **A.** Bluetooth connection
   - ○ **B.** Wi-Fi connection
   - ○ **C.** POP3 connection
   - ○ **D.** Exchange connection
   - ○ **E.** IMAP connection

2. When manually configuring a Wi-Fi connection, which step occurs after successfully entering the SSID?

- ○ **A.** Select POP3.
- ○ **B.** Check whether the device is within range of the WAP.
- ○ **C.** Enter a passcode for the network.
- ○ **D.** Scan for networks.

3. Which of the following allows other mobile devices to wirelessly share a mobile device's Internet connection?

- ○ **A.** NFC
- ○ **B.** Airplane mode
- ○ **C.** IMAP
- ○ **D.** Mobile hotspot

4. Which of the following identifies the user of a device?

- ○ **A.** IMSI ID
- ○ **B.** IMEI ID
- ○ **C.** S/MIME
- ○ **D.** VPN

5. Which of the following is used to synchronize contacts from an iPad to a PC? (Select the best answer.)

- ○ **A.** Gmail
- ○ **B.** Google Play
- ○ **C.** iTunes
- ○ **D.** Sync Center

6. You oversee a midsized enterprise and are supporting 300 smartphones. Which of the following would best allow you to configure them from a centralized location?

- **A.** GPS
- **B.** MDM
- **C.** Location services
- **D.** SSL/TLS

7. What should you do after you have found a Bluetooth device for pairing? (Select two.)

- **A.** Enter the appropriate PIN code
- **B.** Enable Bluetooth
- **C.** Disable pairing
- **D.** Test connectivity

8. What is the secure port for POP3 email connections that make use of SSL/TLS?

- **A.** 110
- **B.** 465 or 587
- **C.** 993
- **D.** 995

9. Which is a policy that governs employees bringing personally owned devices (laptops, smartphones, and the like) to the workplace and the use of those devices to access company data?

- **A.** CYOD
- **B.** COPE
- **C.** ITU IMT-2020
- **D.** BYOD

Cram Quiz Answers

1. **C and E.** POP3 and IMAP email connections require an incoming mail server (either POP3 or IMAP) and an outgoing mail server (SMTP). Bluetooth and Wi-Fi connections do not require a username or SMTP server. Bluetooth might require a PIN, and Wi-Fi will almost always require a passcode. Exchange connections require a username and password but no SMTP server. Exchange Server acts as the incoming and outgoing mail server.

2. **C.** After you enter the correct SSID, you enter the passcode (or passphrase) for the network. POP3 has to do with configuring an email account. If you have already entered the SSID, then you should be within range of the wireless access point (WAP). Scanning for networks is the first thing you do when setting up a Wi-Fi connection.

3. **D.** Mobile hotspot technology (sometimes referred to as Wi-Fi tethering) allows a mobile device to share its Internet connection with other Wi-Fi-capable devices. Another possibility would be USB tethering, but that is done in a wired fashion. NFC, which stands for near-field communication, is a technology that allows two mobile devices to send information to each other when they are in close proximity. Airplane mode disables all wireless connectivity, including (but not limited to) cellular, Wi-Fi, and Bluetooth. IMAP is another email protocol similar to POP3.

4. **A.** International Mobile Subscriber Identity (IMSI) or an IMSI ID is used to identify the user of a device. IMEI, which stands for International Mobile Equipment Identity, identifies the phone used. In other words, the IMEI ID identifies the device itself. S/MIME (Secure/Multipurpose Internet Mail Extensions) is used for authentication and message integrity and is built into some email clients. In other words, it is used to encrypt email. Virtual private network (VPN) technology is used to make secure connections by tunneling through the provider's radio network.

5. **C.** PC users need iTunes to synchronize contacts and other data from an iPad to a PC. You can also use the new Apple Devices app to do this as well. While Gmail can work to synchronize contacts,

it is completely based on web storage; nothing is actually stored on the iPad. Google Play is a place to get applications and other items for Android. Sync Center is a Control Panel utility that enables synchronization across Windows devices.

6. **B.** Mobile device management (MDM) allows a person to centrally administer many mobile devices from a single workstation. The Global Positioning System (GPS) is a satellite-based navigation system that allows a mobile device to help you find your way to wherever it is you want to go. Location services is a more generic term that means any and all services that help to locate a mobile device and provide mapping information to apps. Secure Sockets Layer/Transport Layer Security (SSL/TLS) is a secure communication protocol that encrypts data sent between devices on the Internet to keep it private and secure.

7. **A and D.** CompTIA lists the Bluetooth connection process in the following order: Enable Bluetooth, enable pairing, find a device for pairing, enter the appropriate PIN code, and finally, test connectivity.

8. **D.** The secure port for POP3 email connections that make use of SSL/TLS is 995. Port 110 is the POP3 default non-encrypted port. Ports 465 and 587 are the secure port numbers for SMTP. Port 993 is the secure port number for IMAP.

9. **D.** Bring your own device (BYOD) is a policy governing employees bringing personally owned devices (laptops, smartphones, and the like) to the workplace and the use of those devices to access company data. Choose your own device (CYOD) is policy where an organization allows employees to select the mobile devices they would like to use, typically from a limited number of company-approved options. With a corporate-owned personally enabled (COPE) policy, the business owns and pays for the mobile devices. This model allows employees to use company-owned devices for both work and personal use. The BYOD, CYOD, or COPE policies should address how data and corporate-owned applications will be handled when employees are hired,

terminated, quit, or retire. The fifth generation of cellular, 5G, is known as the ITU IMT-2020 standard and has data transfer rates of up to 20 gigabits per second (Gbps).

Kudos for your time and effort in reaching the end of Domain 1.0: Mobile Devices! Take some time to review this chapter and then review the entire first domain (Chapters 1 through 3) before you move on to Domain 2.0: Networking.

This part of the journey may be over, but the adventure continues!

Core 1 (220-1201)

Domain 2.0: Networking

CHAPTER 4 TCP and UDP Ports and Protocols

CHAPTER 5 Wireless Technologies

CHAPTER 6 Networked Hosts

CHAPTER 7 Network Configuration Concepts

CHAPTER 8 Network Devices

CHAPTER 9 SOHO Network Configuration

CHAPTER 10 Network Types

CHAPTER 11 Networking Tools

Chapter 4

TCP and UDP Ports and Protocols

This chapter covers the following A+ 220-1201 exam objective:

- **2.1** – Compare and contrast transmission control protocol (TCP) and user datagram protocol (UDP) ports, protocols, and their purposes.

We're back. Welcome to Domain 2.0: Networking. Knowing how to build computers and configure mobile devices is all well and good, but if they can't communicate with each other, very little gets done. That means you, as the technician, should have a good understanding of networking connections between computers on the local area network (LAN) and over the Internet. This chapter and the seven that follow will set the foundation for your networking knowledge.

This first networking chapter discusses the TCP/IP ports and protocols that you should know for the exam (for example, Domain Name System [DNS] on port 53). To prepare for this objective, we'll discuss the differences between TCP and UDP, why you would use each, and which protocols use them. Then we'll get into individual protocols such as FTP, HTTP, RDP, and many more. These protocols are at the core of network communications between computers. And now, it's time to dive into the first of the networking objectives.

ExamAlert

Objective 2.1 concentrates on the following concepts: ports and protocols such as FTP, SSH, Telnet, SMTP, DNS, DHCP, HTTP, POP3, IMAP, NetBIOS/NetBT, LDAP, HTTPS, SMB/CIFS, and RDP. It also covers the differences between TCP and UDP.

Note

It's imperative that you know this section—for the exam and for the real world. You need to know more than the acronyms and port numbers; you also need to understand how the protocols work in real-world scenarios with real hardware and software. We'll try to incorporate these "use cases" as often as possible.

TCP vs. UDP

Network sessions on an IP network are normally either TCP or UDP sessions. Let's briefly discuss these two.

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 will ask the sending computer to transmit the packet again.

TCP establishes network connections with a *three-way handshake*, a process that includes three steps:

1. **SYN:** The client computer attempts to initiate a session to a server with a synchronize packet of information. (This is known as a SYN packet.)
2. **SYN + ACK:** The server responds to the client request by sending a synchronize/acknowledgment packet. (This is known as a SYN-ACK packet.)

3. **ACK:** The client sends an acknowledgment packet to the server. (This is known as an ACK packet.)

Once the server receives that ACK packet, it acknowledges the session, and the network connection is established. This is also known as a *TCP socket connection*. With TCP, the synchronization, acknowledgment, and sequencing of packets guarantee delivery. Not a single packet is left behind! In addition, TCP uses a method known as *flow control*, which prevents a sender from overwhelming a server by sending too many packets too quickly.

User Datagram Protocol (UDP) sessions are known as *connectionless sessions*. One example of UDP usage is with streaming media sessions. With UDP, if a packet is dropped, it is not asked for again. Let's say you are listening to some streaming music, and you hear a break in the song or a blip of some kind. That indicates some missing packets, but you wouldn't want those packets back because by the time you get them, you would be listening to a totally different part of the music stream! Unlike TCP, UDP does not use a handshake process or flow control. It's expected that you might lose packets in UDP streams but not when making TCP connections.

Both TCP and UDP utilize protocols and ports to make connections. Let's further discuss these protocols and ports now.

Ports and Protocols

Computers use many ports and protocols to transmit information. The protocol used is based on the type of data being transmitted and the application being used. We'll begin with HTTP and HTTPS.

HTTP vs. HTTPS

For two computers to communicate, they must both use the same protocol. For an application to send or receive data, it must use a particular protocol designed for that application, and it must open a port on the network adapter to make a connection to another computer.

For example, let's say you want to visit a website. You type the name of that website into the address bar of a web browser, and one of two protocols will be initiated: HTTP or HTTPS. Take a look at Table 4.1.

TABLE 4.1 **Comparing HTTP and HTTPS**

Protocol	Full Name	Default Port Number
HTTP	Hypertext Transfer Protocol	80
HTTPS	Hypertext Transfer Protocol Secure	443

HTTP and HTTPS both use TCP as their connection mechanism. HTTP was used for decades, but its use has been reduced drastically in favor of the more secure HTTPS. For security reasons, most websites that you connect to today use HTTPS. Primarily, HTTPS is designed to keep a user's information private and to prevent tampering and eavesdropping. Try connecting to some of your favorite websites and identify which protocol is being used. Most of them should use HTTPS, and those that are not should be avoided.

Let's say you open a web browser and connect to a website by typing **example.com**. When you do so, the address is automatically changed to example.com. (If you can't see the full web address and the HTTPS protocol, simply click on the domain name you typed.) That domain is configured to use HTTPS for security. HTTPS is the protocol that makes the connection to the example.com web server. The HTTPS protocol selects an unused port on your computer (known as an *outbound port*) to send and receive data to and from example.com. On the other end, the example.com 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 the HTTPS protocol. This is known as an *inbound port*. Figure 4.1 illustrates this.

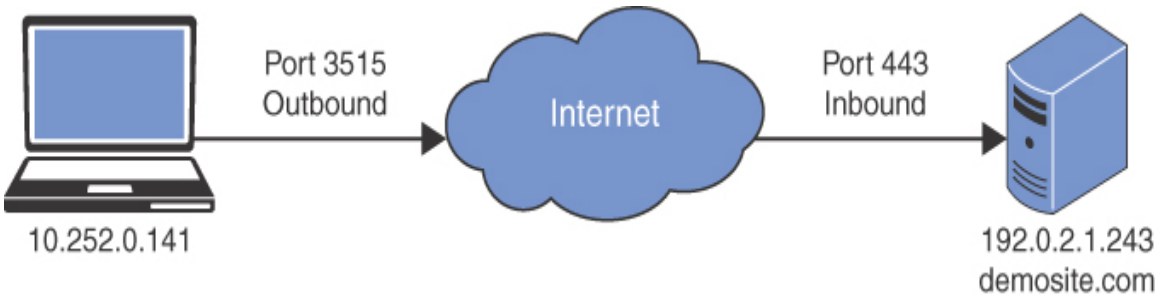


FIGURE 4.1 **HTTPS in Action**

The local computer on the left in Figure 4.1 has been given the IP address 10.252.0.141. This is a private internal address. It uses port 3515 to go out to the Internet and start a session with demosite.com. For security purposes, this is a dynamically assigned port and will be different every time you connect to another web server, but it will normally be somewhere in the thousands. The session is accepted by demosite.com's web server, using the public IP address 216.97.236.245 and inbound port 443. Conversely, if you want to run your own web server at home and sell widgets and such, that web server needs to have port 443, or the less secure port 80, open to the public at all times. If it were ever closed, you would lose sales! Computers that connect to your web server would use dynamically assigned ports.

HTTPS is used by the majority of websites today. It is recommended because of the secure connection it makes—which it does via a secure protocol such as Transport Layer Security (TLS) and using an encrypted certificate. We'll discuss this process more in Chapters 43 through 52, which focus on security.

ExamAlert

Use HTTPS for web servers whenever possible—usually on port 443. Also remember that HTTPS is connection oriented (as it uses TCP).

Email Protocols

For people who share written communications with each other, email protocols are a must. Email is sometimes accomplished using a web browser (HTTPS) or within an app that works in the same manner. This is great for home users and for small businesses. However, for larger organizations using desktop computers, or if you simply need to connect directly to specific email servers, you'll have to configure email protocols. When setting up an email client, you might need to know the protocols and

ports involved. Email can be sent and received, so you will have to configure an outbound server and an inbound server—which could be one and the same. Generally, the outbound server will use SMTP, and the inbound server will use either POP3 or IMAP:

- **SMTP:** Simple Mail Transfer Protocol sends email. When you send email from the email client, it goes to an SMTP server and is then sent off to its destination. The email server could be at an Internet service provider (ISP) or could be supplied by the organization you work for, and it could be either in-house or in the cloud. A good way to remember this acronym is by using the mnemonic device *Send Mail To People*. The original default port for SMTP was 25, but to make use of an SSL- or TLS-encrypted session, you would use either port 587 or port 465, depending on the type of encryption used and which protocol your ISP or administrator has (or *you* have) selected.
- **POP3:** Post Office Protocol Version 3 is very common and is used by email clients to retrieve incoming email from a mail server. The original POP3 server port was 110, but for secure transmissions, the default port is 995.
- **IMAP:** Internet Message Access Protocol is an email protocol that enables messages to remain on the email server so they can be retrieved from any location. IMAP also supports folders, so users can organize their messages as desired. IMAP email servers used port 143 for many years, but for secure transmissions, they use 993 by default.

ExamAlert

Know your secure ports! SMTP uses 587 or 465, POP3 uses 995, and IMAP uses 993.

On the client side, you must specify the server name and the correct ports for both the sending and receiving of email. The protocols and ports must exactly match the configuration of the email server(s). Email clients include Outlook, Mozilla Thunderbird, and a host of others. You can also use the Gmail application to connect to separate accounts using these protocols.

On the server side, several options are available; for example, Microsoft Exchange can handle SMTP, POP3, and/or IMAP, as well as HTTPS connections from web browsers and from mobile devices, by using Exchange ActiveSync, which is part of Exchange Online. Configuration of email servers is beyond the scope of the A+ exams.

FTP, SSH, and Telnet

If you need to communicate with an external host to send and receive files and/or run commands on the external host, you might be interested in FTP or SSH. Telnet, on the other hand, is deprecated, because it is insecure, and should be avoided. This is what you need to know about these protocols:

- **FTP:** File Transfer Protocol allows computers to transfer files back and forth. When you connect to an FTP server, that FTP server has port 21 open. Some type of FTP client software is necessary to connect to the FTP server; this could be done in the command line within the FTP shell or by using a GUI-based application (such as FileZilla). However, default FTP is not considered secure today. Instead, organizations usually prefer SFTP (discussed in the next bullet), or FTP Secure (FTPS), which uses SSL/TLS and utilizes ports 989 and 990. So far, all the FTP options listed here have been connection oriented. But Trivial File Transfer Protocol (TFTP), which is commonly used for booting a system from a network, is connectionless.

  Note

  The exam objectives list FTP port 20. Historically, after connecting to an FTP server on port 21, a client would use port 20 for the actual data transfer. That is still possible, but today, most FTP client programs randomly and dynamically assign ports for data transfer.

- **SSH:** Secure Shell enables the remote control of computers and enables data to be exchanged between computers on a secured channel. This

protocol offers a more secure replacement to FTP and Telnet. To access a Secure Shell server, the server must have port 22 open. There are additional protocols that use SSH as a way of making a secure connection. One of them is the commonly used Secure FTP (SFTP). As mentioned, regular FTP can be insecure. SFTP provides file access over a reliable data stream that is generated and protected by SSH. Other protocols that "ride" on SSH include SCP and rsync. SSH is an example of a connection-oriented protocol that uses TCP.

- **Telnet:** Short for Telecommunication network, Telnet provides remote access to other hosts using the command-line interface (CLI). It uses port 23 but is an insecure and somewhat deprecated protocol. However, because some companies *might* still use it to access routers and other hosts, and to test and manage network connectivity, you might see a question about it on the exam. Generally, Telnet is disabled, if it even exists, in the OS. If you are wondering if it is enabled in Windows, you can do a quick check for it in the Services console window (**Run > services.msc**). If it is not listed, then it is not enabled. It can be enabled or disabled in the **Turn Windows features on or off** window. (By default, only the Telnet client is listed in Windows.)

DHCP

Dynamic Host Configuration Protocol (DHCP) is used to automatically assign IP addresses to hosts. These hosts could be computers, printers, servers, routers, and so on. In most small office/home office (SOHO) networks, a router uses DHCP to assign IP addresses to the client computers. However, your ISP will also use DHCP to assign an IP address to you; usually your router gets this. Finally, small-to-midsized businesses (SMBs) and enterprise organizations alike use DHCP—often implemented as a separate server.

The DHCP service makes life easier for a network administrator by automatically assigning IP addresses, subnet masks, gateway addresses, DNS servers, and so on from a central location. If you get your address from a DHCP server, you are getting your address assigned dynamically, and it could change periodically. The reason is that a lease is attached to the IP address, which only lasts for a certain amount of time (a month, a week,

or even less). Computers that obtain IP addresses from a DHCP server have the advantage of automatically getting new addressing when they are moved to a different network segment. However, some computers require a static address—one that is assigned by a network administrator manually. It is better in many situations for servers and printers to use static addresses so you know exactly what the address is and so it won't change.

By default, in a typical IPv4 network, the DHCP server needs to have inbound port 67 open, and a DHCP client uses port 68 to connect out to that DHCP server. We would refer to such a DHCP server as a "DHCPv4" server. (DHCPv6 servers use port 547, and clients use port 546. We'll discuss the differences between IPv4 and IPv6 later in the book.) DHCPv4 servers are connectionless, which means they use UDP as the main transport protocol. By the way, DHCP is also sometimes referred to as *BOOTP*—short for Bootstrap Protocol.

ExamAlert

Typical DHCPv4 servers use port 67 and clients use port 68. Remember that DHCP is considered connectionless (because it uses UDP).

We'll discuss DHCP further in Chapter 7, "Network Configuration Concepts."

DNS

Domain Name System (DNS) is the group of servers on the Internet that translates domain names to IP addresses. For instance, a domain name such as *example.com* might translate to the IP address 93.184.216.34. When you connect to a website by name, the DNS server takes care of resolving the name to the IP address so that your computer and the web server can communicate via IP. To find out the DNS server that your Windows computer talks to, type the command **ipconfig /all** in the Command Prompt, and you will see the IP address of that DNS server.

A DNS server has inbound port 53 open by default. We'll discuss DNS servers further in Chapter 6, "Networked Hosts," and in Chapter 7.

LDAP

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 Active Directory (AD), and also directory services or domain services. It includes the user accounts, computer accounts, groups, and the authentication and permissions involved with those accounts—collectively known as a Windows domain. To implement a Windows domain, at least one Windows server must be promoted to a domain controller. When you do this, LDAP is installed and runs on inbound port 389 by default. A more secure version of LDAP (Secure LDAP) runs on port 636.

ExamAlert

Remember that LDAP is a protocol used to access and query compliant directory services systems, such as Microsoft Active Directory. It uses port 389 for unencrypted communication and port 636 for encrypted communication.

RDP

To facilitate connections to remote computers and allow full remote control, Microsoft uses the Remote Desktop Connection program, which is based on Remote Desktop Protocol (RDP).

RDP works in three ways. First, users can be given limited access to a remote computer's applications (such as Word or Excel). Second, administrators can be given full access to a computer so that they can troubleshoot problems from another location. Third, another part of the program, known as Remote Assistance, allows users to invite a technician to view their desktops in the hopes that the technician can fix any

encountered problems. These invitations can be made via email. The RDP port, 3389, is also used by Remote Desktop Services, which is the server-based companion of Remote Desktop Connection.

Figure 4.2 shows the results of running a **netstat** command on a Windows server. You can see that port 3389 is open, which allows for remote control of the server (which is exactly what the figure shows happening). Inbound port 389 is also open, indicating that LDAP is running and that the server is indeed a domain controller.

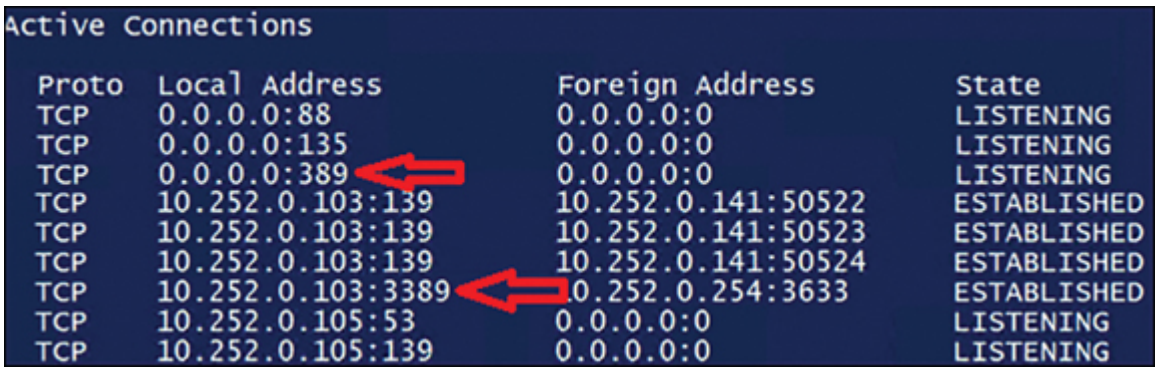


FIGURE 4.2 **LDAP and RDP Ports on a Windows Server**

More Protocols and Ports

There are a few more protocols that you should know for the exam, including SMB/CIFS and SNMP:

- **SMB:** The Server Message Block protocol provides access to shared items such as files and printers. These are actual packets that authenticate remote computers through what are known as interprocess communication (IPC) mechanisms. They can communicate directly over TCP using port 445 or by working with the legacy NetBIOS/NetBT protocol using a port between 137 and 139. In the past, SMB was also referred to as the Common Internet File System (CIFS) protocol.
- **SNMP:** Simple Network Management Protocol is used as the standard for managing and monitoring devices on a network. It is used to manage routers, switches, UPS devices, and computers and is often incorporated

in 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 the NMS to monitor those managed devices and alert the SNMP manager software—and ultimately the administrator. If there is an alert to be sent to an administrator, it is known as a trap. SNMP by default uses port 161, and SNMP traps use port 162. SNMPv3 is the latest and most secure version of SNMP and allows for the use of strong cryptographic algorithms, such as HMAC-SHA, HMAC-MD5, and AES, to ensure data integrity and confidentiality.

Wow, that was a mouthful of acronyms. Study them and their port numbers! Use Table 4.2 to help. You will note that there are secure versions of some of the protocols and that each uses a different port number than the insecure version. You will also see in this table whether a protocol rides on TCP, or UDP, or both. The protocol name is listed in the first column, but the table is sorted by port number for easier reference.

TABLE 4.2 **Protocol and Port Listing**

Protocol	Original Port	Secure Port	TCP/UDP Usage
FTP	20–21	989/990	TCP
SSH	22	22	TCP or UDP
Telnet	23	Not considered a secure protocol	TCP or UDP
SMTP	25	587 or 465	TCP
DNS	53		TCP or UDP
DHCP	67 (server) 68 (client)		UDP
HTTP	80	443 (HTTPS)	TCP

Protocol	Original Port	Secure Port	TCP/UDP Usage
POP3	110	995	TCP
NetBIOS/NetBT	137–139		TCP or UDP
IMAP	143	993	TCP
LDAP	389	636	TCP or UDP
SMB/CIFS	445		TCP
RDP	3389		TCP or UDP

ExamAlert

Know your protocols/ports and their functions for the exam! Write 'em down or make flash cards to commit them to memory.

Note

There are 65,536 ports, but you only need to know a handful of them for the exam. If you want to find out about more of them, check out the complete list provided by the Internet Assigned Numbers Authority (IANA): https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml.

Cram Quiz

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

1. Which protocol uses port 22?

- **A.** FTP
- **B.** Telnet
- **C.** SSH
- **D.** HTTPS

2. Which of these would be used for streaming media?

- **A.** TCP
- **B.** RDP
- **C.** UDP
- **D.** DHCP

3. Which ports are used by the IMAP protocol?

- **A.** 53 and 68
- **B.** 80 and 443
- **C.** 110 and 995
- **D.** 143 and 993

4. A user can receive email but cannot send any. Which protocol is not configured properly?

- **A.** POP3
- **B.** FTP
- **C.** SMTP
- **D.** SNMP

5. Which of the following is the default inbound port of a DHCPv4 server?

- **A.** 67
- **B.** 22
- **C.** 995

- **D.** 3389

6. Which of the following does HTTPS use to make a secure Internet connection?

   - **A.** Hypertext Transfer Protocol
   - **B.** SNMP
   - **C.** SNMPv3
   - **D.** TLS

Cram Quiz Answers

1. **C.** SSH (Secure Shell) uses port 22. FTP uses port 21, Telnet uses port 23, and HTTPS uses port 443.

2. **C.** User Datagram Protocol (UDP) is used for streaming media. It is connectionless, whereas TCP is connection oriented and not a good choice for streaming media. RDP, which stands for Remote Desktop Protocol, is used to make connections to other computers. DHCP, which stands for Dynamic Host Configuration Protocol, is used to assign IP addresses to clients automatically. Don't forget: DHCP is connectionless and uses UDP, too!

3. **D.** Internet Message Access Protocol (IMAP) uses port 143 by default and port 993 as a secure default. DNS uses port 53. DHCP uses port 68. HTTP uses port 80. HTTPS uses port 443. POP3 uses ports 110 and 995 as a secure default. Know those ports!

4. **C.** Simple Mail Transfer Protocol (SMTP) is probably not configured properly. It deals with sending mail. POP3 receives mail. FTP sends files to remote computers. SNMP is used to manage networks.

5. **A.** The default inbound port of a DHCPv4 server is 67 (and clients use port 68 outbound). Port 22 is the inbound port of an SSH server. Port 995 is the secure inbound port of a POP3 server. Port 3389 is the default inbound port of a server that is running RDP.

6. **D.** HTTPS uses port 443 and is used by the majority of websites today. It is recommended because of the secure connection it makes—which it does via a secure protocol such as Transport Layer Security (TLS) and using an encrypted certificate. Hypertext Transfer Protocol (HTTP) uses port 80. It is not secure and sends data in plain text over the Internet. Simple Network Management Protocol is used as the standard for managing and monitoring devices on a network. SNMPv3 is the latest and most secure version of SNMP and allows for the use of strong cryptographic algorithms, such as HMAC-SHA, HMAC-MD5, and AES, to ensure data integrity and confidentiality.

Another chapter done! Memorize those protocols and port numbers, take a quick breather, and move on!

Chapter 5

Wireless Technologies

This chapter covers the following A+ 220-1201 exam objective:

- **2.2** – Explain wireless networking technologies.

Welcome back! Sometimes you will wire computers to the network, and other times—perhaps more often—you will use wireless. Wireless takes the cable out of the mix and allows for mobility and ease of use. But we caution you: The air is shared! So, when planning your wireless technologies, especially Wi-Fi, you have to take into account such things as frequencies, desired data transfer rates, distance between devices, and much more. This is a shorter chapter, but it is chock full of technical information.

In this chapter, we'll discuss the IEEE 802.11 wireless protocols and some other wireless standards available for mobile devices. Bluetooth and NFC are also listed in the CompTIA objective, but we covered them previously in Chapter 2, "Mobile Device Accessories and Connectivity Options," and Chapter 3, "Mobile Device Network Connectivity and Application Support." Make sure you know them. Here we go!

ExamAlert

Objective 2.2 focuses on the following concepts: 802.11 standards (a, b, g, n, ac, ax, and be), frequencies/bands, channel selection/widths, Bluetooth, NFC, and RFID.

802.11 Wireless

To standardize *wireless LAN (WLAN)* communications—also known as Wi-Fi—the Institute of Electrical and Electronics Engineers (IEEE) developed the 802.11 series of protocols. The 802.11 standard defines the various speeds, frequencies, and protocols used to transmit data over radio waves in small geographic areas using unlicensed spectrums.

There are several different 802.11 derivatives you need to know for the exam: 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ax, and 802.11be. Table 5.1 shows these technologies and the characteristics that differentiate them.

TABLE 5.1 **802.11 Standards**

802.11 Version	Maximum Data Rate	Frequency
802.11a	54 Mbps	5 GHz
802.11b	11 Mbps	2.4 GHz
802.11g	54 Mbps	2.4 GHz
802.11n (Wi-Fi 4)	600 Mbps	5 and/or 2.4 GHz
802.11ac (Wi-Fi 5)	3.5 Gbps	5 GHz
802.11ax (Wi-Fi 6)	9.6 Gbps	5 and 2.4 GHz
Wi-Fi 6E (an extension of Wi-Fi 6)	5.4 Gbps	6 GHz
802.11be (Wi-Fi 7)	46 Gbps	2.4 GHz, 5 GHz, and 6 GHz

Note

The data rates in Table 5.1 are potential maximums. Typical numbers will be less and are limited by factors such as bandwidth,

interference, and the distance of a wireless device from the transmitter.

ExamAlert

Know the frequencies used for each of the 802.11 versions! Remember that 802.11n and 802.11ax can use either the 2.4 GHz or 5 GHz bands and 802.11ac uses only the 5 GHz band. 802.11be uses 2.4, 5, or 6 GHz bands.

Note

As of this writing, 802.11bn (dubbed Wi-Fi 8) is currently under development. It's designed to improve the reliability of Wi-Fi, with a main focus on service availability and delay guarantees.

One thing we left out of the table is coverage, or distance. It is difficult to put an exact number on the maximum wireless transmission distances for each standard because it depends on the signal strength of the WAP's antenna, the use of additional features, and environmental factors such as obstructions and interference. But generally, the wireless range from WAP to client increases with each standard listed in the table.

Note

New technologies being developed as of the writing of this book use higher frequency ranges and can transmit much more data per second. Always be on the alert for emerging networking technologies! You can keep up with advances in wireless technologies by visiting The Wi-Fi Alliance at https://www.wi-fi.org.

The data transfer rates of newer wireless network technologies are increased using a concept known as *multipath propagation*. This occurs when an antenna (or antennas) receives radio signals on two or more paths. A common example of this is multiple-input, multiple-output (MIMO) technology, which is incorporated into 802.11n, ac, ax, and be wireless networks. For example, a typical 802.11ac wireless device uses three or four antennas; the 802.11ac, ax, and be standards comply with multiuser MIMO (or MU-MIMO), which can have four simultaneous downlinks. The latest Wi-Fi standard Wi-Fi 7 (802.11be) enables multiple devices to both transmit and receive data simultaneously. This dramatically increases network capacity compared to the previous Wi-Fi standards; in fact, Wi-Fi 7 supports 16×16 MU-MIMO, doubling the spatial streams (the technology that uses multiple antennas) compared to Wi-Fi 6.

Depending on the frequency used, different channels can be utilized by the average home or company. We touched on these previously, but let's summarize them in Table 5.2 and then look more closely.

TABLE 5.2 **2.4 GHz and 5 GHz Channels**

Frequency	Typical Channels	Example
2.4 GHz	1 through 11	802.11g
5 GHz	36, 40, 44, 48, 149, 153, 157, 161, 165	802.11ac and 802.11ax

Note

Although it's not listed in Objective 2.2, we suggest you also look into 6 GHz. It has a larger frequency width and the potential to offer more channels than 5 GHz. As of the writing of this book, the 802.11ax standard can also use the 6 GHz range, but it must be with compatible Wi-Fi *6E* devices.

Let's take it to the next level. More accurately, 2.4 GHz, 5 GHz, and 6 GHz are frequency *ranges*. The exact range for these will vary from one country to the next. For example, the range for 2.4 GHz Wi-Fi in the United States

is between 2.412 GHz and 2.462 GHz, broken up as channels 1 through 11—each spaced 5 MHz apart from the next. When you set up a 2.4 GHz Wi-Fi network, it has a *channel width* associated with it. By default, this is often 20 MHz—an amount that spans multiple channels. We therefore usually recommend placing wireless networks (and access points) on separate channels that are distant from each other. In the United States, the 2.4 GHz nonoverlapping channels are 1, 6, and 11. For example, one Wi-Fi network could be on channel 1 (2.412 GHz), and the next could be on channel 6 (2.437 GHz), which allows for 25 MHz of space—which in most cases is more than enough to avoid interference.

Channel selection is a critical aspect of configuring a Wi-Fi network to ensure optimal performance and minimal interference. Selecting the right channel reduces overlap with neighboring networks and improves the quality and stability of the wireless connection. This is especially important in environments with many competing Wi-Fi signals, such as apartment complexes or office buildings. When setting up a wireless access point (WAP), start by conducting a wireless site survey using tools like Wi-Fi analyzers to identify less crowded channels in your frequency band. For 2.4 GHz networks, prioritize nonoverlapping channels like 1, 6, or 11 in the United States. In the case of 5 GHz networks, which offer more channels, select channels that are sufficiently separated to avoid overlap, particularly when using channel bonding for higher data rates. Proper channel selection ensures that your Wi-Fi network operates in a "clear space," enhancing speed, reliability, and user satisfaction.

To increase data rates, you can increase the channel width on many routers to 40 MHz for 2.4 GHz networks and up to 80 MHz for 5 GHz networks. This is known as *channel bonding*. As you can guess, the chance for interference increases as well, so this notion can be risky. If we used 40 MHz channel bonding with our previous example, we would have interference from one Wi-Fi network to the next. Channel 6 is too close to channel 1 in this case. We would need to go to at least channel 9 (2.452 GHz) to avoid overlapping of the two Wi-Fi networks. The same goes for 5 GHz Wi-Fi networks. For example, channel 36's center frequency is actually 5.180 GHz. Channel 40 is 5.200 GHz. That is 20 MHz of channel width. If we wanted a separate Wi-Fi network on each of those channels, it would work fine by default, but if we wanted to perform channel bonding,

then we would have to select another channel, such as channel 149 (5.755 GHz), which would allow for 40 or 80 MHz channel bonding and, possibly, higher data rates.

Note

All the wireless frequencies and channels that we have discussed so far are *unlicensed*. This means that anyone can use them, and they are not reserved for any government or organizational entity.

But air is free, right? So, we should perform a wireless site survey and identify other companies' and homes' Wi-Fi networks that are nearby. They could be using channels that are too close and cause interference. A *Wi-Fi analyzer* program is the best way to go when it comes to seeing who is using which frequencies and then selecting frequencies that you can use (even with channel bonding) without causing overlap and interference. Vendors develop these programs for Windows, Android, and iOS. A Wi-Fi analyzer makes it easier for a person to discern where Wi-Fi networks exist in a given frequency range by showing the information in a graphical format, such as a chart or something similar. It also shows the strength of the signal of each network. All this information can help you decide on the right channel to use when you are performing your wireless site survey.

ExamAlert

Don't stand so close to me! Seriously, make sure your selected Wi-Fi channel is in its own "space" by investigating the airwaves with a Wi-Fi analyzer.

Long-Range Fixed Wireless

The term *long-range fixed wireless* has no formal definition. However, we could apply it to any wireless technology that can send data more than 100 meters (or so) and uses equipment that is stationary, or "fixed."

One example of fixed wireless would be a small office or home office that purchases a fixed wireless Internet plan from a communications provider, or *wireless Internet service provider (WISP)*. Such a plan requires the use of a capable device that is mounted in a fixed position to the building or the home. This type of plan is common in rural areas that do not have broadband Internet access and is also used in mobile home parks, assisted living facilities, and other areas where service providers may have a difficult time laying fiber-optic and/or coaxial cable due to environmental factors. Due to recent rule changes, such plans are also seen more in metropolitan areas as well.

Some long-range fixed wireless services use unlicensed frequency ranges (or bands), such as 900 MHz, 1.8 GHz, 2.4 GHz, and 5 GHz. Other services make use of licensed frequencies, some of which may use the UHF band (300 MHz to 3 GHz) and the Local Multipoint Distribution Service (LMDS) on the 26 and 29 GHz bands. Licensed frequencies have the potential for better quality of service (QoS) and higher Internet speeds.

In general, a long-range fixed wireless device requires power from the electrical grid (public utilities) as opposed to other mobile access points that are powered by batteries. In the United States, the Federal Communications Commission (FCC) oversees regulations for the use of fixed wireless technology, including frequency bands that can be used, types of antennas that are allowed, and how those antennas distribute signals.

ExamAlert

A WISP is an Internet service provider (ISP) that uses wireless technology to connect subscribers to the Internet. WISPs use technologies like fiber, Wi-Fi, and fixed wireless to provide Internet access to homes and businesses. They may also use proprietary equipment that operates on different frequency bands.

RFID

Radio-frequency identification (RFID) is a wireless technology used to read information that is stored on tags that can be attached to, or embedded in, just about anything. They are used in many industries and have many uses, such as access control, commerce, advertising, manufacturing, agriculture, and so on.

For example, RFID tags can be used in a retail store to help with the tracking of inventory and protection from theft. Tags are attached to clothing or other items and are read by an RFID reader as part of the checkout process. After a customer pays for an item, the RFID reader deactivates the item's tag. To detect cases of customers failing to pay for items, an RFID detector placed at the entrance/exit reads tags and sends alerts. These readers and detectors must be nearby, but not necessarily within line of sight, which is an improvement over a basic barcode system. In addition, an RFID tag can hold a lot more information and can be programmed, if necessary. For readers that can track items over larger distances—beyond close proximity—an active RFID system would be necessary, where the reader is AC powered.

When it comes to computers, networks, and authentication, RFID plays a vital role. For instance, as part of an access control solution, RFID tags are used as ID badges—proximity cards, dongles, and so forth—and can take the place of older and less secure magnetic stripe cards. Entrances to a building, specific offices, server rooms, data centers, and so on can be equipped with RFID readers. Simply placing an RFID badge on or near the reader activates the reader so it can verify the ID of the employee. Of course, badges can be stolen; that's why a second factor of authentication is common, such as a passcode, which we will discuss in the security chapters. RFID is also present in smartphones and some other computing devices. Many smartphones are furnished with NFC, which is actually a subset of RFID. These readers are often locked down so that they can only read tags from a certain manufacturer or for a specific purpose.

That closes out this section on the electromagnetic spectrum. Transmission of data over radio waves can be done in many ways. Be sure to know the basics of each technology discussed in this chapter.

ExamAlert

RFID (radio-frequency identification) is a technology that uses radio waves to automatically identify and track objects or people. RFID systems consist of RFID tags, which are small electronic devices containing a unique identifier, and RFID readers or antennas, which are used to read the information stored on the tags.

Cram Quiz

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

1. Which of the following would a company most likely use for authentication to a server room?

   - ○ **A.** 802.11ac
   - ○ **B.** Fixed wireless
   - ○ **C.** RFID
   - ○ **D.** MIMO

2. Which standard can attain a data transfer rate of 1 Gbps over a wireless connection?

   - ○ **A.** 802.11a
   - ○ **B.** 802.11b
   - ○ **C.** 802.11g
   - ○ **D.** 802.11ac
   - ○ **E.** 802.3ab

3. Which of the following is often broken down into groups of channels including 1–5, 6–10, and 11?

   - ○ **A.** 802.11ac

- **B.** 2.4 GHz
- **C.** 5 GHz
- **D.** 802.11a

4. You are servicing a customer with a cable broadband Internet connection and an 802.11ac wireless network that is experiencing interference from a nearby office. The customer's WAP is mounted to the ceiling. Which of the following is the easiest and best solution?

- **A.** Move the wireless access point to another location.
- **B.** Reconfigure the WAP to use 2.4 GHz instead of 5 GHz.
- **C.** Change the broadcasting channel on the WAP to one that is not used by any neighbors.
- **D.** Recommend a long-range fixed wireless service.

5. Which wireless system is composed of readers and tags and can be used for access control, commerce, advertising, manufacturing, and agriculture?

- **A.** 802.11ax
- **B.** Wi-Fi 6
- **C.** RFID
- **D.** FCC

6. Which of the following allows multiple devices to both transmit and receive data simultaneously, dramatically increasing network capacity compared to previous standards? (Select all that apply.)

- **A.** 802.11be
- **B.** Wi-Fi 7
- **C.** Wi-Fi 6
- **D.** WISP

Cram Quiz Answers

1. **C.** Radio-frequency identification (RFID) is commonly used for access to areas of a building such as a server room. It is often implemented as a proximity-based ID card or badge. The other options are not usually associated with authentication. 802.11ac is a WLAN (Wi-Fi) standard that runs on 5 GHz and can provide 1 Gbps of data transfer. Fixed wireless is a wireless service that uses a fixed wireless device to provide Internet access to users in a building or a home. MIMO (multiple-input, multiple-output) is a multiple propagation technology used to increase data transfer in 802.11n and 802.11ac wireless networks, which is further enhanced with MU-MIMO in 802.11ax and 802.11be.

2. **D.** 802.11ac (and 802.11ax) can attain speeds in excess of 1 Gbps over wireless. 802.11a and g have a typical maximum of 54 Mbps. 802.11b (rarely used today) has a maximum of 11 Mbps. 802.3ab is the IEEE specification for 1 Gbps transfer over twisted pair cables; it is wired, not wireless (and is also known as 1000BASE-T).

3. **B.** In the United States, the 2.4 GHz frequency range is broken into three categories: Channels 1–5, 6–10, and 11. By placing separate wireless networks on separate distant channels (such as 1 and 11), you can avoid overlapping and interference. 802.11ac and 802.11a are standards, not frequencies. 5 GHz uses channels such as 36, 40, 149, 153, and so on.

4. **C.** The easiest (and best) solution to this scenario would be to change the WAP's broadcasting channel to one that is not used by any neighbors. That would first require a wireless site survey to find out what frequencies are being used. Moving the wireless access point is a potential solution but would require a bit of hands-on work because the WAP is mounted to the ceiling. Reconfiguring the WAP to use 2.4 GHz doesn't ensure a reduction in interference; you would still need to do a wireless site survey to make sure there is no channel overlap, which is actually more likely with 2.4 GHz than with 5 GHz. And if you are doing a

survey anyway, you might as well find an open channel on the 5 GHz band. A long-range fixed wireless service is the most expensive, time-consuming, and difficult solution on the list, and it isn't necessary because the customer already has broadband Internet access!

5. **C.** Radio-frequency identification (RFID) is a wireless technology used to read information that is stored on tags. The IEEE 802.11ax standard, also referred to as Wi-Fi 6, operates using the 2.4 GHz and 5 GHz frequency bands (and 6 GHz for Wi-Fi 6E). In the United States, the Federal Communications Commission (FCC) oversees regulations for the use of fixed wireless technology, including frequency bands that can be used.

6. **A and B.** The latest Wi-Fi standard Wi-Fi 7 (802.11be) allows multiple devices to both transmit and receive data simultaneously. This dramatically increases network capacity compared to the previous Wi-Fi standards; in fact, Wi-Fi 7 supports 16×16 MU-MIMO, doubling the spatial streams (the technology that uses multiple antennas) compared to Wi-Fi 6. A WISP is an Internet service provider (ISP) that uses wireless technology to connect subscribers to the Internet. WISPs use technologies like fiber, Wi-Fi, and fixed wireless to provide Internet access to homes and businesses.

You are doing fantastic! Great job with the chapter. Keep going. There's lots more!

Chapter 6
Networked Hosts

This chapter covers the following A+ 220-1201 exam objective:

- **2.3** – Summarize services provided by networked hosts.

Let's get a little bit deeper into networking. In this chapter, we'll focus mostly on servers. We're referring not only to commonly known servers such as web servers, file servers, and email servers but also servers that provide less-well-known underlying services, such as DHCP servers, authentication servers, and load balancers. This chapter also briefly describes Internet appliances, legacy/embedded systems, and IoT devices. Rock on.

ExamAlert

Objective 2.3 concentrates on the following concepts: server roles (DNS, DHCP, fileshare [file servers], print servers, mail servers, syslog, web servers, AAA servers, database servers, NTP servers), Internet appliances, legacy/embedded systems, and IoT devices.

Server Roles

Servers take care of centralizing data, allowing access to a network, making connections to printers, controlling the flow of email, and much more.

Whatever the role, the concept of the server is to do it in a centralized fashion, reducing the burden on client computers. Regardless of whether a server is in the organization's LAN or in the cloud, it will have the same purpose.

If the data you need is not stored at the local computer, then you look to servers to provide it. In the following sections, we'll discuss the various server roles that you should know for the exam: file servers that provide access to data files of all kinds; web servers that provide websites and e-commerce; email servers that provide a central administration and storage point for email messages; and print servers that provide the ability to print to remote printers. We'll also get a bit more technical and cover some of the essential servers on a midsized to large computer network, including DHCP, DNS, proxy, syslog, and authentication servers.

File Servers/Fileshare

File servers store, transfer, migrate, synchronize, and archive files. Any computer can act as a file server of sorts. All you need to do is create a share on your local system and point remote computers to that share, either by browsing or through a mapped network drive.

A *fileshare* is a shared network location where files and folders are stored, making them accessible to multiple users or systems within a network. Fileshares are commonly set up on file servers or network-attached storage (NAS) devices to centralize file storage and improve collaboration among users.

On a typical Windows client computer, however, those shares are limited in the number of simultaneous connections allowed (usually 20 maximum). So, for larger network environments, you need a real server of some sort. Examples of actual server software include Microsoft Windows Server and the various types of Linux server versions, such as Red Hat Enterprise Linux (RHEL) and Ubuntu Server. Like most other servers, a file server can be a physical box or a virtual machine, and it can be located within the LAN or in the cloud.

Note

You could also purchase or build a network-attached storage (NAS) server, which is a basic box that often contains two or more storage drives and connects directly to the network. A NAS server usually runs some variant of Linux. We'll discuss NAS further in Chapter 15, "Storage Drives."

Web Servers

A *web server* houses the website of an organization. Examples of web servers include Microsoft's Internet Information Services (IIS), which is part of Windows Server, and Apache HTTP Server (for Linux and FreeBSD). Small and midsized companies often host their websites with an external provider. Larger companies might choose to host their websites on web servers physically located in their data centers, though many also choose to use the cloud. An organization's choice usually depends on the resources and human power available.

Print Servers

Print servers are basic servers that take control of multiple printers on the network. All caching of information, spooling, printer pooling, sharing, and permissions are controlled centrally by the print server. While a Windows client computer (or another client) could act as a print server, and you can also purchase a basic print server device that plugs into your network, enterprise-level print servers run software such as Windows Server so that they can handle lots of simultaneous print requests from client computers. A *Windows Server printer server role* refers to a specific role/function on a Windows Server system that allows it to act as a central point for managing and sharing printers across a network. This basically makes it a dedicated print server, where users can access and print to multiple networked printers by connecting to that server.

Mail Servers

Mail servers (or *email servers*) are part of the message server family. When we refer to a *message server*, we mean any server that deals with email, faxing, texting, chatting, and so on. But for the purposes of the A+ exams, we concentrate strictly on the email server. The most common of these is Microsoft Exchange. An Exchange server might run POP3, SMTP, and IMAP, and allow for Outlook and Windows Mail connections via a web browser. That's a lot of protocols running. So, it's not surprising to hear some Exchange admins confess that running an email server can be difficult at times.

For the A+ exams, you should know how to connect a client to an email server such as Microsoft Exchange. This is done by using appropriate email client software (such as Outlook or Windows Mail) and knowing the server name, the protocols and ports used, the username and password, and whether there is additional security involved. For more details about email client configuration, see Chapter 3, "Mobile Device Network Connectivity and Application Support."

Database Servers

Database servers store, manage, and retrieve data for applications and users. These servers are fundamental for handling structured data in environments such as websites, enterprise resource planning (ERP) systems, and customer relationship management (CRM) tools. Examples of popular database management systems include Microsoft SQL Server, Oracle Database, MySQL, and PostgreSQL. Database servers use query languages like Structured Query Language (SQL) to interact with data efficiently. They can also handle large volumes of data and support concurrent access by multiple users or applications. For instance, an e-commerce website might use a database server to track inventory, process orders, and manage customer accounts. Depending on the scale and requirements, a database server can be hosted on-premises, in the cloud, or in a hybrid configuration. Proper database server configuration ensures data security, integrity, and performance.

Proxy Servers

A *proxy server* is used primarily as a go-between for a client and the website accessed. It is commonly used to cache information so that the information exists on the proxy server, and another user accessing the same web page won't have to get it from the Internet; this increases general performance and efficiency. For a client computer to use a proxy server, the web browser needs to be configured properly (as described in Chapter 38, "Windows Networking"). In addition, the proxy server can analyze data as it passes through and filter it accordingly; this is referred to as content filtering. Plus, you can have proxies for FTP, SMTP, and other protocols. There are also proxies that reside on the Internet and are designed to hide users' IP addresses, allowing users to browse the web anonymously. Quite often, organizations block these types of connections.

To protect a web server, an organization might implement a *reverse proxy*. This device is placed in the area of the network where the web server resides. Requests from clients on the Internet are forwarded by the reverse proxy to the web server so that the clients will be unaware of the identity of the web server. Reverse proxies can also be used for encryption of web sessions and for load balancing, where client requests can be distributed to multiple web servers.

ExamAlert

A proxy server is a server that acts as a go-between for a workstation and the Internet. A proxy server typically provides an increased level of security, caching, NAT, and administrative control.

DHCP Servers

Some servers have less tangible—though no less important—duties. For example, the *DHCP server* is in charge of handing out IP addresses to clients. But don't underestimate this function; if an organization has a couple of thousand computers that rely on obtaining IP addresses from a DHCP server, it becomes one of the most important servers on the network. If it fails, computers will have great difficulty doing anything on the network. DHCP server functionality is built into Windows and Linux

servers, SOHO routers, and many other devices. Whenever a device or computer obtains an IP address automatically (dynamically), chances are that a DHCP server was involved. We'll discuss DHCP further in Chapter 7, "Network Configuration Concepts."

DNS Servers

A *Domain Name System (DNS) server* takes care of resolving domain names to IP addresses. For instance:

```
example.com  =  93.184.216.34
```

Try running the **ping** command in the Command Prompt and ping a domain name of your choice, perhaps:

```
ping example.com
```

The results should display the IP address of that domain. This is a basic example of DNS being performed. DNS servers also take care of reverse DNS—or resolving IP addresses to domain names.

In smaller networks, the DNS server is at the ISP. However, larger networks might decide to run DNS servers internally. In fact, it becomes a necessity for a company that has a domain controller because the domain relies on DNS name resolution for just about everything that needs to be accessed. DNS functionality can be implemented in most server operating systems, such as Windows Server or Linux. We'll discuss DNS further in Chapter 7.

ExamAlert

A DNS server resolves hostnames to IP addresses and vice versa.

Syslog Servers

Syslog is a protocol that can take logged event information from a router or other network device and send it to a logging server—also known as a

syslog server. The syslog server uses special software to store these logs in real time and is designed so that administrators can easily read, analyze, and save the information. This information might consist of status, events, diagnostics, entry attempts, and so on. Best of all, administrators can do all this from their workstation, without having to log in to each network device separately. Linux has syslog integrated with the operating system, but there are third-party examples of syslog too, including Kiwi Syslog Server, PRTG, and Syslog Watcher.

ExamAlert

Remember that syslog (system logging protocol) is a standard used to send log messages (system or event) to a syslog server. These events include driver failures, device conflicts, read/write errors, timeouts, and bad block errors.

Network Time Protocol

Network Time Protocol (NTP) is a service that synchronizes the clocks of computers and devices across a network. Accurate timekeeping is essential for logging, authentication, scheduling, and other network functions. Without synchronized clocks, activities like correlating logs between systems or ensuring time-based authentication mechanisms would become unreliable. NTP servers can be set up locally within an organization or accessed from public time servers, such as those maintained by NIST or pool.ntp.org. Most modern operating systems and network devices support NTP, making it a seamless yet critical component of network management. For high accuracy, organizations may deploy dedicated NTP servers synchronized with atomic clocks or GPS time sources. Ensuring accurate time synchronization improves network reliability, security, and overall functionality.

Tip

To change the time server in Windows 11, go to **Settings > Time & Language > Date & Time**. Then toggle Set Time Automatically to **Off** and manually enter the desired time server address in the Additional Settings section; you can also use the Command Prompt to change the time server using **w32tm /config /server:** [*new_time_server_address*].

AAA Servers

In the computer security world, AAA stands for authentication, authorization, and accounting. The terms can be broken down as follows:

- **Authentication:** Establishing a person's identity with proof and confirming it via a system. Typically, this requires a digital identity of some sort, a username/password, security card, biometric data, or other authentication scheme—and hopefully more than one!
- **Authorization:** Giving a user access to certain data or areas of a building. Authorization happens after authentication and can be determined in several ways, including via permissions, access control lists, time-of-day restrictions, and other login and physical restrictions.
- **Accounting:** Tracking data, computer usage, and network resources. Often it means logging, auditing, and monitoring data and resources. Part of this concept is the burden of proof. If it is believed that someone committed an unauthorized action, a security administrator must provide proof that it happened. When you have indisputable proof of something users have done and they cannot deny it, this is known as *nonrepudiation*.

A server can oversee one or more of these security functions.

For example, an *authentication server* acts as a central repository of user accounts and computer accounts on the network. All users in a given network log on to this server. The most common example of this would be a Windows Server system that has been promoted to a domain controller (meaning it runs Active Directory). This type of server validates the users

who attempt to log on. Authentication servers utilize some kind of authentication protocol, such as the Lightweight Directory Access Protocol (LDAP), or Kerberos, or both, as is the case for a Windows domain controller.

One example of a server that oversees the entire AAA family of protocols is a Remote Authentication Dial-In User Service (RADIUS) server. RADIUS servers can act as the backend for WLAN authentication and with port-based network access control protocols such as 802.1X. We'll cover these concepts later in the book.

ExamAlert

Know the differences between file servers (fileshares), web servers, print servers, email servers, proxy servers, DHCP servers, DNS servers, syslog servers, and AAA servers. You might also want to tie in these concepts to the ports that the servers use (see Chapter 4, "TCP and UDP Ports and Protocols").

So, there's a little primer on servers. The server is the home of the system administrator/network administrator. A lot of you reading this are probably very interested in servers. The Core 1 (220-1201) A+ exam focuses more on the client side of things, but you should attempt to learn as much as you can about the various servers we just discussed. Ultimately, you will be working on them!

Internet Security Appliances

A variety of security and networking devices can be used to block unauthorized access, decrease garbage messages, and increase availability. Firewalls, UTMs, and IDS and IPS solutions can help block access to a system or network. These are examples of Internet appliances—or, more accurately, Internet *security* appliances. Spam filters can be used to reduce the amount of junk email that an organization receives. And load balancers can be used to distribute data in an efficient manner so that servers are not "overloaded." Let's discuss these networked hosts now.

Network Firewall

Almost every organization has a *network firewall* protecting its network. Such a firewall is usually a rack-mountable hardware device that connects to the LAN on one side (private network) and to the Internet (public network) on the other (and possibly to a secondary network using a third connection). The primary function of a network firewall is to close ports (such as HTTP port 80) to prevent unwanted intrusion. A typical firewall implementation closes all inbound ports so that external users are blocked from access to the LAN of an organization. However, in some cases, you will find that a port on a firewall was opened previously to allow communication by a service or an application that is no longer in use. If that happens, you need to disable (or close) that port or delete the rule that was created for that type of communication. These rules are also known as access control lists (ACLs).

Note

We discuss firewalls in more detail later in Chapter 8, "Network Devices," when we cover Exam Objective 2.5: Compare and contrast common networking hardware devices.

UTM

A firewall can be part of a *unified threat management (UTM)* gateway solution as well. UTM incorporates the features of a firewall along with antivirus/antimalware, antispam, content filtering, and intrusion prevention for the entire network. It might also incorporate data loss prevention (DLP) by way of content inspection. The idea behind UTM is that it can take the place of several units doing separate tasks and consolidate them into one easily administered system. The drawback to this is that it can act as a single point of failure. So, many organizations will consider secondary UTM units or fallback firewalls.

Note

You might not hear the term *UTM* used much today, but it's still on the A+ objectives, so remember that a UTM is an approach to threat management that combines multiple security-related products (antivirus/antimalware software, IPS, and so on) into a single management console.

IDS/IPS

Even though these terms are not listed in the CompTIA 1201 exam objectives, it's important that you understand a few other networking terms, *IDS* and *IPS*, and that you know the difference between them. An *intrusion detection system (IDS)* can determine whether an unauthorized person has attempted to access the network and then alert the system administrator of its findings. In this case, an admin is alerted to the problem, but the unauthorized user might actually gain access to the network; the damage might be done before the admin has a chance to rectify the situation. Building on this concept, an *intrusion prevention system (IPS)* not only detects unauthorized access to the network but attempts to thwart it, making the admin's job somewhat easier. IDS and IPS solutions are available as security appliances for an entire network, and when they are, they are also referred to as network-based IDS (NIDS) and network-based IPS (NIPS), respectively. They are often incorporated into UTM devices, most commonly NIPS. However, IDS and IPS solutions are also available for individual hosts. In this case, they are referred to as host-based IDS (HIDS) and host-based IPS (HIPS).

Spam Gateways

Have you ever received an email asking you to send money to some strange person in a faraway country? Or an email offering extremely cheap Rolex watches? Or the next best penny stock? All of these are examples of spam. Spammers abuse electronic messaging systems such as email, texting, social media, broadcast media, instant messaging, and so on.

For the A+ exams, you need to be most concerned with spam email. There are many ways to try to reduce the amount of spam that is received. Of these antispam techniques, email filtering is at the top. One example of email filtering is the use of a *spam gateway*, also known as a gateway spam filter or email security gateway. This is a software solution that is either incorporated into an email server or installed as a virtual appliance—generally, just behind an organization's firewall (that is, on the LAN).

Antispam policies and filtering can be configured in Microsoft Exchange Server (with Exchange Online Protection, or EOP) or with third-party offerings. Organizations using Microsoft 365 and Exchange are automatically protected to a certain extent from spam (or junk) email.

Load Balancers

Load balancing is the process of distributing tasks over all available resources. The "load" is essentially the packets of data that are sent across the network.

Say that you have three file servers taking care of requests for files from clients. Ideally, you would want each of those servers to work at the highest level of efficiency, and one way to ensure that would be to have the client requests for files distributed equally to those servers. A load balancer is a hardware or software solution that monitors the servers in question and routes client requests to servers in a uniform fashion, making sure that no servers are overloaded and that no servers are idle. Essentially, a load balancer provides for the balancing of IP traffic across a set of servers. The concept of load balancing is popular with web servers and can be used with other technologies as well. Remember that a load balancer is a network device or software component that distributes incoming network traffic across multiple servers, systems, or resources in a network, ensuring optimal utilization of resources, high availability, and improved performance. Load balancers operate at the application layer (Layer 7) or transport layer (Layer 4) of the Open Systems Interconnection (OSI) model and use various algorithms, such as round-robin, least connections, or weighted distribution, to evenly distribute incoming requests or connections among the backend servers.

A properly configured load balancer can distribute the network load and any client requests efficiently among servers, ensure high availability/redundancy of those servers, and offer flexibility when servers need to be added or removed. There are a variety of load-balancing algorithms that you can employ, including

- **Round-robin:** Client requests are distributed across all servers sequentially.

- **Least connections:** New client requests are sent to the server with the fewest concurrent connections.

The concept of load balancing is closely linked to high availability (HA) and clustering.

ExamAlert

A load balancer provides for equal distribution of IP traffic among a set of servers, increasing redundancy and performance.

Embedded Systems and IoT

Some groups of networked hosts are designed to run on-premises only—and you are sure to see them at some point. These include embedded devices in industrial systems, such as supervisory control and data acquisition (SCADA), and devices that are part of the Internet of Things (IoT), such as smart security systems and fire alarms, medical sensors, and appliances. They all connect to the network, so networking knowledge is crucial!

ExamAlert

Know that supervisory control and data acquisition (SCADA) is a system operating with coded signals to remotely control a device or equipment.

Embedded Systems

Embedded systems are devices that have integrated CPU and RAM and can process information internally without the need for a controlling system. They are commonly found in home appliances, office automation, thin clients, security systems, telecommunications, automotive systems, medical systems, and assembly systems, and more.

One place where you will find embedded systems is in heating, ventilation, and air conditioning (HVAC). Larger infrastructures—electrical power grids, water treatment plants, gas/oil pipelines, hydroelectric systems, sewage systems, traffic systems, building controls, and so on—often use SCADA systems. Compared to typical home offices and small offices, SCADA solutions must be heavily secured because they are often used in protected environments and infrastructures. Teams of engineers are employed to design and secure SCADA solutions.

Some buildings might require *legacy systems* to control their older HVAC, plumbing, and other technologies. Some of these legacy systems might be single-board computers such as a PC/104 embedded system, which typically runs at 33 MHz and has 16 to 32 MB of RAM. (Note that the preceding sentence says MHz and MB—instead of GHz and GB—which helps you see what we mean by *legacy*!) These boards can go bad over time and need to be replaced. Or, a particular technology might be controlled by a legacy thin client computer with an embedded operating system—and no hard drive. These are also generally single-board designs where a failure means a total board or unit replacement. If you are in charge of this type of technology, be ready to scour the Internet and locate reliable distributors so that you can get quality replacements at a decent price.

IoT

The *Internet of Things (IoT)* is a global network of physical objects that have embedded processors (of some sort) that can communicate with computers across the Internet.

Collectively, tablets, smartphones, e-readers, and other mobile devices—not to mention their wearable counterparts—make up a portion of the IoT. But IoT devices also include household appliances such as smart refrigerators, digital thermostats, Ring doorbells, home automation devices, and so on. However, IoT isn't limited to just personal devices; it also includes devices used in the medical, manufacturing, and transportation industries, among others. Depending on the organization you work for, you will need to install, configure, secure, and troubleshoot a specific subset of IoT devices. If you apply the methods and techniques in this book, you will be able to work with any device in any market.

Strictly speaking, technicians (and many consumers) look at IoT as a group of technology goodies found in home automation, within appliances, and as voice-activated digital assistants—devices that go beyond desktops, laptops, smartphones, and tablets. The key is that they connect to the network and ultimately to the Internet to receive updates and so that they can be controlled from a mobile device or other computing system.

IoT devices include thermostats, light switches, security cameras, door locks, refrigerators (and other appliances), and smart speakers. In some cases, these "smart" devices incorporate Bluetooth Low Energy (BLE) technology, which uses less power than a standard Bluetooth device. Ultimately, IoT devices connect to the Internet and collect and exchange data. Configuring these devices is usually an intuitive process. It is important to pay attention to how they are connected to the network and how they are secured because IoT devices all connect to the Internet, and the apps that control them may or may not have the most brilliant programming—and security vulnerabilities abound.

Some of the ways to increase security include updating IoT devices' firmware and associated apps, updating SOHO routers (or other routing devices), keeping IoT devices on a separate network, using Bluetooth PIN codes, using strong passwords (and possibly multifactor authentication), and carefully selecting and monitoring cloud-based services that are used by the IoT devices.

Cram Quiz

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

1. While looking at the details of a server in your provider's control panel, you notice that it says "Apache" in the HTTP summary. What kind of server is this?

   - ○ **A.** File server
   - ○ **B.** Web server

- ○ **C.** Email server
- ○ **D.** Authentication server

2. Which type of server acts as a go-between for clients and websites?

- ○ **A.** Proxy server
- ○ **B.** Print server
- ○ **C.** Syslog server
- ○ **D.** DHCP server

3. Which type of server runs Microsoft Exchange?

- ○ **A.** File server
- ○ **B.** Authentication server
- ○ **C.** Email server
- ○ **D.** Web server
- ○ **E.** SCADA

4. Which type of device category would a smart thermostat fall under?

- ○ **A.** SCADA
- ○ **B.** IoT
- ○ **C.** Load balancer
- ○ **D.** Spam gateway

5. You have been tasked with installing a solution that will cache and monitor Internet traffic. Which of the following devices is the best solution?

- ○ **A.** Proxy server
- ○ **B.** AAA server

- ○ **C.** Authentication server
- ○ **D.** Spam gateway

Cram Quiz Answers

1. **B.** Apache is a type of web server that runs on Linux. It is also known as Apache HTTP Server. File servers are used to store and transfer files but not websites. Email servers deal with the sending and receiving of email via POP3, IMAP, and SMTP. Authentication servers verify the identity of users logging in and computers on the network.

2. **A.** A proxy server is a caching server used to store commonly accessed websites. Such a server can be incorporated into a web server but often runs as a standalone server. A print server manages network printers and their spooling of print jobs, priorities, and so on. A syslog server gathers logging data from network devices and allows for the easy analysis of those logs from a client workstation. A DHCP server hands out IP addresses (and other TCP/IP information) to client computers.

3. **C.** Microsoft Exchange is a type of email server software. While you could run multiple services on a single server—for example, you could run a web server and an email server on the same machine—doing so isn't recommended. Unless you have a small office, all servers (such as file servers, authentication servers, email servers, DHCP servers, and so on) should be separate entities. SCADA is not a server; it stands for supervisory control and data acquisition and is a type of system used to control larger organizations' infrastructures, such as heating/cooling, electricity, and so on.

4. **B.** A smart thermostat is a type of Internet of Things (IoT) device. SCADA is an industrial system that controls an organization's infrastructure facilities. A load balancer is in charge of distributing IP traffic among multiple servers. A spam gateway is an email

filtering device that removes unwanted spam (or junk) email from all email accounts on the network.

5. **A.** A proxy server is the best solution in this scenario because it is used to monitor, control, and cache Internet traffic. It acts as an intermediary between the LAN and external networks, helping to prevent unauthorized access and providing additional security for the LAN. An AAA server is used to verify and manage user access, an authentication server identifies users and grants or denies access, and a spam gateway filters and blocks unwanted emails.

A wise person once said, “Learning is a life-long endeavor.” Continue!

Chapter 7
Network Configuration Concepts

This chapter covers the following A+ 220-1201 exam objective:

▶ **2.4** — Explain common network configuration concepts.

Let's get deeper into network configurations. Two technologies are integral to just about every network out there: DNS and DHCP. DNS provides name resolution, and DHCP provides automatic IP addressing. Without these two services, not much would get done in a typical organization, and not much fun would be had at home! DNS and DHCP are fundamental networking services that allow systems to interoperate properly.

Of course, it's great to develop systems and networks in a physical, tangible way, but it isn't always the most sensible way. Sometimes, going *virtual* is the best solution. Anything can be virtualized, from individual computers to entire networks. In this chapter, we'll briefly cover two virtual technologies: VLANs and VPNs. A VLAN helps to organize a LAN in a virtual manner. A VPN allows for external connections to a network while making it appear that the user is physically working at that network.

ExamAlert

Objective 2.4 focuses on the following concepts: DNS, DHCP, VLANs, and VPNs.

DNS

The Domain Name System (DNS) is a worldwide system of domains, hosts, and DNS servers. The primary function of DNS is to resolve hostnames to IP addresses. This "translation" takes place all the time between computers. For an example, see the section "DNS Servers" in Chapter 6, "Networked Hosts." In that example—and any time a client connects to a domain—a DNS server somewhere on the Internet (or possibly in an organization's LAN) oversees hostname-to-IP resolution. Once that is done, the computer can communicate directly with the host via the IP address, which is how all data packets are sent.

Sometimes, you'll connect to a domain such as demosite.com. And sometimes you'll connect to a specific host within a domain—for example, server1.demosite.com. In this example, server1 is the hostname, and demosite.com is the domain name. Together, they form a *fully qualified domain name (FQDN)*, also sometimes referred to as an *absolute domain name* or simply as a *DNS name*.

ExamAlert

Hostname + Domain name = FQDN (fully qualified domain name).

As mentioned, a DNS server does the actual resolution work. DNS servers house the records of various systems. A common DNS record type is the *address record*. An address record (A record for short) stores the IPv4 address of a host or of a domain, as well as the corresponding name. It is used to do forward lookups of a system, which means it resolves from name to IP address. This is a very common type of DNS record, but there are plenty of others. Table 7.1 shows some of the most common resource records (RRs) that you will encounter.

TABLE 7.1 **DNS Record Types**

Record Type	Description
A record	Stores the IPv4 address of a domain or host for forward lookup (name to IP address). Example on a DNS server: `server1.example.com  A  10.0.2.4`
AAAA record	Stores the IPv6 address of a domain or host.
CNAME record	Canonical Name record. Aliases one domain name to another, simplifying DNS management. Example: `www.example.com`
NS record	Name Server record. Stores the DNS server record.
SOA record	Start of Authority record. Stores the administrative information for a domain.
MX record	Mail Exchange record. Directs mail to an email server. Example on a DNS server: `example.com.  1936  IN  MX  10  mail.example.com.`
PTR record	Pointer record. Does reverse lookup (IP to name). Example on a DNS server: `4.2.0.10.in-addr.arpa.  PTR  server1.example.com.`
TXT record	Is used for administrative text-based notes and with email authentication methods.

DNS resource records are written into zone files, either statically by the administrator or dynamically by a system. Table 7.1 shows an example of an A record. This example shows that the hostname is server1.example.com, the type is an address record, and the IP address of that host is 10.0.2.4. This type of record is used for forward lookups (from name to IP address), and the record is stored in a forward lookup zone.

However, sometimes systems need to go in reverse, using the IP address to find out the hostname. In such a case, you need a pointer record (PTR). Table 7.1 shows an example of this, where the IP address is shown in reverse (4.2.0.10) and the hostname is also listed. This type of record is written into a reverse lookup zone.

ExamAlert

Be able to identify DNS Address (A and AAAA) records, Mail Exchange (MX) records, Canonical Name (CNAME) records, and Text (TXT) records for the exam.

Table 7.1 also shows an example of a Mail Exchange (MX) record. In this case, if a person were to send mail within the example.com domain, that mail would be forwarded to the mail.example.com host. As you can imagine, email and DNS are heavily intertwined.

Email Authentication Methods

Do you want to know what the biggest challenge is for email administrators? Spam. You could say it's the bane of humankind! So, it follows that an email administrator needs to pay strict attention to spam management. We've already mentioned that this can be done with the use of filters at both the server and the clients. However, an admin can employ some other methods and protocols to reduce spam and email spoofing in general. (With email spoofing, a sender uses a forged sending address, such as with spam and phishing.) Here are a few methods for detecting email spoofers and reducing spam email:

- **DomainKeys Identified Mail (DKIM):** DKIM is an authentication method for email that attempts to detect email spoofers. DKIM enables the email recipient to check the domain that an email supposedly came from using a digital signature. A receiving email server can check the DKIM signature—which is part of the email header—and verify it by doing a DNS lookup and then checking the public key that is associated with that domain. DKIM records are listed in a DNS server with a

domainkey subdomain label such as selector._domainkey.example.com. Here is an example of a DKIM TXT record in DNS:

```
selector._domainkey.example.com.  TXT v=DKIM1;p=<public key>
```

Here you see the FQDN (selector._domainkey.example.com), the resource record type (TXT), and the version of DKIM (1). You can also see that we are using a public key, perhaps an RSA key. (Public keys are long hexadecimal strings of information, and for simplicity we just used **<public key>** here.)

- **Sender Policy Framework (SPF):** SPF also detects email spoofers. A receiving email server can attempt to check mail by verifying the IP address of the domain that the mail claims to have come from. It does this by checking the DNS records for that domain and systems. Unlike DKIM records, SPF records only use the domain name in their records. Here's a basic example of an SPF TXT record in DNS:

```
v=spf1 ip4:93.184.216.34 include:example.com -all
```

This indicates that you are using SPF version 1, and it defines the IP address of the mail server (93.184.216.34) and the domain name (example.com).

- **Domain-based Message Authentication, Reporting & Conformance (DMARC):** This email authentication protocol helps protect email domains from spoofing and other unauthorized use. It is used in conjunction with the older DKIM and/or SPF methods, which by themselves are less potent solutions. For example, SPF cannot check the From field of an email header, but DMARC can. DMARC enables an admin to publish a policy in the DNS server's records that states which mechanism to use and what to do in the event of failures. DMARC records might be listed in a DNS server with a DMARC subdomain label such as

```
_dmarc.example.com.
```

Here's a more advanced example of a DMARC TXT record on a DNS server:

```
"v=DMARC1;p=reject;pct=100;rua=mailto:postmaster@example.com"
```

This example specifies several things: First, you are using DMARC version 1; second, there is a policy for "rejecting" emails; third, it will do this for 100 percent of the email messages; and fourth, reporting (rua) will go to the email address postmaster@example.com. For more information on DMARC, visit https://dmarc.org.

Note

Don't confuse the email authentication protocol DMARC with the term *demarc* (short for *demarcation point*), which is mentioned in Chapter 8, "Network Devices."

ExamAlert

For the exam, be able to explain spam management configurations and concepts including DomainKeys Identified Mail (DKIM), Sender Policy Framework (SPF), and Domain-based Message Authentication, Reporting & Conformance (DMARC).

Note

For more information about DNS, see IETF RFC 1591: https://datatracker.ietf.org/doc/html/rfc1591. Also consider looking into commonly used DNS server software, such as BIND: https://www.isc.org/bind/.

DNSSEC

For a computer to do anything today, proper credentials have to be supplied and verified. However, DNS by itself does not check for credentials. Case in point: An attacker can cause DNS poisoning by delegating a false name to the DNS server and providing a false address for the

server. That can then spread to other DNS servers. Enter DNSSEC. The Domain Name System Security Extensions (DNSSEC) protocol was developed to strengthen DNS through the use of digital signatures and public key cryptography. It protects against attacks by providing a validation path for records. Although you might not see it on the A+ exams, DNSSEC is an integral part of today's DNS technology. To learn more, see the IETF RFCs 4033, 4034, and 4035.

What can we say? DNS is massive; there are a lot of moving parts. We're just scratching its surface in this book. People just expect it to work, but to make it work well, an admin must configure and secure it properly and monitor it carefully.

DHCP

In Chapter 6, we discussed DHCP as a service and what a DHCP server does. To review, a DHCP server is used to automatically assign IP addresses (and other pertinent IP information) to clients. Now let's get into some more fine-grained DHCP concepts.

DHCP Process

DHCP clients get their IP addresses from a DHCP server through the use of a four-step process referred to by the acronym *DORA*, which stands for discovery, offering, request, and acknowledgment. Let's briefly discuss this process now, using TCP/IP version 4 (or simply IPv4) as our example. In this scenario, the DHCP server uses the IP address 192.168.1.1:

1. **Discovery:** Normally, a client computer is configured to automatically obtain an IP address from a DHCP server. When a typical client on a network is first booted, it attempts to discover DHCP servers by broadcasting over the network. Broadcasting essentially means sending a message to all recipients on the network at the same time. The client computer does this because it doesn't have an IP address yet and doesn't know the IP address of the DHCP server. If a DHCP server exists on the network, and that server is listening for requests, the client will discover it. With IPv4, the DHCP server uses inbound port 67 to listen for DHCP requests. The client uses outbound port 68

to discover a DHCP server. Once a DHCP server is discovered, the next step occurs.

2. **Offering:** For simplicity, let's say there is a single DHCP server on the network. (This is common.) If that DHCP server is listening and has been discovered, it then makes an offer to the client. The offer usually consists of an IP address, a subnet mask, a gateway address, and a DNS server IP address, though it could include more information. The IP address that is offered to the client is selected from a range of IP addresses that the server has been preconfigured to provide. This preconfiguration is done by the admin and is also known as an IP pool, or a *DHCP scope*. In this example, let's say the admin has configured the scope as a range of IP addresses spanning 192.168.1.101 through 192.168.1.200. That's a range of 100 addresses, so the server could hand out addresses to 100 clients in total before running out. If the client in this example were the first one to be used on the network, it would normally be offered the first IP address in the scope (in this case, 192.168.1.101), although it is possible to configure the DHCP server to hand out addresses dynamically instead. In a SOHO network, the scope is part of the same IP network that the DHCP server is on—in this case, 192.168.1 (also referred to as 192.168.1.0).

ExamAlert

A DHCP scope is a range of IP addresses that a DHCP server can hand out to clients.

3. **Request:** In most cases, especially if there is a single DHCP server, the client requests the IP address and additional TCP/IP information that has been offered by the DHCP server. That means that the client is agreeing to use the IP address, and it lets the server know this.
4. **Acknowledgment:** In the last step, the server acknowledges that the client has requested the offered IP configuration. It then creates an *IP lease* for the client. The lease is available for a limited time, and that time is specified in the DHCP server's configuration file. It could be

as little as 1 hour (3600 seconds), or it could be 24 hours, or possibly 8 days, depending on the environment, organizational policies, type of system used, and administrator preferences. The lease information is written to a file on the server. That information typically includes the IP address the client will be using (in this example, 192.168.1.101), the client's MAC address, the length of the lease, and possibly the hostname of the client. The server confirms with the client, and the client can now communicate over the network via TCP/IP. At this point, the server knows not to hand out the 192.168.1.101 IP address to any other clients. Instead, the next client that boots on the network will most likely receive the 192.168.1.102 IP address.

ExamAlert

An IP lease is the amount of time that a client can use an assigned IP address in a DHCP system.

Table 7.2 summarizes the four-step DORA process.

TABLE 7.2 **DHCP Four-Step Process—DORA**

Step	Description
Discovery	The client looks for and discovers a DHCP server.
Offering	The server offers an IP address to the client.
Request	The client picks an address and requests that it be assigned.
Acknowledgment	The server acknowledges the request, and the client can then use the IP address for a set amount of time, which is known as a *lease*.

Note

The DORA process happens in a flash, and oftentimes, only half of the process is necessary. Remember that an IP lease is finite. When it expires, the client typically requests the same IP address again (if the client is still a part of the network). The original dynamic address is stored at the client computer, so the client simply requests the same IP address, which means only the request and acknowledgment steps are required—so the process in this case is simply RA. In many situations, the client receives the same IP address, but this is not always the case. Be prepared for clients to obtain new IP addresses at random.

DHCP Exclusions

DHCP exclusions allow administrators to specify IP addresses within a DHCP scope that should not be assigned to clients. These excluded addresses can be reserved for specific purposes, such as static assignments for servers, printers, or network devices like routers and firewalls. Exclusions ensure that the DHCP server does not allocate these addresses dynamically, avoiding IP conflicts and ensuring efficient network management.

DHCP Reservations

Sometimes, you might want to reserve certain IP addresses within a DHCP scope—such as for servers or other special systems. *DHCP reservations* are IP addresses within the DHCP scope that are permanently reserved for special computers/devices that need to use DHCP but don't want the IP address to change over time (which can happen periodically in DHCP environments). These special computers/devices might include printers or web servers, for example.

An IP reservation is configured at the DHCP server and specifies the IP address to be reserved and some type of identifying information about the client that it is reserved for—typically the client's MAC address. That client will be allowed to use the IP address exclusively, without any concern that it will change over time. In this example, an IP reservation isn't really

necessary because there are open IP addresses on the network (from 192.168.1.2 to 192.168.1.100 and from 192.168.1.201 to 192.168.1.254). However, you might encounter a DHCP scope that was originally configured to use the entire range of usable IP addresses in a given network (for example, 192.168.1.2–192.168.1.254, excluding the DHCP server on 192.168.1.1). If you want to have servers with exclusive IP addresses that will not change, you need to set up reservations for those servers within that DHCP scope.

ExamAlert

DHCP reservations are IP addresses within the DHCP scope that are permanently reserved.

Note

For more information about DHCP, see RFC 2131: https://datatracker.ietf.org/doc/html/rfc2131. Also, for a real (and commonly used) DHCP server example, learn more about ISC Kea by visiting https://www.isc.org/kea/.

VLANs

A virtual LAN (VLAN) is implemented primarily to segment a network. But it can also be used to reduce data collisions, organize the network, potentially boost performance, and, possibly, increase security. A device such as a switch often controls a VLAN. A VLAN compartmentalizes a network and can isolate traffic. VLANs can be set up in a physical manner; for example, with a port-based VLAN, a switch's physical ports are grouped and configured to act as individual VLANs. To set up a VLAN this way, you would need a managed switch—one that you can log in to and configure for VLAN use. But there are lots of switches from different manufacturers out there, right? So, the Institute of Electrical and Electronics Engineers (IEEE) developed the 802.1Q networking standard, which

supports and ensures interoperability of VLAN technologies from different vendors.

There are also logical types of VLANs, such as protocol-based VLANs. A VLAN can be set up in such a way that each VLAN is on a different IP network number (for example, 192.168.0.0, 192.168.1.0, 192.168.2.0, and so on). Or, you could take it to the next level and incorporate a technology called IP subnetting, which involves dividing a network into two or more subnetworks by changing the subnet mask that is used (for example, from 255.255.0.0 to 255.255.240.0). Some administrators prefer the use of IP subnetting over VLANs, and some use them together; for example, they might use a group of physical port-based VLANs, each of which is on a different IP subnetwork.

ExamAlert

Remember that VLANs are commonly used for network segmentation.

Note

VLANs and subnetting go a bit beyond what a typical A+ technician will be asked to perform, but you should know the basic definitions for these terms.

VPNs

Let's say you want to connect to your network, but you are at a remote location. Enter the VPN. Virtual private networks (VPNs) were developed so that data commuters, salespeople, and others could connect to the office from a remote location. If a VPN is set up properly, the remote logon connection is seamless, and it appears as if you are actually on the LAN in the office. You log on just as you would if you were at your desk at headquarters. A VPN gives a user access to all the resources available when

logging on locally. VPNs take advantage of the infrastructure of the Internet and fast connections (such as cable, fiber, DSL, 5G, and so on).

In Windows, a VPN connection can be identified by an additional network connection in the notification area, as an additional network connection when using the **ipconfig** command, or as a pop-up window that appears during the logon process. Connections to VPNs can be initiated in a couple of ways in Windows:

- Go to **Start > Settings > Network & Internet > VPN**. Then click the + sign (Add a VPN connection).
- Navigate to the Network and Sharing Center. Select the **Set up a new connection or network** link. From there, select **Connect to a workplace** and **VPN**.

There are also third-party offerings from companies such as Cisco and Check Point. Regardless of the software used, you need to know VPN-specific details such as the VPN provider, the IP address or name of the VPN server you are connecting to, or the username and password to get into the VPN. Alternate IP configurations are sometimes used with VPN connections so that the main IP configuration is not disturbed, especially if it is configured statically.

ExamAlert

Know that a VPN extends a LAN by establishing a secure connection tunnel through a public network such as the Internet.

Cram Quiz

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

1. Your system needs to renew its IP address from a DHCP server. What has expired?

- **A.** IP lease
- **B.** IP reservation
- **C.** DHCP scope
- **D.** MAC address

2. Which type of DNS record associates an IPv6 address with a hostname?

- **A.** A
- **B.** AAAA
- **C.** SOA
- **D.** MX

3. Which of the following is the best solution for protecting email domains against spoofing and other unauthorized uses?

- **A.** SPF
- **B.** DORA
- **C.** DMARC
- **D.** VLAN

4. You have been tasked with compartmentalizing a network. Which of the following technologies should you use?

- **A.** APIPA
- **B.** VPN
- **C.** VLAN
- **D.** IPv6

5. Which of the following DNS record types directs email to an email server?

- **A.** A
- **B.** AAAA
- **C.** TXT
- **D.** MX

Cram Quiz Answers

1. **A.** The IP lease has expired. When this happens, the client needs to renew the address (or seek a new one from another DHCP server). An IP reservation is a reserved address to be used exclusively by a server or another special system. A DHCP scope is the range of IP addresses that a DHCP server assigns to clients. A MAC address is a unique address written to a network interface card.

2. **B.** An AAAA record associates an IPv6 address with a hostname for use with forward lookup (name to IP address). An A record associates an IPv4 address with a hostname. SOA is the Start of Authority record. MX is a Mail Exchange record, which directs email to the proper email server.

3. **C.** The best listed solution is DMARC, which enables an admin to make use of the SPF or DKIM protocols (or both) in a more secure way. SPF by itself is not as functional as DMARC. DORA is the four-step DHCP process. A VLAN is a virtual LAN, designed to organize and compartmentalize a LAN.

4. **C.** You would create a virtual LAN (VLAN). Another valid option would be to implement IP subnetting. APIPA (also known as link-local) is an IP technology that auto-assigns addresses on the 169.254 network. A virtual private network (VPN) allows remote clients to connect to a network over the Internet using a secure tunnel. IPv6 in and of itself does not compartmentalize the network. However, an IPv6 network that has been *subnetted* would be acceptable.

5. **D.** The DNS Mail Exchange (MX) record directs mail to an email server. An A record type stores the IPv4 address of a domain or

host for forward lookup (name to IP address). An AAAA record stores the IPv6 address of a domain or host. A TXT record is used for administrative text-based notes and with email authentication methods. Know those DNS record types!

Do you like bad dad jokes? Your New Year's *resolution* should be to know DNS, DHCP, and virtual networking concepts. Anyway…nice work so far!

Chapter 8
Network Devices

This chapter covers the following A+ 220-1201 exam objective:

- **2.5** – Compare and contrast common networking hardware devices.

In this second chapter about networking, we will discuss networking devices—the devices that make communications happen between computers. Need your computers to talk to each other in a wired fashion? You want a switch. Need them to communicate wirelessly? Use a wireless access point. Want to connect two or more networks or connect to the Internet? Routers do just this. These are just a few examples of networking devices that make our computers more "talkative." And know this: Some are multifunction devices, meaning that they can do the work of more than one network device.

While you read this chapter, apply what you learn to the devices in your own network. Whenever you encounter a device, think about its function in a network environment. The A+ Core 1 (220-1201) exam covers only the basics about networking, but it is still a lot of material to cover, so let's get to it!

ExamAlert

Objective 2.5 focuses on the following concepts: routers, switches (managed and unmanaged), access points, patch panels, firewalls, Power over Ethernet (PoE), cable modems, digital subscriber line

(DSL), optical network terminals (ONTs), and network interface cards.

Switches

A *switch* is a central connecting device that computers connect to in a wired fashion. Each computer is connected to its own physical port on a switch. The switch is in charge of sending data directly to the correct computer instead of broadcasting it out to every port (the way an older hub would). It does this by identifying the media access control (MAC) address of each computer. The MAC address is the physical address (for example, 00-0C-29-C6-XX-XX) that is programmed into the network adapter. (In Windows, run a quick **ipconfig /all** to find out your MAC address, also called a *physical address*.) By identifying each computer's MAC address, the switch can effectively make every port on the switch an individual entity. To further accomplish this, switches employ a matrix of copper wiring—and everything is interconnected between the ports.

Switches are intelligent, and they use their intelligence to pass information to the correct port. This means that each computer has its own bandwidth (for example, 1000 Mbps). In today's networks, switches are commonly found in 1000 Mbps (1 Gbps), 10 Gbps, and 40 Gbps networks.

ExamAlert

A switch is responsible for transmitting data from two or more wired computers. It often works at data transfer rates of 1000 Mbps or 10 Gbps.

Switches work within the Ethernet standard, which is the most common networking standard used today. It was ratified by the IEEE and is documented in the 802.3 set of standards. For example, a typical Ethernet network running at 1000 Mbps and using twisted pair cable is classified as 802.3ab. 10 Gbps Ethernet over twisted pair cable is 802.3an.

Understand the difference between a managed switch and an unmanaged switch. Managed switches can be configured when accessed from a browser or from the command line, using SSH or a similar configuration tool. For example, you can change a device's IP address, turn on Spanning Tree Protocol (STP) to avoid network looping, enable system logging (syslog), and monitor the switch and other devices with SNMP. On the other hand, unmanaged switches don't have these capabilities; they simply connect devices and computers together for transmission of data over the Ethernet network. Unmanaged switches provide an inexpensive method of adding computers to your network.

ExamAlert

A managed switch can enable an admin to control settings and network traffic. An unmanaged switch simply allows LAN devices to communicate without user intervention.

As mentioned, a switch connects computers together in a wired fashion. From a design standpoint, this is known as a *star topology* (or hub-and-spoke topology), with the switch in the center of it all. A switch is also the basis for a local area network (LAN). But what if you want to connect two LANs together? Enter the router.

Routers

A *router* is used to connect two or more networks to form an internetwork. Routers are used in LANs and WANs and on the Internet. A router is a device that routes data from one location to another, usually by way of IP addresses and IP network numbers. Routers are intelligent and even have their own operating systems. A router enables connections with individual high-speed interconnection points. A common example would be an all-in-one device or multifunction network device that might be used in a home or small office. These devices route signals for all the computers on the LAN out to the Internet. Larger organizations use more advanced routers that can make connections to multiple various networks as well as the Internet.

ExamAlert

Know that a router connects networks and uses software-configured network addresses to make forwarding decisions. It is a device that works at the network layer of the OSI model to control the flow of data between two or more network segments.

Access Points

A *wireless access point (WAP)*—or simply an *access point*—enables data communications over the air when a computer is equipped with a wireless networking adapter. The WAP and the wireless networking adapter transmit data over radio waves either on the 2.4 GHz, 5 GHz, or 6 GHz frequencies. Wireless access points are everywhere you look: hotels, restaurants, shopping centers, you name it. They allow people to easily connect to the Internet with smartphones, tablets, and laptops.

WAPs are also included in most multifunction network devices, known as SOHO (small office/home office) routers or simply routers. They enable wireless computers to not only communicate with each other but also access the Internet. Whereas switches deal with wired networks, WAPs deal with wireless connections. WAPs are also based on Ethernet, but now we are talking about the IEEE 802.11 group of standards, which defines wireless LANs (WLANs), simply referred to as Wi-Fi. A WAP acts as a central connecting point for Wi-Fi-equipped computers. Like a switch, a WAP identifies each computer by its MAC address.

ExamAlert

A transmitter and receiver (transceiver) device is commonly used to facilitate communication between a wireless client and a wired network. Wireless APs (or WAPs) are used with the wireless infrastructure network topology to provide a connection point between WLANs and a wired Ethernet LAN. Remember that a wireless access point is responsible for transmitting data between

two or more wireless computers, usually at 6 GHz, 5 GHz, or 2.4 GHz frequencies.

Firewalls

A *firewall* is a hardware appliance or software application that protects a computer from unwanted intrusion. In the networking world, we are more concerned with hardware-based devices that protect an entire group of computers (such as a LAN). When it comes to small offices and home offices, firewall functionality is usually built into the router. In larger organizations, a firewall is a separate device, or it could be part of a more complex all-in-one solution. A firewall stops unwanted connections from the outside and can block basic network attacks. We'll discuss firewalls more in Chapter 43, "Physical Security," Chapter 44, "Logical Security," and Chapter 51, "SOHO Security."

ExamAlert

A firewall provides controlled access between networks. Firewalls can be hardware or software based and are essential to network security.

Network Interface Cards

A network interface card (NIC, pronounced *nick*), also known as a network adapter, is a physical device that can be added to a computer or networking device that has an open and compatible slot. For example, a computer with an open PCI Express slot (x1, x4, x8) can be used with a NIC for connectivity to a computer network. Most PCs and laptops have NICs built into the motherboard; these are known as *integrated NICs*. However, workstations and servers often require more powerful, separate, network interface cards, or require multiple NICs. A server may use special network cards that have two, four, or more RJ-45 ports to allow for increased data throughput as well as higher availability.

Every network interface card is uniquely identified by its media access control (MAC) address, also known as the physical address. This MAC address is a 48-bit identifier, typically represented in hexadecimal format (e.g., 00-0C-29-C6-XX-XX). It is embedded in the NIC by the manufacturer and is critical for data communication within a local area network (LAN). The MAC address operates at the data link layer of the OSI model and ensures that data packets reach the correct device. When a NIC sends or receives data, the MAC address is used by network devices like switches to direct traffic to the appropriate destination. This interplay between the NIC and the MAC address is foundational to network functionality, enabling reliable and efficient communication between devices.

We'll discuss NICs further in Chapter 16, "Motherboards and Add-on Cards."

Patch Panels

A *patch panel* is a physical hardware device that acts as a termination point for all of the network cables in a building. It is often located in a wiring closet, server room, or data center, depending on the size of the organization. It consists of multiple RJ-45 ports on the front that connect to switches by way of twisted pair patch cables, and 110 IDC termination points on the back for connecting all of the individual wires in twisted pair cables. Those cables lead out to the various computer ports in the building. While it isn't necessary to have a patch panel, it makes for easier and more reliable patching of ports. A typical physical data path from a user to a server is Computer > RJ-45 jack > twisted pair cable > patch panel > switch(s) > server.

Power over Ethernet

Power over Ethernet (PoE) is an Ethernet standard that allows for the passing of electrical power in addition to data over Ethernet cabling. It is described in several IEEE 802.3 standards (for example, IEEE 802.3bt-2018). PoE can deliver between 15.4 and 100 watts maximum to a variety

of devices, as long as the sending and receiving devices are both PoE compliant.

PoE is an excellent solution for devices that require specific placement but where no electrical connection can be made (for example, with outdoor video cameras or WAPs that need to be mounted to the ceiling). In these cases, all that needs to be run is a twisted pair network cable, which takes care of power *and* data. No AC electrical connection is necessary.

PoE technology is broken down into the two devices:

- **Power sourcing equipment (PSE):** This could be a switch or other similar device.
- **Powered device (PD):** This could be an IP-based camera, an IP phone, a wireless access point, a router, a mini network switch, an industrial device, a lighting controller, and more. If the device to be powered is not PoE compliant, then a PoE splitter can be used in between the device to be powered and the network connection.

ExamAlert

Remember that Power over Ethernet (PoE) is a technology that enables electrical power to be transmitted over twisted pair Ethernet cable. The power is transferred, along with data, to provide power to remote devices. PoE devices include power sourcing equipment (PSE) and a powered device (PD).

For organizations with a group of remote devices, a 24- or 48-port PoE-enabled switch is the way to go. For a smaller organization that has only one or two remote devices that need to be powered, a *PoE injector* is a decent, cheaper PSE solution. This device is installed where the main network switch is and plugs into one of the switch's ports. It is also powered normally from an AC outlet. But the injector has a second RJ-45 port that is used to connect out to the remote device. This port sends Ethernet data as well as power over the Ethernet connection. This way, the organization can get power and data to a PoE-compliant access point, IP

camera, or other device that needs to be located in an area where it would be difficult (not to mention expensive) to add an electrical outlet. However, the correct type of cabling must be used to handle the amperage required. Generally, this is Category 5 twisted pair cabling and higher.

Table 8.1 shows some of the IEEE standards for PoE, their associated maximum power levels, and the modes of power usage. Mode A delivers power on the two data pairs of wires in a twisted pair connection. For example, using the T568B wiring standard, this would be the orange and green pairs, or wires 1, 2, 3, and 6. Mode B delivers power on the spare pairs, which in T568B would be the blue and brown pairs, or wires 4, 5, 7, and 8. However, it's more common in newer standards to use all four pairs of wires in a twisted pair cable. This is done using phantom power, which allows for data *and* power to be sent on each pair of wires. For more information about the T568B wiring standard, see Chapter 13, "Cables and Connectors."

ExamAlert

Newer versions of PoE use all four pairs of wires on a twisted pair cable and also implement phantom power, allowing data and power to be sent simultaneously over all pairs. Know what a PoE injector does and that Ethernet switches are available with PoE capability.

TABLE 8.1 **IEEE PoE Standards**

Standard	Maximum Provided Power (watts)	Power Modes
802.3af (Type 1) (PoE)	PSE: 15.4 W PD: 12.95 W	Mode A and Mode B
802.3at (Type 2) (PoE+)	PSE: 30 W PD: 25.5 W	Mode A and Mode B

Standard	Maximum Provided Power (watts)	Power Modes
802.3bt (Type 3) (PoE++)	PSE: 60 W PD: 51 W	Mode A, Mode B, and 4-pair
802-3bt (Type 4) (PoE++)	PSE: 100 W PD: 71 W	4-pair only

Note

The second column of Table 8.1 shows the power sourcing equipment (PSE) first and the powered device (PD) second. Power dissipation over the twisted pair cable is between 10 and 30 percent, depending on the standard.

You should also consider *load testing* a PoE system. Do this before anyone uses it to make sure that the system can handle the amount of electricity you plan to send over it. Load testing has the added benefit of making a PoE-enabled switch work more efficiently. For example, a typical Type 2 PD will be rated as a 30 W device. However, many of those PDs will be able to function with less power, and you can configure each one's power usage on a port-by-port basis at the PoE-enabled switch.

Cable/DSL Modems

Essentially, a cable or DSL modem is a device that allows a computer (or SOHO network) to access the Internet. Cable Internet and digital subscriber line (DSL) Internet connections use separate devices to connect. For example, a person with a cable Internet connection will use a device that has an RG-6 port for the provider's incoming coaxial cable. A DSL modem, on the other hand, will have an RJ-11 port that makes use of a person's telephone line. Both, however, use an RJ-45 port that connects to the consumer's computer or SOHO router by way of a twisted pair patch cable.

Note

The term *modem* is a combination of the words *mo*dulate and *dem*odulate. It originated with the dial-up modem that uses a standard telephone line. While it is arguable whether cable and DSL Internet devices are actually "modems," the plain truth is that the term is commonly used—even by some manufacturers.

Network Interface Devices

A *network interface device (NID)* is a device installed at the perimeter of a customer's premises. It is the connection point between a provider's cabling and the customer's cabling—also known as a demarcation point, or demarc. It is often a gray box on the outside of a building that is maintained by providers of cable Internet, cable TV, DSL, or fiber optic–based services, though it could be inside the building as well. It could act as a basic wiring termination point or provide more functionality, intelligence, and possibly power, depending on the technology involved. (A NID goes by several other names, including network interface unit, telephone network interface, or network termination device.)

One example of a NID is an *optical network terminal (ONT)*. When you see the word *optical*, think fiber optic cables, which have the ability to transmit massive amounts of data. In some urban areas, businesses and homes can get fiber to the premises, which means that a fiber optic cable is run directly to the premises by the provider. It terminates at an ONT, where it can be split off for services such as voice, data, and television, which will usually run on copper-based cables from the ONT to the inside of the customer's premises. The ONT (and any type of NID) is normally accessible only by employees of the fiber optic provider.

Note

Don't confuse an optical network terminal (ONT) with an optical line terminal (OLT). An OLT is an endpoint for fiber optic cables

that are run *inside* an organization's premises for use with high-speed data transfer between hosts and/or networks.

Cram Quiz

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

1. Which of the following is most often used to connect a group of computers in a LAN? (Select all that apply.)

   - ○ **A.** Router
   - ○ **B.** Switch
   - ○ **C.** Bridge
   - ○ **D.** WAP

2. What device protects a network from unwanted intrusion?

   - ○ **A.** Switch
   - ○ **B.** Router
   - ○ **C.** Access point
   - ○ **D.** Firewall

3. Which of the following network devices moves frames of data between a source and destination, based on their MAC addresses?

   - ○ **A.** Hub
   - ○ **B.** Switch
   - ○ **C.** Router
   - ○ **D.** Modem

4. Which of the following network devices allows a remote device to obtain Ethernet data as well as electrical power?

   - **A.** PD
   - **B.** PoE injector
   - **C.** Firewall
   - **D.** Router

5. Which of the following devices can be configured when accessed from a browser or SSH or similar configuration tool?

   - **A.** Managed switch
   - **B.** Unmanaged switch
   - **C.** Patch panel
   - **D.** Network interface card

6. Which of the following acts as a demarcation point for fiber optic services?

   - **A.** SDN
   - **B.** ONT
   - **C.** Patch panel
   - **D.** NIC

Cram Quiz Answers

1. **B and D.** Computers in a LAN are connected by a central connecting device, the most common of which are switches and wireless access points (WAPs). Hubs can also be used, but those are deprecated devices; they are predecessors of switches. A router is designed to connect two networks. Now, you might say, "Wait! My router at home has four ports on the back for computers to talk to each other." Well, that is actually the switch portion of a SOHO "router." The actual *router* functionality is in the connection

between the two networks—your switched LAN and the Internet. Although not mentioned in the chapter, a bridge is used to connect two LANs or separate a single LAN into two sections.

2. **D.** A firewall is a hardware appliance or software application that protects one or more computers from unwanted intrusion. A switch is a device that connects multiple computers together on a LAN. A router is used to connect two or more networks. An access point (or wireless access point) allows Wi-Fi-enabled computers and devices to communicate on the LAN wirelessly.

3. **B.** A switch sends frames of data between computers by identifying the systems by their MAC addresses. A hub broadcasts data out to all computers. The computer that it is meant for accepts the data; the rest of the computers drop the information. Routers enable connections with individual high-speed interconnection points, and route signals for all the computers on the LAN, out to the Internet. A modem is a device that allows a computer to access the Internet by changing the digital signals of the computer to analog signals used by a typical land-based phone line.

4. **B.** A Power over Ethernet (PoE) injector sends Ethernet data and power over a single twisted pair cable to a remote device. A PD, which stands for powered device, is a PoE-compliant remote device that is receiving the power. A repeater extends the distance of a network connection. A firewall is a device (or software) that secures ports on a network or on an individual system. A router makes connections from one network to another or from the LAN to the Internet.

5. **A.** Managed switches can be configured when accessed from a browser or SSH or similar configuration tool. For example, you can change the device's IP address, configure ports, and monitor the switch and other devices using SNMP. On the other hand, unmanaged switches don't have these capabilities; they simply connect devices and computers for transmission of data over the Ethernet network. A patch panel is a physical hardware device that acts as a termination point for all of the network cables in a

building. A network interface card (NIC) allows for connectivity to a computer network. It is a physical device that can be added to a computer or networking device that has an open and compatible slot.

6. **B.** An optical network terminal (ONT) is a type of network interface device (gray box) used to take an incoming fiber optic line from a provider and split it off to a customer's premises for the purposes of Internet access, voice calls, and television. Often, the cables that go from the ONT to the inside of the customer's premises are copper based (coaxial or possibly twisted pair). Software-defined networking (SDN) is a method of administering multiple network devices with a controller program. A patch panel is a device that terminates twisted pair cables on one side and has ports for patch cables on the other (to be connected to a switch). A network interface card (NIC) is an adapter card that can be installed to a PC that allows the system to access a wired network. Don't confuse a NIC with a NID!

You are unstoppable. Be sure to review the ExamAlerts and continue!

Chapter 9

SOHO Network Configuration

This chapter covers the following A+ 220-1201 exam objective:

- **2.6** – Given a scenario, configure basic wired/wireless small office/home office (SOHO) networks.

In Chapter 6, "Networked Hosts" we discussed a lot of theory about servers, services, and networked hosts. Now, let's get more hands-on, especially with TCP/IP configurations. In this chapter, we'll discuss IP addressing, dynamic IP assignment, name-to-IP address resolution, and gateway IP addressing.

Without IP addresses, computers can't communicate, so it's vital that you know IP addressing frontward and backward. This could be considered one of the most important chapters in the book, and it's packed with information. It's time to network!

ExamAlert

Objective 2.6 focuses on the following concepts: Internet Protocol (IP) addressing; IPv4 and IPv6; Automatic Private IP Addressing (APIPA); and static, dynamic, subnet mask, and gateway addressing.

Configuring IPv4

Let's look at how to configure IPv4 addresses in Windows. First, you navigate to the Internet Protocol (TCP/IP) Properties window, which we often refer to as the IP Properties dialog box. To do this, open the Network Connections window (search for it, or go to Run and type **ncpa.cpl**). Then right-click the **Ethernet** icon and select **Properties**. Finally, highlight **Internet Protocol Version 4** and then click the **Properties** button.

> **Note**
>
> Navigation may differ slightly depending on the version of Windows and the way it is configured. Be ready for alterations over time and be ready to use the search tool to simplify the process (or the Run prompt, whenever possible).

The first item to be configured is the IP address, which is the unique assigned number of a computer on the network. An IPv4 address consists of four octets, with each octet's value ranging between 0 and 255. The octets are separated by dots (for example, 192.168.0.100). The binary equivalent of 0–255 would be 00000000 through 11111111. For example, 192 is equal to 11000000 in binary. Because each octet contains 8 bits and there are four octets, the IP address collectively is a 32-bit number but is normally expressed in dotted-decimal notation.

There are two main types of addresses: dynamic and static. Dynamically assigned addresses are more common for a client computer; with this type of address, a computer seeks out a DHCP server so that it can get its IP information automatically. Figure 9.1 shows a radio button labeled **Obtain an IP address automatically**. When you select this, the rest of the information becomes grayed out, and the computer attempts to get that IP information from a DHCP server (such as a SOHO router or Windows Server). That DHCP server has a range of IP addresses configured by an administrator—also known as a DHCP scope. One of those addresses in the range will be selected for the client computer.

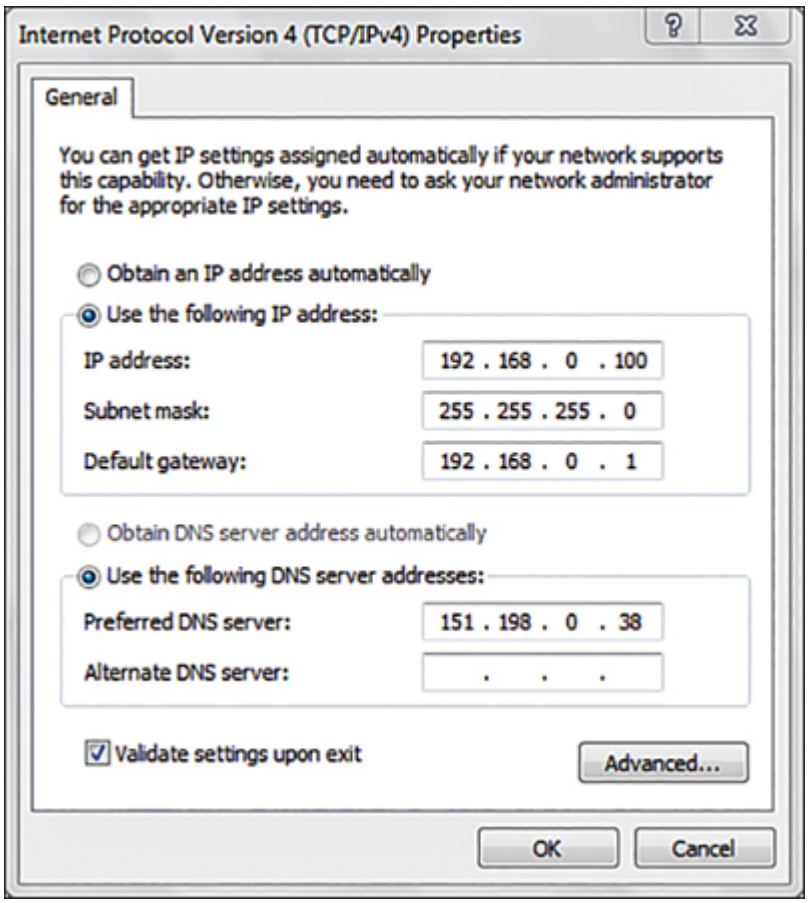


FIGURE 9.1 **Internet Protocol Version 4 Properties Dialog Box in Windows**

For client computers, DHCP is common; in fact, it's the default configuration for Windows. On the other hand, static addresses are generated when you configure the IP information manually. Figure 9.1 shows an example of statically configured IP settings. The computer is configured to use the address 192.168.0.100, but the IP address differs from machine to machine, depending on several factors. Remember that the address should be unique for each computer on the network.

ExamAlert

Know the difference between static and dynamic IP addresses.

IP addresses can also be self-assigned by the computer. In Windows, this process is known as *Automatic Private IP Addressing (APIPA)*, and it occurs when a computer cannot contact a DHCP server to obtain an IP address. When APIPA self-assigns an address, the address is on the 169.254.0.0 network. Addresses on this network are also known as *link-local* addresses.

ExamAlert

APIPA (Automatic Private IP Addressing) is a system used on Windows to automatically self-assign an IP address in the 169.254.x.x range in the absence of a DHCP server.

IP addresses are 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 number of the individual computer. The subnet mask defines which portion of the IP address is the network number and which portion is the individual host number. In this case, the subnet mask is 255.255.255.0. The 255s indicate the network portion of the IP address. So, 192.168.0 is the network this computer is a member of. The 0s (or, in this case, only one zero) indicate the host number, so 100 is the individual number of this computer. Quite often the subnet mask is configured automatically by Windows after you type the IP address.

ExamAlert

Remember that an IPv4 subnet mask is a 32-bit address used to mask, or screen, a portion of an IP address to differentiate the part of the address that designates the network and the part that designates the host. IPv6 uses a prefix length instead of a subnet mask, which is an integer between 1 and 128. The prefix length determines how many bits of an address define the network to which it belongs.

The gateway address is the IP address of the host that enables access to the Internet or to other networks. The IP address of the gateway should always be on the same network as the computer(s) connecting to it. In Figure 9.1, you can see that it is because the first three octets are 192.168.0. If a computer is not configured with a default gateway address, it cannot connect to the Internet.

ExamAlert

Remember that a default gateway is normally a router or a multihomed computer to which packets are sent when they are destined for a host on a different or remote network. To use the gateway, computers must be on the same network number as the gateway device.

The DNS server address is the IP address of the host that takes care of domain name translation to IP. When you use your browser to connect to a website, you might type something like **www.demosite.com**. What you need to remember, however, is that computers actually communicate using IP addresses, not names. So, the DNS server takes care of translating the name demosite.com to its corresponding IP address and forwarding that information back to your computer. When your computer knows the IP address of the website, it can start a session with the website and transmit and receive files. Notice in Figure 9.1 that the DNS server address is on a completely different network from my computer. This is typical; in this case, the DNS server is run by the Internet service provider (ISP) that provides the Internet connection. However, DNS servers can also be run internally by a company; this happens most often with larger companies.

ExamAlert

Know where and how to configure client-side DNS and DHCP settings.

Notice the checkbox labeled Validate Settings Upon Exit. If you set up a static IP address on a computer, you should select this checkbox. This way, when you click the OK button for the IP Properties dialog box, Windows checks whether the configuration works properly and lets you know when any basic errors arise. The IP configuration might have an incorrect DNS server, gateway address, or IP network number.

Challenge: Configuring IP with PowerShell

Tired of clicking around the GUI? Use PowerShell! For example, to set a static IP address for a Windows computer, the syntax would be

```
netsh interface ip set address "connection name" static <IPv4 addr
<IPv4 mask> <gateway>
```

Here's a real example:

```
netsh interface ip set address "Ethernet" static 192.168.0.100
255.255.255.0 192.168.0.1
```

Try configuring a new IP address on a (test) Windows system now. Because this is an important task, you need to run PowerShell as an administrator. To do this, go to **Start**, type **Windows PowerShell**, right-click on **Windows PowerShell**, and select **Run as administrator**. Alternatively, you can open the Run prompt (Windows+R), type **powershell**, and then press Ctrl+Shift+Enter. Remember to return your computer back to normal when you are done. If your system was obtaining an IP address automatically from a DHCP server, then you could reset that in the IP Properties dialog box or use the following syntax:

```
netsh interface ip set address "connection name" dhcp
```

Chances are, you'll need PowerShell in the field. Find it and use it.

You're not done yet! If your IP Properties dialog box is set to Obtain an IP Address Automatically, then you will also see the Alternate Configuration tab. This tab enables you to have a secondary IP configuration. Let's say that you use a laptop at work and get your IP address from a DHCP server, but you also go on the road as part of your job. The alternate configuration would kick in automatically when you are away from the office and allow you access to the Internet or to virtual private networks, depending on your

configuration. The alternate configuration can be on a completely different IP network from the main configuration.

Speaking of secondary IP addresses, every computer running TCP/IP has an additional address known as a *loopback* address. By default, this is 127.0.0.1 in IPv4 (::1 in IPv6), and it can be used to test TCP/IP on the local machine, regardless of whether the system is plugged into the network. Try running **ping 127.0.0.1** or **ping loopback -4** in PowerShell or the Command Prompt to test your system internally. Remember that replies are good!

Private vs. Public Addresses

Let's consider the difference between private and public IP addresses.

- **Private:** Private IP addresses are internal to your network and do not communicate directly with the Internet. The IP address assigned to the client in Figure 9.1 (192.168.0.100) is an example of a private IP address. Contrast this with the public IP address.
- **Public:** A public IP address is an address that communicates directly with the Internet. The DNS server IP address in Figure 9.1 (151.198.0.38) is an example of a public IP address.

You use private IP addresses on LANs and internal networks to provide a certain level of protection and anonymity to client computers, as well as to conserve IPv4 addresses in general. However, the client computers need to access the Internet, so your network needs some sort of gateway device that connects all of the private systems to the Internet by way of a public IP address. Similarly, if you have a server that needs to be accessed by users on the Internet, it needs to have access to a public IP address—either directly or indirectly.

Private IP network numbers can be used by anyone in the internal network. The reserved private IP address ranges include

- **Class A addresses:** 10.0.0.0–10.255.255.255
- **Class B addresses:** 172.16.0.0–172.31.255.255

- **Class C addresses:** 192.168.0.0–192.168.255.255

Public IP addresses are assigned to customer equipment by ISPs. The Internet Assigned Numbers Authority (IANA) is responsible for global coordination of public IP addresses.

Let's look at an example of a device that uses both types of addresses—a typical small office/home office (SOHO) router.

A SOHO router normally obtains a public IP address from the ISP; it is dynamically assigned and is also known as the WAN address. The public address is visible on the Internet. The router also has a private address (or LAN address), which is visible only to the computers on the network. That is the address you use to log in to the router (for example, 192.168.0.1 or 192.168.1.1) and also acts as the gateway address for the clients on the network. Figure 9.2 shows the LAN and WAN settings on a typical SOHO router.

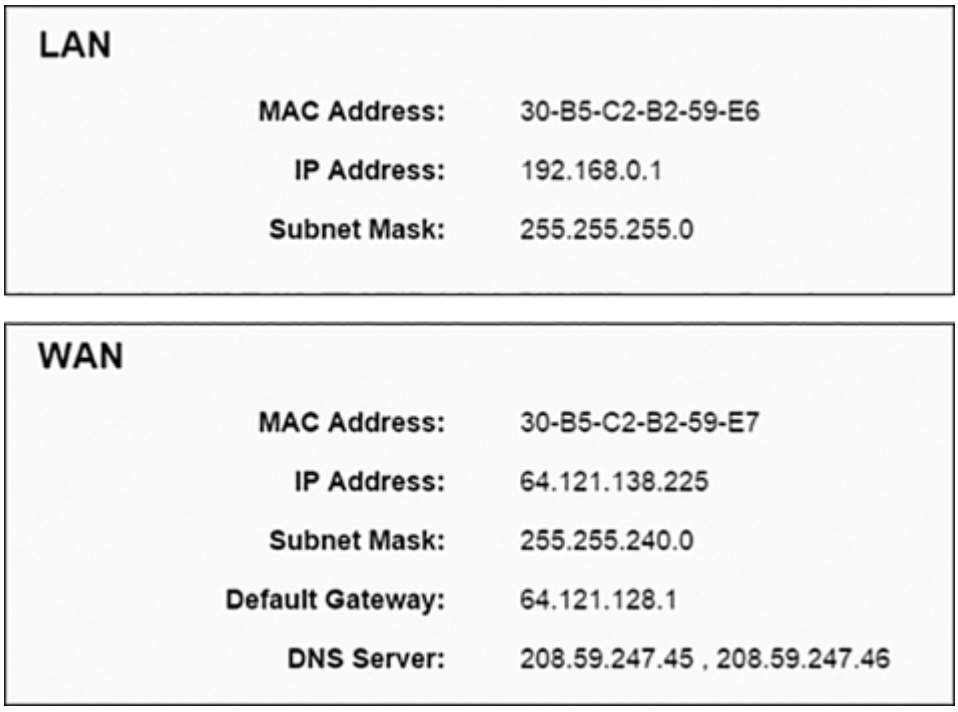


FIGURE 9.2 **LAN and WAN Settings on a Typical SOHO Router**

As you can see in this figure, the router's LAN address is 192.168.0.1. This device makes use of DHCP, which can be turned on or off. When on, it

automatically assigns IP addresses to most of the clients on this network, starting with 192.168.0.100 and ascending from there—192.168.0.101, 192.168.0.102, and so on. The router and all of the clients are on the same local area network number (192.168.0.0), using the same subnet mask (255.255.255.0), which means they can all communicate with each other.

The public address allows the entire network access to the Internet. The router acts as the connection between the private and public networks. It allows for the transmission of data between the clients and the Internet, using a technology called Network Address Translation (NAT).

NAT modifies IP addresses as information crosses a router. It hides an entire IP address space on the LAN (for example, 192.168.0.1 through 192.168.0.255). Whenever an IP address on the LAN wants to communicate with the Internet, NAT converts the IP address to the public IP address of the router (for example, 64.121.138.225), which is whatever IP address the ISP assigned to the router. This way, it looks like the router is the only device making the connection to remote computers on the Internet, providing a modicum of safety for the computers on the LAN. To summarize, with NAT, a single public IP address does the work for many private IP addresses in the LAN.

ExamAlert

Private IP addresses are internal and do not connect directly to the Internet. Public IP addresses allow direct connectivity to the Internet and are visible by anyone with an Internet connection.

Classful vs. Classless IP Addresses

The IPv4 system of IP addresses is divided into classes A, B, and C, where specific subnet masks correspond to each class; this is known as classful IP addressing. For example, class C addresses use subnet mask 255.255.255.0. While IP address classes can still be used, most companies today opt for a network that is classless, using CIDR (classless interdomain routing)—pronounced *cider*. With CIDR, any subnet mask can be used for any IP network.

The important part to understand is that the 255s of a subnet mask relate to the network portion, and the 0s correspond to the host portion of the IP address. For example, if the IP address

10.252.0.101 uses the subnet mask 255.255.0.0, then the network portion is 10.252. The IP address and subnet mask can be written together in the following manner: 10.252.0.101/16.

Configuring IPv6

Although acceptance has been slow over the years, IPv6 is the next generation of IP addressing. IPv6, which is used on the Internet and on some LANs and WANs, is designed to address the inadequacies of IPv4. One of the main reasons for the development of IPv6 was the rapidly approaching global shortage of IPv4 addresses. Whereas IPv4 (a 32-bit system) can have approximately 4 billion total theoretical addresses, IPv6 (128-bit) can have a total of 340 *undecillion* theoretical addresses—a far greater total. Various limitations of the system will drastically reduce that number, but the remaining result is still orders of magnitude above and beyond the IPv4 system. However, IPv6 is also known for security. One feature of IPv6 security is IPsec (IP Security), which authenticates and encrypts data packets that are sent over IP networks. IPsec is a fundamental piece of the IPv6 puzzle and, if used properly, it can offer much more secure communications than IPv4. IPv6 also supports larger packet sizes, known as jumbograms. Table 9.1 summarizes some of the differences between IPv4 and IPv6.

TABLE 9.1 **IPv4 vs. IPv6**

IPv4	IPv6
32-bit	128-bit
4 billion addresses	340 undecillion addresses
Less secure	More secure; uses IPsec
65,536-byte maximum packet size	4 billion-byte maximum packet size

IPv6 addresses are 128-bit hexadecimal numbers that are divided into eight groups of four numbers each. The most commonly used type is the unicast address, which defines a single IP address on a single interface (such as a network adapter). Windows autoconfigures a unicast address when IPv6 is installed. The address starts with FE80, FE90, FEA0, or FEB0.

Collectively, this range is shown as FE80::/10, and it comprises all of the link-local addresses for IPv6. These link-local addresses are often based on the MAC address of the network adapter. Every Windows computer with IPv6 installed also receives the loopback address ::1. The IPv6 address ::1 is the equivalent to IPv4's loopback address 127.0.0.1. To test it, type **ping ::1** or **ping loopback -6** in PowerShell or the Command Prompt.

ExamAlert

Know the loopback addresses for IPv6 and IPv4.

Here's an example of an IPv6 address:

2001:7120:0000:8001:0000:0000:0000:1F10

An IPv6 address is broken down into three sections: the global routing prefix (in this case, 2001:7120:0000), a subnet (in this case, 8001), and the individual interface ID (in this case, 0000:0000:0000:1F10).

This is the full address, but you will more commonly see truncated addresses. There are two ways to truncate, or shorten, an IPv6 address. The first is to remove leading zeros. Any group of four zeros can be truncated to a single zero; basically zero is always zero, so the additional zeros are not necessary. Also, a single consecutive group of zeros can be truncated as a double colon (::). The example shows 12 consecutive zeros that can be truncated to a double colon. (A double colon can be used only once in an address.) The following is the end result of both of these abbreviations:

2001:7120:0:8001::1F10

ExamAlert

Understand how IPv6 addresses can be truncated.

Although it is not common, IPv6 addresses can be assigned statically as well; this can be done within the Internet Protocol Version 6 Properties dialog box, which can be accessed from Local Area Connection Properties.

Cram Quiz

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

1. Which of these addresses needs to be configured to enable a computer access to the Internet or to other networks?

   - ○ **A.** Subnet mask
   - ○ **B.** Gateway address
   - ○ **C.** DNS address
   - ○ **D.** MAC address

2. Which technology assigns addresses on the 169.254.0.0 network?

   - ○ **A.** DHCP
   - ○ **B.** Static IP
   - ○ **C.** APIPA
   - ○ **D.** Class B

3. You want to test the local loopback IPv6 address. Which address would you use?

   - ○ **A.** 127.0.0.1
   - ○ **B.** ::1
   - ○ **C.** FE80::/10
   - ○ **D.** ::0

4. Which of the following IP addresses would you configure so that the computer can take advantage of hostname-to-IP address resolution?

   - ○ **A.** 127.0.0.1 (local loopback)
   - ○ **B.** 192.168.0.1 (gateway)
   - ○ **C.** 8.8.8.8 (DNS)
   - ○ **D.** 255.255.255.0 (subnet mask)

5. Of the following, which is a common use for NAT?

   - ○ **A.** Defining the network portion of an IPv4 address
   - ○ **B.** Connecting multiple computers using a single public IP address
   - ○ **C.** Resolving hostnames to IP addresses
   - ○ **D.** Automatically assigning TCP/IP addresses

Cram Quiz Answers

1. **B.** The gateway address must be configured to enable a computer access to the Internet through the gateway device. By default, the subnet mask defines the IP address's network and host portions. The DNS server takes care of name resolution. The MAC address is the address that is burned into the network adapter; it is configured by the manufacturer.

2. **C.** If you see an address with 169.254 as the first two octets, then Automatic Private IP Addressing (APIPA) is in use. This is the link-local range for IPv4. Dynamic Host Configuration Protocol (DHCP) assigns IP addresses automatically to clients but by default does not use the 169.254 network number. Static IP addresses are configured manually by the user in the IP Properties window. Class B is a range of IP networks from 128 through 191.

3. **B.** You would use the ::1 address, which is the local loopback address for IPv6. 127.0.0.1 is the local loopback address for IPv4.

FE80::/10 is the range of unicast autoconfigured addresses. ::0 is not valid but looks similar to how multiple zeros can be truncated with a double colon.

4. **C.** You would use a DNS server IP address. 8.8.8.8 is an example of a DNS server IP address run by Google. Anyone in the United States and many other countries is allowed to use it for DNS resolution. Remember that the DNS server is in charge of resolving (or translating) hostnames and domain names to their respective IP addresses. Note that in this example (and in Figure 9.1), the DNS server uses a public IP address. However, depending on your network configuration, clients might be set up with a DNS server that uses a private IP address (such as 192.168.1.1), which simply means that DNS is being forwarded by that system out to a DNS server on the Internet. 127.0.0.1 (the local loopback address) is the internal loopback address on any system running TCP/IP. The gateway address (for example, 192.168.0.1) allows a system access to the Internet or to other networks. The subnet mask (for example, 255.255.255.0) defines the network and host portions of an IP address.

5. **B.** Network Address Translation (NAT) is used to convert private IP addresses to public IP addresses. It allows for the connection of multiple private computers through a single public IP address (usually using some sort of router). The subnet mask defines the network portion of an IP address. DNS is in charge of resolving hostnames to IP addresses. DHCP is responsible for automatically assigning TCP/IP addresses.

Whoa! That was a power packed chapter. We strongly suggest you *carefully* review this one. Keep up the great work!

Chapter 10
Network Types

This chapter covers the following A+ 220-1201 exam objective:

- **2.7** – Compare and contrast Internet connection types, network types, and their characteristics.

In this chapter, we'll discuss the types of Internet connections available to the typical small office/home office (SOHO) user, as well as the basics of enterprise Internet connectivity. But first we'll cover computer network *types*—such as local area networks and wide area networks. Be prepared; there are a lot of acronyms when it comes to network types. Be ready to take notes and write down each acronym and what it stands for as we progress through the chapter.

ExamAlert

Objective 2.7 concentrates on the following concepts: Internet connection types (cable, DSL, fiber, satellite, cellular, and WISP), and network types (LAN, WAN, PAN, MAN, SAN, and WLAN).

Network Types

It's important to know how networks are classified. Two common terms are LAN and WAN. But you should also know the terms MAN, SAN, PAN,

and WLAN. Let’s begin with LAN and WAN.

LAN and WAN

A local area network, or *LAN*, is a group of computers and other devices usually located in a small area: a house, a small office, or a single building. The computers all connect to one or more switches, and a router allows the computers access to the Internet. Generally, there are no other routers internally. Technicians might use phrases such as “Connect the computer to the LAN” or “How many computers are on your LAN?” A LAN is usually based on a network design called the star, or hub-and-spoke, topology, where all hosts connect to a central connecting device such as a switch, an access point, or a SOHO router. Figure 10.1 shows an example of a typical LAN configured using the hub-and-spoke/star topology.

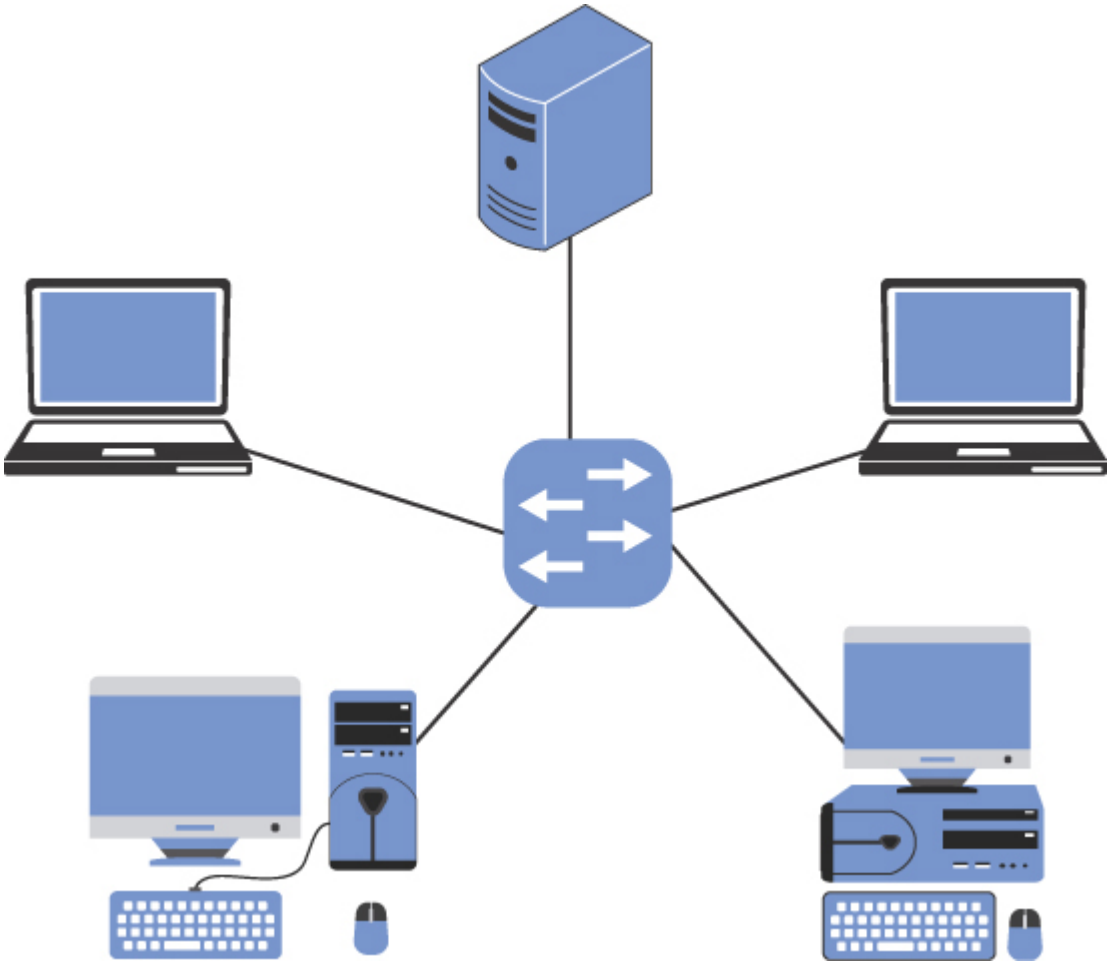


FIGURE 10.1 **A Typical LAN Using the Hub-and-Spoke/Star Topology**

A wide area network, or *WAN*, is a group of one or more LANs over a large geographic area. Let's say a company has two LANs: one in New York and one in Los Angeles. Connecting the two would result in a WAN. However, to do this, the company would require the help of an Internet service provider (ISP) or a telecommunications company. This provider would supply the high-speed connection required for the two LANs to communicate quickly. Each LAN would need a router for the two to connect to each other. A network administrator or network engineer or facilities department would be in charge of selecting an Internet service for the link between the offices. We'll discuss some of those Internet service options later in the chapter.

MAN

There is a smaller version of a WAN known as a metropolitan area network (*MAN*) and sometimes called a municipal area network. Say that a company has two offices in the same city and wants to make a high-speed connection between them; the connected offices' networks form a MAN. It's different from a WAN in that it is not a large geographic area, but it is similar to a WAN in that an ISP is needed for the high-speed link.

SAN

A storage area network (SAN) is a dedicated network designed specifically for the storage of data. Moreover, it is a network of data storage devices that are connected together on a typical LAN or by way of a special high-speed fiber optic connection such as Fibre Channel. The network consists of components such as network-attached storage (NAS) devices, RAID arrays, tape backup devices, and a switch to connect it all together. The idea is to allow for high-speed access to data without bogging down the servers that control and request that data. This separates the servers' functionality from the data storage and also allows for an admin to potentially make data more secure, redundant, and highly available. SANs are subsets of LANs and

offer block-level data storage that appears within the operating systems of the connected devices as locally attached devices.

ExamAlert

Fibre Channel is widely used for high-speed fiber networking and has become common in enterprise SANs.

WLAN

A wireless local area network (*WLAN*) is really a subdivision of a LAN. A WLAN is formed when multiple computers are connected by way of one or more wireless access points. (We use the term *computers* loosely here to refer to PCs, laptops, tablets, smartphones, IoT devices, and so on.) WLAN protocols are defined in the IEEE 802.11 set of technical standards. Common standards that you should know include 802.11a, b, g, n, ac, ax, and be. For more information on WLANs and Wi-Fi, refer to Chapter 5, "Wireless Technologies."

WMN

Another network type is a wireless mesh network (*WMN*). Generally, with a mesh, wireless access points (or nodes) have multiple connections to each other in a matrix (or *mesh*) pattern. Implementing a mesh can help greatly with redundancy and availability.

In a WMN, multiple wireless access points are used on the same channel. This allows for greater coverage in larger environments. As mobile devices move around the building or buildings, they quickly transition from one access point to another. In a WMN, the APs do not have to be physically cabled to a wired port, as is the case with a traditional AP or wireless extender. However, the APs must have built-in mesh capability, which often means increased cost. This technology can provide a more efficient solution than traditional wireless extenders, and it also enables centralized management. Although it is not listed in the current A+ exam objectives,

you should know that a WMN can be used in larger infrastructures and also in simpler SOHO environments (where it might be referred to as mesh Wi-Fi, Wi-Fi ad hoc, or a similar name).

PAN

A personal area network (*PAN*) is a smaller computer network used for communication by small computing devices. Take this to the next level by adding wireless standards such as Bluetooth, wireless USB, NFC, Zigbee, or Z-Wave, and you get a wireless PAN (*WPAN*). PANs are sometimes ad hoc, meaning there is no single controlling device, server, or access point. However, they might be controlled by a hub and gain access to the Internet from that device.

ExamAlert

Remember that a PAN is a network layout whereby devices work together in close proximity to share information and services, commonly using technologies such as Bluetooth or infrared.

ExamAlert

Be able to define, compare, and contrast LAN, WAN, MAN, SAN, WLAN, and PAN.

Internet Connection Types

There are a lot of different options for connecting to the Internet, including fiber-based systems, DSL, cable Internet, 5G and even the venerable dial-up, and more. The type of Internet connection dictates download speeds to the clients on a network. Let’s discuss some of the options available, starting with cable Internet.

Cable Internet

Broadband cable, used for cable Internet and cable TV, is very common in the United States and many other countries. It offers download transfer rates from 50 Mbps to 1000 Mbps (depending on the ISP). Upload speed is almost always slower—a fraction of the download speed. Like most other Internet connectivity options, cable Internet is shared by the customer base. The more users who are on the Internet, the slower it becomes for everyone. Cable Internet is a common option for home use and for SOHO networks that use a router to allow multiple computers access to the Internet via a cable. An RG-6 coaxial cable is run into the home or office and connected to a cable modem by way of a screw-on F-connector. The cable modem also has an RJ-45 connection for patching to the router or to an individual computer's network adapter.

Note

We'll discuss cables and ports in Chapter 13, "Cables and Connectors."

ExamAlert

Know that cable Internet connections use RG-6 coaxial cable and F-connectors to the cable modem.

Note

Dial-up Internet is still used by some people around the world. It is based on POTS (plain old telephone service) and landlines that connect to phones and dial-up modems by way of an RJ-11 connection, resulting in a typical data transfer rate of 56 Kbps—much slower than today's broadband Internet solutions. This might be the only solution for people in some rural areas and also areas where it is impossible to get access to any broadband technologies.

DSL

Digital subscriber line (DSL) builds on dial-up by providing full digital data transmission over phone lines but at higher speeds. DSL modems connect to the phone line and to the PC's network adapter or to a SOHO router to enable sharing among multiple computers. One of the benefits of DSL is that you can talk on the phone line and transmit data at the same time. There are several derivatives of DSL, including

- **ADSL (Asymmetrical Digital Subscriber Line):** ADSL enables transmission over copper wires that is faster than dial-up. It is generally geared toward consumers who need more downstream bandwidth than upstream. Because the downloading and uploading speeds are different, it is known as an *asymmetric* technology. A group of ADSL technologies offer data transfer rates of anywhere from 8 Mbps download/1 Mbps upload to 52 Mbps download/16 Mbps upload, although newer broadband options like fiber and advanced cable services have become more widely available. ADSL is often offered to consumers who cannot get cable Internet.
- **SDSL (Symmetrical Digital Subscriber Line):** SDSL is installed (usually to companies) as a separate line and is usually more expensive than ADSL. With SDSL, upload and download speeds are the same, or *symmetrical*. Maximum data transfer rates for typical versions of SDSL are 1.5 Mbps and 5 Mbps (depending on the version).

Fiber

Instead of using a copper connection to the home or business in the way cable Internet, DSL, and dial-up do, some companies offer fiber optic connections directly to the customer. With fiber to the premises (FTTP), optical fiber is installed and used from a central point directly to individual buildings, such as residences, apartment buildings, and businesses.

FTTP service typically runs over a fiber optic line to a network interface device (NID) at the home or office (specifically an optical network

terminal); from there, it changes over to copper, which then makes the connection to the customer's router or individual computer. This copper connection could be a twisted pair patch cable (for example, a Cat 6 cable) or a coaxial cable using the Multimedia over Coax Alliance (MoCA) protocol. Examples of companies that offer FTTP include Verizon (Fios) and Google (Google Fiber).

Note

There are other varieties of fiber available to the customer, and they are defined by the point where the fiber ends and the copper begins. Collectively, they are referred to as "fiber to the *x*," where *x* equals the endpoint for the fiber run.

Fiber optic cables can run at much higher data transfer rates than copper-based cables. Home-based fiber optic Internet connections can typically download data between 100 Mbps and 1000 Mbps. Upload speeds are typically less, as they are in most other Internet services, but they are substantially higher than other broadband options.

Satellite

With satellite connectivity, a parabolic antenna (satellite dish) connects via line-of-sight to a satellite; it is used in places where standard landline-based Internet access is not available. The satellite is in geosynchronous orbit, at 22,000 miles (35,406 km) above the Earth. This is the farthest distance of any Internet technology. A satellite dish connects to coaxial cable that runs to a switching/channeling device for the site's computers. Today's satellite connections offer speeds close to those of traditional broadband access such as cable Internet.

One of the issues with satellite connectivity is electrical and natural interference. Another problem is latency. Due to the distance (44,000 miles in total) of the data transfer, there can be a delay of .5 to 5 seconds. That's the highest latency of any Internet technology. Latency goes hand-in-hand with distance. In the past, satellite-based Internet connections offered high-

speed downloads, but uploads were slow due to the fact that the service would use a dial-up line to upload information. Newer satellite Internet technologies allow for the upload of data to the satellite as well, and while uploads are often still slower than download speeds, it is much faster than uploading via dial-up.

Satellite-based Internet is growing quickly. For example, SpaceX has a growing constellation of orbital satellites and is currently bringing Internet access to people around the world living without access to high-speed Internet.

Wireless Internet Service Provider

A wireless Internet service provider (WISP) is an ISP that specializes in wireless networking and builds a wireless mesh network using one of several licensed or unlicensed frequency bands. A WISP's main function is to provide Internet service to customers who cannot obtain service from cable, DSL, or fiber providers or who do not want those services. Originally, WISPs serviced rural areas and other areas where it is difficult to run cable. Today there are millions of wireless Internet customers in rural, suburban, and urban areas.

The technology starts with a fiber line that is run to the center of the geographic area that will be providing access to customers. That line is extended to a high point such as a radio tower, a tall building, or another tall structure. From there, a mounted access point of some sort is used to communicate with customers or other towers in the wireless mesh network. A customer receives a small antenna (parabolic or another type) that is installed on the customer's roof and aligned to the WISP's nearest antenna. The customer's antenna is then wired down to the customer's network. Some WISP services require that the customer's antenna be line-of-sight. Line-of-sight, or *fixed*, wireless Internet service requires the customer's reception device to face the access point at the tower or ground station of the provider—without obstruction.

Note

Cellular is also listed in the CompTIA objectives. For more information on cellular technologies, see Chapter 3, "Mobile Device Network Connectivity and Application Support."

Cellular

Cellular Internet connections use mobile networks to provide Internet access. These connections are based on technologies such as 4G LTE and 5G, which offer varying speeds and reliability depending on network coverage and provider infrastructure. Cellular Internet is ideal for mobile devices like smartphones, tablets, and laptops with built-in cellular modems or external USB dongles. Speeds typically range from a few Mbps to over 1 Gbps on advanced 5G networks. Cellular connections rely on mobile towers and are particularly beneficial in areas without cable, DSL, or fiber access. These connections also support tethering or mobile hotspots, enabling devices without cellular modems to share Internet access via Wi-Fi or USB. The flexibility and expanding coverage of cellular Internet make it a viable option for home, SOHO, and remote workers.

Cram Quiz

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

1. Which of the following is a group of Windows desktop computers located in a small area?

   - ○ **A.** LAN
   - ○ **B.** WAN
   - ○ **C.** PAN
   - ○ **D.** MAN

2. What kind of cable and connector are used with cable Internet service to connect to the customer's "modem"?

   - **A.** Twisted pair and RJ-11
   - **B.** 802.11ax and antenna
   - **C.** Fiber and ST
   - **D.** RG-6 and F-connector

3. Which of the following might make use of Fibre Channel connections?

   - **A.** WAN
   - **B.** SAN
   - **C.** DSL
   - **D.** Cable Internet
   - **E.** WISP

Cram Quiz Answers

1. **A.** A local area network (LAN) is a group of computers, such as a SOHO network, located in a small area. A wide area network (WAN) is a group of one or more LANs spread over a larger geographic area. A personal area network (PAN) is a smaller computer network used by smartphones and other small computing devices. A metropolitan area network (MAN) is a group of LANs in a smaller geographic area, such as a city.

2. **D.** Cable Internet connections use an RG-6 coaxial cable that is run from a NID to the customer's cable modem. It is connected by way of an F-connector. Twisted pair cables and RJ-11 might be used by DSL or dial-up. 802.11ax is a WLAN protocol. Fiber-based services might indeed use an ST connector, but this question asks about cable Internet service.

3. **B.** A storage area network (SAN) often makes use of Fibre Channel connections and switches to connect NAS points and other data storage devices together into a super-fast network. A wide area network (WAN) is a network that connects two or more LANs together. Digital subscriber line (DSL) is a type of Internet service, as are cable Internet and wireless Internet service providers (WISPs).

Well, at this point you might be suffering from networking on the brain. But there's only one more networking chapter left. Take a small break and continue on. You're doing awesome!

Chapter 11
Networking Tools

This chapter covers the following A+ 220-1201 exam objective:

- **2.8** – Explain networking tools and their purposes

Let's wrap up the computer networking section of this book with a shorter chapter on the types of tools used for network connectivity and network testing.

For this objective, you should know some of the cabling and networking tools that can help you create, modify, and troubleshoot network patch cables and longer network cables that terminate at patch panels and RJ-45 jacks. We'll also briefly talk about network taps that can be used to analyze data, as well as Wi-Fi analyzers that can be used to identify wireless networks.

Of course, you will continue to use your networking knowledge as you progress through the book—especially as you get to the operating systems chapters—and as you advance in the IT field. One of the goals of this book is to help you retain knowledge over the long term. Remember to take notes and quiz yourself often. At the end of each domain (such as this one, Domain 2.0: Networking), review what you have learned throughout the section. This will help you transition to other areas of the book.

ExamAlert

Objective 2.8 focuses on the following networking tools: crimper, cable stripper, Wi-Fi analyzer, toner probe, punchdown tool, cable tester, loopback plug, and network tap.

Network Cabling Tools

If you plan to build or troubleshoot a physical network, you need to stock up on some key networking tools that will aid you when running, terminating, and testing cable. For this short section, imagine a scenario where you are the network installer and are required to install a wired network for 12 computers.

To start, you should check with your local municipality to see if there are any rules and regulations related to running networking cable. Some municipalities require an installer to have an electrician's license. Some require only an exemption of some sort that anyone can apply for at the town or county seat. Due to the low-voltage nature of network wiring (for most applications), some municipalities have no rules regarding this wiring. But in urban areas, you will need to apply for a permit and have at least one inspection done when you are finished with the installation.

Permits and regulations aside, let's say that in this scenario, you have been cleared to install 12 wired connections to computers (known as cable *runs* or *drops*). You have diagrammed where the cables will be run and where they will terminate. All cables will come out of a wiring closet, where you will terminate them to a small patch panel. On the other end, they will terminate at in-wall RJ-45 jacks near each of the computers. Wire termination is the work performed at each end of a cable that allows it to connect to a physical endpoint such as a jack or a patch panel. These are the networking tools that you will use to complete this job.

- **Cable cutter:** The first tool you should have is a good, sharp cutting tool. You need to make a clean cut on the end of the network cable; scissors will not do. Either cut pliers or other cable cutting tools are necessary.

- **Cable stripper:** A cable stripper (or wire stripper) is used to strip a portion of the plastic jacket off the cable to expose the individual wires. At this point, you can separate the wires and get ready to terminate them with a punchdown tool.
- **Punchdown tool:** A punchdown tool is a device that 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. This tool can also be used to terminate twisted pair wires to a punchdown block—either a 110 block for data or a 66 block for telecommunications.
- **Cable testers:** The last tool necessary for the job is a cable testing tool. You have a few options here:
  - The best option is a proper network cable tester, also known as a continuity tester or cable certifier. This device has a LAN testing unit that you can plug into a port on the patch panel and a terminator that you plug into the other end of the cable in the corresponding RJ-45 jack (or vice versa). This tool tests for continuity and tests each wire in the cable, making sure each one is wired properly.
  - Another option is a tone generator and probe kit (also known as a *toner/probe* or *fox and hound*). This kit consists of two parts: a tone-generating device, which connects to one end of the network cable and, when turned on, sends a tone along the length of the cable; and a probing device, also known as an inductive amplifier, which can detect the tone anywhere along the cable length and at the termination point. This tool is not as good as a proper network cable tester because it tests only one of the pairs of the wires. However, it is an excellent tool for finding individual phone lines and is most commonly used for that. You can also use a multimeter to do various tests of individual lines, but it is usually not necessary if you own the other tools mentioned. The cable tester mentioned previously can usually create tone as well.

At this point, the cables have been run, terminated on both ends, and tested. The only other thing you need is patch cables. The patch cables connect the various ports of the patch panel to a switch and the RJ-45 jacks to the computers.

- **Crimper:** You usually buy patch cables for a couple of dollars each and are done with it. However, you can make them too. To do so, you have to purchase cable as well as RJ-45 plugs. Make sure that the cable and plugs meet the cabling standard you decide to use, such as Category 5e, Category 6, or higher. You attach the plugs to the cable ends with an RJ-45 crimping tool. This tool can be especially handy when you need to make a crossover patch cable, which can be used to connect a computer to another computer directly. There are other types of crimpers for coaxial cable as well.
- **Patch tester:** Before connecting the patch cables, you should test them with a patch tester. This device has two RJ-45 jacks; you plug each end of the patch cable into the tester and then press the button to make sure each wire makes a proper connection and has continuity. Remember to always test twice!
- **Loopback plug:** Another tool every PC tech should have is a loopback plug. It simulates a network connection and has two main functions. First, it can help find what port on a switch an RJ-45 jack is wired to. You plug it into an RJ-45 jack on the wall, and it bounces the signal back down the cable to the switch, lighting up the port that the cable is ultimately connected to. This tells you which port on the switch a particular cable is connected to in case it wasn't labeled previously. You can also accomplish this by connecting it to the end of a patch cable because the device usually has male and female RJ-45 connections. Second, you can test the network adapter on a PC and find out if TCP/IP is functioning properly. An easy way to do this is to plug the loopback adapter into the RJ-45 port of the PC, open the command line, and then ping the IP address of the local system. The loopback plug is essentially a really short crossover connection; the appropriate pins are crossed within the device, looping the signal and data back to where it came from.

Figure 11.1 identifies some of the tools described in this section.

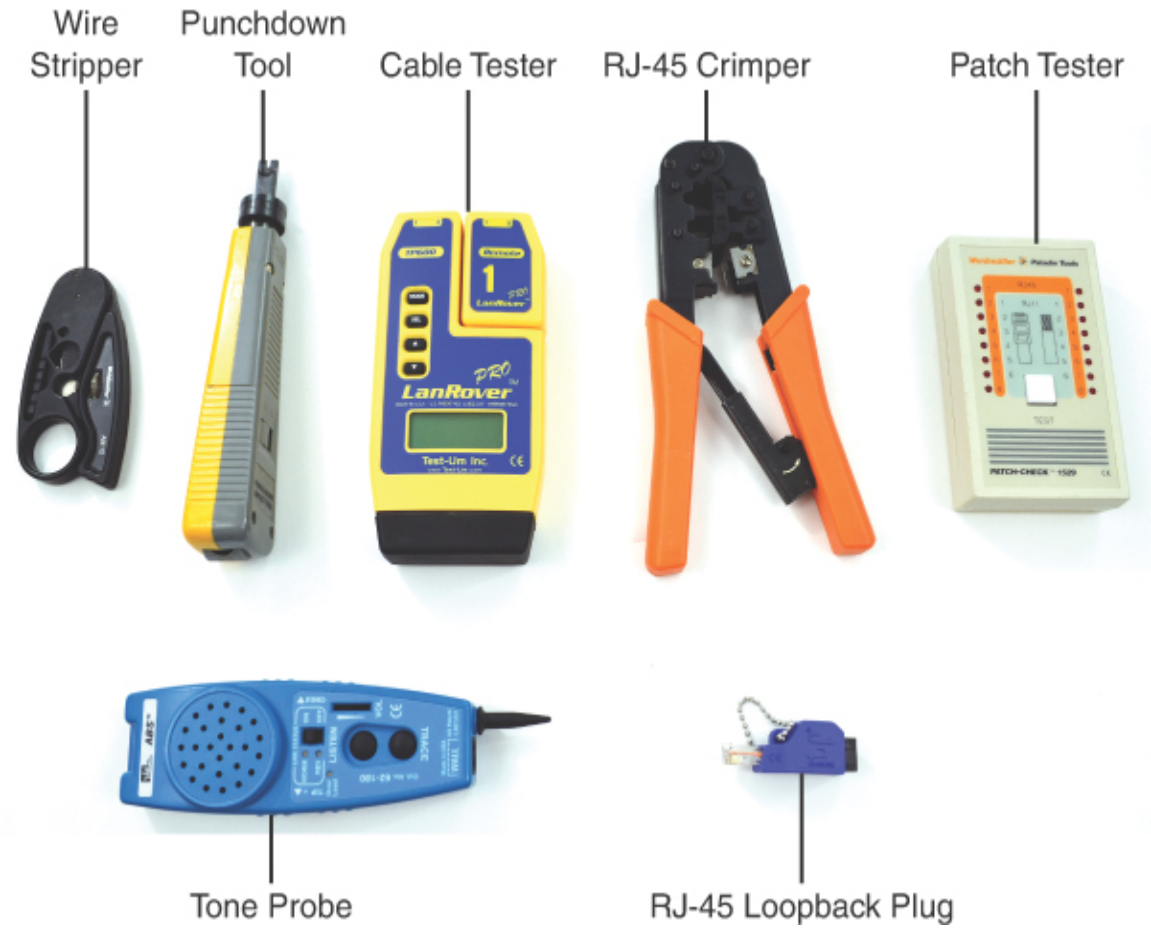


FIGURE 11.1 **Network Cabling Tools**

ExamAlert

Know the following tools for the exam: crimper, wire/cable stripper, tone generator and probe (toner/probe), cable tester, punchdown tool, and loopback plug.

Network Tap

A network tap is a physical device used to make one or more copies of traffic from a network port. It can then send the data to a variety of different monitoring devices. This "traffic mirroring" helps a network analyst gather

data, monitor the network, and check for intrusion detection among other things.

At its simplest, a network tap could be passive (USB-powered) and simply incorporate one additional port for monitoring, passing original traffic through. A more complicated device might run on AC power or could have multiple ports for data analysis. Either way, the key is to know what you want to monitor. Traffic can be taken from an individual system connected to a switch port to mimic that particular system's data flow. However, it can also be taken from an entire switch or a network port that is farther up the network chain to allow for analysis of segments of the network—or even the entire network's data. For example, have you ever wondered why the data LED of your cable modem (or other ISP-provided device) blinks incessantly, even if nothing is happening on your network? Placing a network tap in between the cable modem and the router will allow you to analyze *all* the traffic before it even hits your firewall, giving you a clearer picture of what your cable modem is actually doing.

Ultimately, packets of data can be analyzed with programs such as Wireshark, Snort, or tcpdump. If you are interested in network security, we highly recommend checking out the Wireshark packet sniffer program: https://www.wireshark.org.

Of course, a network tap could be used by malicious individuals as well; to protect against this, an organization should make sure that it has physical security measures and multifactor authentication implemented; it should also ensure that the network is being scanned for unauthorized network taps.

ExamAlert

A network tap is a physical device used to capture and copy data packets for analysis.

Wi-Fi Analyzers

A *Wi-Fi analyzer* is a tool that can identify wireless networks—typically on 2.4 GHz, 5 GHz, or 6 GHz frequencies. This tool shows things such as the channels used by neighboring wireless networks, any overlap that might be occurring between those networks and yours, and the signal strength of access points. Wi-Fi analyzers come in two types. A Wi-Fi analyzer may be a (relatively expensive) handheld, all-in-one device with a built-in Wi-Fi antenna and incorporated analysis programs; or it may be an app for Windows, Android, or iOS. Whatever device you run the app on must have a wireless network adapter that is set up properly. Figure 11.2 shows an example of a basic Wi-Fi analyzer app that is displaying the 2.4 GHz Wi-Fi networks in the vicinity. In this example, you can see that the lower channels (1–5) are being used much more than the upper channels. This type of data should play into your decision-making process when setting up a new Wi-Fi network or when selecting an access point to connect a client to—if there is more than one.

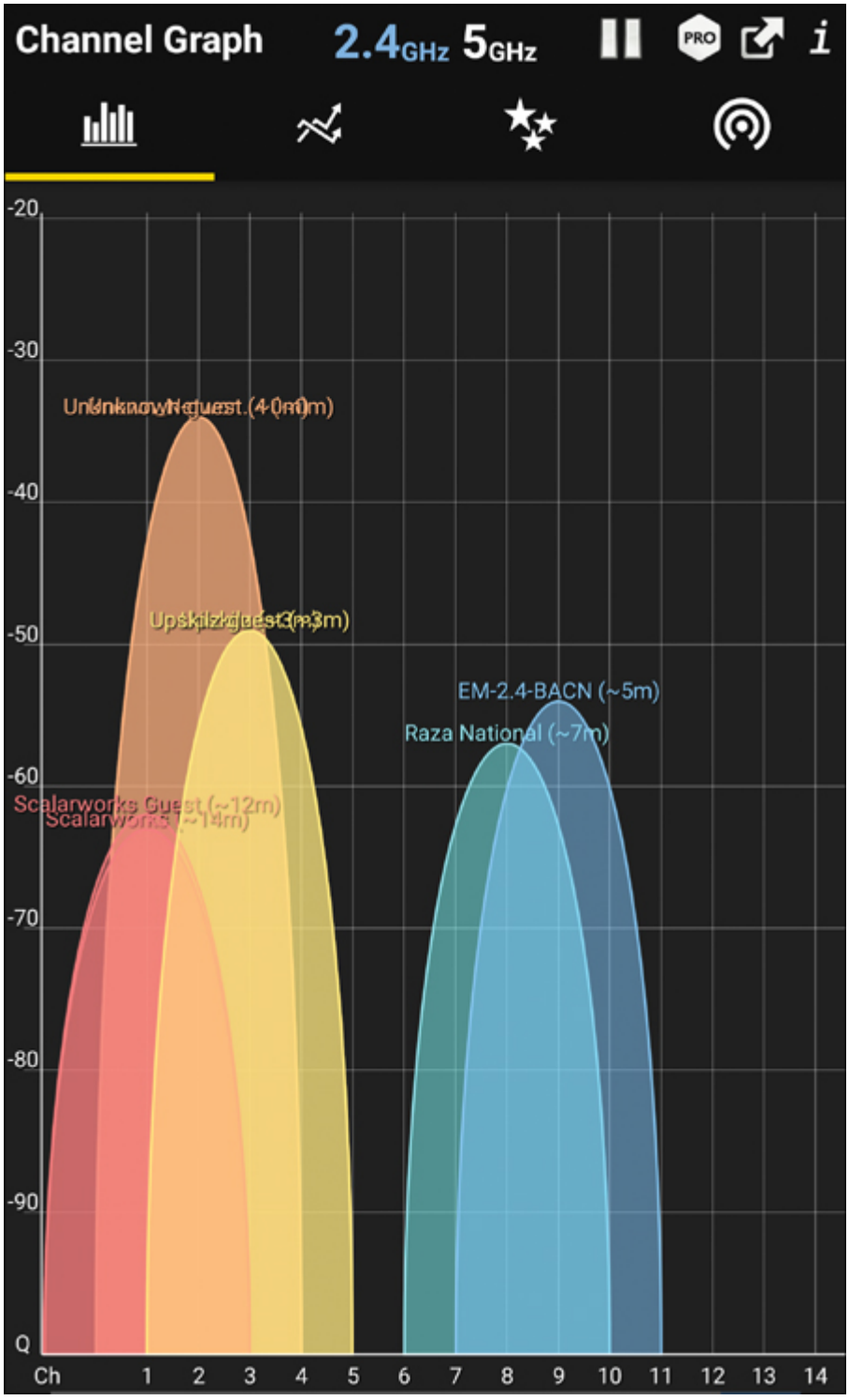


FIGURE 11.2 **Wi-Fi Analyzer Viewing the 2.4 GHz Range**

ExamAlert

A Wi-Fi analyzer is a tool that can identify wireless networks and the channels/frequencies they use.

Cram Quiz

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

1. Which tool is used to test a network adapter without a network connection?

   - ○ **A.** Punchdown tool
   - ○ **B.** Cable tester
   - ○ **C.** Loopback plug
   - ○ **D.** Tone generator and probe

2. Your boss is concerned about overlapping wireless networks from neighboring companies using 802.11ac. Which tool should you use to analyze the problem, and which frequency should you display for analysis?

   - ○ **A.** Wi-Fi analyzer; 5 GHz
   - ○ **B.** Cable certifier; 5 GHz
   - ○ **C.** Loopback plug; 2.4 GHz
   - ○ **D.** Wi-Fi analyzer; 2.4 GHz

3. What would be required to attach RJ-45 plugs to the ends of a single patch cable?

   - ○ **A.** Tone and probe kit
   - ○ **B.** Multimeter
   - ○ **C.** Cable stripper

- **D.** Crimper

4. Your organization is terminating Category 6 cable to a 110 block. Which of the following tools should you use to perform the task?

   - **A.** Punchdown tool
   - **B.** Crimper
   - **C.** Cable stripper
   - **D.** Tone generator

5. Say that you are responsible for the network security of your organization. You decide to perform packet sniffing on your switch by using Wireshark. Which of the following tools will help you to do this?

   - **A.** Tone and probe kit
   - **B.** Network tap
   - **C.** Wireless analyzer
   - **D.** Loopback plug

Cram Quiz Answers

1. **C.** To test a network adapter without a network connection, you use a loopback plug. This tool simulates a network connection. It can also be used to test a switch port. Punchdown tools are used to punch individual wires to a patch panel. Cable testers such as continuity testers test the entire length of a terminated cable. A tone generator and probe kit can also test a cable's length, but it tests only one pair of wires at a time.

2. **A.** To analyze the problem, use a Wi-Fi analyzer. Because your boss is concerned about wireless networks using 802.11ac, you should display the results for 5 GHz networks, not 2.4 GHz networks. Cable certifiers are used to check long-distance *wired* connections, such as from a patch panel to an RJ-45 jack. A loopback plug is used to simulate a network connection, which can

help with identifying switch ports and testing a PC's network connection.

3. **D.** RJ-45 plugs are attached to cable ends with a tool called a crimper. A tone generator and probe kit (toner probe) is used to trace hard-to-find telecommunication and data communication cables/wires. A multimeter can be used to test the continuity of a patch cable. A cable stripper is used to strip a portion of the plastic jacket off the cable and expose the individual wires.

4. **A.** Use a punchdown tool to terminate the individual wires of a Category 6 cable to a 110 punchblock. Use a crimper to connect plugs to the ends of a cable. Use a cable stripper to remove a section of the plastic jacket of a cable. Use a tone generator to create tone at one end of a cable and then use a tone probe to find the same cable at the other end.

5. **B.** A network tap is used to intercept network traffic and make a copy of it for analysis with programs such as Wireshark. (Side note: Be sure to use a quality network tap; lesser ones will reduce your network bandwidth, which could affect everyone!) A tone and probe kit is used to trace signals on cables. A wireless analyzer (or Wi-Fi analyzer) is used to view the frequencies used in nearby wireless networks. A loopback plug is used to simulate a network connection (and test it) but can't be used as a network tap.

You did it! You've completed the networking section of this book. Great work! Be sure to review the networking chapters, ExamAlerts, and your notes before moving on to the next domain.

Core 1 (220-1201)

Domain 3.0: Hardware

CHAPTER 12 Device Display Components

CHAPTER 13 Cables and Connectors

CHAPTER 14 RAM

CHAPTER 15 Storage Drives

CHAPTER 16 Motherboards and Add-on Cards

CHAPTER 17 CPUs

CHAPTER 18 Power

CHAPTER 19 Multifunction Devices/Printers

CHAPTER 20 Printer Maintenance

Welcome to Domain 3.0: Hardware. This domain accounts for 25 percent of the overall percentage of the examination. Every chapter covering this domain is brimming with hardware information you need to know. Treat these chapters accordingly!

Chapter 12

Device Display Components

This chapter covers the following A+ 220-1201 exam objective:

- **3.1** – Compare and contrast display components and attributes.

As a technician, you should understand the differences between the various laptop display types, including LCD, LED, Mini-LED, and OLED. Going further, you need to know the basics about the display's inverter and digitizer technology.

ExamAlert

Objective 3.1 focuses on the following concepts: LCD, IPS, TN, VA, OLED, Mini-LED, touch screen/digitizer, inverter, and screen attributes including pixel density, refresh rates, screen resolution, and color gamut.

Note

The CompTIA A+ objectives list important concepts that you need to know for the exam, but the list is not *finite*. By this, we mean that there might be other associated technologies that are not listed but that you might be tested on. So, at times, we add content to this book

that goes further than the listed objectives. Be ready to study beyond the objectives to fully prepare for the exam—*and* for the real world.

Display Types

A laptop might use one of a few types of displays, depending on the age and the price of the laptop. These include LCD, LED, and OLED:

- **LCD:** The liquid-crystal display (LCD) is a flat-panel display that consists of two sheets of polarizing material surrounding a layer of liquid-crystal solution. It connects to the motherboard by way of a flex ribbon cable or an all-in-one power/signal cable and gets its power from an inverter board. Most LCD screens are thin-film transistor (TFT) active-matrix displays, meaning they have multiple transistors for each pixel. These transistors are contained within a flexible material and are located directly behind the liquid-crystal material. In general, LCDs generate a small amount of heat and cause little in the way of interference and emissions. However, they use more electricity than newer types of displays because they utilize a high-powered bulb, quite often a cold cathode fluorescent lamp (CCFL). LCD screens can be broken down into several types of active-matrix technologies, including
  - **TN:** Twisted nematic (TN) displays use liquid crystals that can twist to allow light to pass through. This older technology was used on small mobile devices but is not seen as often today.
  - **IPS:** In-plane switching (IPS) and Super-IPS are LCD technologies that align liquid crystals on a plane parallel to a glass substrate. IPS provides for a wider viewing angle than TN and was very popular on laptops for a long time.
  - **VA:** Vertical alignment (VA) displays align liquid crystals vertically to a glass substrate. VA can offer a higher contrast ratio and deeper black levels compared to IPS, but they sacrifice viewing angle in the process.
- **LED:** Light-emitting-diode (LED) monitors utilize two-terminal electronic components known as diodes to display images. These diodes are red, green, and blue (RGB)—the “primary” colors when it comes to

computer monitors. LEDs use less power than traditional LCDs and are therefore more efficient. LED monitors use a different backlight than traditional LCD monitors. Whereas older LCD monitors use a CCFL as the illumination source, LED monitors use light-emitting diodes, which release photons; this process is known as *electroluminescence*. It is so much more energy efficient that you will find hybrid designs known as LED-backlit LCDs. Such a device does not use a CCFL but instead uses diodes with an LCD screen.

- **OLED:** OLED stands for organic light-emitting diode. The main advantage of OLED over LED is manufacturing cost; OLEDs can be printed onto just about any substrate using simple printing processes—and they can be incredibly small (even one per pixel), all lighting individually. The technology uses an organic compound to emit light in response to an electric current. OLED displays have the best black levels, but you might opt for a different type of LED if you are more concerned with brightness and some other specifications. One example is quantum dot light-emitting diode (QLED), which has a quantum dot layer built into it that enhances colors and the brightness of images.
- **Mini-LED**: Mini-LEDs refer to a newer class of light-emitting diode technology that is smaller than traditional LEDs. Mini-LEDs are used to create displays with better contrast ratios, brightness, and energy efficiency compared to older LED technologies. With that said, mini-LED TVs are capable of delivering far deeper black levels than regular LED TVs. Because they have considerably more LED lights and dimming zones, the screens of mini-LED TVs are more evenly backlit than LCD TVs

Note

OLED has better contrast and black levels plus more even lighting, but mini-LED can get much brighter for better HDR. Mini-LED is also offered in faster refresh rates right now (refresh rates, not response times)—up to 240 Hz, while the fastest OLEDS on most laptops are 120 Hz.

Inverter and Backlight

A typical older laptop's LCD display incorporates a backlight and an inverter. The backlight is a bulb (for example, a CCFL). It emits light through the screen so that you can see the images that the computer is attempting to display. The inverter—or, more accurately, the *screen* inverter—is a device that converts direct current (DC) that comes from the motherboard into alternating current (AC) to be used by the display's backlight. This section focuses on LCDs because LEDs (and OLEDs) don't need an inverter; they are DC only by design and don't use a CCFL or similar lamp.

Note

Cold cathode fluorescent lamp (CCFL) technology is not widely used in most regular consumer electronics anymore. However, it is used in some applications like certain medical devices, industrial equipment, and legacy displays, due to its cost-effectiveness in those specific situations. The majority of modern displays now use LED backlighting due to its superior energy efficiency and performance.

ExamAlert

Know that a screen inverter's job is to convert DC voltage from the motherboard into AC voltage to be sent to the backlight.

The video display in a laptop is integrated; however, while this is a main feature of the portability of laptops, it can be a point of failure as well. Minor issues such as intermittent lines on the screen suggest that the display cable needs to be reconnected or replaced. However, complete display failures suggest a worse problem that will take longer to repair. Aside from a damaged screen, LCD display failures can be broken down into a couple of categories: a damaged inverter or a worn-out backlight.

Damaged Inverter

To review, on a laptop with an LCD-based screen, the LCD is usually lit by a CCFL (basically a bulb); it is that LCD backlight which requires AC power. The backlight is driven by a high-voltage inverter circuit. Because the inverter runs at high voltage, and possibly at high temperatures, it is prone to failure. If the inverter fails, the display will go dark; however, an external monitor should work properly. Another possibility is that the backlight has failed. You can verify if it is an inverter/backlight issue by shining a flashlight directly at the screen; this works best in a dark room. When you do this, you should be able to make out the operating system! This means that the display is getting the video signal from the motherboard and the problem, most likely, is indeed the inverter or the backlight. If the display's cable that connects the LCD to the motherboard were loose or disconnected, or if the video adapter failed, nothing would show up on the screen at all. The inverter circuit is usually situated on its own circuit board. The inverter often has two connectors: one for the high-voltage connection that leads to the power source and one for a cable that connects to the display. Disconnect these and carefully remove the inverter. Always hold circuit boards by the edges and try not to touch any actual circuits or chips.

ExamAlert

Warning! The inverter should not be handled if the laptop is on! Incorrect handling could result in personal injury. Be sure to turn off and unplug the laptop and remove the battery before removing an inverter.

Worn-Out Backlight

A laptop's backlight usually lasts a long time. However, at some point, the lamp starts to wear out. You might notice a dimmer screen than before, or a reddish/pinkish hue to the screen, or maybe a loss of color. All of these things indicate the possibility of a worn-out lamp.

To replace either the inverter or the lamp, you need to disassemble the display. This usually means removing a screen bezel and taking out the screen, which gives way to those items. Be ready to have mobile device tools on hand, especially a thin but strong plastic shim. Consider purchasing a pry tool repair kit that includes a variety of shims, prying tools, and so on. Don't forget to keep a variety of small screwdrivers on hand.

Note

As you can guess, LED and OLED screens do not suffer as many failures as CCFL-based LCDs do, mainly because LEDs and OLEDs do not incorporate (or need) an inverter or a lamp. Consider that when making technology purchases. LEDs' greatest overall benefit is their energy efficiency. LEDs require a relatively lower voltage to reach peak luminance compared to CCFLs. In turn, LEDs also have a longer lifespan, lower health concerns, and lesser environmental impact than their CCFL counterparts.

Digitizers and Touchscreens

A touchscreen—also known as a *digitizer* screen—is a screen that allows for tapping or writing on the screen. Many allow users to simply use their finger, while others also allow for the use of a stylus. A *stylus* is a writing tool, usually a thin plastic "pen" type of device used to take the place of a mouse; it enables you to tap and "write" on the digitizer with great accuracy.

These methods are widely used in smartphones, tablets, handheld computers, Chromebooks, and some laptops. For example, usually, when you sign for a package from a shipping company, you sign with a stylus on a touchscreen/digitizer instead of using pencil and paper.

More accurately, a digitizer is a device that converts tapped or written impulses (analog) on the screen into instructions (digital) for the operating system to follow.

Removal of a touchscreen requires some disassembly. Screen bezels, plastics, and so on have to be removed before the screen can be unscrewed and disconnected.

To calibrate a digitizer in Windows settings, open the Control Panel, navigate to **Tablet PC Settings**, and select **Calibrate**. This will launch the on-screen calibration tool, where you can adjust the touch points by tapping the crosshairs that appear on the screen as instructed; you can also access this feature by searching **"calibrate"** in the Windows search bar.

To calibrate a touchscreen in Windows, open the **Start** menu, go to **Settings > System > Tablet PC settings** (or simply search for **"Calibrate the screen for pen or touch input"**), and then follow the on-screen instructions to adjust the touch sensitivity and accuracy of your screen by tapping the designated points on the display.

ExamAlert

Know how to calibrate digitizers and touchscreens.

Note

Be prepared to have very small screwdrivers available. Laptop and mobile device repair kits often come with these types of screwdrivers. Also be prepared for more "proprietary" types of screws that require fewer common screwdrivers.

Digitizer overlays also can be added to a laptop screen. Generally, these touchscreen kits are strapped on to the display with Velcro and connect via USB. Be ready to install custom drivers and perform touchscreen orientation and/or calibration.

Attributes

In addition to understanding what's under the hood of a screen, you must also understand the attributes of a computer display. These include

- Pixel density
- Refresh rate
- Screen resolution
- Color gamut

The pixel density is measured in *PPI*, or *pixels per inch*. This is similar to the term *DPI*, or *dots per inch*; however, DPI refers to print output and PPI refers to digital output. They are similar in nature. The more pixels you have in a square inch, the higher resolution the output will be. A higher PPI will result in greater detail. Monitors were 72 PPI for many years, which is why many older pictures on the Internet are 72 PPI. Because why would you post a picture on a website of a higher quality than a monitor can display? Modern displays can range from 72 to 140 PPI, with 140 being extremely high density for specialized displays. The majority of computer displays now are a standard of 96 PPI with the exception being the super high pixel density of certain Apple Retina displays. This is why you will find many Internet images are now 96 PPI instead of the older 72 PPI standard.

Note

Have you ever printed an image from the Internet and noticed that it's much more blocky-looking in print than what's on your screen? The reason is that printers prefer 300 DPI for high-quality prints. For smaller prints, 180–240 still look good, but that's much higher than the standard monitor's 96 PPI output. This is why it's a good idea to save those photos from your phone directly to your computer if you want to print. Often, when you upload to a photo cloud service, it "optimizes" your photos to save space. This means lowering the PPI to 96; the photos look great on your monitor but won't print as nicely.

Refresh rate is measured in Hertz (Hz). This is the number of times per second an image on your screen is refreshed. This measurement often equates to how smooth moving images look on your screen. Most computer monitors are 60 Hz. Some gaming monitors are 120, 144, and even 240 Hz! You will hear gamers speak of *FPS*, or *frames per second*. There is a direct comparison to Hz. Gamers will often put overlays on their screen to display the FPS their graphics card is outputting during a gaming session. However, it is important to note that even if their overlay states 140 FPS, it won't matter if they are viewing images on a monitor that is 60 Hz. If the monitor is 60 Hz, then it will display only 60 FPS! Professional gamers will state that higher refresh rates result in smoother gameplay and better performance. While it can be debated whether people can tell the difference on refresh rates above 120 Hz, just know that the majority of standard monitors are 60 Hz. If you are one of the eagle-eyed gamers who can tell, then look for 120 Hz displays and above.

Note

An interesting note on Hertz and frames per second is that traditional TV was broadcasted at 29.97 FPS and movies were traditionally shown at 24 FPS. New 4K TV broadcasts and Blu-ray movies are 60 FPS. This is why when many people first bought 4K televisions, they were unhappy because the images looked unnatural. This effect is often called the "soap opera effect" because the TV is artificially doubling the frame rate of non-4K video to 60 FPS. This can create an overly smooth and offputting experience.

Screen resolution is the number of pixels a display shows and is measured by width times height. Monitors have often followed television resolutions, but this is not always the case. For instance, TVs marketed as Full HD or 1080p display a resolution of 1920×1080; Quad HD (called 2K in monitors) is 2560×1440; 4K is 3840×2160; and 8K is 7680×4320. This means a Full HD display has 1920 pixels horizontally and 1080 pixels vertically. Many desktop monitors follow these common resolutions; however, some laptops have different resolutions. The reason is the shape of the monitor and the aspect ratio. TVs are often 16:9 ratio, which means they are more

rectangular. If you take the ratio of 1920:1080 and reduce it, you will get 16:9! That's the relationship between the two terms. While many laptops are 16:9, some are 4:3 and even 3:2. This would have a direct change on the resolutions they display. For instance, there are laptops with a display resolution of 1400×1050—making them a 4:3 ratio.

An important note is that most displays have what is termed a *native resolution*. This is the resolution the monitor is optimized for and will provide the sharpest image quality. It is generally recommended to set your display at its native resolution for an optimal viewing experience. If the text is too small, instead of changing the resolution, look at changing the scaling of the text in the operating system's settings.

Lastly, an important attribute of displays is the *color gamut*. This is the range of colors a display can show. Modern displays are capable of displaying 16.7 million colors. This is called *standard dynamic range*. However, you have probably heard of *high dynamic range*, or *HDR*, displays and movies being broadcasted in HDR. This means the color gamut is capable of displaying over 1 billion visible colors! This leads to richer contrasts between colors and more vibrant colors. But remember, if you watch a movie in HDR, your display must be capable of displaying HDR as well.

ExamAlert

Be able to differentiate the various attributes of displays. Know pixel density is measured in PPI; refresh rates are measured in Hertz; native resolution is the default resolution; and color gamut is the range of colors.

Cram Quiz

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

1. Which of the following uses an organic compound that emits light?

   - **A.** Mini-LED
   - **B.** IPS
   - **C.** OLED
   - **D.** LCD
   - **E.** LED

2. Which of the following are possible reasons a laptop's LCD suddenly went blank with no user intervention? (Select the two best answers.)

   - **A.** Damaged inverter
   - **B.** Damaged LCD
   - **C.** Burned-out backlight
   - **D.** Incorrect resolution setting

3. Which term refers to pixel density?

   - **A.** Hz
   - **B.** PPI
   - **C.** SDR
   - **D.** FPS

Cram Quiz Answers

1. **C.** Organic light-emitting diode (OLED) displays use an organic compound or film that emits light. In-plane switching (IPS) is a type of LCD technology that increases the available viewing angle compared to older technologies, such as twisted nematic (TN) matrix LCDs. However, IPS is generally considered inferior to OLED screens when it comes to brightness and contrast ratio when viewed from an angle. LED screens use a film and diode, but not organically in the way that OLED does, and not at such a small

size. Mini-LEDs do not rely on organic matter or organic coatings and are more resistant to burn-in than OLEDs.

2. **A and C.** A damaged inverter or burned-out bulb could cause a laptop's display to go blank. You can verify whether the LCD is still getting a signal by shining a flashlight at the screen. A damaged LCD usually works to a certain extent and will either be cracked, have areas of the Windows interface missing, or show other signs of damage. An incorrect resolution setting can indeed make the screen suddenly go blank (or look garbled), but that scenario will most likely occur only if the user has changed the resolution setting—and this question specifies "with no user intervention."

3. **B.** PPI, or pixels per inch, measures the pixel density in a display. Hz, or Hertz, measures how often a display refreshes the screen every second. This has a direct relation to FPS, or frames per second, which is how many frames are drawn per second. If you are watching something that is displaying 60 FPS, then you need at least a 60 Hz display to see all of the frames without the risk of frames dropping. SDR is the standard color gamut of most displays that is capable of displaying 16.7 million colors, while HDR is a color gamut capable of displaying over 1 billion colors.

Okay, first chapter of Hardware down! Let's keep it going.

"Any sufficiently advanced technology is indistinguishable from magic." — Arthur C. Clarke

Chapter 13

Cables and Connectors

This chapter covers the following A+ 220-1201 exam objective:

- **3.2** – Summarize basic cable types and their connectors, features, and purposes

Even though wireless technology usage is widespread, cables are still necessary and used in many applications. This chapter will get you familiar with all the cables and connectors you need to hook network systems together, add peripherals, and adapt or convert from one technology to another. Everything can be linked together!

ExamAlert

Objective 3.2 concentrates on the following concepts: network cables, peripheral cables, video cables, hard drive cables, adapters, and connector types.

Network Cables

Cable types are broken down into two categories: cables that use electricity and cables that use light. Ethernet twisted pair and coaxial cables use copper wires as their transmission media and send electricity over those

wires. Fiber optic, on the other hand, uses glass or plastic as the transmission medium and sends light (photons) over those cables.

Twisted Pair

The most common type of cable used in today's networks is *twisted pair*. It is referred to as twisted pair because the copper wires inside the cable are twisted together into pairs throughout the entire length of the cable. Administrators regularly use unshielded twisted pair (UTP) cable. Typical versions of twisted pair include *Category 6* and *Category 5e* (often abbreviated Cat 6 and Cat 5e). Table 13.1 shows the various categories of twisted pair currently in use today.

Note

Category 5 was deprecated in 2001 and superseded by the Category 5e specification. The Category 6 specification improves upon the Category 5e specification by extending frequency response and further reducing crosstalk. The improved performance of Cat 6 provides 250 MHz bandwidth.

TABLE 13.1 **UTP Categories and Speeds**

UTP Category	Rated For
Category 5e	100 Mbps and 1 Gbps networks (100 MHz/350 MHz)
Category 6/6a	1000 Mbps (1 Gbps) and 10 Gbps networks (250 MHz/500 MHz)

Data transfer rate (also known as *speed* or *bandwidth*) is normally measured in bits because networks usually transfer data serially, or 1 bit at a time. 100 Mbps is 100 megabits per second. 1 Gbps is equal to 1 gigabit per second (and a network capable of this speed is known as a gigabit network), or 1000 Mbps. 10 Gbps is equal to 10 gigabits per second. Now, a cable might

be rated for 10 Gbps networks (for example, Cat 6), but you probably won't attain that speed over the cable. Typically, the actual speed (known as *throughput*) might be 250 Mbps, 500 Mbps, 1 Gbps, or possibly more. The speed depends on many factors, including the frequency of the cable (for example, Cat 6 is 250 MHz and Cat 6a is 500 MHz), the technology used to send data, the encoding rate, whether duplexing is involved, the length of the cable, the quality of the installation, and so on. So, it's difficult to put a specific number to each category of cable. Just remember what network speeds each category of cable is rated for.

Note

Bits and bytes are often confused. A *bit* is always in one of two physical states, similar to an on/off light switch. The state is represented by a single binary value, a 0 or 1. It takes 8 bits to make a byte. A *byte* is the unit most computers use to represent a character such as a letter, number, or typographic symbol. Four bits is a *nibble*; seriously, IT folks have a certain brand of humor. Usually, speed is measured in bits and storage in bytes.

ExamAlert

Know the difference between T568A and T568B wiring as well as the wiring of a crossover cable.

The Telecommunications Industry Association (TIA) defines standards for cabling and wiring, such as the T568A and T568B standards. Generally speaking, the most common standard you see is the T568B standard. Table 13.2 shows the color sequence for each of the eight wires (or pins) for the T568B and T568A standards. Figure 13.1 shows a close-up of the wires organized for a T568B connection.

TABLE 13.2 **T568B and T568A Wiring Standards**

Pinouts	T568B	Pinouts	T568A
Pin 1	White/orange	Pin 1	White/green
Pin 2	Orange	Pin 2	Green
Pin 3	White/green	Pin 3	White/orange
Pin 4	Blue	Pin 4	Blue
Pin 5	White/blue	Pin 5	White/blue
Pin 6	Green	Pin 6	Orange
Pin 7	White/brown	Pin 7	White/brown
Pin 8	Brown	Pin 8	Brown

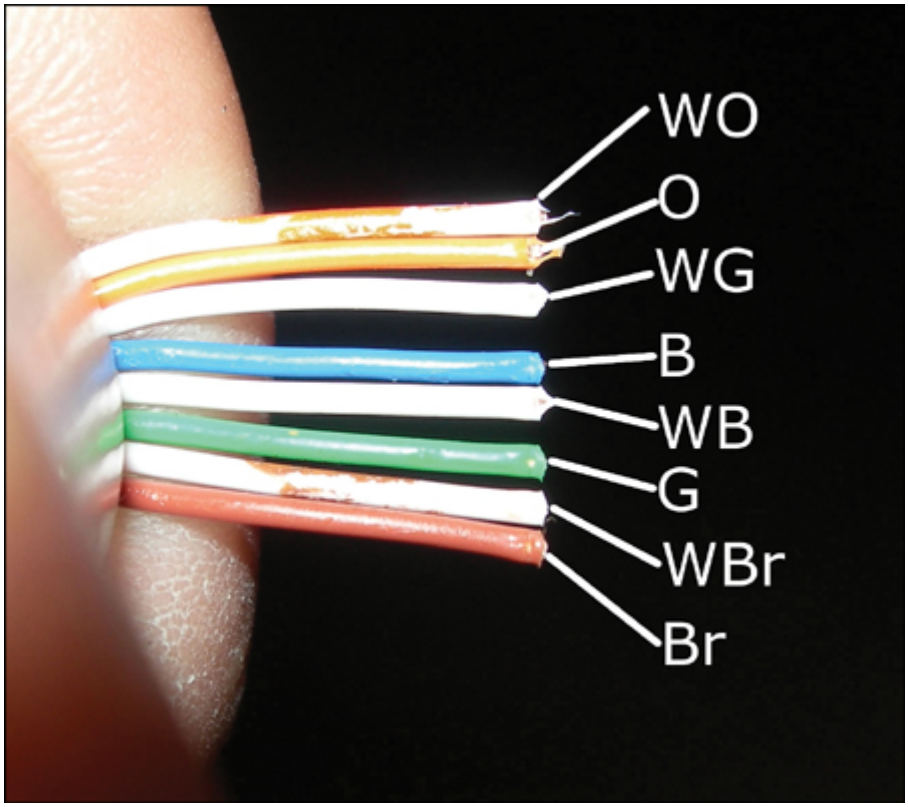


FIGURE 13.1 **Wires Organized for the T568B Standard**

ExamAlert

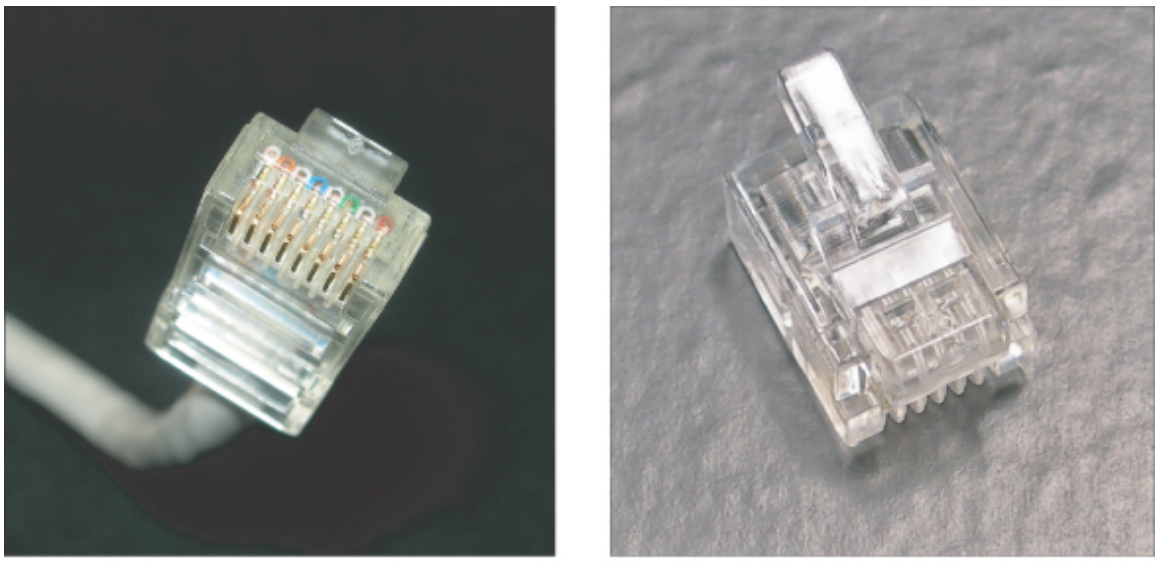
Remember that T568A/T568B are telecommunications standards from the Telecommunications Industry Association (TIA) and the Electronics Industry Alliance (EIA). These 568 standards specify the pin arrangements for the RJ-45 connectors on UTP or STP cables. The number 568 refers to the order in which the wires within the UTP cable are terminated and attached to the connector.

Any physical cabling equipment used in a network must comply with the standard chosen for that network, including cables, patch panels, jacks, and connectors. The connector used with twisted pair networks is known colloquially as the RJ-45 (or, more specifically, the 8P8C connector). RJ-45 plugs connect to each end of the cable, and these cables connect to RJ-45 sockets within network adapters and on network switches.

ExamAlert

If a computer cannot connect to the network, check the network cable first. Make sure the RJ-45 plug has a solid connection.

As you can see in Figure 13.2, RJ-45 plugs look a lot like the landline telephone plugs (known as RJ-11 plugs). However, the RJ-45 plug is larger and contains eight wires, whereas the RJ-11 plug holds only a maximum of six wires (and normally only uses four).



RJ-45 RJ-11

FIGURE 13.2 **RJ-45 and RJ-11 Plugs**

ExamAlert

RJ-45 is mostly used with Ethernet cables, whereas RJ-11 connects to telephone units. RJ-45 has 8 wires inside, while RJ-11 has 4 wires.

A standard twisted pair patch cable that you would use to connect a computer to a switch or an RJ-45 jack is wired for T568B on each end. That makes it a *straight-through cable*. However, if you wanted to connect a computer directly to another computer, you would need to use a *crossover cable*. This type of cable is wired for T568B on one end and T568A on the other. You can see in Table 13.2 that certain pins are "crossed" to each other from T568B to T568A. Pin 1 on T568B crosses to pin 3 on T568A, and pin 2 crosses to pin 6. You can also use a crossover cable to connect one switch to another—although this is usually not necessary because most switches auto-sense the type of cable you plug into them.

Note

The way that a crossover cable's pins are wired is the basis for a loopback—a connection made to test the local computer or system (for example, an RJ-45 loopback plug).

UTP has a few disadvantages:

- It can be run only 100 meters (328 feet) before *signal attenuation*—that is, weakening or degradation of signal—occurs.
- Its outer jacket is made of plastic, and it has no shielding, making it susceptible to electromagnetic interference (EMI) and vulnerable to unauthorized network access in the form of wiretapping.

Because the UTP cable jacket is made of PVCs (plastics), when they catch on fire, they can be harmful to humans. For this reason, most municipalities require that plenum-rated cable be installed in any area that cannot be reached by a sprinkler system. A *plenum* is an enclosed space used for airflow. For example, if cables are run above a drop ceiling, building code requires that they be plenum rated. This means that the cable has a special Teflon coating or is a special low-smoke variant of twisted pair, reducing the amount of PVC chemicals that are released into the air in the event of a fire.

ExamAlert

Plenum is the space between the structural ceiling and a drop-down ceiling. It is commonly used for heating, ventilation, and air-conditioning systems and to run network cables. To meet fire code, use plenum-rated cable above drop ceilings and anywhere else necessary.

Because UTP is susceptible to EMI, a variant known as shielded twisted pair (STP) was developed. STP includes metal shielding over each pair of wires, reducing external EMI and the possibility of unauthorized network access. A couple of disadvantages of STP include higher cost of the product

and installation and the fact that the shielding needs to be grounded to work effectively. Keep in mind that all server room and wiring closet equipment —such as patch panels, punch blocks, and wiring racks—should be permanently grounded before use.

ExamAlert

STP cable is resistant to EMI.

Speaking of "ground," there is also specially rated cable for use underground. When twisted pair cable (for example, Cat 5e, Cat 6, or greater) needs to be run outdoors, *direct burial* cable should be used, and it should be placed approximately 8 inches underground and at least 8 inches away from any buried power lines. This cable does not degrade when exposed to the elements because it is protected by an additional plastic or metal conduit.

Note

Objective 3.2 lists "punchdown block," which is a place to terminate many twisted pair cables. This concept is discussed briefly in Chapter 11, "Networking Tools."

Coaxial

Coaxial cable provides another way to transfer data over a network. This cable has a single conductor surrounded by insulating material, which is then surrounded by a copper screen and, finally, an outer plastic sheath. Some networking technologies still use coaxial cable; for example, cable Internet connections use RG-6 coaxial cable (and possibly the older RG-59 cable). This cable screws on to the terminal of a cable modem using an F-connector (also called F-type connector). It is the same cable and connector used with cable TV set-top boxes (STBs) and digital video recorders (DVRs).

Generally, RG-6 cable can be run as far as 500 to 1000 feet. The maximum distance varies because several factors play into how far the data can travel before attenuation occurs—including the frequency used and the protocol used. Its speed also varies depending on what type of transmission is sent over it. A typical RG-6 cable has a minimum bandwidth of 1 GHz, which can loosely translate to 1 Gbps, but the data throughput will most likely be capped at some number below that. For example, cable Internet providers offer different tiered download speeds (50 or 100 Mbps and so on), and some fiber optic providers (who change the cable type from fiber optic to coaxial at the house or business) might cap it at anywhere between 100 Mbps and 500 Mbps. This all varies according to the provider and how many services are being transmitted over the same line.

There are two derivatives of RG-6 that you should know: RG-6/U, which is double-shielded, and the more common RG-6/UQ, which is quadruple-shielded and is often referred to as *quad shield*. It is a better option if you are running RG-6 in ceilings or near any electrical appliances.

ExamAlert

Make sure you know cable terminology such as RJ-11, RJ-45, and F-connector for the exam.

Optical

Optical, or fiber optic, cable is fast, and unlike copper-based cables, it is not subject to EMI. Because fiber optic cables transmit data by way of light instead of electricity, they can send signals much faster and farther than do copper wires. Optical cable can be more secure than copper-based cable as well. EMI doesn't even play into the equation because optical cables don't use electricity. Plus, fiber optic cables are more difficult to tap (splice) into than copper-based cables.

You might encounter single-mode and multimode fiber; for the most part, single-mode fiber is used over longer distances, but both types are easily capable of supporting 1000 Mbps and 10 Gbps networks and can be run

farther than twisted pair cable. Straight tip (ST) and subscriber connector (SC), shown in Figure 13.3, are a couple of types of connectors used with fiber. Another connector is the Lucent Connector (LC), which looks quite similar to the SC.

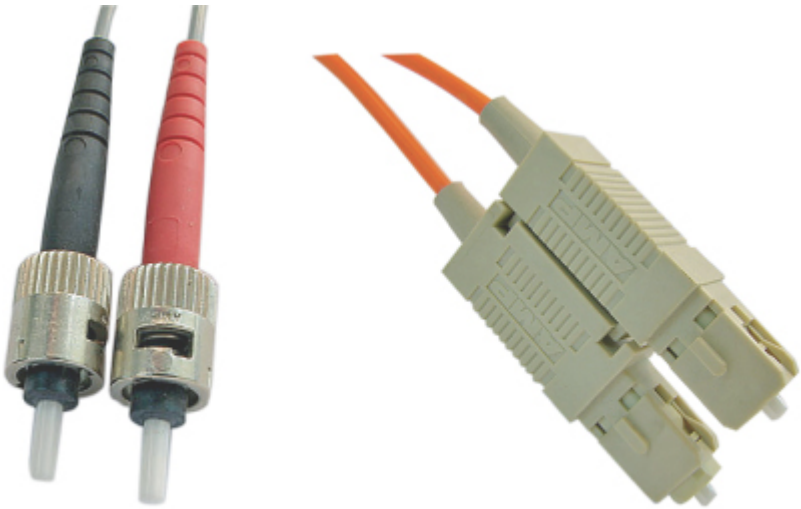


FIGURE 13.3 **ST and SC Connectors**

ExamAlert

Be able to identify straight tip (ST), subscriber connector (SC), and Lucent Connector (LC) fiber optic connectors.

Multimode cables have a larger core diameter than do single-mode cables. It is the more commonly used fiber optic cable in server rooms and when making network backbone connections between buildings in a campus. It transmits data approximately 600 meters. Single-mode, on the other hand, is used for longer-distance runs, perhaps from one city to the next (as far as thousands of kilometers). At shorter distances, single-mode cable can go beyond 10 Gbps.

ExamAlert

Remember that multimode is a type of optical fiber commonly used in computer networking for short-distance data transmission. It has a larger core diameter compared to single-mode fiber, allowing multiple light modes to propagate through the fiber. Single-mode fiber often uses a laser light source while multimode typically uses an LED or vertical-cavity surface-emitting laser (VCSEL) light source.

Peripheral Cables and Connectors

This section is sort of the catch-all for several types of cables: USB, Lightning and Thunderbolt (Apple) cables, and serial cables.

USB

USB ports are used by many devices, including keyboards, mice, printers, flash drives, and more. A USB port enables data transfer between a device and a computer and usually powers the device as well. The speed of a USB device's data transfer depends on the version of the USB port, as shown in Table 13.3.

TABLE 13.3 **Comparison of USB Versions**

USB Version	Name	Data Transfer Rate
USB 2.0	High-Speed	480 Mbps
USB 3.0	SuperSpeed	5 Gbps
USB 3.1	SuperSpeed+	10 Gbps
USB 3.2 (USB-C)	SuperSpeed+	10/20 Gbps
USB 4 (USB-C)	USB 40 Gbps	40 Gbps

The USB-C generation determines the maximum data transfer rate that the cable can support. For example, USB 3.1 Gen 2 is faster than USB 3.1 Gen 1.

The number of lanes used affects the data transfer rate:

- **USB 3.0 and USB 3.1:** Uses one transmit lane and one receive lane, for a maximum data transfer rate of 5 Gbps and 10 Gbps, respectively.
- **USB 3.2 Gen 1x2:** Uses two lanes of 5 Gbps, for a maximum data transfer rate of 10 Gbps.
- **USB 3.2 Gen 2x2:** Uses two lanes of 10 Gbps, for a maximum data transfer rate of 20 Gbps.

USB4 Gen 4 is normally referred to as a speed of 40 Gbps or 40 Gbit/s, with the full connections based on it being referred to as 80, 120/40, 40/120 Gbit/s. But since the actual signaling is no longer binary, the actual raw bit rates no longer match those numbers exactly. The USB-C specification can get a bit confusing. For more information, visit https://www.usb.org/.

Note

USB 4 devices are required to support 20 Gbps but can optionally support 40 Gbps if they use a shorter cable.

You might see USB data transfer rates written as *Mbit/s* and *Gbit/s*, which mean the same thing as *Mbps* and *Gbps*. Finally, note that USB 1.0 (1.5 Mbps) and 1.1 (12 Mbps) have been deprecated. If you encounter an older computer that has only these ports, consider installing a USB adapter that adheres to a higher version of USB.

ExamAlert

Memorize the specifications for USB 2.0 (480 Mbps) through 3.2 (10/20 Gbps) and USB 4 (40 Gbps).

Various plugs are used for the different types of USB connections. Figure 13.4 illustrates these connectors.

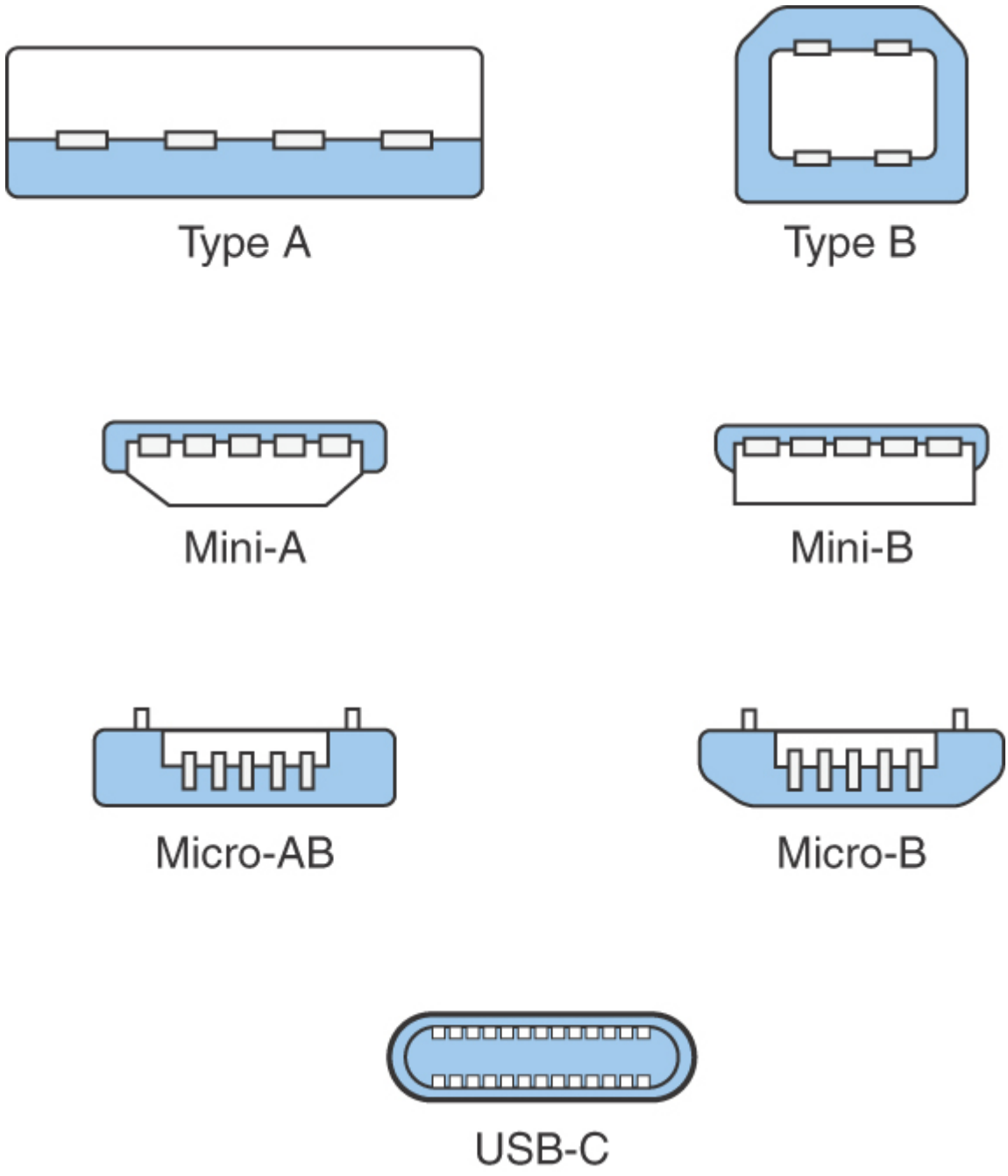


FIGURE 13.4 **USB Connectors**

Type A and Type B connectors are commonly used for printers and other larger devices. Mini- and Micro- connectors are often used for handheld computers, smartphones, mice, digital cameras, portable music players, and cell phones. USB-C is used for smartphones and other devices developed after 2017. However, some companies create proprietary cables and

connectors for their devices, based on the USB specifications. Such devices cannot connect properly to Type A, Type B, and Mini- or Micro-connectors.

Note

As of December 2024, all smartphones and small electronics sold in the European Union (EU) must be USB-C. While we still see older electronics with proprietary cables existing for the next few years, it will mark a dramatic shift in the industry, so the future will only be USB-C.

The USB-C connector is quite common. Aside from its increased speed, it is found on a plethora of devices, and the cable end can be connected to the port in either direction (that is, there is no "upside down"). So, unlike with older versions of USB, you can plug it in either way without having to worry (and without having to look carefully at the port). Also, it has higher power flow. It can provide up to 5 amps of current, allowing for faster charging of devices, but it is important to use quality USB-C cables that can handle the higher amperage. Finally, back to the increased speed: With USB-C, today's USB technology has progressed to the point where it can be used as a video connection (for example, to provide HD video and audio to an external monitor connected to a laptop). It is one mighty connector.

ExamAlert

Exam Objective 3.2 specifically calls out Micro-USB, Mini-USB, USB-C, as well as many other connector types. Be sure you can identify them and summarize their features and purposes.

Lightning and Thunderbolt

Lightning is a proprietary port built into older Apple devices such as the iPad and iPhone. It's an 8-pin connector that replaced the (now legacy) 30-

pin dock predecessor. As with USB-C, the Lightning connector can be inserted face up or face down. It supports USB 3.0 speeds. As mentioned earlier, because of the EU's mandate, all *new* Apple devices currently use USB-C. The Lightning connector, while still used on many older devices, will be considered legacy moving forward.

Thunderbolt is a high-speed hardware interface developed by Intel. As of the writing of this book, this is used primarily by Apple computers. It combines elements of PCI Express and DisplayPort technologies. Versions 1 and 2 use the Mini DisplayPort connector, and version 3 uses the USB-C connector. Thunderbolt 2 provides access to 4K monitors. Because Thunderbolt is based on DisplayPort technology, it provides native support for the Apple Thunderbolt Display and Mini DisplayPort displays.

Thunderbolt can be used to transfer data at high rates to external storage devices or to displays (or both; up to six devices can be daisy-chained, or wired together in sequence). If you look at the ports of a computer and see the Thunderbolt icon next to the Mini DisplayPort port, then it is meant to be used for data transfer to peripherals. If you see a Display icon, then it can be used with a monitor. While you can physically connect a Thunderbolt device to a Mac with DisplayPort, the device will not work; however, if you connect a DisplayPort device to a Mac with Thunderbolt, the device will work. Table 13.4 describes the different versions of Thunderbolt.

TABLE 13.4 **Comparison of Thunderbolt Versions**

Thunderbolt Version	Data Transfer Rate	Connector Type	PCI Express Version Required
Version 1	10 Gbps	DisplayPort	Version 2.0
Version 2	20 Gbps	DisplayPort	Version 2.0
Version 3	40 Gbps	USB Type-C	Version 3.0
Version 4	40 Gbps	USB Type-C	Version 4.0

Note

While the transfer rate is the same as for version 3, Thunderbolt 4 supports USB4.

ExamAlert

Know the Thunderbolt versions, speeds, and connection types.

Serial

The term *serial* is used with many technologies: USB, Serial Attached SCSI, bit streams over network cables, and so on; but generally, a person who refers to serial connections for peripheral devices is talking about the Recommended Standard 232 (RS-232) data transmission standard. Although it is an old technology, it is still used in many environments. For example, the RS-232 standard describes how DTEs (computers) and DCEs (dial-up modems) communicate using serial ports.

RS-232 communicates via serial cables that have either 9 wires (DE-9, also known as DB9) or 25 wires (DB-25). RS-232 has been used for many years, and it will most likely continue to be used due to its simple design and the vast array of devices out there that use RS-232 interfaces, such as handheld and mountable terminals, networking equipment, industrial machines, and analytical instruments. Because of this, you can still find motherboards with built-in RS-232 ports (usually DE-9). If a computer does not have one, and you need to access RS-232-based equipment, you can use a PCIe add-on card. For laptops and other mobile devices, you can use USB-to-RS-232 converters.

RS-232 and other Recommended Standards (such as RS-422 and RS-485) are published by the TIA, the same organization that publishes the T568A/T568B cabling standards.

ExamAlert

Remember that DE-9 (DB-9) is a 9-pin connector used for serial cable and RS-232 data transmissions.

Video Cables and Connectors

Your choice of video card will probably dictate the cable and connector that you use. Most of today's PCIe video cards come with either DVI, HDMI, or DisplayPort outputs. Some monitors also have VGA connections for legacy compatibility. Table 13.5 details some of the common connectors you will see in the field. Figure 13.5 shows some of the typical video ports you will use.

TABLE 13.5 **Video Card Connectors**

Connector Type	Full Name	Description
DVI	Digital Visual Interface	High-quality connections used with LCD displays. Carries uncompressed digital video; is partially compatible with HDMI. Types include ▶ **DVI-D:** Digital-only connections ▶ **DVI-I:** Digital and analog connections ▶ **DVI-A:** Analog-only connections Dual-link connections are available for DVI-D and DVI-I. Non-dual-link versions have a gap in the center of the pins, using one-third fewer pins total.

Connector Type	Full Name	Description
HDMI	High-Definition Multimedia Interface	Used mainly for high-definition television. Can carry video and audio signals. ▶ **Type A:** Supports all HD modes; compatible with DVI-D connectors ▶ **Type B:** Double-video bandwidth; supports higher resolutions; also known as dual-link; uncommon ▶ **Type C:** Mini-HDMI; used in portable devices ▶ **Type D:** Micro-HDMI; smallest connector; also used in portable devices ▶ **Type E:** Used in automobiles; has a locking tab
DisplayPort	DisplayPort	▶ Royalty-free interface similar to HDMI; designed to be the replacement for HDMI and DVI ▶ Often has a locking tab ▶ Uses packet transmission similar to Ethernet ▶ Mini version developed by Apple
VGA (also known as SVGA)	Video Graphics Array	15-pin, usually blue, known as DE15 (also sold as DB15 or HD15). Used for older monitors that display VGA, SVGA, and XGA resolutions. Signal quality degrades over shorter distances than with HDMI, DVI, and DisplayPort.

Connector Type	Full Name	Description
USB-C	Universal Serial Bus Type-C	Can carry video in three different modes if the actual cable/port is rated for it: ▶ DisplayPort Alternate Mode (DP Alt Mode) ▶ Thunderbolt 3/4 support ▶ USB3.1 and greater

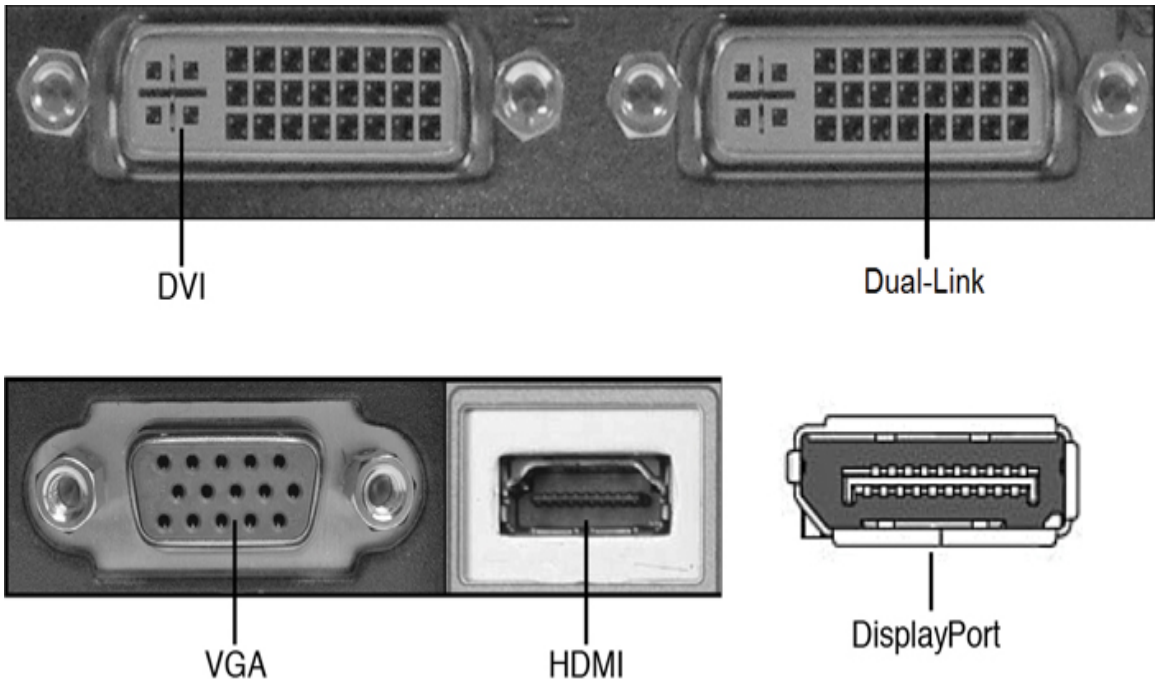


FIGURE 13.5 **Typical Video Ports**

ExamAlert

Be able to identify VGA, HDMI, Mini-HDMI, DisplayPort, USB-C, and DVI video connectors and ports.

There are adapters, splitters, and signal boosters available for just about every type of video connection: HDMI to DVI, DVI to VGA, and so on. In

some cases, a passive adapter or splitter works fine. In other cases, an active (AC-powered) connection is required. This is common with DVI and HDMI, especially if you want a clean, quality signal over any length beyond 1 meter.

Storage Drive Cables and Connectors

The three types of storage drive/hard drive are as follows:

- **Serial ATA (SATA):** A very common connection for internal drives (SATA) and external drives (eSATA). It uses a 7-pin data connector and a 15-pin power connector.
- **Integrated Drive Electronics (IDE):** A much older type of connection that runs in parallel (8 bits at a time) instead of serially (1 bit at a time). It uses a 40-pin ribbon cable for data and a 4-pin Molex connector for power. (The chances of seeing this type of connector are slim.)
- **Small Computer System Interface (SCSI):** Around since the 1980s, SCSI at first was designed as a parallel technology that could run faster than IDE and other connections. Today, a common type of SCSI is Serial Attached SCSI (SAS), which can transfer data as fast as 22.5 Gbps (SAS version 4); faster speeds are being developed.

We'll discuss some of these drive cables and connections more in Chapter 15, "Storage Drives."

ExamAlert

Know your storage drive cables, including SATA, SCSI, and eSATA.

Adapters

You can't put a square peg in a round hole (normally). Sometimes you need to make a connection, but the devices and/or cables don't match up. In such cases, you need an adapter, and there are adapters for virtually everything you might want to do. Let's say you need to make a connection to a USB

Type B connector from a USB Type A connector, or you need to connect from USB to RJ-45, or you need to connect a DisplayPort to an HDMI port. Well, there are adapters for all those situations and more.

Video can be especially troublesome. For example, what if your laptop has an HDMI output, but the monitor you want to connect to only has DVI and VGA? An HDMI-to-DVI output would be necessary. But remember, DVI does not normally carry audio signal the way that HDMI does, so you might also need to run an audio cable from the 3.5 mm audio output of the laptop to a set of speakers. You might need to switch from DVI to VGA or from DVI to HDMI. Be ready to use adapters and research whether the length of your connection and/or the quality of signal requires an active AC-powered adapter.

A common adapter today is the USB-to-Ethernet adapter. This type of adapter allows you to use just about any USB port and send data from the computer (or device) over an Ethernet network. There are adapters that go from USB (Type A) to RJ-45, USB-C to RJ-45, and so on. USB-C is preferred for many devices because it can handle higher data throughputs with less latency.

Most PC technicians carry a variety of adapters with them just in case they need them. That's something to think about for your toolkit.

Note

While the objectives do not separate the terms *adapter* from *converter*, know that there is a difference. If you are just changing the physical connection type, then you would use an adapter. However, if you are changing a signal format from, say, a VGA (analog) to an HDMI (digital) signal, you are technically getting a converter, which changes the signal type and the physical connection type.

Cram Quiz

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

1. Which of the following uses a 7-pin data connector and a 15-pin power connector?

   - **A.** VGA
   - **B.** IDE
   - **C.** SATA
   - **D.** Molex
   - **E.** Cat 6

2. Which type of cable would you use if you were concerned about EMI?

   - **A.** Plenum rated
   - **B.** UTP
   - **C.** STP
   - **D.** Coaxial

3. You have been tasked with connecting a newer Android smartphone to an external TV so that you can display the CEO's smartphone screen during a meeting. Which of the following adapters would typically be the best solution?

   - **A.** Micro-USB to HDMI
   - **B.** Micro-USB to DVI
   - **C.** USB-C to DVI
   - **D.** USB-C to Ethernet
   - **E.** USB-C to HDMI

4. Which type of cable can connect a computer to another computer directly?

- **A.** Straight-through
- **B.** Crossover
- **C.** T568A
- **D.** SATA
- **E.** T568B

5. Which connector is used for cable Internet?

- **A.** LC
- **B.** F-connector
- **C.** Direct burial
- **D.** RJ-45
- **E.** DE-9

6. Which cable type would be suitable for longer distances, such as connecting two cities?

- **A.** Coaxial
- **B.** Twisted pair
- **C.** Multimode fiber
- **D.** Single-mode fiber

7. You need to make a high-speed connection to an external storage device that can handle 40 Gbps. Which of the following is the best solution?

- **A.** USB 3.2
- **B.** Thunderbolt
- **C.** HDMI
- **D.** Cat 6a

Cram Quiz Answers

1. **C.** SATA connections include a 7-pin data connector and a 15-pin power connector. VGA ports have 15 pins that are used to transmit video signal. An older IDE hard drive cable has 40 pins. Molex is a power connection that has 4 wires. Category 6 (Cat 6) cable is twisted pair cable that has 8 pins (wires).

2. **C.** Shielded twisted pair (STP) is the only cable listed here that can reduce electromagnetic interference. However, fiber optic cable is another good solution, though it is more expensive and more difficult to install. Plenum-rated cable is used where fire code requires it; it doesn't burn as fast as regular cable, and it releases fewer PVC chemicals into the air.

3. **E.** Typically, you would use USB-C to HDMI. If it is a newer Android smartphone, then chances are it will have a USB-C port. If you are attempting to connect it to a TV, HDMI is the most likely port to use. Micro-USB is used with some mobile devices, but newer devices (especially Android devices) have switched to USB-C. You wouldn't want USB-C to DVI because TVs normally don't have DVI inputs. USB to Ethernet helps convert from a computer or mobile device to the Ethernet network. These devices can ultimately allow a device or computer with a USB port to access the Internet. This wired connection might be favored over wireless for its speed, quality connection, and low latency.

4. **B.** A crossover cable is used to connect like devices: computer to computer or switch to switch. Straight-through cables (the more common patch cable) connect different devices (for example, connect a computer to a switch). T568B is the typical wiring standard you see in twisted pair cables; T568A is the less common standard. A crossover cable uses the T568B wiring standard on one end and T568A on the other end. SATA is used to connect storage drives internally to desktop or laptop computers.

5. **B.** Cable Internet connections use RG-6 coaxial cable (usually) with an F-connector on the end. LC is a type of fiber optic connector. Direct burial is a type of cable that you can purchase for underground installations. RJ-45 is the connector used on twisted

pair patch cables. DE-9 (or DB-9) is a serial connector used with RS-232 connections.

6. **D.** Single-mode fiber is used for longer-distance runs, perhaps from one city to the next (as far as thousands of kilometers). Coaxial is common for connections between utility poles and houses/buildings. Twisted pair is common in LANs. Multimode cables have a larger core diameter than single-mode cables. Multimode is the more commonly used fiber optic cable in server rooms and for making network backbone connections between buildings in a campus.

7. **B.** A Thunderbolt connection is the best solution to the scenario—specifically, Thunderbolt version 3, which can handle 40 Gbps over USB Type-C. USB 3.2 is limited to 10 or 20 Gbps, though it also uses the USB Type-C connection. HDMI is used for video (and audio) connections. Cat 6a is a type of twisted pair cable used in Ethernet networks; it is rated for 1000 Mbps and 10 Gbps.

Today, it seems that just about everything is *interconnected*. And sometimes, a person just needs to disconnect! As this was one of the longer chapters of the book, now is such a time. Take a break, stretch, review, and then continue!

Chapter 14

RAM

This chapter covers the following A+ 220-1201 exam objective:

- **3.3** – Compare and contrast RAM characteristics.

This chapter and the next one are all about how data is accessed and stored—over the short term and the long term. We use random-access memory (RAM) for the short term and storage drives over the long term. In this chapter, we'll focus on the short term and RAM.

When people talk about the RAM in their computer, they are almost always referring to the "sticks" of memory that are installed into the motherboard. This is known as *dynamic random-access memory (DRAM)*, or main memory, and often comes in capacities of 4, 8, 16, 32, or 64 GB. This type of RAM has its own speed and must be compatible with the motherboard's RAM slots. It's not the only type of RAM, but it's the type you should be most concerned with for the exam. For all practical purposes, the terms *stick*, *DIMM*, and *memory module* mean the same thing: They refer to the RAM installed in a motherboard's RAM slots.

The most important concept in this chapter is *compatibility*. There are a lot of RAM technologies to know, and you always need to determine whether a particular technology will be compatible with your motherboard. The best way to find out is to go to the RAM manufacturer's website and search for your motherboard, which should list the matching RAM.

Let's discuss the types of RAM you should know.

ExamAlert

Objective 3.3 concentrates on the following concepts: form factors (SODIMM/DIMM), double data rate (DDR) iterations, error-correcting code (ECC) vs. non-ECC RAM, and channel configurations.

RAM Types

There are many types of RAM, but for the exam you need to know about two types: *desktop RAM* and *laptop RAM*. Generally, desktops use dual-inline memory modules (DIMMs), and laptops use small outline dual-inline memory modules (SODIMMs). We discuss SODIMM types and installation in Chapter 1, "Monitoring, Maintaining, and Replacing Mobile Device Hardware."

Both DIMMs and SODIMMs use RAM that is based on double data rate (DDR) technology. DDR originally got its name because it doubles the data per cycle compared to older types of RAM. A typical data transfer rate for DDR version 1 was 1600 MB/s. This is not nearly enough for today's computers, so let's skip over DDR and DDR2 and move on to more common versions of RAM, including DDR3, DDR4, and DDR5.

DDR3

DDR3 was designed for lower power consumption and higher reliability while enabling higher levels of performance compared to older versions of DDR. DDR3 has 240 pins and common voltages of 1.2 or 1.5 V.

Figure 14.1 shows a typical DDR3-1333 memory module, which is also known as PC3-10600. That means that it can perform 1333 megatransfers per second (MT/s) and has a total data transfer rate of 10,600 MB/s. All the numbers you need to know are in the names!

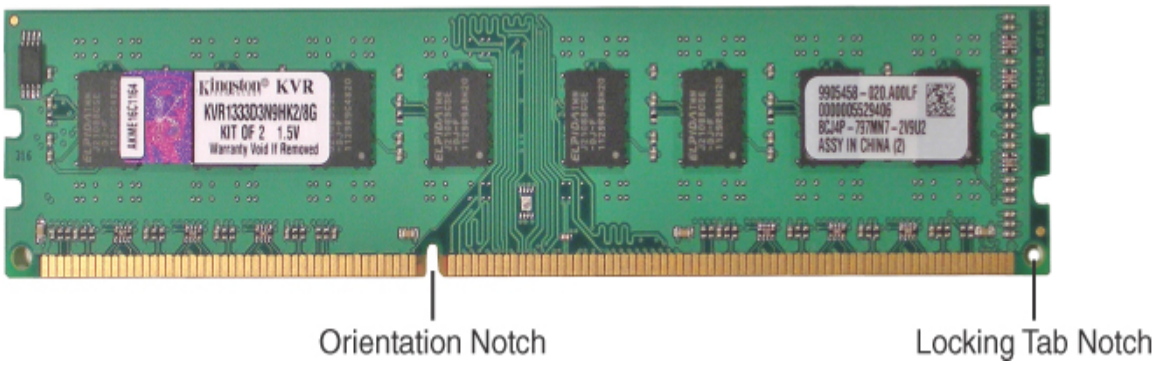


FIGURE 14.1 **A 240-Pin PC3-10600 4-GB DIMM (DDR3-1333)**

The DDR3 module in Figure 14.1 has a sticker on the left that shows an identification code. You might not be able to read it, but it says KVR1333D3N9HK2/8G and Kit of 2, 1.5 V. The 1333 and D3 in the code tell you that this is DDR3-1333 RAM. The 8G tells you the capacity (8 GB) but only when installed as a kit of two memory modules—as the label goes on to say. Finally, it tells you that the memory runs at 1.5 volts.

Leave the sticker on the memory module. This way, the warranty will not be voided, and you can find out important characteristics of the RAM later. Often you will come across sticks of RAM just lying about, and you might not remember what they are without the code on the sticker, which tells you everything you need to know.

DDR4

At 1.2 to 1.35 V, DDR4 has a lower voltage range than most DDR3. It also has a higher module density and a higher data transfer rate. As is the case with all versions of DDR, it is not backward compatible. This type of RAM has 288 pins and has a different physical configuration than DDR3. Table 14.1 compares some typical DDR4 types, and Figure 14.2 shows an example of DDR4.

TABLE 14.1 **Comparison of DDR4 Types**

DDR4 Standard	Transfers per Second	Maximum Transfer Rate	Module Name

DDR4 Standard	Transfers per Second	Maximum Transfer Rate	Module Name
DDR4-2133	2133 MT/s	17,066 MB/s	PC4-17000
DDR4-2400	2400 MT/s	19,200 MB/s	PC4-19200
DDR4-2666	2666 MT/s	21,333 MB/s	PC4-21333
DDR4-3200	3200 MT/s	25,600 MB/s	PC4-25600

Note

The standards listed in Table 14.1 are based on the JEDEC standards (www.jedec.org). JEDEC develops various open standards for the microelectronics industry.

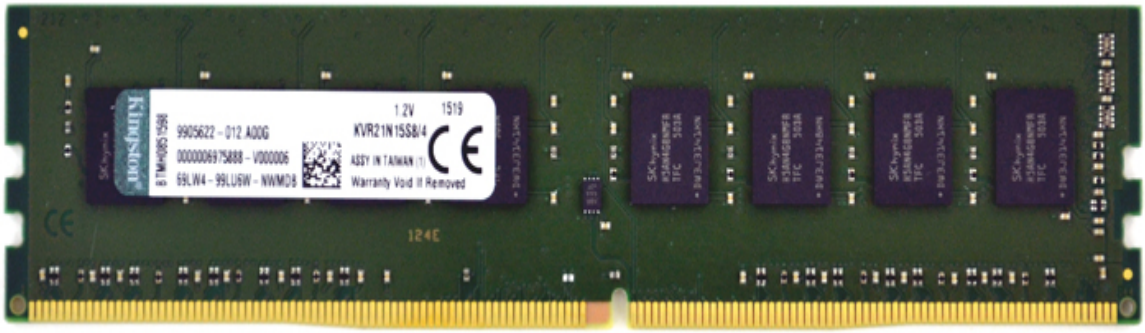


FIGURE 14.2 **A 288-Pin PC4-17000 4-GB DIMM (DDR4-2133)**

As you have probably guessed, the RAM in Figure 14.2 can perform 2133 MT/s and has a maximum data transfer rate of 17,000 MB/s. Note how both connectors are slightly angled. This and the number of pins (among other things) make it incompatible with DDR3 slots.

ExamAlert

Be able to identify a 288-pin DDR4 module.

DDR5

As of the writing of this book, DDR5 is the latest of the DDR standards. It was released in 2020, and modules began arriving to the consumer market in 2021. The voltage for standard DDR5 memory modules is 1.1 V, so it uses less power than DDR4. Like DDR4, it has 288 pins, but there are physical differences, so it is *not* backward compatible with DDR4. One of those physical differences is that the module stack measures 1.0 mm—slightly smaller than DDR4's 1.2 mm. The maximum density of a DDR5 module is 64 GB, compared to DDR4's 16 GB.

A typical speed for DDR5 is 4800 MT/s (also simply referred to as 4800 MHz). At that speed, that RAM can transfer a maximum of 38,400 MB/s. Another typical speed is 6400 MT/s, which can transfer a maximum of 51,200 MB/s (or 51.2 GB/s). As with previous versions of DDR, the goals for DDR5 are to reduce power consumption and increase bandwidth so that it can ultimately work faster and more efficiently.

As the author of this chapter, I personally use ECC, DDR5 5600 MHz in a quad-channel configuration—16 GBx4 for a whopping 64 gigabytes—for my work desktop. We'll speak more about ECC and quad-channel configurations later.

ExamAlert

Remember: DDR3 is 240-pin; DDR4 and DDR5 are 288-pin—and *none* of them are compatible with each other!

Note

Some mobile devices use *low-power* versions of DDR (known as LPDDR3, LPDDR4, and LPDDR5).

Note

DDR6 is the next generation of RAM technology for computers, servers, and notebooks. It's expected to have the following advantages over DDR5, including

- **Higher performance:** DDR6 is expected to offer higher performance than DDR5.
- **Lower power consumption:** DDR6 is expected to consume less power than DDR5.
- **Greater capacity:** DDR6 is expected to support higher memory capacities per module, potentially reaching up to 128 GB per DIMM (dual in-line memory module).
- **More memory channels and banks:** DDR6 has four memory channels and 64 memory banks, which is double the number of each compared to DDR5 and DDR4, respectively.

While DDR6 is still in development, its release is expected to happen in the next few years. It is expected that DDR6 will gradually replace DDR5 memory.

Installing RAM

Installing DRAM is fun and easy. It can be broken down into these basic steps:

1. Orient the RAM properly.
2. Insert the RAM into the slot.
3. Press down with both thumbs until the ears lock.
4. Test.

Easy! But let's take it a little further. Remember that some people refer to memory modules as DIMMs, DRAM, RAM sticks, or just plain RAM, and you could encounter any of these terms on the exam as well. Once you have selected the correct memory module for your motherboard and employed ESD prevention (by using an antistatic strap), you can install the RAM.

Be careful with the RAM and the RAM slot! They are both delicate! Hold the RAM by the edges and do not touch any pins or other circuitry on the memory module. If you need to put it down, put it down on an antistatic mat or in the container it shipped in.

Take a look at the slot; there should be a break in the slot somewhere near the middle (but not in the exact middle). This is where the notch in the memory module will go. Gently place the memory module in the slot, pins down. If the notch does not line up with the break in the slot, you might need to turn the module around. When it appears that the RAM is oriented correctly, press down with both thumbs on the top of the memory module. Keep your thumbs as close to the edge as you can so that you can distribute even pressure to the memory module. Press down with both thumbs at the same time until the tab (or tabs) on the edge of the RAM slot closes and locks on to the memory module. You should hear a click or two when it is done. You might need a bit of force to fully insert the RAM—but don't go overboard! If the motherboard is bending excessively, you are using too much force. If this is the case, make sure that the RAM is oriented correctly; the notches should match up, and the RAM should be straight within the slot. Figure 14.3 shows a bank of DDR4 memory modules installed into the gray DIMM slots in a quad-channel configuration. Each of these is 4 GB, giving a total of 16 GB of RAM.

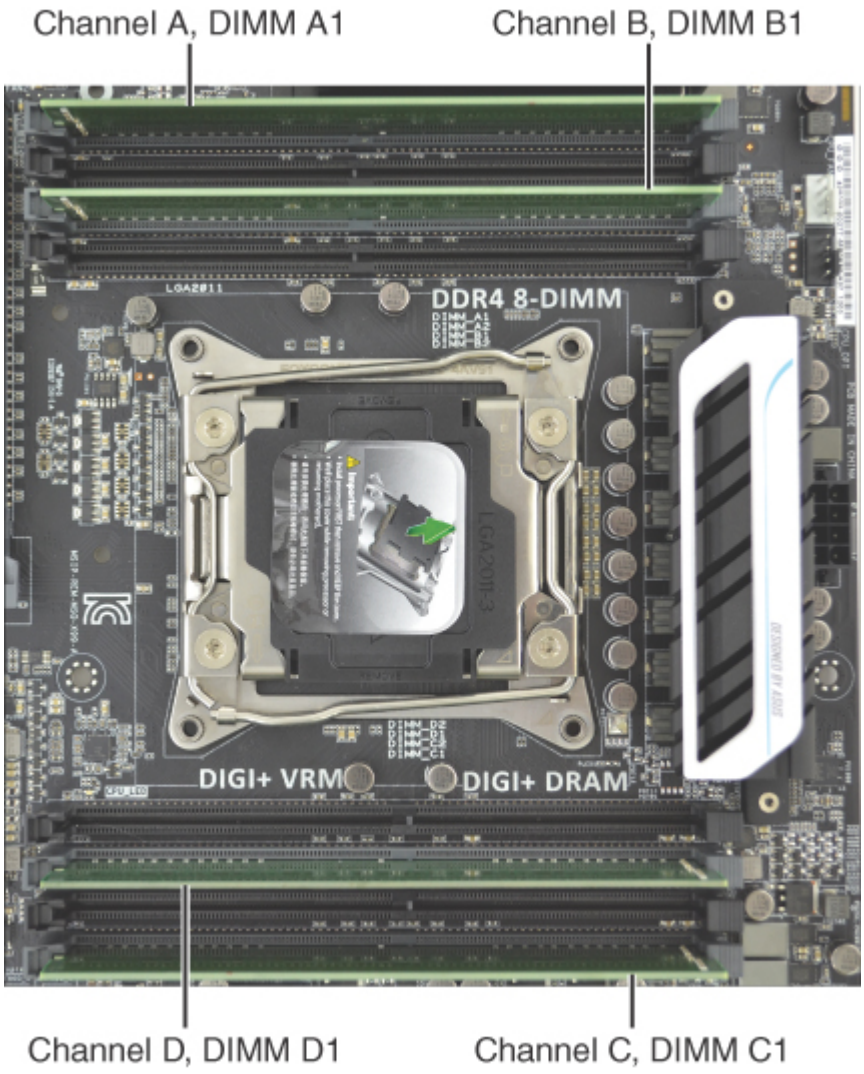


FIGURE 14.3 **Installed Bank of DDR4 Memory Modules**

Now, the most important thing to do with any installation is to *test*. With the case still open, boot the computer, access the BIOS/UEFI, and make sure that the system recognizes the new RAM as the right type and speed. The amount is often on the main page, but you might need to look deeper for the exact configuration, depending on the motherboard. Next, access the operating system (after the OS is installed) and make sure it boots correctly. Complete several full cycles and warm boots. Also, at some point, you should view the RAM within the operating system. For example, in Windows, use the System Window or the Task Manager to verify that the operating system sees the correct capacity of RAM:

- **System Window:** Go to **Settings > System > About**, or **Control Panel > All Control Panel Items > System**. The total RAM should be listed within this window.
- **Task Manager:** You can view the Task Manager by right-clicking on **Start** or on the taskbar and selecting **Task Manager**. There are several other ways to open this. I like this one: Press Windows+R to bring up the Run prompt and type **taskmgr**. When it is open, go to the Performance tab and view the Memory section. It should show the total physical memory as well as the memory that is in use. Figure 14.4 shows a computer running Windows 10 Pro, displaying 32 GB of RAM in the Task Manager or, more accurately, 31.9 GB, as circled toward the upper left of the figure. The in-use amount is 6.1 GB.

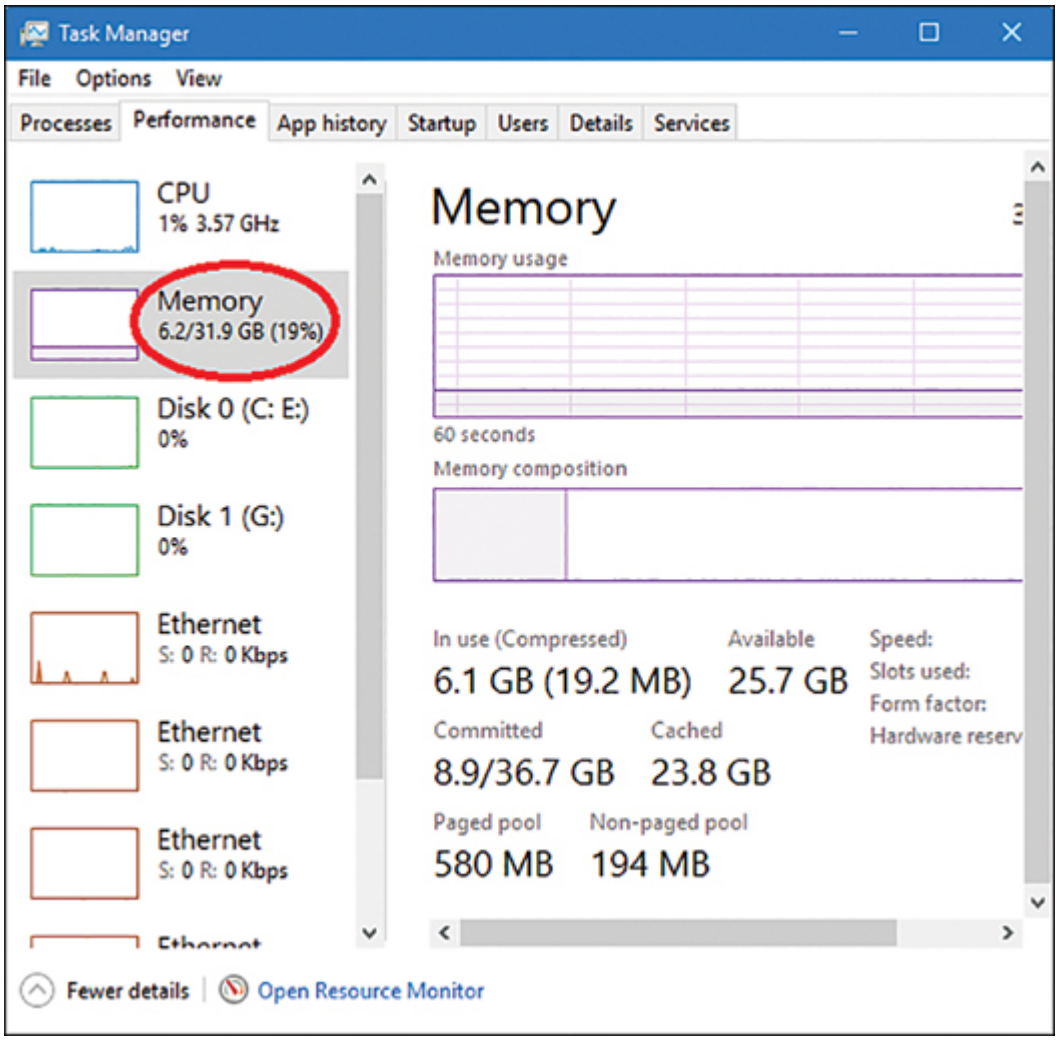


FIGURE 14.4 **Task Manager Showing 32 GB of RAM**

Note

There are plenty of good third-party tools for analyzing RAM as well, such as CPU-Z. See https://www.cpuid.com/softwares/cpu-z.html. For more information on installing RAM, see https://www.crucial.com/articles/about-memory/how-to-upgrade-desktop-memory.

Another good test of RAM is to make sure you can open several applications at once without any issues or delays. Finally, if everything looks okay, close up the case, and if all went well, congratulate yourself on another job well done!

ExamAlert

Be familiar with SODIMM and DIMM form factors and know how to select, install, and verify RAM.

There are a few other important things to mention here.

First, if you were for some reason to install two different speeds of RAM, the system would most likely run at the lower of the two speeds. This is an example of *underclocking*, and it means you won't get the most out of the computer. However, a mismatch like this could also cause the system to fail because some motherboards insist that the modules be identical.

Second, if you install the very latest type of RAM that is supposed to be compatible with a motherboard, be prepared to update the BIOS/UEFI so that the system can recognize the new RAM. The firmware update (also known as a *flash*) is one of the most important jobs a PC technician will perform.

Third, much of the RAM you buy has a stated speed that is actually an *overclocked* speed. This means that if you do not go into BIOS/UEFI and enable the overclocking setting, it will run at the stock speed. For Intel, this

is called XMP in the BIOS/UEFI. AMD's original overclocking setting was called DOCP, but newer, more modern AMD motherboards use the new and improved EXPO setting. These settings allow for RAM timings and speeds to be automatically configured to profiles the RAM manufacturers set. This is commonly why you will hear users gripe that they bought DDR5 6000 MHz RAM but it's only running at 4800 MHz. While there could be issues with compatibility, the most likely cause is that they did not enable XMP/DOCP/EXPO in their BIOS/UEFI and the RAM is running at stock, nonoverclocked speeds.

A Final Word About Installing RAM

The main thing to remember when working with RAM is that it needs to be compatible with the motherboard. Check your motherboard's documentation regarding capacity per slot (or channel), channel/slot configuration, maximum capacity, and speed. The best thing to do is to run a search on your particular motherboard at the RAM manufacturer's website to obtain a complete list of compatible RAM and then cross-reference that with your motherboard's manual.

RAM Technologies

Once you have chosen the type of RAM to use, you must then decide on more technical details, such as the configuration of channels, which will be dictated in part by the motherboard. Your particular solution might also require the use of error correction memory, which is less common for desktop PCs and laptops but might be necessary for more customized computers. Let's begin with memory channels.

Single-Channel vs. Multichannel Architectures

Single-channel is the original RAM architecture for PCs. It means that there is a 64-bit address bus (or data channel) between the memory and the memory controller (usually within the CPU). One or more sticks of RAM can be installed into the motherboard, but they share the same channel.

Dual-channel is a technology that essentially doubles the data throughput. Two separate 64-bit channels are employed together, resulting in a 128-bit

bus. To incorporate this, the proper motherboard has color-coded matching banks divided into Channel A and Channel B. Triple-channel architecture accesses three memory modules at the same time and is, in effect, a 192-bit bus.

Quadruple-channel (or simply quad-channel) architecture takes this idea to the next level. It works only when four identical memory modules are placed in the correct slots. Quad-channel is common in computers that use DDR4 or higher. Four 64-bit-wide buses work together, and a module of RAM must be installed in each of the four banks for best results. If only three modules are installed (thus only three banks are used), the architecture downgrades to triple-channel automatically. Likewise, if only two are used, the motherboard scales back to dual-channel architecture. However, in some cases, the reduction in performance is negligible.

DDR5 RAM has two independent channels, each 40 bits wide, with 32 data bits and 8 ECC bits. This improves memory access efficiency by allowing for more precise data transfers.

Figure 14.5 shows an example of a motherboard's RAM slots making use of quad-channel technology. As you can see in the figure, there are four banks, each with two slots (one of which is black and one of which is gray). By installing a memory module into each of the gray slots (known as A1, B1, C1, and D1), you can harness the collective power of the quad-channel technology.



FIGURE 14.5 **A Motherboard with Quad-Channel-Capable RAM Slots**

ExamAlert

Know the difference between single-, dual-, triple-, and quad-channel for the exam.

ECC vs. Non-ECC

Error correction code (ECC) in RAM can detect and correct errors. Real-time applications might use ECC RAM. When using ECC, additional information needs to be stored, and more resources are used in general. This RAM is the slowest and most expensive of RAM types. DDR ECC modules are identified with either the letter E or ECC (for example, PC3-10600E). DDR5 has another advantage: on-die ECC. This provides further protection against single-bit errors in DDR5 memory modules. For every 128 bits of data, DDR5 stores an additional 8 bits for ECC. If ECC is enabled, whenever data is read, the actual data and the ECC data are read together, and so DDR5 can repair single-bit errors on any data bits right away.

ExamAlert

Know that ECC RAM can prevent data loss and potential system crashes by automatically correcting memory errors. Non-ECC RAM is suitable for most consumer-grade computers and less demanding workloads.

Note

ECC RAM is typically used in servers where mission-critical applications are run and errors can be detrimental. In fact, most consumer desktop motherboards do not even support ECC RAM. Intel is a classic example of only supporting ECC RAM in servers and professional-level motherboards. However, AMD unofficially supports ECC RAM in many of its motherboards. There is a trend among many people, this author included, of finding consumer

motherboards that support ECC RAM and buying compatible ECC RAM to increase stability. While there is a slight performance hit, the added error correction can make the system significantly more stable.

Virtual RAM

Virtual RAM is a term that can be applied to several technologies. Two examples include Windows virtual memory and virtual RAM, as it is configured on a smartphone. Both of these address the problem of limited RAM by using other, long-term storage in the place of RAM—this becomes *virtual RAM*.

In Windows, virtual memory is space used to emulate RAM on a storage drive of some sort: hard disk drive, solid-state drive, flash drive, and so on. It's also known as a paging file. Let's say you are working on a laptop that has only 2 GB of RAM. That amount might not be enough for today's applications and processes. When the memory in use by all the existing processes in Windows goes beyond the amount of physical RAM that is installed, Windows moves pages of information to the storage drive. The beauty of this is that a typical PC or laptop now has virtually unlimited storage. The drawback is that the virtual storage space will be much slower than physical RAM. Remember when you opened your 40th tab in your web browser and the computer started going noticeably slower? Yeah, you probably ran out of RAM and were using your virtual memory.

Note

In Linux, the paging file is usually a dedicated partition called Swap. It is essentially the same thing as Window's page file (pagefile.sys).

The Windows utility for virtual memory can be accessed in the Performance section of the System Properties window. To get there quickly, type **systempropertiesadvanced** (all one word) at the Run prompt or in the Search tool. Then, under Performance, click the **Settings** button. The Performance Options window appears. Click the **Advanced** tab, and then, in the Virtual Memory section, click **Change**. From there, you can modify how Windows uses virtual memory. We'll discuss this more in the 220-1202 portion of the book.

On a different note, virtual RAM is a feature in some smartphones that allows a system (such as Android) to run more applications in memory than the actual RAM would normally allow. It does this by using the device's regular long-term storage as additional RAM storage space. This is similar to Windows virtual memory.

For example, say that you have an Android-based smartphone with 4 GB of physical RAM and 64 GB of long-term storage. Let's also say that you run a lot of resource-hungry apps. The system can be configured to use a certain amount of long-term storage to act as additional RAM. For example, perhaps it was configured as 8 GB. That would mean you now have 4 GB of actual RAM, plus the ability to run 8 GB of additional applications. However, that will reduce the total amount of long-term storage that you can use for pictures, videos, and so on from 64 GB to 56 GB.

Remember that 8 GB isn't *actual* RAM; it's *virtual* RAM! The long-term storage (typically flash memory) used as virtual RAM will be much slower than actual RAM. So, Android will prioritize the applications that are running. More demanding applications such as video players and games will get a higher level of importance and will be the first applications to use actual RAM. Less demanding and lesser-used applications (such as a calculator or note-taking program) will get a lower priority, and as the RAM fills up, those applications may be moved to virtual RAM.

In the past, this was a technique that could only be done if you "rooted" the phone (which is not recommended). However, today it is becoming more commonplace as a feature of the OS or through the use of special virtual RAM apps.

Cram Quiz

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

1. What is the transfer rate of DDR4-2133?

- ○ **A.** 17,066 MB/s

- **B.** 19,200 MB/s
- **C.** 21,333 MB/s
- **D.** 25,600 MB/s

2. A technician attempts to install a DDR5 module into a motherboard, but it doesn't appear to fit. Which of the following are possible reasons for this? (Select the two best answers.)

- **A.** The motherboard doesn't allow DDR5 memory.
- **B.** Windows doesn't allow DDR5 memory.
- **C.** The RAM stick is being installed backward.
- **D.** The BIOS/UEFI hasn't been updated.

3. Which of the following technologies allows for a 256-bit-wide bus?

- **A.** ECC
- **B.** Quad-channel
- **C.** Virtual RAM
- **D.** Task Manager

4. A technician has just installed additional RAM into a Windows-based graphics-intensive workstation to meet software application requirements. What should the technician do next to ensure that the correct amount of RAM is installed and that it is working properly? (Select the two best answers.)

- **A.** Increase the size of the paging file.
- **B.** Test the RAM.
- **C.** Go to **Settings > System > About**.
- **D.** Press down with both thumbs until the ears lock.

5. A technician has installed dual-inline memory modules that each have 288 pins and use 1.1 V. What kind of RAM has the tech

installed?

- ○ **A.** DDR4 DIMMs
- ○ **B.** DDR3 DIMMs
- ○ **C.** DDR4 SODIMMs
- ○ **D.** DDR5 DIMMs

6. A technician is considering RAM types for a server where mission-critical applications are run and errors can be detrimental. What type of RAM is currently the best option for the tech to consider installing in the server?

- ○ **A.** Non-ECC RAM
- ○ **B.** Virtual RAM
- ○ **C.** DDR6
- ○ **D.** ECC RAM

Cram Quiz Answers

1. **A.** The transfer rate of DDR4-2133 is 17,066 MB/s. It is also known as PC4-17000. 19,200 MB/s is the speed of DDR4-2400 (PC4-19200). 21,333 MB/s is the speed of DDR4-2666 (PC4-21333). 25,600 MB/s is the speed of DDR4-3200 (PC4-25600).

2. **A and C.** It is possible that the technician is attempting to install DDR5 RAM into a motherboard that only accepts DDR4. Remember, DDR memory is not backward compatible, so you can't install DDR5 to a DDR4-based motherboard and vice versa. It's also possible that the RAM module simply needs to be turned around; always line up the notch on the RAM with the break in the RAM slot. A physical problem with the RAM wouldn't be caused by the operating system or the BIOS/UEFI.

3. **B.** The quad-channel memory architecture can allow for a 256-bit-wide bus (64-bit per channel). However, this will only be the case if all four channels have memory installed to them. ECC, which

stands for error correction code, can detect and correct errors in RAM. Virtual RAM is used in smartphones to "extend" the amount of usable RAM to the phone's long-term storage. (It is known as virtual memory in Windows.) The Task Manager is a Windows program that is used to analyze the system.

4. **B and C.** The most important thing to do after installation is to test the RAM. Access the BIOS/UEFI and make sure the system recognizes the new RAM as the right type and speed. Next, view the RAM within the operating system. For example, in Windows, use the System window: Go to **Settings > System > About**. Virtual RAM or virtual memory, also known as the paging file, uses part of the storage drive to expand physical RAM. Pressing down with both thumbs is part of the installation process that, according to the scenario, has already been performed.

5. **D.** DDR5 dual-inline memory modules (DIMMs) have 288 pins and operate at 1.1 volts (V). Although DDR4 modules do have 288 pins, the architecture is different, and the voltage ranges between 1.2 and 1.35 V. DDR3 has 240 pins and common voltages of 1.2 or 1.5 V. Laptops use small-outline dual-inline memory modules (SODIMMs). Two common types of SODIMMs in laptops are DDR3 (which has 204 pins) and DDR4 (which has 260 pins).

6. **D.** ECC RAM is typically used in servers where mission-critical applications are run and errors can be detrimental. In fact, most consumer desktop motherboards do not even support ECC RAM. Non-ECC RAM is suitable for most consumer-grade computers and less demanding workloads. Virtual RAM is space used to emulate RAM on a storage drive of some sort: hard disk drive, solid-state drive, flash drive, and so on. DDR6 is still in development; its release is expected to happen in the next few years.

Another chapter done. Keep it up—I believe in you! "Memory is the diary that we all carry about with us." —Oscar Wilde

Chapter 15
Storage Drives

This chapter covers the following A+ 220-1201 exam objective:

- **3.4** – Compare and contrast storage devices.

Everyone needs a place to store data. Whether it's business documents, audio/video files, or data backups, users must decide on the right storage medium. This can be solid-state media, magnetic media, or optical media. Devices include hard disk drives, solid-state drives, optical drives, and flash-based drives, among others. The media used depends on what is stored and how often and where it is needed. This chapter concentrates on the categories of storage media and how to identify and troubleshoot them.

The two main types of internal storage drives are solid-state (which contains no disk) and magnetic (hard disk drive). These are the most common options for the location of the operating system. However, users also store frequently accessed data, such as documents, music, pictures, and so on. These could be stored on any of the media types mentioned so far. We'll discuss all of these media types in more depth, but first, let's take a look at a common standard for storage—SATA.

ExamAlert

Objective 3.4 focuses on the following: hard drives, solid-state drives, form factors, drive configurations, removable storage, and

optical drives.

SATA

Serial AT Attachment (also known as Serial ATA, or just SATA) is a serial bus communication interface used to move data to and from storage drives. To transmit that data, the drive has a 7-pin data port, as shown in Figure 15.1. You use a SATA cable to connect that port to the motherboard or SATA adapter card of the computer.

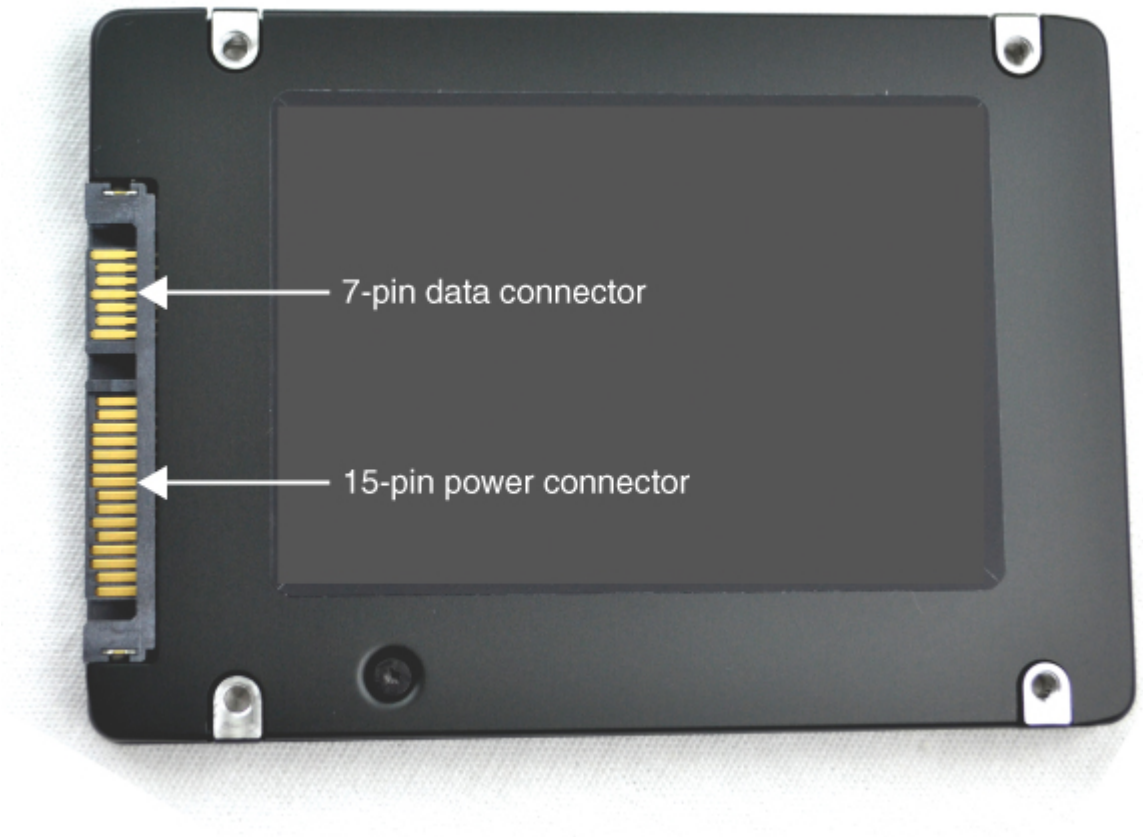


FIGURE 15.1 **SATA Data and Power Connectors on a 2.5-Inch SSD**

For power, a SATA drive utilizes a 15-pin power connector, as shown in Figure 15.1. The drive's connectors have vertical tabs in the center, making for easier orientation when connecting the cables. Power supplies send 3.3 V, 5 V, and 12 V to the SATA drive.

SATA technology is used by magnetic hard drives and solid-state drives. What has been described so far is SATA Revision 3.0. However, there is also SATA Revision 3.2. It is less common than 3.0 and requires either a SATA Express port or an M.2 slot to operate. SATA Express ports are like triple connectors with 18 pins (7 pins + 7 pins + 4 pins). SATA Express isn't very common. Many people, including technicians, prefer other technologies over it, such as NVMe-based M.2 cards, which we'll discuss in a little bit. Table 15.1 shows these two SATA revisions.

TABLE 15.1 **Comparison of SATA 3.0 and 3.2**

Standard	Maximum Data	Transfer Rate
SATA Revision 3.0	6 Gb/s	600 MB/s
SATA Revision 3.2	16 Gb/s	1969 MB/s

ExamAlert

Know the maximum data transfer rates for SATA Revisions 3.0 and 3.2.

Note

You might also see some organizations refer to SATA measurements using the units Gbit/s or Gbps, instead of Gb/s, but they mean the same thing.

ExamAlert

Also listed in the objectives is mSATA (which is short for Mini-SATA). This type of connector was used in laptops for SSDs. An mSATA drive has a single notch, as opposed to two notches on laptop-based M.2 devices that use the 2242 form factor. M.2, by the way, supersedes the mSATA specification.

Data Transfer Discrepancy

If you divided by 8 to determine rates for SATA Revision 3.0, the actual data written to the drive would be less than you would expect. This is due to overhead in the form of encoding. That brings Revision 3.0 down from 6.0 to 4.8 Gb/s (which equates to 600 MB/s). SATA 3.2 is not affected by this issue.

Magnetic Hard Drives

Magnetic hard drives, or *hard disk drives (HDDs)*, were the most common form of magnetic media for many years. A hard disk drive contains one or more platters with a magnetic surface. As the platters rotate at high speed, read/write heads store and read information to and from the disk.

HDDs came in two main widths: 3.5 inch and 2.5 inch. The 3.5-inch drives were used in desktop computers, network-attached storage (NAS), and other larger devices. The 2.5-inch drives were used in laptops and other smaller devices. Generally, HDDs used the SATA communications interface. They were typically sold with data storage capacities of 500 GB, 1 TB, 2 TB, 4 TB, and beyond.

ExamAlert

Remember that HDDs come in two main widths: 3.5 inch and 2.5 inch. The 3.5-inch drives are used in desktop computers and other larger devices. The 2.5-inch drives are used in laptops and other smaller devices.

Note

A typical operating system such as Windows displays a 500 GB drive as having a capacity of 476 GB (or 465 GB or a similar number). This is due to a difference in numbering systems used to

measure the drive. A hard drive manufacturer uses the base 10 system, whereas Windows uses the base 2 system, resulting in a slightly lower number. No actual space is lost during this conversion!

This discrepancy seems to favor the manufacturer of drives. This is also where you will see conflicting information regarding sizes. For example, many people state that there are 1000 bytes in a kilobyte (KB). While this is true, it is better to learn there are 1024 bytes in a kilobyte (KB), because this is how the operating system sees it since it uses binary, which is a base 2 numbering system. You will get more accurate results doing this.

For example, if you're formatting a partition on a drive and want a 50 gigabyte (GB) partition, the partition manager will show the space in megabytes. So, take 50 and multiply it by 1024 because there are 1024 megabytes in a gigabyte. The answer would be that 50 GBs are equal to 51,200 MBs. Notice, if you did this calculation in base 10, the answer would be 50 times 1000 and equal 50,000. The operating system would see this as smaller than the 50 GB partition you wanted.

HDDs are still somewhat common because they have been available for a long time and are generally cheaper than solid-state drives. However, a couple of things set them apart, such as these specifications:

- **Rotational spindle speed:** The platters in an HDD rotate at a certain speed. For example, 7200 revolutions per minute (RPM) is common; other typical speeds for hard drives include 5400 RPM (slower access time) and 10,000 RPM and 15,000 RPM (faster access times).
- **Latency:** Latency is the delay in time after a track has been reached by the read head and before a particular sector on the platter can be read. It is directly related to rotational speed and is usually half the time it takes for the disk to rotate once. For example, a 7200-RPM drive has an average latency of 4.2 ms (milliseconds), but a 10,000-RPM drive has an average latency of 3.0 ms.

The average desktop HDD is 3.5 inches in measurement, whereas laptop HDDs are 2.5 inches. Also, generally, desktop HDDs are 7200 RPM, whereas laptop HDDs are 5400 RPM. Laptop HDDs usually use 5400 RPM HDDs because they run cooler than 7200 RPM HDDs. Please note that the measurement is the measurement of the platters inside the HDD. For instance, a 3.5-inch HDD actually measures about 4 inches in width externally.

ExamAlert

Know the different hard drive spindle speeds for the exam!

Although there are faster and more efficient technologies than HDDs, they still offer the best bang for your buck when dealing with larger storage requirements—think 5 terabytes (TB) and beyond. However, when you're looking at 1–2 terabytes, the price point is not that much different than a newer, faster technology out there. Enter the SSD.

Solid-State Drives

A *solid-state drive (SSD)* is used to store operating systems and files, similar to a magnetic hard disk drive. However, SSDs don't use spinning disks or read/write heads; they instead write data to non-volatile microchips. Because of this, they are silent and more resistant to physical shock, and they have lower access time and less latency than magnetic hard drives. Because there are no moving parts, rotation speed is not an issue.

SATA-based SSDs normally measure 2.5 inches in width. Installation requires either a 2.5-inch internal bay, special screw holes drilled directly into the computer case, or an adapter kit for installation in a 3.5-inch internal bay. If you are dealing with a laptop that has a 2.5-inch internal HDD, then you can normally swap it out directly with an SSD because they are the same measurement! Talk about an increase in speed! Just remember that if you swap out the HDD with an SSD on a laptop, you will need to copy over the operating system or reinstall.

However, there are other types of SSDs, such as the M.2-based SSD. These are small form factor cards that are installed directly into a motherboard or to an adapter card if the motherboard doesn't have an M.2 slot. Either way, the M.2 card is installed at a slight angle and then pressed flat against the board and screwed in. There are a variety of different M.2 card sizes. A common example is 2280, which means it is 22 mm wide by 80 mm long. M.2 cards are known to offer several times the data transfer rate of a typical 2.5-inch SATA 3.0 SSD. While the M.2 slot can be used with different types of technologies, the most common and fastest (as of the writing of this book) is Non-Volatile Memory Express (NVMe), which is a specification for accessing storage while using PCI Express (PCIe). Essentially, the M.2 slot on a motherboard taps into the PCIe bus (x4) and uses a portion of the total bandwidth associated with that bus. This usually results in the loss of one PCIe version 3, 4, or 8 slot, and depending on the type of CPU and motherboard, it could also mean a battle for bandwidth between the video card and the M.2 card (and possibly other devices). In addition, NVMe-based M.2 cards tend to run hot. So, careful planning is required before installing an M.2 card. There are also PCIe drives that exist as cards that you can plug directly into a PCIe slot. We'll discuss the PCIe bus in more detail in Chapter 16, "Motherboards and Add-on Cards."

Another type of solid-state drive is the Serial Attached Small Computer System Interface (SAS). SAS is a high-speed data transfer technology designed primarily for computer storage devices. It's a serial communication protocol, meaning it transmits data bit by bit, and is widely used in enterprise environments due to its reliability and performance. In relation to solid-state drives, SAS provides a robust interface for high-throughput data access, essential for applications demanding rapid data retrieval, such as servers and data centers.

Essentially, SAS acts as a communication pathway between a computer and storage devices like SSDs. It builds on the traditional SCSI command set but uses serial connections for improved speed and scalability. This makes SAS a strong choice for applications requiring high performance and reliability, and therefore, SAS is commonly used in enterprise-level servers that house large amounts of SSDs.

Note

PCIe has many improvements over older standards, including much higher maximum system bus throughput, lower I/O pin count, and a smaller overall physical footprint. PCIe slots come in different configurations of bidirectional lanes, including x1, x4, x8, x16, and x32. As a technician, you should keep up with the newer PCIe specifications. To learn more, visit https://pcisig.com/specifications.

ExamAlert

Be sure you are able to compare and contrast the various SSD communication interfaces, including NVMe, SATA, PCIe, and SAS for the exam.

Note

M.2 drives can be confusing for the consumer because there are two main types: M.2 SATA and M.2 NVMe. They look the same because they have the same form factor—M.2. However, the technology is different. We discussed M.2 NVMe, which is the faster of the two technologies because it uses the PCIe lanes. However, M.2 SATA is still quite fast but will be the same speed as a 2.5-inch SSD because it uses the same communication protocol—SATA. In fact, often when you use an M.2 SATA drive, it will disable a SATA port on the motherboard. So be sure to read the motherboard manual carefully. The major benefit to using M.2 is that there is no need for separate power and data cables. When you plug the M.2 into the motherboard, it transfers power and data through the one port. Imagine that!

Note

To learn more about M.2, SATA, PCIe, and NVMe SSDs, visit https://www.crucial.com/articles/about-ssd/m2-with-pcie-or-sata.

Note

SSD technology can be combined with magnetic disk technology to form what is known as a hybrid drive, or SSHD drive. This could be accomplished in a drive that incorporates NAND flash memory (for caching of data and speed) and a magnetic disk (for increased capacity). There are also M.2-based caching cards that can be used in combination with a magnetic disk to increase performance.

Storage Drives Can Be a Bottleneck in a System

We often say that your computer is only as fast as its weakest link. A weak component can slow down your entire system, acting as a bottleneck when it comes to processing data, opening and running programs, and saving and rendering information. This can ultimately lead to decreased performance of the entire system. So, pay careful attention to the selection of storage drives when building or upgrading computers. If funds allow, make sure that you are taking full advantage of your system's capabilities.

RAID

Redundant array of independent (or inexpensive) disks (RAID) technologies are designed to either increase the speed of reading and writing data or to create one of several types of fault-tolerant volumes—or both. Fault tolerance is the capability of a storage drive system to continue working after there is a problem with one of the drives.

To create a RAID array, you need two or more drives. Then, you need to set up the array through either software or hardware. Some operating systems support the software option, but it is not usually recommended. Hardware-based RAID is more common, and it involves one of three things: either using the motherboard's built-in RAID support, if present; using a RAID

adapter card; or using an external device such as network-attached storage (NAS) that has RAID capability.

The exam requires you to know RAID levels 0, 1, 5, 6, and 10. Table 15.2 describes them.

TABLE 15.2 **RAID 0, 1, 5, 6, and 10**

RAID Level	Description	Fault Tolerant?	Minimum Number of Disks
RAID 0	Striping. Data is striped across multiple disks in an effort to increase performance.	No	2
RAID 1	Mirroring. Data is copied to two identical disks. If one disk fails, the other continues to operate. When each disk is connected to a separate controller, this is known as disk duplexing. See Figure 15.2 for an illustration.	Yes	2 (and 2 only)
RAID 5	Striping with parity. Data is striped across multiple disks; the fault-tolerant parity data is also written to each disk. If one disk fails, the array can reconstruct the data from the parity information. See Figure 15.3 for an illustration.	Yes	3
RAID 6	Striping with double parity. Data is striped across multiple disks; there are two fault-tolerant parity blocks written to each disk. If two disks fail, the array can reconstruct the data from the parity information.	Yes	4
RAID 10	Combines the advantages of RAID 1 and RAID 0. Requires a minimum of four or more disks. The system contains at least two mirrored disks that are then striped. Also known as “stripe of mirrors.”	Yes	4

Figure 15.2 shows an illustration of RAID 1 (mirroring). You can see that data is written to both disks and that both disks collectively are known as the M: drive or M: volume. So, even though there are two 2 TB drives, this volume has a total capacity of only 2 TB.

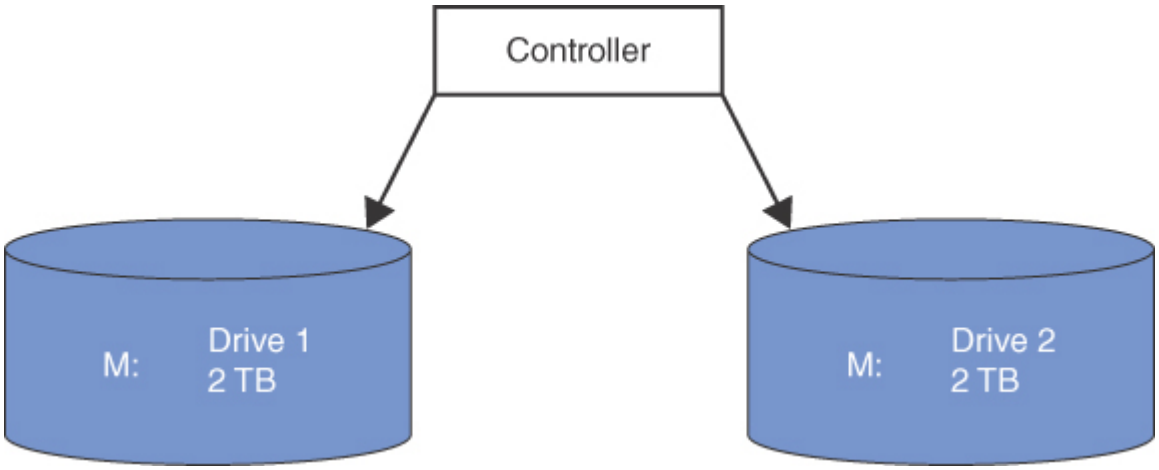


FIGURE 15.2 **RAID 1 Example**

Figure 15.3 shows an illustration of RAID 5 (striping with parity). In a RAID 5 array, blocks of data are distributed to the disks—A1 and A2 are a block, B1 and B2 are a block, and so on—and parity information is written for each block of data. It is written to each disk in an alternating fashion (Ap, Bp, and such) so that the parity is also distributed. If one disk fails, the parity information from the other disks will reconstruct the data.



FIGURE 15.3 **RAID 5 Example**

Some organizations prefer RAID 6, which requires four drives minimum and writes two sets of parity, also known as double parity. This can allow for the failure of two disks simultaneously. It works well for larger arrays—that is, arrays with more drives. In larger environments, *hot-swappable* capability is a must; this means drives can be removed and inserted while the system is on.

Figure 15.4 illustrates RAID 1+0 (pronounced RAID one plus zero), which is commonly known as RAID 10. RAID 10 is a type of nested, or hybrid, RAID that combines RAID 1 and RAID 0. In RAID 10, two or more mirrored drives are then striped. The figure shows a RAID 1 mirror consisting of two drives: disk 0 and disk 1. Then, there is a second RAID 1 mirror with two more drives: disk 2 and disk 3. The two RAID 1 mirrors are then striped as RAID 0. Together, they become RAID 10. This makes for a more powerful version of mirroring that can use more drives.

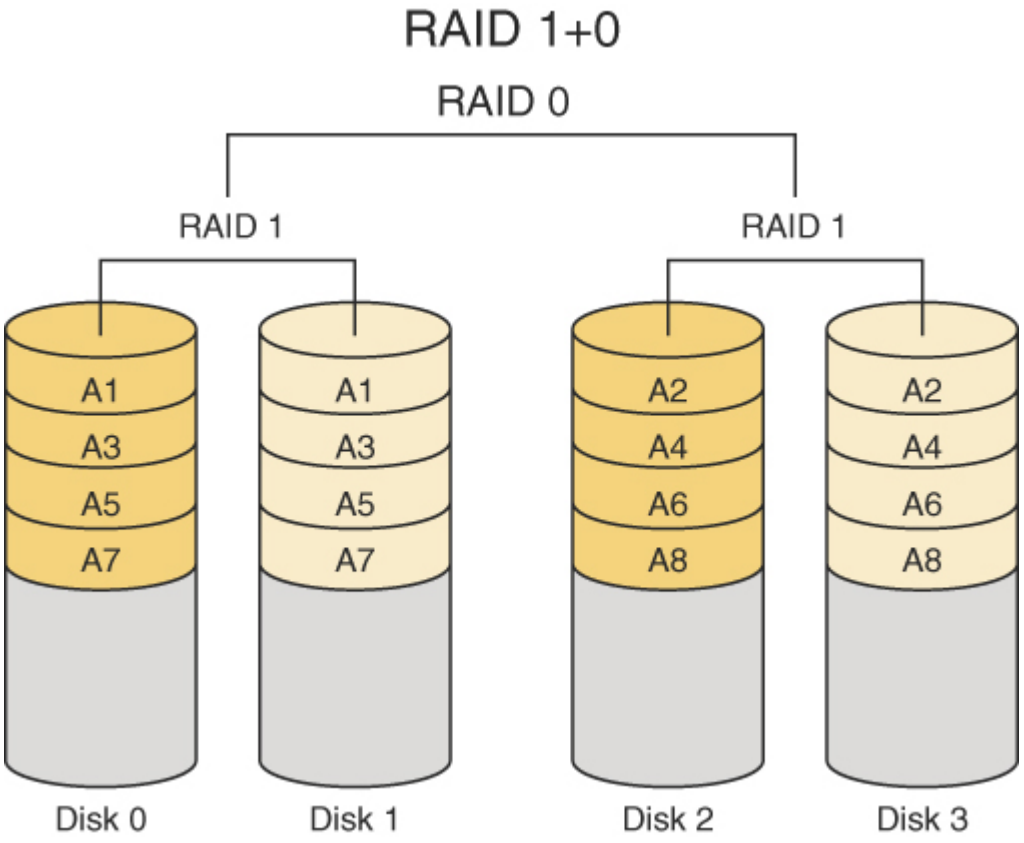


FIGURE 15.4 **RAID 10 Example**

Remember that drive arrays should be built using identical drives. This means using a group of the same magnetic disk drives or a group of the same solid-state drives. Deviate from this suggestion at your own risk!

RAID can provide a type of fault tolerance. It is important to make the distinction between fault tolerance and backup. *Fault tolerance* means that the drives can continue to function (with little or no downtime) even if there is a problem with one of the drives; for example, RAID 1 and RAID 5 provide fault tolerance. *Backup* means copying the data (and possibly compressing it) to another location for archival in the event of a disaster. An example of a disaster would be if two drives in a RAID 5 array were to fail. Keep in mind that RAID 0 is *not* fault tolerant. It harnesses the power of multiple drives but cannot recover after a single drive failure.

ExamAlert

Know the differences between the various types of RAID: RAID 0 (striping), RAID 1 (mirroring), RAID 5 (striping with parity), RAID 6 (striping with double parity), and RAID 10 (stripe of mirrors).

Flash

Flash memory is used in all kinds of solid-state technologies. Most of these technologies use NAND-based flash memory. In this section, we'll focus on removable storage in the form of USB flash drives and Secure Digital cards.

USB Flash Drives

The USB flash drive is probably the most familiar of all flash media. Also known as USB thumb drives, these drives are often retractable and can be carried on a keychain.

When you plug in a USB flash drive on a Windows system, the drive shows up as a volume within File Explorer. Connecting the drive is easy: Just find an open USB port. But remember that you should eject the flash drive in the operating system before disconnecting the drive physically. Failing to do so

can cause electrical irregularities that can damage the data on the drive. In Windows, right-click the **Safely Remove Hardware and Eject Media** icon in the notification area and then click **Eject** to shut down power to the selected USB device. Then you can safely remove it from the physical USB port. The icon appears as a USB cable connector with a check mark. If your USB device has a light, make sure that light is off before physically removing the device. You can also "eject" optical drives and virtual drives in this manner.

ExamAlert

Remember to *safely remove* USB flash drives in the operating system before physically disconnecting them.

Tip

Sometimes a USB or other flash-based solid-state device can't be removed with the Safely Remove Hardware option in Windows. If this happens, consider shutting down the computer before physically disconnecting the device to avoid data corruption or loss.

The advantages of a USB flash drive are obvious: quick and efficient moving of data—and a lot of data at that. However, such a drive is not meant for long-term storage in the way that a magnetic or solid-state drive is; it is meant for transferring data from one system to another. It can also be used to boot systems for installation purposes or for troubleshooting.

Let's talk about the type of memory used in this solid-state device. NAND flash memory is the core of a USB flash drive. This memory is divided into blocks that are generally between 16 KB and 512 KB. A USB flash drive's blocks can be written to only so many times before failures occur. With some flash drives, manufacturers estimate this limit is 1 million write/erase cycles, or 10 years of use. However, just as storage drives will never attain their maximum data transfer rate, it is doubtful that a flash drive will ever

attain that maximum number of write/erase cycles. In addition, the number of years is subjective; it all depends on how often a user works with the flash drive. Basically, if you take the number given by the manufacturer and cut it in half, you should be in good shape, unless you are an extreme power user.

Now back to NAND flash failures: Because this type of memory incurs a small number of faults over time (as opposed to NOR flash, which should remain free of faults), a method known as Bad Block Management is implemented. Bad Block Management maintains a table of the faulty blocks within the USB flash device, making sure not to save data to those blocks. Blocks are divided into pages, which can be between 512 bytes and 4 KB. Each page has error detection and correction information associated with it. All this is done to prolong the lifespan of devices that use NAND memory.

Normally, USB flash drives are shipped in a formatted state (for example, FAT32). This enables the drive to be accessed by just about any computer on the market and makes for easy repair of corrupted files with Windows utilities. If the user so chooses, these drives can also be formatted as NTFS or other file systems, which may be necessary to interface with certain systems or perform particular installations. Sometimes NAND flash devices (such as USB flash drives) act up intermittently. Unless a device has failed completely, a quick reformat usually cures the flash drive of its woes. Just be sure to back up your data first! This method applies to other forms of solid-state, NAND-based media as well. After reformatting, test the drive by moving files to it and then opening them. Of course, after a certain point, the drive will fail and will need to be replaced. Periodically check USB flash drives for stability.

Some USB flash drives are preloaded with software that can restore data and possibly secure transferred data.

Note

As stated, USB flash drives are normally formatted as FAT32 for compatibility reasons. However, FAT32 is limited to files under 4 GB because of the limitation of 32 bits. If you are moving large video files or operating system images—like ISOs (International

Organization for Standardization)—you will have issues because they are often over 4 GB in size. This might have happened to you: You try to move a Windows ISO file that is 5 GB to a flash drive that is 32 GB, and your operating system responds with an error stating that you can't do it. You know you have the room, so what gives? The reason is that your flash drive is formatted in FAT32. You could format it as NTFS, which is great and offers a ton of features, but only if you use Windows. If you want maximum capability, format that drive to exFAT, also called FAT64. This will allow those large files to be transferred as long as you have the room. All modern operating systems now support exFAT—thanks Linux kernel 5.4+ and macOS 10.6.5+!

Note

An ISO image is a digital copy of an optical disc, such as a CD, DVD, or Blu-ray, that is saved as a single file. ISO images are used to archive, share, or replicate data without the need for the physical disc.

One problem with USB flash drives is that although they are small, they can't fit inside most digital cameras, smartphones, and other handheld devices. For that, you need something even smaller. Enter the SD card.

Secure Digital Cards

SD cards, for the most part, are technically the same type of device as a USB flash drive. They are solid-state drives, they use NAND memory, and they have most of the same pros and cons as a USB flash drive. However, SD technology can write and transfer data much faster. The other main difference is the form factor of the SD device; because of this, SDs are used differently. Instead of connecting an SD card to a USB port of a computer, you slide it into a memory card reader. As with USB flash drives, be sure to use the **Safely Remove Hardware and Eject Media** icon in Windows

before physically removing an SD card. There are three sizes of SD cards, each smaller than the last: standard (32 mm × 24 mm), miniSD (21.5 mm × 20 mm), and microSD (15 mm × 11 mm). You can still find many standard-sized SD cards used in cameras and some other devices, but note that most cell phones and smartphones use microSD cards for additional memory. Figure 15.5 shows a full-size SD card and a microSD card.



FIGURE 15.5 **A Typical microSD Card (Left) and a Standard SD Card (Right)**

Standard SD cards have capacities up to 4 GB. High-capacity (SDHC) cards range up to 32 GB. eXtended Capacity (SDXC) has a maximum capacity of 2 TB and supports up to 90 MB/s. Secure Digital Ultra Capacity (SDUC) supports up to 128 TB and 985 MB/s data transfer over the SD Express bus.

When it comes to data transfer rate, SD cards are divided into a variety of classes: SD 2, 4, 6, and 10 as well as UHS 1 through 3 and SD Express bus, each with a different range of speeds. For example, Class 10, required for

Full HD video recording (1080p), has a minimum data writing speed of 10 MB/s. To record 4K video, you would need at least UHS 3, which has a minimum data writing speed of 30 MB/s. To simplify things a bit, SD cards are labeled with a video speed class rating. For example, V30 means that the card can write 30 MB/s minimum. Today's SD cards will often display their maximum transfer rate as well.

Optical Drives

The three main types of optical media in use today are compact discs (CDs), digital versatile discs (DVDs), and Blu-ray discs (BDs). These discs have a variety of functions, including audio, video, applications, data, and so on. Some discs can be read from, some can also be written to, and some can be rewritten to as well. It all depends on which media you use. Optical drives are usually 5.25 inches wide and use the SATA communications interface. With the advent of broadband Internet and USB flash drives, optical drives are not used nearly as much as they used to be, but they are available as internal drives or external add-ons. Let's briefly look at some of the optical media options.

Note

Because the need for physical media has decreased. Most modern computers and laptops no longer come with built-in optical drives. Despite their decline in popularity, optical drives can still be useful in certain situations. People primarily access movies, music, and software online through streaming services and downloads rather than physical discs. USB drives, external hard drives, and cloud storage offer more convenient and higher capacity data storage options compared to optical discs. If you purchase a newer computer, you will have to purchase an optical drive as an add-on if needed.

- **Compact disc (CD):** A CD is a flat, round optical disc used to store music, sounds, or other data. Some computers use compact disc-read-only memory (CD-ROM) drives. A typical CD-ROM drive speed is

48x. The x equals 150 KB/s. So, to calculate a CD-ROM drive's maximum read speed, you multiply the number preceding the x by 150 KB. In this example, this would be 48 × 150 KB = 7.2 MB/s. A typical CD can hold up to 700 MB of data. Most optical drives that you can purchase for a computer have all three compact disc functions: They can read from CD-ROMs, write to CD-Rs, and write/rewrite to CD-RWs. Usually, the read speed and CD-R speed are the same.

- **Digital versatile disc (DVD):** For data, digital versatile discs, also known as digital video discs, have a much greater capacity than CDs. The reason is that the pits etched into the surface of a DVD are smaller than CD pits (.74 micrometers compared to 1.6 micrometers). Also, DVDs can be written to faster than CDs. There are read-only DVDs and writable DVDs. One typical example of a DVD is the single-sided, single-layer (SS, SL) DVD-5 technology, which can store 4.7 GB of data. But some DVDs can be written to two sides (known as dual-sided, or DS); simply flip the DVD to access the information on the other side. By using a combination of sides and layering, the DVD-18 technology can store up to 17 GB of data. A typical DVD drive reads a disc at 16x. However, the x in DVD speeds is different than the x in CD-ROM speeds. For DVDs, the x means approximately 1.32 MB/s, or about nine times the core CD speed. So, a typical 16x DVD is equal to 21 MB/s.
- **Blu-ray:** Currently, Blu-ray is *the* optical standard for high-definition video. It is used for high-def movies, with console games, and for storing data (up to 50 GB per disc, which is 10 times the amount of a typical DVD-5 disc). The standard disc is 12 cm (the same size as a standard DVD or CD), and the mini-disc is 8 cm. A typical Blu-ray disc can store between 25 GB and 128 GB of data. Drive speeds range from 1x to 16x. 1x is equal to 36 Mb/s, or 4.5 MB/s. At 16x, the speed would be 16 times the core amount, which comes to 576 Mb/s, or 72 MB/s; this is superior to other optical drive write speeds. If you want to record data to a Blu-ray disc, you can use one of two methods of "burning": Blu-ray Disc Recordable (BD-R), which can write to a disc once, and Blu-ray Disc Recordable Erasable (BD-RE), which can be erased and re-recorded multiple times. Burning speed depends on the drive, but generally, you will see a typical data transfer rate of 50 MB/s when writing data to a Blu-ray disc.

Note

Mb/s stands for megabits per second, whereas MB/s stands for megabytes per second.

Note

While physical Blu-rays, whether regular Blu-ray or Ultra HD Blu-ray, are becoming harder to find with the proliferation of streaming services, they still offer much better video and audio quality than most streaming services. Remember, streaming services use bandwidth to deliver those movies; bandwidth costs money to both the host and client (here's looking at you ISP data caps). Consequently, most streaming services heavily compress the videos to reduce the file size. While a Blu-ray is still compressed, it is generally far less compressed than offerings from streaming services. Convenience over quality? That is the question.

ExamAlert

If an optical disc gets jammed in an optical drive tray, use a paper clip! You can insert it into the small hole next to the tray. Add one to your PC toolkit!

Cram Quiz

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

1. How much data can a SATA Revision 3.0 drive transfer per second?

- **A.** 50 MB/s
- **B.** 90 MB/s
- **C.** 1969 MB/s
- **D.** 6 Gb/s
- **E.** 16 Gb/s

2. Which level of RAID stripes data and parity across three or more disks?

- **A.** RAID 0
- **B.** RAID 1
- **C.** RAID 5
- **D.** Striping
- **E.** RAID 10

3. A customer complains that an important disc is stuck in the system's Blu-ray drive. What should you recommend to the customer?

- **A.** Get a screwdriver and disassemble the drive.
- **B.** Format the disc.
- **C.** Use a paper clip to eject the tray.
- **D.** Dispose of the drive and replace the media.

4. Which of the following best describes a specification for accessing storage while using PCI Express?

- **A.** NVMe
- **B.** 7200 RPM
- **C.** Hot-swappable
- **D.** 3.5-inch and 2.5-inch

5. Which RAID level is referred to as striping with double parity and requires a minimum of four or more disks?

   - **A.** RAID 6
   - **B.** RAID 10
   - **C.** Striping with parity
   - **D.** Non-Volatile Memory Express

6. Which is the optical standard for high-definition video and can store between 25 GB and 128 GB of data?

   - **A.** DVD
   - **B.** DVD-5
   - **C.** DVD-18
   - **D.** Blu-ray

Cram Quiz Answers

1. **D.** SATA Revision 3.0 drives can transfer 6 Gb/s, which, after encoding, amounts to 600 MB/s. SATA Revision 3.2 is 16 Gb/s (1969 MB/s) but requires SATA Express or M.2. 50 MB/s is a typical write speed for Blu-ray discs and some flash media. 90 MB/s is a typical write speed for an SD card.

2. **C.** RAID 5 stripes data and parity across three or more disks. RAID 0 does not stripe parity; it stripes data only and can use two disks or more. RAID 1 uses two disks only. Striping is another name for RAID 0. RAID 10 contains two sets of mirrored disks that are then striped.

3. **C.** Tell the customer to use a paper clip (or mobile device tray pin) to eject the Blu-ray tray. Disassembling the drive is not necessary; the customer shouldn't be told to do this. If the disc is rewritable, formatting it would erase the contents, even if you could format in this scenario. Never tell a customer to dispose of optical drives. They rarely fail; and if one did, it should be recycled.

4. **A.** Non-Volatile Memory Express (NVMe) is a specification for accessing storage while using PCI Express. Essentially, the M.2 slot on a motherboard taps into the PCI Express bus (x4) and uses a portion of the total bandwidth associated with that bus. The platters in a hard disk drive (HDD) rotate at a certain speed. For example, 7200 RPM is common; other typical speeds include 5400 RPM and 10,000 RPM. Hot-swappable capability means drives can be removed and inserted while the system is on. SATA-based drives come in two main widths: 3.5-inch and 2.5-inch. The 3.5-inch drives are used in desktop computers, network-attached storage, and other larger devices. The 2.5-inch drives are used in laptops and other smaller devices.

5. **A.** RAID 6 is called striping with double parity and requires a minimum of four or more disks. Data is striped across multiple disks; two fault-tolerant parity blocks are written to each disk. If two disks fail, the array can reconstruct the data from the parity information. RAID 10 is known as "stripe of mirrors." It combines the advantages of RAID 1 and RAID 0 and requires a minimum of four or more disks. The system contains at least two mirrored disks that are then striped. Striping with parity describes RAID 5, which requires a minimum of three disks. Non-Volatile Memory Express (NVMe) is a specification for accessing storage while using PCI Express (PCIe). Know your RAID levels for the exam!

6. **D.** Blu-ray is the optical standard for high-definition video. It is used for high-definition movies and console games. A typical Blu-ray disc can store between 25 GB and 128 GB of data. Although digital versatile discs (DVDs) have a much greater capacity than CDs, they have less storage capability than Blu-ray discs. DVD-5 technology can store 4.7 GB of data. But some DVDs can be written to two sides known as dual-sided (or DS); simply flip the DVD to access the information on the other side. By using a combination of sides and layering, the DVD-18 technology can store up to 17 GB of data.

Time for a break. You've been storing a lot of facts and figures in your brain—the ultimate storage device—but it needs to rest now and then.

"The more storage you have, the more stuff you accumulate."—Alexis Stewart

Chapter 16

Motherboards and Add-on Cards

This chapter covers a portion of the following A+ 220-1201 exam objective:

- **3.5** – Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards.

Without a doubt, the motherboard is the foundation of a computer. Everything connects to the motherboard, and all data is transferred through this matrix of circuitry.

Over the years, we have found that if a student is going to lack knowledge in one area, it's quite often going to be the motherboard. This is one of the key elements in a computer system. It's the starting point for a quick and efficient computer. Because it connects to everything in the computer system, you need to know many concepts concerning it. Let's get right into it.

Note

Objective 3.5 covers a *lot*. That's why we broke it into two chapters. This chapter covers motherboards and add-on cards. The next chapter covers CPUs and cooling.

ExamAlert

This portion of **Objective 3.5** concentrates on the following concepts: motherboard form factors and connector types; BIOS/Unified Extensible Firmware Interface (UEFI) settings; virtualization support; encryption and expansion cards.

Motherboard Form Factors and Connector Types

A computer form factor specifies the physical dimensions of some of the components of a computer system. It pertains mainly to the motherboard but also specifies compatibility with the computer case and power supply. The form factor defines the size and layout of components on the motherboard. It also specifies the power outputs from the power supply to the motherboard. The form factors you need to know for the exam are ATX, microATX, and ITX. Let's discuss them now.

ATX

Advanced Technology eXtended (ATX) was originally designed by Intel in the mid-1990s to overcome the limitations of the now-deprecated AT form factor. It has been the standard ever since. The motherboard shown in Figure 16.1 is ATX. Full-size ATX motherboards measure 12 inches × 9.6 inches (305 mm × 244 mm). An ATX motherboard has an integrated port cluster and normally ships with an I/O plate that snaps into the back of the case, filling the gaps between ports and keeping airflow to a minimum.

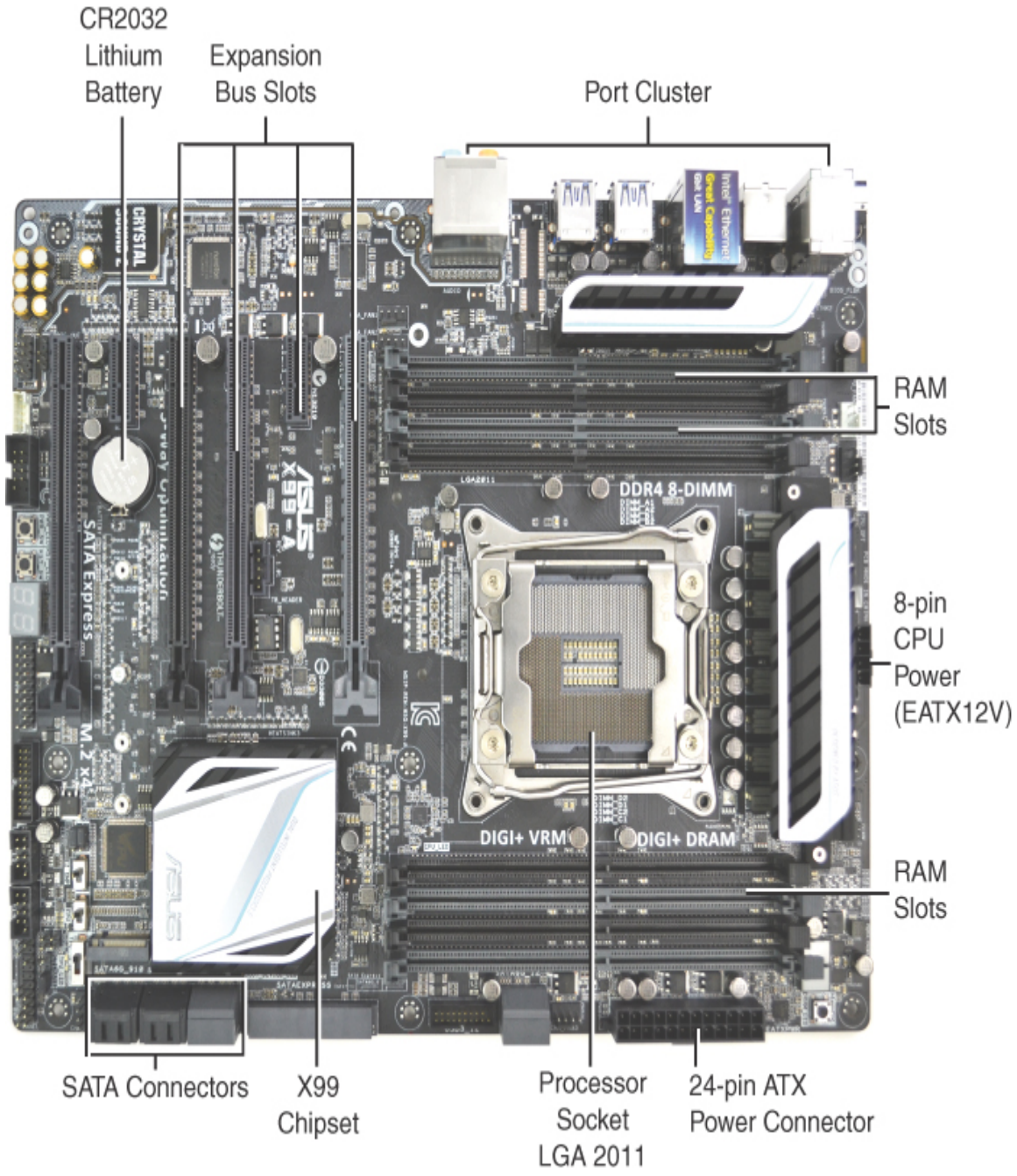


FIGURE 16.1 **ATX Motherboard and Its Components**

One identifying characteristic of ATX is that the RAM slots and expansion bus slots are perpendicular to each other. The ATX specification calls for the power supply to produce +3.3 V, +5 V, +12 V, and –12 V outputs and a 5 V standby output. These are known as *rails* (for example, the +12 V rail). The original ATX specification calls for a 20-pin power connector (often

referred to as P1); the newer (and much more common) ATX12V version 2.x specification calls for a 24-pin power connector. You can test these voltages with a power supply tester, which typically comes with a 24-pin input as well as other inputs for SATA power, PCI Express 6-pin and 8-pin, and Molex.

ExamAlert

Know the voltages supplied to an ATX motherboard by a power supply: +3.3 V, +5 V, +12 V, and –12 V outputs and +5 V standby output.

An ATX motherboard is attached to the computer case with several screws. Before you screw it in, though, attach the I/O plate to the back of the case and dry fit the motherboard to see where the screws will attach to the case. Apply rubber standoffs, if required. Then attach the accepting screws to the case wall according to where the motherboard screws will be placed; be sure that the motherboard will be properly supported. Angle the motherboard slightly so that the port cluster fits into the I/O plate. Then line up the screw holes and attach the screws. Finally, connect the CPU, RAM, power connections, adapter cards, fans, and anything else necessary!

microATX

microATX (or mATX) was introduced as a smaller version of ATX; these motherboards can be a maximum size of 9.6 inches × 9.6 inches (244 mm × 244 mm) but can be as small as 6.75 inches × 6.75 inches (171.45 mm × 171.45 mm). microATX boards are usually square, whereas full-size ATX boards are rectangular. microATX is backward compatible with ATX, meaning that most microATX boards can be installed within an ATX form factor case, and they use the same power connectors as ATX. Often, they have the same chipsets as ATX as well. microATX works well for desktop cases, small rackmount servers, and home theater PCs (HTPCs).

One major difference between ATX and microATX motherboards is the number of expansion slots and limited I/O ports on microATX. For

instance, it is common for an ATX motherboard to have four Dual Inline Memory Module (DIMM) slots while microATX motherboards often have only two DIMM slots. The same type of memory can go in both, but you can put fewer RAM sticks in a microATX. This applies to expansion slots such as PCIe slots. While an ATX motherboard might have two PCIex16 slots, a microATX motherboard might have only one. This is purely a space-saving measure, but it is something you should be aware of when choosing between the two.

ITX

Information Technology eXtended (ITX) is a group of form factors developed by VIA Technologies, Inc., between 2001 and today, for use in small, low-power motherboards. The ITX group includes several versions, each smaller than the last:

- **Mini-ITX (6.7 × 6.7 inch/170 × 170 mm):** Smaller than microATX, but screw-compatible with it. Normally comes with one PCIe slot. Good for HTPCs and other small footprint systems. Of all the ITX systems, this is one that you might see more often.
- **Nano-ITX (4.7 × 4.7 inch/120 × 120 mm):** Designed for DVRs, media centers, and automotive PCs.
- **Pico-ITX (3.9 × 2.8 inch/100 × 72 mm):** Used in industrial automation, transportation, and thin client systems.
- **Mobile-ITX (2.4 × 2.4 inch/60 × 60 mm):** Designed for ultra-mobile personal computers (UMPCs) and smartphones. This board has no embedded ports, so it needs a separate I/O board to communicate with devices.

Next Unit of Computing (NUC)

Another small form factor you should know about is Intel's NUC. A NUC is actually a barebones kit that includes a case, a motherboard (typically 4 × 4 inch/10.16 × 10.16 cm), a fan, and an external power supply. If you are looking for a basic computer system with video, network, and USB ports that can fit in the palm of your hand, this is it.

ExamAlert

Know the different sizes of motherboards—particularly ATX, microATX, and ITX—and why one would be chosen over another.

Expansion Buses

There are two main expansion buses and their corresponding adapter card slots that you need to know for the exam: PCI Express and PCI. Let's discuss those now.

- **PCI Express (PCIe):** Currently the king of expansion buses, PCIe is the high-speed serial replacement for the older parallel PCI standard and the deprecated AGP standard. The most powerful PCIe slots—such as x16—connect directly to the processor (or northbridge). The lesser PCIe slots—such as x1—connect to the chipset. The PCIe expansion bus sends and receives data within *lanes*. These lanes can send and receive data simultaneously. There are several versions of PCIe, and their data rates are shown in Table 16.1. Commonly, PCIe video cards are x16 (pronounced "by 16"), which means they use 16 lanes, and usually require version 3 at a minimum. They can typically transfer 16 GB/s in each direction. Most other PCIe adapter cards are x1, but you might work with some x4 cards as well, which would go in a x4 or x8 slot *if* you have one, or a x16 slot *if* you only have x1 and x16 slots. Of course, compatibility is key. A x1 card can go in a x1 slot or larger, but a x16 card will fit only in a x16 slot—and nothing smaller. Figure 16.2 shows three x16 slots and one x1 slot.

TABLE 16.1 **Comparison of PCIe Versions and Data Transfer Rates**

PCIe Version	Frequency	Maximum Data Rate
Version 1.0	2.5 GHz*	2 Gb/s (250 MB/s) per lane
Version 2.0	5 GHz	4 Gb/s (500 MB/s) per lane
Version 3.0	8 GHz	8 Gb/s** (1 GB/s) per lane

PCIe Version	Frequency	Maximum Data Rate
Version 4.0	16 GHz	16 Gb/s** (2 GB/s) per lane
Version 5.0	32 GHz	32 Gb/s** (4 GB/s) per lane
Version 6.0	64 GHz	64 Gb/s** (8 GB/s) per lane
Version 7.0***	128 GHz	128 Gb/s** (15 GB/s) per lane

* This is also measured in transfers per second, referring to the number of operations that send and receive data per second. It is often closely related to frequency. For example, PCIe v1 is 2.5 gigatransfers per second (2.5 GT/s), and PCIe v4 is 16 GT/s.

** These numbers are approximate.

***PCIe 7.0 is expected to come out in 2025, but we won't see it on devices until a couple of years afterward.

Note

Maximum data transfer rates are never attained, even in a lab environment. You can expect actual throughput to be substantially lower, but professionals use the maximum data rate as a point of reference and as a means of comparison.

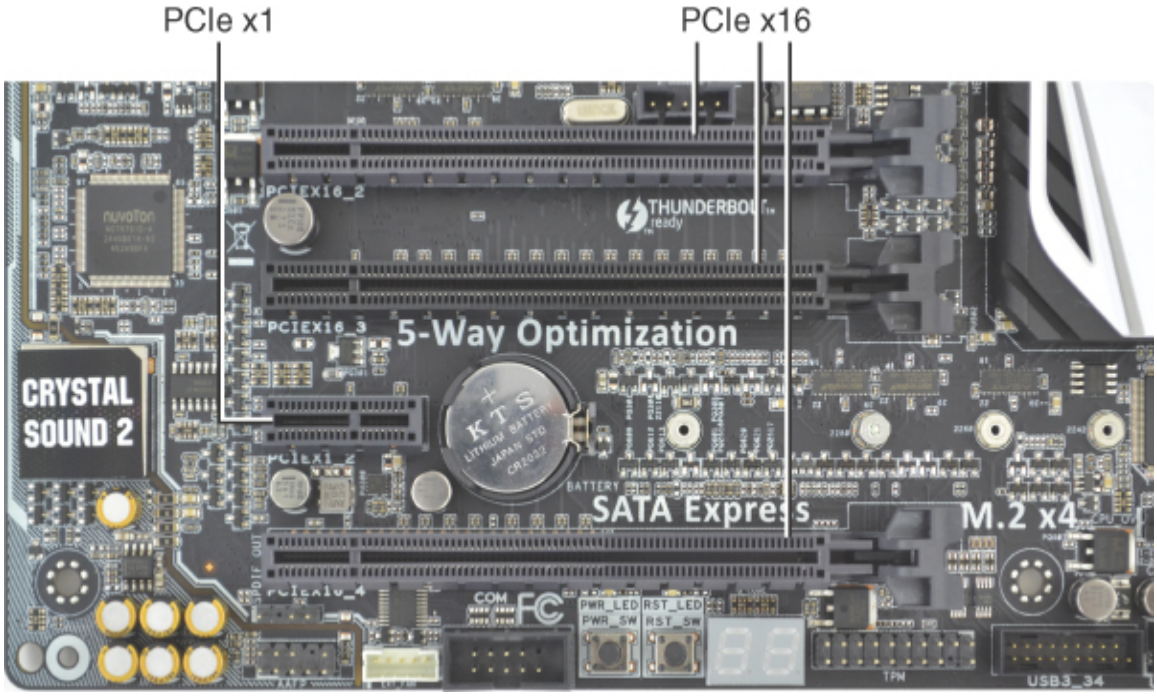


FIGURE 16.2 **PCIe x16 and PCIe x1**

ExamAlert

Make sure you can identify the PCIe x16 and x1 expansion slots for the exam.

- **PCI:** The Peripheral Component Interconnect (PCI) bus was developed in the 1990s by Intel as a faster, more compatible alternative to the deprecated ISA bus. It allows for connections to modems and to video, sound, and network adapters. This uncommon bus connects exclusively to the chipset (or southbridge). Because of this, other high-speed video alternatives were developed that could connect directly to the processor (or northbridge). PCI version 2.1 cards are rated at 66 MHz, and their corresponding PCI bus is 32 bits wide, allowing for a maximum data transfer rate of 266 MB/s. Derivatives of PCI include PCI-X, which was designed for servers using a 64-bit bus and rated for 133 MHz/266 MHz, and Mini PCI, which is used by older laptops. PCI slots are seldom found on today's motherboards. For the most part, they have been overtaken by PCIe technology.

Note

We've mentioned the *chipset* several times. The chipset connects all of the motherboard's secondary device interfaces together, such as USB, SATA 3.0, the network card, and more. The chipset then connects to the CPU, which has connections to the primary devices (RAM and video card). The motherboard displayed in Figure 16.1 uses the X99 chipset, which is quite old at this point. To see a diagram of a newer chipset, and all of its connections, use the following link and scroll down to Intel 700 Series Chipset Block Diagram or search the Internet for "Intel Z790 chipset block diagram":
https://www.intel.com/content/www/us/en/products/docs/chipsets/desktop-chipsets/z790-chipset-brief.html.

This is just one example. Most motherboard manufacturers have chipset diagrams available for you to view. Analyze them to understand how your system works!

Also, note that the northbridge and southbridge are components of a motherboard that manage the flow of data and system performance. In modern computers, the northbridge and southbridge have been replaced by other components or integrated into the CPU.

Expansion Cards

If a motherboard does not have a necessary integrated component, you will have to add an expansion card to a PCIe slot. You should make sure one is available and then determine the requirements of the card: the version of PCIe, bus width, and so on. There are plenty of different expansion cards that you might add, but the most common is probably the video card. Some computers come with integrated video cards (also known as on-board cards). In some cases (such as with some AMD systems), these cards use powerful processing that is built into the board, but many times the integrated video card is designed for basic computing and does not perform well enough for any high-end computing. In such cases, a video card is often necessary.

Installing Video Cards

A video card is like a little self-contained computer! It has a processor, known as a graphics processing unit (GPU), and a substantial amount of RAM. When you're choosing a video card, there are several things to consider, including the expansion bus that the card connects to, the card's GPU speed and amount of memory, the connectors it offers, whether an expansion slot is available for it on the motherboard, whether the video card can fit in the case, and whether the case has adequate power and cooling capabilities for the card.

Video cards, like other adapter cards, are inserted into an expansion bus slot and then screwed into the chassis of the case to keep them in place. When

deciding on a video card for a new system or a system to be upgraded, make sure it will fit in the computer case! The following steps describe how to install a PCIe video card:

1. **Check whether the card is compatible:** Verify that there is an open, compatible slot on the motherboard. Also make sure that the card is compatible with the operating system.
2. **Ready the computer:** Make sure that the computer is turned off and unplugged. Then implement ESD prevention measures (antistatic mat, antistatic wrist strap, and so on).
3. **Ready the video card:** Remove the card from the package and keep it in the antistatic bag until it is ready to be inserted. (Make sure the card is sealed when first opening it.)
4. **Document:** If the computer had a video card already, document how and where it was connected, either by taking a photo or by drawing a diagram. Otherwise, review the documentation that came with the motherboard and video card. Plan where to install the card and what cables need to be connected to the card and how they should be routed through the case.
5. **Prepare the slot:** Use a Phillips-head screwdriver to remove the slot cover (or covers) where the card will be installed. Bigger PCIe cards inhabit the space used by two slot covers. On most PCIe slots, there will be a thumb lever. Open this gently. When the card is inserted, the lever locks the card into place.
6. **Install the card to the slot:** Insert the card using both thumbs, applying equal pressure straight down into the slot. Try not to wiggle the card in any direction. Press down until the card snaps into place and you can't see any of the "gold" edge connectors. If it doesn't seem to be going in, don't force it. There might be something in the way (for example, one of the slot covers might not have been removed or the thumb lever might not be in the correct position).
7. **Connect cables:** A PCIe card needs its own power connection (or two). These cards use 6- or 8-pin PCIe power connectors or the new 16-pin 12VHPWR connector used in the most current generation of video cards. Most cases come with PCIe power connectors, but if

yours does not, you can use a PCIe to Molex adapter (or two), which will work with older cases and power supplies and older-generation video cards. When complete, your video card should look similar to Figure 16.3.

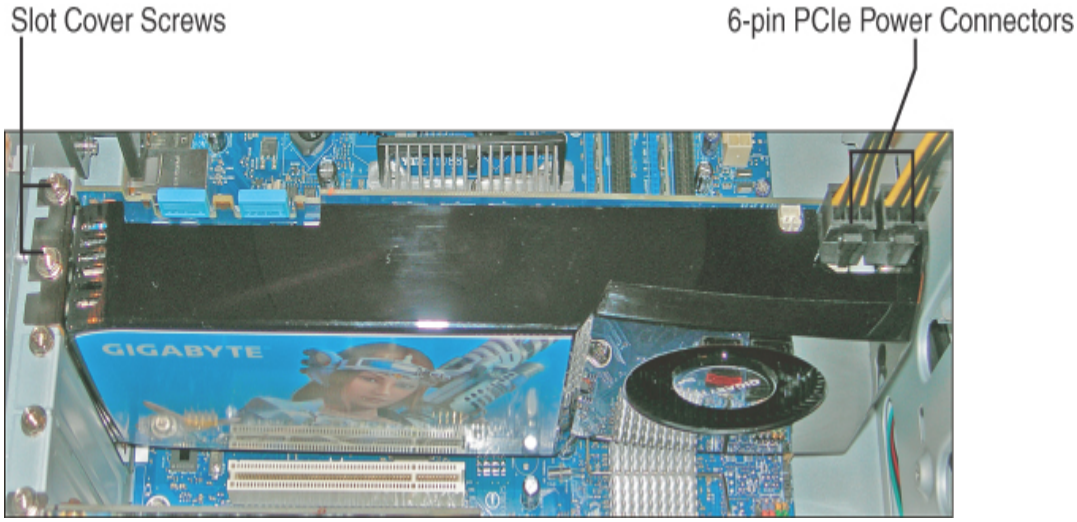


FIGURE 16.3 **An Installed PCIe Video Card**

Note

Starting with the 4xxx series Nvidia video cards, a new type of power connector entered the scene—the 12VHPWR. This 16-pin connector can deliver a whopping 600 watts of power! There were early reports of fires happening from such high power over these cables, so make sure you do not bend the connecting cables too tightly when connecting them to your video card.

See https://knowledge.seasonic.com/article/72-psu-recommendations-for-nvidia-rtx-4000-cards for more information.

8. **Test:** Testing is simple: Plug in the monitor to the video card's port and boot the computer. If you don't get anything on the display, it's time to troubleshoot. Make sure the monitor is securely connected to

the correct port. Then shut down the PC and make sure the card is seated properly and the power connections and any other connections are connected firmly. Listen for any beep codes that might be issued by the BIOS POST or watch for any POST codes displayed. Check whether the computer is booting without video; this can be done by watching the LED lights on the front of the case and listening for the power supply fan and hard drive activity.

> **Note**
>
> POST is power-on self-test. It is a series of diagnostic tests that BIOS/UEFI runs when a computer is powered on to check whether critical hardware such as CPU, RAM, and video card is installed and running properly. For more information, see "The Post" section later in this chapter.

9. **Install the driver:** When the system boots properly, install the driver from the manufacturer's disc. If no disc was supplied with the device or if it is missing, or if you don't have an optical drive on the computer in question, go to the manufacturer's website and download the latest version of the driver for the exact model of the video card.

> **Note**
>
> You will find that sometimes the operating system installs a driver automatically. At times, this driver is good enough, but many times you will want the latest drive from the manufacturer.

10. **Test again:** Now that the driver is installed, test again. Verify whether the card is shown as the correct make and model in the Device Manager (**Run > devmgmt.msc**), under Display Adapters. Then make sure the monitor can output the desired resolution. Keep in mind that some video cards can output a higher resolution than a monitor can

support. If the computer is used for graphics or gaming, open the appropriate application and verify that it works as expected. For example, check for fluidity, quick response, frame rate, and so on.

ExamAlert

Know how to install and test a video card and driver. Remember that if its driver doesn't work, you can use Device Manager to roll back to a known good driver.

Note

Check out a step-by-step overview of how to install a video card on this website: https://www.xda-developers.com/how-to-install-graphics-card/.

Challenge: Open and Analyze a Computer's Video Card

If you have a PC that you own or are allowed to open, open the case and analyze the system. Attempt to find out the following:

- The type of video card that is installed
- The type of motherboard you are using

You shouldn't have to actually disassemble anything to find out these things. Be sure to unplug the computer before opening it and employ antistatic prevention methods. If you are unsure about antistatic prevention, see Chapter 59, "Safety Procedures."

After you have booted up the computer again, do the following:

- Go to the Device Manager (if using Windows) and locate the name of the display adapter. Does it match with what you found?

- Check the manufacturer's motherboard documentation to find out what version of PCIe your video card is using.

The bottom line: It's one thing for us to tell you about computer technology, but it's another thing altogether for you to see it for yourself. Try to learn in a hands-on manner whenever possible; doing so will increase your overall knowledge greatly. If you don't have a PC, consider getting an older one to practice with. Ask family members and friends, check out yard sales, search online neighborhood marketplaces, and visit online auction sites to find something inexpensive to use for learning.

Sound Cards

A sound card is responsible for generating sound from the data sent to it by the operating system. Audio devices can be integrated into the motherboard, installed to PCIe slots, and connected to USB, but a sound card is typically installed to a PCIe slot on the motherboard.

Sound cards are not used as often as they once were. With the advent of USB 3.0 and beyond, many manufacturers choose to design their speakers and headphones with USB-only connectivity—or they are wireless. However, some still utilize connections that require a traditional sound card. And some audiophiles are concerned with the potential for USB latency or wireless interference and prefer the direct connectivity—and ports—that a sound card offers. Generally, the connections are 1/8 inch (3.5 mm).

Most sound card connections are color-coded. This color scheme is defined within the *PC System Design Guide*, version PC 2001, and the colors are still the same today. This guide specifies the following colors for the TRS 1/8 inch (3.5 mm) mini-jacks like the ones shown in Figure 16.4:

- **Light blue:** Line input.
- **Pink:** Microphone input.

> **Note**
>
> The light blue and pink ports are often confused. This confusion is understandable because both are for accepting sound input. An easy way to distinguish the difference is to look at their purpose.

The pink port is for connecting directly to a microphone. It is optimized for microphone audio amplification. The light blue port is meant to receive audio from other external devices such as sound mixers, DVD players, and so forth. A basic rule of thumb here is if the device you are plugging in to capture sound from has a volume knob, plug it into the light blue port. If it is a standalone microphone, plug it into the pink port.

- **Lime green:** Main output for stereo speakers or headphones. Can also act as a line out.
- **Black:** Output for surround sound speakers (rear speakers).
- **Silver/Brown:** Output for additional two speakers in a 7.1 system (middle surround speakers).
- **Orange:** Output for center speaker and subwoofer.

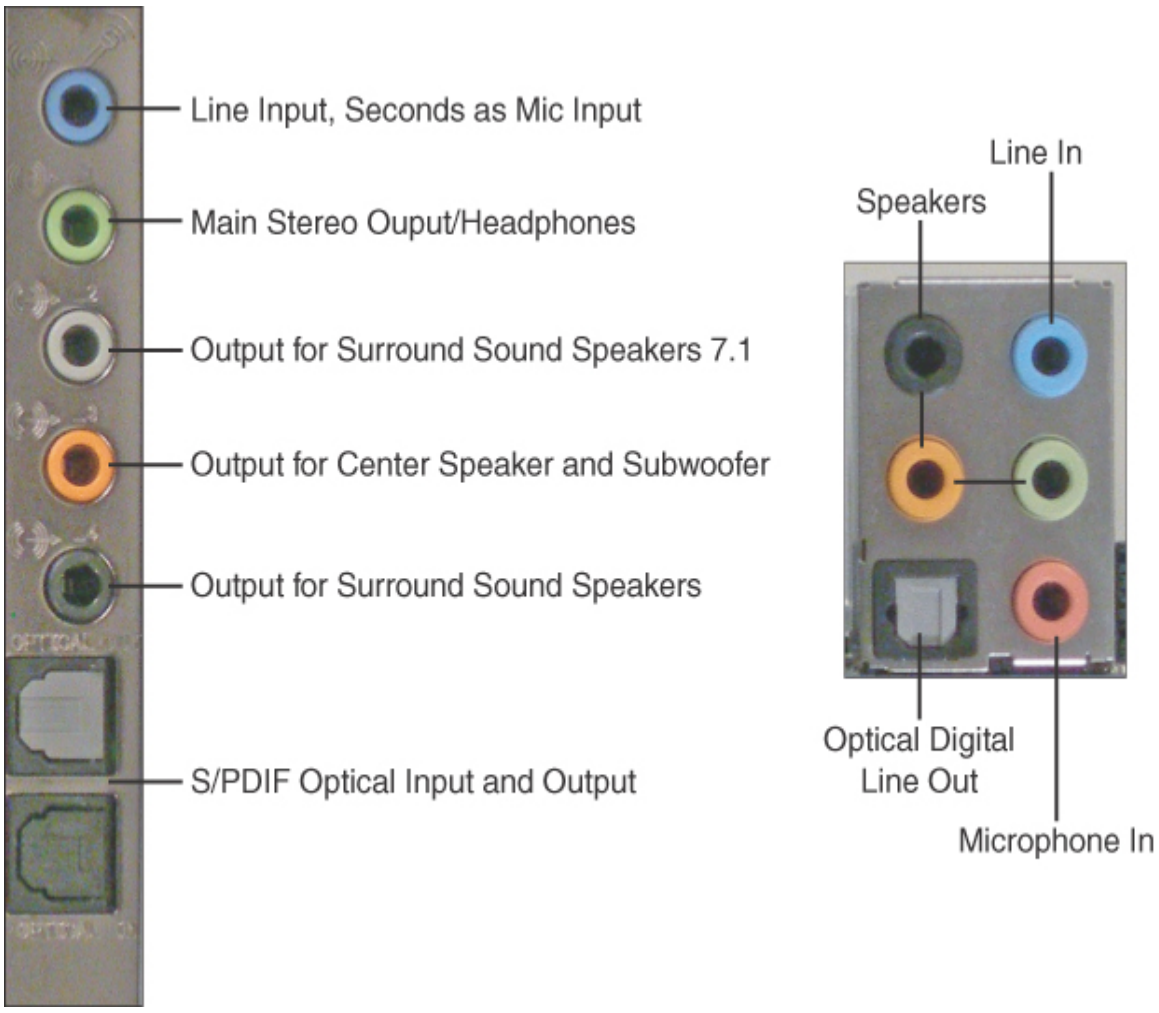


FIGURE 16.4 **A Typical Sound Card's Ports and Integrated Audio Ports on a Motherboard**

On the sound card shown in Figure 16.4, note the optical input and output. This is known as a Sony/Phillips Digital Interconnect Format (S/PDIF) port. This particular version of S/PDIF is called TOSLINK. It delivers high-quality digital sound over fiber optic cable. It is also known as a *digital optical port*.

Some users prefer to use an external audio interface that connects via USB but provides plenty of different connectivity options that are easily accessible on top of a person's desk. These interfaces usually offer high-fidelity sound (for example, 24-bit/192 kHz). They require USB 2.0 or

higher, but for greater productivity and less latency, USB 3.0 or higher is often recommended.

Other Expansion Cards

There are expansion cards for just about anything you can think of. Many motherboards come with integrated network cards, USB ports, and so on. But sometimes a user simply needs a more powerful solution or more ports.

A motherboard usually has one RJ-45 port for a wired Ethernet connection (the network interface card [NIC]). However, a system might require more. Network interface cards are available with one or more RJ-45 ports that can be used for connections to other networks, or they can be "teamed" or "bonded" together to provide link aggregation (that is, to combine the bandwidth of the ports) or to offer redundancy in case one port fails. This feature is often used in Linux systems, especially servers.

Most motherboards have plenty of USB ports, but if you need more, USB hubs can be connected to a USB port in order to add devices. But what if the motherboard doesn't have the right *version* of USB? For example, what if your motherboard has USB 3.0 SuperSpeed ports, but you want to make use of a device that can run USB 3.2 SuperSpeed+ at 20 Gbps; in such a case, you would need to add a USB 3.2 expansion card.

There are also external SATA-based devices (eSATA). A few motherboards come with these ports, but if you need to connect to external storage drives that use eSATA, you might need an adapter card.

A storage area network (SAN) is a dedicated high-speed network that allows a pool of storage devices to be networked together. This creates a "network" of storage and allows servers to treat the storage like local disks. To connect a SAN to a motherboard, you will most likely need a host bus adapter, or HBA. This HBA is often plugged into a PCIe slot. Such a card can be used to connect a PC to other Fibre Channel equipment by way of an LC connector or other fiber optic connection.

Don't forget about capture cards. These are adapter cards that can "capture," or record, video or audio, essentially turning the PC into a video or audio editing workstation. While professionals often use external

devices, an internal adapter card can provide an easier, less expensive solution for small businesses and hobbyists.

All of these cards are installed in a similar way to a video card, but their installation is even easier. Simply unscrew the slot cover and insert the expansion card straight down into the slot. Try not to wiggle the card and only hold the card from the edges to avoid ESD or other damage. Then screw the card in. Check the card in the Device Manager (or similar tool in an OS other than Windows) to make sure it is seen properly; if it is not seen correctly, download the driver from the manufacturer and install it. Test the card to make sure it works properly and then pat yourself on the back for another tech job that's been well done!

ExamAlert

Know how to install, configure, and test sound, network, USB, SAN, and eSATA expansion cards.

More Ports and Connectors

The main type of drive technology on motherboards is Serial ATA (SATA). SATA supports the connection of storage/hard drives and optical drives. Most motherboards come equipped with several 7-pin SATA connectors and possibly one or more 18-pin SATA Express connectors. For more information about drive technologies, see Chapter 15, "Storage Drives."

Another drive technology on motherboards that has rapidly gained traction is the M.2 slot. This port allows for M.2 devices such as M.2 SSD and M.2 NVMe drives to be directly connected to the motherboard without the need for external power and data cables. For more in-depth information about M.2 technology, also see Chapter 15.

You will find other ports as well, such as integrated audio ports, for use with an optical drive or sound card; internal USB ports, used with the front panel USB connections; and a variety of power connections that we will discuss further in Chapter 18, "Power."

Then there's the case connector group, which is usually on the edge of the motherboard and allows connectivity to the front panel connectors on a computer case. These wires start at the inside front of the case and have thin 2-, 3-, or 4-pin plugs on the other end. They are labeled with names such as POWER LED, POWER SW (for power switch), HDD LED, and so on. These plugs connect to *headers* on the motherboard, such as the power button, reset button, and LED light headers. These are often referred to as *front panel headers* because the cables come from the front panel of the case where the buttons and lights are located. Using the more specific term helps to distinguish these input pins from other headers on the motherboard, such as fan headers, where you plug case fans into the motherboard. Refer to the coverage of fan settings in the next section, "BIOS/UEFI Settings," for more information.

A computer with limited motherboard space might come with a riser card. A *riser card* can provide for additional expansion slots, such as PCIe. It generally plugs into one of the expansion slots and typically allows for an additional two slots. This allows a person to take advantage of three-dimensional space, but it could decrease airflow, leading to increased heat. Riser cards are most common in small proprietary designs and with small form factor motherboards.

BIOS/UEFI Settings

Historically, the Basic Input/Output System (BIOS) has been the firmware loaded on most desktop and laptop computers. However, since 2005, the Unified Extensible Firmware Interface (UEFI) has gained popularity, and in 2014, it became the predominant type of firmware shipped with motherboards. But many technicians (and even some manufacturers) still just refer to it as "BIOS," or possibly as "BIOS/UEFI." For simplicity in this book, we often refer to a motherboard's firmware simply as BIOS.

UEFI communicates more effectively with the operating system, allows for a mouse-driven firmware-based setup program (instead of the menu-based BIOS setup program), and includes advanced system diagnosis (except for the worst of errors, such as the CPU failing). It also has a built-in Secure Boot mode, which prevents digitally unsigned drivers from being loaded

and helps prevent rootkits from manifesting. It has faster startup times than the BIOS and supports more storage drive partitions.

The firmware is loaded onto a chip on the motherboard and can (and should) be updated, or "flashed," periodically to take advantage of the latest functionality and security updates. There are several ways to update the firmware, but generally you do it either from within Windows or by using some kind of bootable media (such as a USB flash drive) to boot the system and rewrite the firmware; this process is known as "flashing the BIOS."

This firmware stays resident in the computer after restarts. However, time and the individual settings that you select are stored elsewhere, such as in a complementary metal-oxide semiconductor (CMOS). This chip is *volatile*, meaning that the settings could be lost if the computer is restarted. That's why the motherboard comes with a lithium battery (also known as a CMOS battery). That battery retains the individual settings and keeps time while the computer is shut down. A common battery used on motherboards is the CR2032, a nickel-sized battery that snaps into the motherboard and has a shelf life of anywhere from 2 to 10 years, depending on usage. The more you leave the computer on, the longer the battery lasts.

Note

These CMOS batteries do die over time. An easy way to spot a dead CMOS battery is that the time and date on your operating system, when first booted, will be wrong—often by months and years! The reason is usually that the operating system gets the system time from the CMOS at boot before it synchronizes with an online time server. If the CMOS has been cleared because the battery is dead, it will set its time back to the original BIOS time/date. This can cause all sorts of strange issues with the operating system! If the system clock/date is wrong when you first boot, replace that CMOS battery!

The BIOS is where you go to set a password, change boot options, configure time and date, configure devices, overclock the computer, and much more. You must access the BIOS before the operating system boots.

For PCs and laptops, you can accomplish this by pressing a key on the keyboard (for example, F2 or Delete). Different manufacturers use different keys. The particular key should be displayed on the screen when your system boots, so watch carefully for it! For some mobile devices, you might need to press a button combination (such as the volume-up and power buttons). Here are a couple of examples of settings you might modify in the BIOS:

- **Boot options:** Also known as BIOS boot order or device priority, this setting enables you to select which media will be booted: hard drive/SSD, USB, optical drive, over the network, and so on. Usually, this option should be set to hard drive first. But if you install an operating system (OS) from removable media such as a flash drive, you will want to temporarily configure that removable media as first on the boot options list. For a secure and trouble-free system, it is recommended that you set this to hard drive—HDD, SSD, or M.2, depending on what your OS is installed on—first when you complete an installation of an OS, as shown in Figure 16.5. If you don't modify this setting, and removable media (such as a USB flash drive) is inserted, then it could cause the operating system to fail to load properly and could also pose a security risk. Note that the first boot device in the figure says Windows Boot Manager, P1, and the name of the device—a 250-GB Samsung solid-state drive. Windows Boot Manager is the primary boot file in Windows, and it is the first file on the hard drive that the BIOS looks for when it starts up. P1 means the first physical SATA port connection.

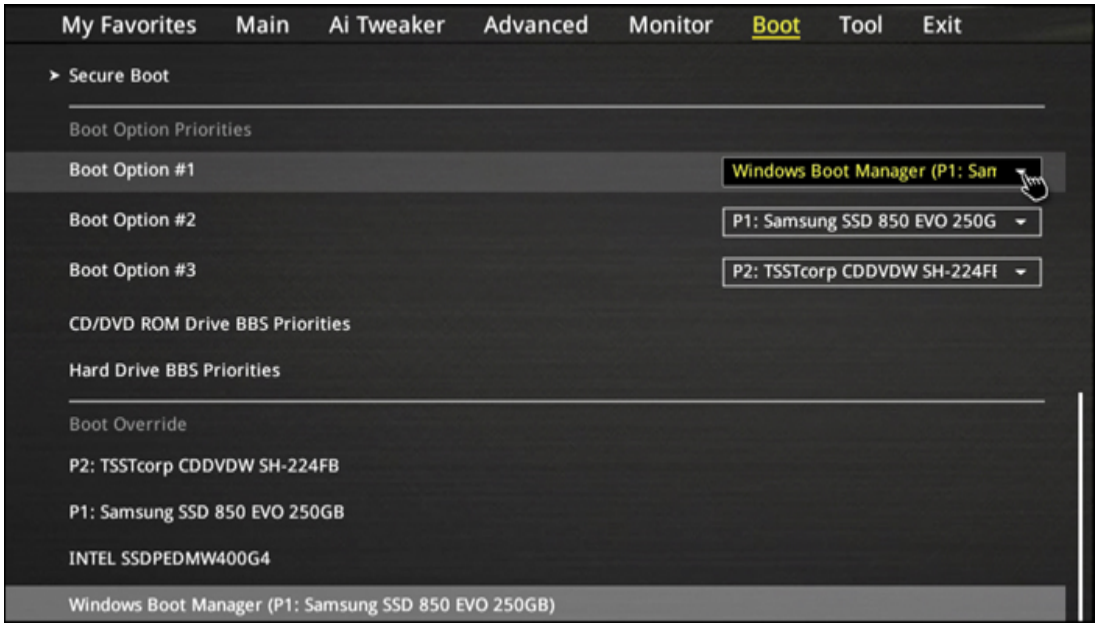


FIGURE 16.5 **Configuring the BIOS Boot Order**

ExamAlert

Know how to set the BIOS boot options! Also, if you boot a PC and see a black screen with a white blinking underscore on the top left, the issue could be the boot order.

- **Fan settings:** Most of today's motherboard BIOS programs have the ability to set whether case fans and CPU fans are turned on and at what speed they spin. In lieu of exact revolutions per minute (RPM; or how many times the fan spins in a minute) settings for the fans, the BIOS might offer simplified settings, such as optimal, low, high, and so on. If any fans are not working and you don't know what to set them to, read the motherboard manual for best procedures or reset the BIOS to default settings. (Note that doing this will erase any other settings you might have configured previously.)

Note

Your motherboard can control only case fans that are plugged into the fan headers on the motherboard. If you plug a fan directly into a Molex or SATA power connector, the motherboard doesn't know it exists and, therefore, cannot control the speed. This is also an issue when you're using case fan hubs. They are prevalent in many custom cases and allow you to install many case fans in one power hub. This hub is usually powered by a SATA power connector and has one cable to connect to a motherboard fan header. If you use one of these fan hubs, the motherboard will see all the fans as one fan. Consequently, it cannot control the individual fan speeds—it's all or none!

- **Temperature monitoring:** Virtually all motherboards have sensors in specific areas to monitor the temperature of vital components. These components are often the CPU, GPU, and chipset. The readings of these sensors can ramp up or down the RPMs of the fans connected to the fan headers. See the previous note about the use of fan hubs. You can also set a maximum temperature limit on these sensors. If the sensor hits the maximum, you can set it to warn you, shut down the computer, or do a combination thereof. Monitoring is vital to make sure the temperature is set properly to avoid serious harm to your computer! Refer to your motherboard, CPU, or GPU manufacturer's website for your specific components to see what the upper temperature limit should be.
- **Passwords:** In most cases, two passwords are available on BIOS: user and administrator. The user password authenticates a user before it enables the operating system to boot; this is also known as a boot password. Most organizations do not use this password because it requires the user to know a second password. The administrator password authenticates a user to the BIOS Setup Utility itself. For a secure system, enter a strong administrator password.
- **More security settings:** *Secure Boot* is an option on UEFI-equipped systems. If enabled, it can potentially block rootkits and other malware from launching boot loaders that have been tampered with. Windows makes use of a certificate stored in the UEFI that checks the boot loader for authenticity—meaning whether it has been digitally signed by

Microsoft. If the drive's boot loader is not authentic, the computer will not boot to that drive. You can also create Secure Boot keys with a *hardware security module (HSM)*, which can come in several forms, including as an adapter card; however, it must be enabled properly within the BIOS. The HSM is a device that includes a cryptoprocessor that generates, stores, and manages digital keys and has the ability to perform performance-optimized cryptographic operations. To allow for drive encryption, most motherboards come with a *Trusted Platform Module (TPM)*, a chip that provides hardware-based protection for sensitive data and user authentication and stores encryption keys. This can be enabled in the BIOS if it is not already active. To run Windows 11, you must have a TPM 2.0 chip on your motherboard. This chip is required for BitLocker encryption—drive encryption to secure your data, and Windows Hello—a user authentication that allows biometric authentication such as facial recognition or fingerprint scans. Luckily, almost all motherboards made since 2016 have this chip.

You can also set permissions for USB usage in the BIOS, such as whether USB can be utilized at all, disabling the ability to boot from USB drives, and so on. This capability is especially important to mitigate the risk of USB drop attacks. This type of attack occurs when an attacker drops an infected USB stick in a public area, hoping individuals will insert it in their computers and become infected. Disabling USB ports is a way to mitigate this type of attack. While doing this might be unrealistic in most situations because people use USB ports for so many general purposes, setting permissions might be necessary in high-security environments. We'll discuss some of these computer security terms in more depth in the 220-1202 portion of the book.

ExamAlert

It is crucial to secure UEFI-equipped systems with Secure Boot and a TPM. And remember that a hardware security module (HSM) is a removable unit that runs on its own. It includes a cryptoprocessor that generates, stores, and manages digital keys, with the ability to perform performance-optimized cryptographic

operations. A TPM is a chip on a motherboard that encrypts a disk on a desktop or laptop computer.

- **Virtualization support:** To support virtual computing, the BIOS/UEFI must be configured properly. This setting is sometimes buried within the BIOS/UEFI in a CPU submenu. For Intel CPUs, the Intel Virtualization Technology (Intel VT) option should be enabled; this is often labeled as VT-x. For AMD CPUs, enable AMD-V, which is more commonly labeled as SVM in the motherboard settings. We'll talk more about virtualization in upcoming chapters. Please see this guide from Microsoft on how to enable virtualization: https://support.microsoft.com/en-us/windows/enable-virtualization-on-windows-c5578302-6e43-4b4b-a449-8ced115f58e1.

Note

Sometimes finding the settings in BIOS can be hard because there are so many menus and submenus. Luckily, if you built the computer yourself and used a major motherboard manufacturer like ASUS, MSI, or Gigabyte, they often have a search feature that allows you to type in the setting you're looking for. This feature makes it much easier to change the settings without having to look through endless menus.

The POST

The power-on self-test (POST) is essentially a piece of code that the BIOS runs to find out which type of processor is on the motherboard and to verify the amount of RAM. It also identifies buses on the motherboard (and other devices) as well as which devices are available for booting.

The BIOS indicates any system problems that the POST finds via either onscreen display codes, beep codes, or an integrated error code readout on the motherboard itself. The exact code(s) depends on the type of BIOS used. Your motherboard should come with documentation about any

possible BIOS error codes. If not, you can usually download the documentation from the manufacturer's website; you just need to know the model number of the board. In the case of a proprietary computer (Dell, HP, and such), you need the model number of the computer to download any necessary documentation from the manufacturer's website. We'll discuss computer troubleshooting more when we get to the chapters in Domain 5.0: Hardware and Network Troubleshooting.

Note

BIOS POST beep codes are audible codes to warn of these issues. One beep means POST cleared and everything is good. Multiple beeps means there is a problem. While audible beep codes are still present in many motherboards, most manufacturers do not install a speaker on the motherboard to hear them anymore. Instead, many manufacturers rely on a visual display to indicate issues. These displays can range from LED lights on the motherboard that go green to show everything is okay or red to show a problem or small LED screens on the motherboard that show codes to indicate success or failure. With any of the methods, it is important to look up these codes on the motherboard manufacturer's website to see what they mean exactly.

ExamAlert

The POST is a built-in troubleshooting tool provided by the motherboard. Use it!

Cram Quiz

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

1. Which motherboard form factor measures 12 inches × 9.6 inches (305 mm × 244 mm)?

- ○ **A.** microATX
- ○ **B.** SATA
- ○ **C.** ATX
- ○ **D.** mITX

2. Which component supplies power to the CMOS when a computer is off?

- ○ **A.** Lithium battery
- ○ **B.** POST
- ○ **C.** Power supply
- ○ **D.** BIOS/UEFI

3. To implement a Secure Boot process, which device should be listed first in the Boot Device Priority screen?

- ○ **A.** Network
- ○ **B.** CD-ROM
- ○ **C.** USB
- ○ **D.** Hard drive

4. Which of the following connectors might you use to power a video card?

- ○ **A.** 24-pin power
- ○ **B.** 8-pin PCIe
- ○ **C.** SATA
- ○ **D.** 3.5-mm TRS

5. Which of the following is a chip that stores encryption keys?

- **A.** Intel VT
- **B.** Secure Boot
- **C.** Firmware
- **D.** TPM

6. Which of the following BIOS/UEFI settings are used to prevent USB drop attacks?
   - **A.** Boot password
   - **B.** USB permissions
   - **C.** BIOS time/date
   - **D.** SAN settings
7. What do the POWER LED, POWER SW, and HDD LED plugs connect to on the motherboard?
   - **A.** Headers
   - **B.** SATA 7-pin
   - **C.** PCIe slots
   - **D.** 24-pin ATX port
8. Which of the following is a removable unit that runs on its own and includes a cryptoprocessor that generates, stores, and manages digital keys?
   - **A.** SAN
   - **B.** POST
   - **C.** HSM
   - **D.** TPM

Cram Quiz Answers

1. **C.** ATX boards measure 12 inches × 9.6 inches (305 mm × 244 mm). microATX boards are square and measure 9.6 × 9.6 inches (244 mm × 244 mm). SATA is a type of storage drive technology and the port used to connect drives to the motherboard. mITX (or Mini-ITX), also square, measures 6.7 × 6.7 inches (170 mm × 170 mm).

2. **A.** The lithium battery (or CMOS battery) supplies power to the CMOS when the computer is off. The reason is that the CMOS is volatile and would otherwise lose the stored settings when the computer is turned off.

3. **D.** To ensure that other users cannot boot the computer from removable media, set the first device in the Boot Device Priority screen to hard drive. (And consider Secure Boot and boot keys!)

4. **B.** A video card is normally powered by a 6-pin/8-pin PCIe connector. Newer video cards are powered by a 16-pin 12VHPWR. Lesser cards are simply powered by the PCIe bus. The 24-pin power connector is the main connector that leads from the power supply to the motherboard. SATA power can be used for fans, hard drives, and other secondary devices. The 3.5 mm (or 1/8 inch) TRS is an audio connection.

5. **D.** To perform drive encryption, most motherboards come with a Trusted Platform Module (TPM), a chip that stores encryption keys and can be enabled in the BIOS/UEFI. Intel Virtualization Technology (VT) is part of the firmware that supports the use of virtualization software such as Hyper-V and VMware. Secure Boot can block rootkits and other malware from launching boot loaders that have been tampered with. Firmware (such as a motherboard's BIOS/UEFI) should be updated, or "flashed," periodically to take advantage of the latest functionality and security updates.

6. **B.** Configure USB permissions to prevent USB drop attacks. In a USB drop attack, a malicious person leaves a USB drive lying around somewhere, in the hopes that someone will pick it up and plug it into their computer. The USB drive contains a virus or other malicious payload and subsequently infects the computer. By

disabling USB altogether in the BIOS/UEFI, you can avoid these types of attacks. A boot password is a good idea also, so no one can modify your settings—once you have made them that is; you still have to configure USB securely first. The BIOS time/date settings allow you to modify the date and time for the system but won't prevent USB drives from being used and therefore won't prevent USB drop attacks. Storage area network (SAN) settings don't have any relationship to USB devices.

7. **A.** Power LED, power switch, and storage drive LED case connectors plug into headers on the motherboard—specifically, the Front Panel header. The actual SATA drive connects to the motherboard's SATA port with a 7-pin data connector. PCIe slots are used for video, audio, and network cards (among other things). The main 24-pin power connection from the power supply connects to the 24-pin ATX port. Know your connections!

8. **C.** A hardware security module (HSM) is a removable unit that runs on its own. It includes a cryptoprocessor that generates, stores, and manages digital keys, with the ability to perform performance-optimized cryptographic operations. A storage area network (SAN) is a dedicated high-speed network that allows a pool of storage devices to be networked together. This creates a "network" of storage and allows servers to treat the storage like local disks. POST, or power-on self-test, is a series of diagnostic tests that BIOS/UEFI runs when a computer is powered on to check whether critical hardware such as CPU, RAM, and a video card is installed or running properly. A TPM is a chip on a motherboard that encrypts a disk on a desktop or laptop computer.

This is a pretty massive chapter with lots of details. Be sure to review carefully before moving on to the next chapter. Give yourself a proverbial pat on the back for getting this far! Better yet, give yourself a literal pat on the back if you want. It'll help stretch those arm muscles.

Chapter 17

CPUs

This chapter covers a portion of the following A+ 220-1201 exam objective:

- **3.5** – Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards.

Here it is, the core of the desktop computer: the CPU. This is the second part of our coverage of Objective 3.5. There's lots to do, so let's not waste any time!

ExamAlert

This portion of **Objective 3.5** concentrates on the following concepts: CPU architecture, motherboard compatibility, and cooling.

CPU Architecture

The central processing unit (CPU) is quite often referred to as the "brain" of the computer. While that terminology may be debatable, the CPU is most definitely at the core of the computer—and it is fast. A typical CPU today runs between 2.4 and 4 GHz or higher. That CPU frequency is known as *speed* or, more accurately, *clock rate*.

Clock Rate

The clock rate is the frequency (or speed) of a component. It is rated in cycles per second and measured in hertz (Hz). For all practical purposes, the term *clock rate* is the same as the more commonly used term *clock speed*.

Components are sold to consumers with a *maximum* clock rate, but they don't always run at that maximum number. To understand better, let's consider a car analogy. The CPU is often called the "engine" of the computer, like a car engine. Well, your car's speedometer might go up to 120 MPH, but you'll probably never drive at that maximum—for a variety of reasons! When it comes to CPUs, the stated clock rate is the *maximum* clock rate, and the CPU usually runs at a speed less than that. In fact, it can run at any speed below the maximum, but there are only a few plateaus that it will usually hover around.

Now, we're all familiar with speeds such as 2.4 GHz, 3.0 GHz, or 4 GHz. But what is the basis of these speeds? Speed can be divided into these categories that are interrelated:

- **Motherboard bus speed:** This is the base clock speed of the motherboard or BCLK. It's no longer as critical to overall system performance as it once was. Modern CPUs rely on internal communication channels that operate at much higher frequencies than the traditional motherboard bus. However, the base clock can still play a role in some data transfers between the CPU and other components. It's often referred to simply as *bus speed* and is generated by a quartz oscillating crystal soldered directly to the motherboard.
- **Internal clock speed:** This is the internal frequency of the CPU and is the well-known number that CPUs are associated with. For example, the motherboard in Figure 16.1 in Chapter 16 is rated at 3.3 GHz. The CPU uses an internal multiplier based on the motherboard base clock. The maximum multiplier for this particular CPU is 33. The math is as follows: Base clock × Multiplier = Internal clock speed. In this example, that would be 100 MHz × 33 = 3.3 GHz. However, as mentioned, the CPU can (and often does) run more slowly. Fewer open

programs means a lower speed (for example, 1.2 GHz). As more programs are opened and more CPU power is required, the CPU throttles up—for example, to 2.4 GHz and, ultimately, 3.3 GHz. Like many boards, this motherboard can support faster and slower CPUs from a variety of CPU families, but the math works in the same way.

- **Modern Considerations:** While the concept of base clock and internal clock speed remains, their importance for overall system performance has decreased. Modern CPUs rely more on factors like core count, cache size, and instructions per clock (IPC) for performance. Additionally, many motherboards now use a chipset—one on the CPU itself and another separate on the motherboard—rather than the outdated northbridge and southbridge separate chipsets, to handle communication between the CPU, memory, and other devices, further reducing the reliance on the traditional motherboard bus speed.

ExamAlert

For today's CPUs, two of the most commonly used terms are *bus speed* (the base clock of the motherboard) and *clock speed* (the frequency of the CPU). These terms might not be completely accurate, technically, but you will see and hear them often, and you could see them on the exam as well.

Note

Many motherboards allow for *overclocking*, which enables the user to increase the CPU multiplier, thereby increasing the clock speed of the CPU. Most motherboards also allow for adjustments to the base clock (BCLK) for more fine-grained control. For example, the Core i7-14700K CPU has a normal top speed of 3400 MHz (3.4 GHz). On this motherboard, increasing the base clock through the use of multipliers from 100 to 125 MHz results in an increase of the CPU top speed from 3400 MHz to 4250 MHz. Now, this is an oversimplistic explanation to overclocking. There is also the problem of modern Intel CPUs having Performance versus

Efficiency cores, which you have to overclock separately. And, of course, there are core voltages that often have to be configured for heat reasons. This concept can get quite complicated. That being said, you can also overclock RAM and some video cards independently of the CPU. While it's not usually advised to overclock CPUs and GPUs, it is normal to overclock RAM—at least to the manufacturer's specifications. This is merely turning on XMP/DOCP/EXPO. See Chapter 14, "RAM," for more information.

As you might guess, overclocking is risky; it increases the voltage, creates more heat, and could possibly cause system instability or even damage to the system—analogous to blowing the engine of a car when attempting to run a 10-second quarter mile. So, approach overclocking with extreme caution! Generally, if you find a system in the workplace that has been overclocked, overclocking should be disabled in the BIOS/UEFI settings.

Types of CPUs

There are two types of CPU architectures you should know about for the A+ exams: x64/x86 and ARM. Let's discuss each briefly.

x86-64

x86-64 technology is typically found in PCs, laptops, and many servers. Simply stated, x64 means newer 64-bit CPUs, and x86 means older 32-bit CPUs. In computer architecture, 64-bit CPUs can handle exponentially higher amounts of data and larger RAM capacities than can 32-bit CPUs.

The 64-bit CPUs were introduced to the mainstream market around 2003. x64 technology is also referred to as Intel 64 (for Intel CPUs), amd64 (for AMD CPUs), and, more generically, x86-64 (which is how we refer to it throughout this book).

x86 32-bit CPUs were common in PCs from the 1980s to the early 2000s. The x in x86 is a variable; for example, the 80386 PC, shortened to 386, works with 32-bit versions of operating systems and software.

The older x86 CPU could only support up to 4 GB of RAM. In comparison, an x86-64 CPU can support 256 TB of RAM (that's terabytes, or trillions of bytes). Because many software programs are still written for the 32-bit platform, 64-bit CPUs are designed to be backward compatible, meaning they can run 64-bit *and* 32-bit software.

An example of an x86-64 Intel CPU is the Core i7-14700, which is a high-performance processor that can run between 3.4 and 5.6 GHz.

We'll discuss x86-64 and the differences between 64-bit and 32-bit software a little more when we get into the 220-1202 portion of this book.

ARM

Advanced Reduced Instruction Set Computer (RISC) Machine (ARM) technology is typically found in smartphones, tablets, and other mobile devices. RISC stands for reduced instruction set computer, which essentially means small, highly optimized sets of instructions as compared to x64. ARM CPUs are designed to run cooler and more efficiently than their PC counterparts.

Like x86-64, there have also been 32-bit and 64-bit versions of ARM CPUs, with 64-bit versions beginning around 2011. ARM CPUs are given version numbers, such as ARMv8 and ARMv9. An example of an ARMv9 CPU is the Cortex-A710 (released in 2021), which has a maximum clock rate between 633 MHz and 5.1 GHz. This huge range allows for incredible power efficiency while still remaining fast when needed. ARM CPUs generally come with less cache memory than x64 CPUs. (More on cache in a little bit.)

So far, the concepts we have discussed can be applied to x86-64 or ARM. However, the examples in the rest of this chapter are geared more toward x86-64 technology.

Note

While not the only CPU architectures that exist, x86-64 and ARM architectures are by far the most common.

Multithreading and Multicore

Multithreading (for example, Intel's Hyper-Threading) enables a single CPU to accept and calculate two independent sets of instructions simultaneously, thereby simulating two CPUs. The technology was designed so that single CPUs could better compete with true multi-CPU systems for lower cost. In a multithreaded environment, only one CPU is present, but the operating system sees two virtual CPUs and divides the workload, or threads, between the two.

Whereas multithreading technology simulates multiple CPUs, *multicore* CPUs physically contain two or more actual processor cores in one CPU package that acts as a single entity. This enables more efficient processing of data and less generated heat.

A typical CPU combines multithreading and multicore technologies. For example, the AMD Ryzen 7650x CPU has 16 cores, each of which can handle 2 threads at the same time, for a total of 32 threads. The Core i7-14700, mentioned previously, has 8 performance cores and 12 efficient cores, and can run 28 threads simultaneously. Most CPUs will handle 2 threads per core. In Windows, the total number of threads can be viewed within the Device Manager under Processors. In Linux, you can find this number in a terminal by running the **top** command and pressing **1**.

Note

Starting with the 12th-generation Intel CPUs, Intel made a move to have what is called *Performance cores* and *Efficiency cores* in its CPU lineups. Performance cores are typically what you would think of when thinking about x64 cores: They are designed for maximum processing power. Efficiency cores are smaller, lower-power cores for light background processes. Normally, threads work only on performance cores, so the i7-14700 with 8 P-cores should have only 16 threads. However, Intel has done some magic to also have some of the E-cores contribute to the thread count. AMD is also using

these efficiency cores in some of its laptop and server processes as of this writing.

ExamAlert

Know the differences between multithreading and multicore technologies. *Multithreading* enables a single-core CPU to calculate two instruction sets simultaneously, whereas *multicore* CPUs have two or more cores, each of which can use multithreading.

Cache Memory

Several types of cache are used in computers, but CPU cache is a special high-speed memory that reduces the time the CPU takes to access data. Because it uses high-speed static RAM (SRAM) and because the cache is often located directly on—or even in—the CPU, using CPU cache can be faster than accessing information from dynamic RAM (DRAM) modules. However, it is limited in storage capacity compared to DRAM.

Cache is typically divided into three levels, which are accessed by the CPU sequentially: L1 (built into the CPU) and L2 and L3 (built onto the CPU). L1 and L2 cache are distributed to each core of the CPU, but L3 cache is shared by all of the CPU's cores. Generally, the more cache, the better. The less the CPU needs to access DRAM, the more quickly it can calculate data.

CPU Compatibility

CPU compatibility boils down to the socket available to you and the manufacturer you decide to use. Intel and AMD dominate the desktop and laptop market.

Intel and AMD

CPU manufacturers use the make/model system—for example, the Intel (make) Core i7-14700K (model) or the AMD (make) Ryzen 9 7650X (model). There are dozens of models of Intel and AMD CPUs. The A+ exam does not require you to know all of the individual models, but you should have a working knowledge of some of the basic makes and models available. Periodically visit the Intel and AMD websites for the latest and greatest CPUs.

A CPU might come with a built-in graphics processing unit (GPU). This means that with a compatible motherboard, no separate video card is necessary, and the monitor can be plugged directly into the video port on the motherboard. Both Intel and AMD have many CPUs with such *integrated GPUs*. AMD refers to this as the Accelerated Processing Unit (APU). Integrated GPUs have come a long way, but for power users (gamers, graphic designers, and so on), a separate video card is usually required for best functionality.

Intel and AMD are both good companies that make quality products, which leads to great competition. Which is better? In all honesty, the answer varies and depends on how you use the CPU. You can find advocates for both (albeit subjective advocates), and the scales are constantly tipping back and forth. On any given day, a specific Intel CPU might outperform AMD; three months later, a different AMD CPU might outperform an Intel. It's been that way for many years now. Whichever CPU you choose, make sure that you get a compatible motherboard. A couple of things to watch for are compatibility with the chipset and the socket type.

The chipset will either be Intel based or AMD based, depending on what type of motherboard you are using. It will only be compatible with a certain group of CPUs. For example, the motherboard in Chapter 16, Figure 16.1, while very old now, uses the Intel X99 chipset. For Intel, the chipset is also known as a Platform Controller Hub (PCH)—although Intel is working on PCH-less designs. This particular chipset can work with Core i7 CPUs and Intel Xeon E5 CPUs. (Xeon CPUs are primarily used in servers.) Verify that the CPU make and model will be compatible with the chipset and, therefore, the motherboard. So, for instance, the motherboard shown in Figure 16.1 is an ASUS X99-A, and it accepts the Core i7-5820K, among others. This is a very old chipset and motherboard, so look on retail sites to

see the newest chipsets and their compatible motherboards. The motherboard's socket type will also dictate compatibility, as we'll discuss in the next section.

Sockets

The *socket* is the electrical interface between the CPU and the motherboard. It attaches directly to the motherboard and houses the CPU. It also physically supports the CPU and heat sink and enables easy replacement of the CPU.

The socket is made of either plastic or metal and uses metal contacts for connectivity to each of the pins/lands of the CPU. One or more metal levers (retaining arms) lock the CPU in place. Figure 17.1 shows an example of an unlocked Land Grid Array (LGA) socket.

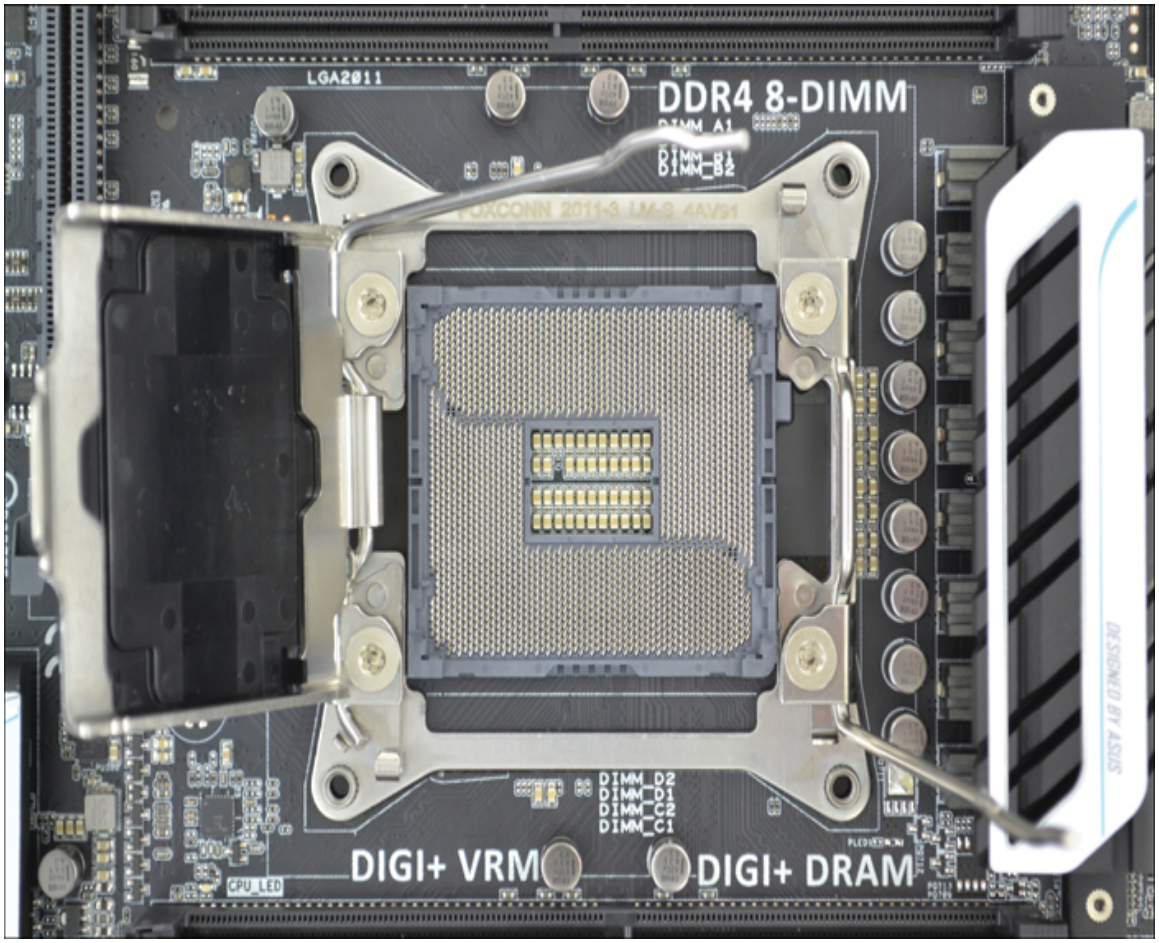


FIGURE 17.1 **An Unlocked LGA 2011 Socket**

Historically, the socket has been considered a ZIF, short for zero insertion force. This means that the CPU should connect easily into the socket, with no pressure or force involved during the installation. The socket will have many pin inserts, or lands, for the CPU to connect to. Pin 1 can be found in one of the corners and can be identified by either a white corner drawn on the motherboard or one or more missing pins or pinholes. This helps you to orient the CPU, which also has the arrow, or missing pin(s), in the corresponding corner. There are two types of sockets you should know for the exam:

- **PGA:** Pin Grid Array sockets accept CPUs that have pins covering the majority of their underside. The pins on the CPU are placed in the pinholes of the socket, and the CPU is locked into place by a retaining arm. Older AMD CPUs used PGA sockets. Starting with the AM5 socket in 2022, AMD moved its new line of CPUs to LGA.
- **LGA:** Land Grid Array sockets use lands that protrude out and touch the CPU's contact points. This type of socket (also known as Socket T) offers better power distribution and less chance to damage the CPU compared to PGA. LGA is commonly used today on Intel motherboards and newer AMD motherboards.

The CPU and socket must be compatible. For example, the Intel i7-14700 uses the LGA 1700 socket. Other Intel CPUs also use this socket, such as the Intel i7-12700. However, note that the chipset, in addition to the socket, must be compatible as well. Both of those CPUs have the same socket type, but the 12700 was designed for the 600 series chipset and the 14700 for the 700 series chipset. While they are somewhat cross-compatible, a BIOS update might be needed for them to work. Just because it's the same socket type doesn't mean it will always work. For instance, the Intel 10th-generation used an LGA 1200 socket as did the 12th-generation Intel; however, the 12th-generation Intel CPU wouldn't work on a motherboard designed for the 10th generation due to electrical compatibility issues with the chipset.

A few sockets from AMD include the AM4 and AM5. You will likely still encounter the older AM4 socket type, which is PGA and still being sold as of this writing, and the newer released AM5 socket type, which is LGA.

Some computers have multiple sockets, allowing them to run more than one CPU at the same time. For example, a rackmount server found in a data center might have a multisocket configuration that runs two or more Intel Xeon CPUs at the same time. A multisocket motherboard is different due to its capacity to house multiple CPUs, enabling the use of several processors to significantly boost processing power and overall performance. This design is prevalent in high-demand environments such as high-end servers and workstations, where efficient multitasking and parallel processing are essential. The capability to distribute workloads across numerous cores accelerates the execution of CPU-intensive applications, while scalability allows for easy performance upgrades by adding CPUs as computing needs increase.

Additionally, multisocket motherboards enhance multitasking by dedicating individual CPUs to separate tasks, leading to improved system responsiveness. They are particularly well suited for high-performance computing tasks like scientific simulations, video editing, and large-scale data analysis, which demand substantial processing power. These motherboards typically feature increased memory capacity through additional RAM slots and offer more PCIe lanes, increasing the connection of multiple high-performance GPUs for applications like machine learning and advanced graphics rendering.

Note

Compatibility is key! Find the correlation between sockets, chipsets, and CPUs by analyzing the motherboard and CPU documentation.

Power Consumption

Power consumption of CPUs is normally rated in watts. For example, the Core i7-14700K is rated as a 125 watt-hour base power CPU with a maximum turbo power of 253 watt-hours! This rating is known as *thermal design power (TDP)*, and it signifies the amount of heat generated by the CPU, which the cooling system is required to dissipate when operating with a complex workload. This number is usually displayed as the maximum; it

could be less, depending on CPU usage, and does not take into account overclocking. The measurement should play into your decision when planning which power supply to use and which kind of cooling system. For more information on power supplies, see Chapter 18, "Power." Common TDP ratings for multicore CPUs range between 60 and 200 watts for higher-end CPUs. Extremely high-end CPUs could have a TDP of over 250 watts. On the low TDP end, that's comparable to one typical incandescent light bulb or 6 to 10 LED light bulbs!

While we are talking electricity, another important factor is voltage. CPUs are associated with a voltage range; for example, the Core i7-14700K runs at about 1.3 V by default. However, a CPU's voltage can increase as applications demand more processing power. The voltage that is received by the CPU can be monitored in the BIOS or, better yet, with applications within Windows. If the CPU goes beyond the specified voltage range for any extended length of time, it *will* damage the CPU. This issue becomes especially important for overclockers.

Table 17.1 summarizes the different types of power connectors.

TABLE 17.1 **Types of Power Connectors**

Connector Type	Description
SATA (Serial ATA)	Primarily used to provide power to SATA storage devices like HDDs and SSDs. It's a 15-pin connector that delivers power directly from the power supply unit (PSU).
eSATA (External SATA)	While *eSATA* mainly refers to a data transfer interface, it can sometimes involve external power solutions. It is designed for external SATA devices. The power is usually supplied by a separate power adapter, not from a single eSATA power cable.
SAN (Storage Area Network)	SAN is a network architecture, not a specific connector. Power delivery in SANs involves various connectors depending on the hardware (servers, storage arrays, and so on). These systems utilize standard server power connectors and often redundant power supplies.

Connector Type	Description
Headers (Motherboard Headers)	These are pins on the motherboard that provide power to various components like fans, front-panel LEDs, and other peripherals. Examples include fan headers (3-pin or 4-pin), and RGB lighting headers.
M.2	M.2 is primarily a form factor for storage devices (SSDs), and it receives power directly through the M.2 slot on the motherboard. Therefore, it is a slot that provides both data and power.

ExamAlert

Know the various power connectors that connect to components.

Cooling Mechanisms

Now that you know a CPU uses a good deal of electricity, you can understand why it gets so hot. Hundreds of millions of transistors are hammering away in these powerhouses, and you need to keep the CPU and other devices in the computer cool. This is done in a few ways, as outlined in this section.

Heat Sinks

A *heat sink* is a block of metal made to sit right on top of the CPU, with metal fins stretching away from the CPU. It uses conduction to direct heat away from the CPU and out through the fins. On secondary processors that use a passive heat sink, that's all there is to it: It dissipates heat and requires no moving parts; it is "fanless." But that's not enough for the main CPU in a typical PC. With an active heat sink, a fan is attached to the top of or on the side of the heat sink. The fan plugs into the motherboard for power. If installed on top, the fan blows air into the heat sink and toward the CPU, helping to dissipate heat through the heat sink fins. If installed on the side

of a larger heat sink, it blows air sideways through the heat sink toward the case's exhaust fan. More powerful aftermarket CPU heat sinks/fans can be installed as well; just make sure that your power supply can handle the increased power requirements and that you have the space needed because some CPU heat sinks and fans are *big*.

In a PC-based motherboard, the chipset usually has a passive heat sink, but all new CPUs come with active heat sinks. Traditionally, heat sinks have been made of aluminum, but now copper heat sinks are also used due to their superior conductivity. An important point about heat sinks: If they come loose, they could adversely affect the performance of the CPU or cause overheating, which could lead to random reboots. Make double sure that the heat sink is attached securely.

Thermal Paste/Pads

The CPU cap and the bottom of the heat sink will have slight imperfections in the metal. Surface area is key; the best heat dissipation from CPU to heat sink would occur if the metal faces on each were completely and perfectly straight and flat—but we live in the real world. Thermal paste is used to fill the tiny gaps and imperfections. (Thermal paste is also known as thermal compound or thermal interface material.) One example of thermal paste is Arctic Silver, available online and at various electronics stores.

In a new installation, thermal paste might not be needed. Some new CPUs' heat sinks have factory-applied thermal paste that spreads and fills the gaps automatically after you install the heat sink and boot the computer. This is sometimes referred to as a thermal pad. However, if you need to remove the heat sink for any reason (for example, to clean it, or when upgrading, or if the CPU did not come with a heat sink), then you should apply thermal paste to the CPU cap before the heat sink is installed or upgraded.

To do this, first clean any old thermal paste off the CPU cap and the heat sink with thermal paste remover. The best thermal paste remover is plain, old isopropyl alcohol. The higher the percentage, the better. For example, you can buy 90 percent isopropyl alcohol from most grocery stores. The higher percentage leaves less residue. Apply the isopropyl alcohol to a lint-free cloth and wipe off the old thermal paste. Never reuse a CPU heat sink

with old thermal paste. Always clean off the old thermal paste from the heat sink and CPU and reapply new thermal paste! Then apply new thermal paste to the CPU cap. The application method will vary depending on the CPU used, but usually, applying one pea-sized dot in the middle of the CPU is the most common. There are other methods as well; review your CPU's documentation to find out which method is recommended. Finally, install the heat sink. Try to do so in one shot, without jostling the heat sink excessively. See Intel's website for a brief overview of installing thermal paste: https://www.intel.com/content/www/us/en/gaming/resources/how-to-apply-thermal-paste.html.

ExamAlert

Reapply thermal paste whenever removing and reinstalling a heat sink.

Fans

Case fans are also needed to get the heat out of the case. The power supply has a built-in fan that is adequate for lesser systems. However, more powerful systems should have at least one extra exhaust fan mounted to the back of the case, and many cases today come with one for this purpose. An additional fan on the front of the case can be used as an intake for cool air. If you aren't sure which way the fan blows, connect its power cable to the computer but don't mount it; then hold a piece of paper against the fan. The side that pulls the paper toward it should be the side facing the front of the computer when it is mounted. Some cases come with fans that are mounted to the top, which is ingenious because heat rises.

Another thing to consider is where the heat goes after it leaves the case. If the computer is in an enclosed area, the heat has a hard time escaping and might end up back in the computer. Make sure there is an area for air flow around the computer case.

Of course, three or four fans can make a decent amount of noise, and they still might not be enough for the most powerful computers, especially the

overclocked ones, which leads us to our next option.

Note

There is a point where having too many case fans might actually harm performance. Too many case fans can actually cause airflow turbulence, which ends up causing swirling air currents that don't allow the hot air to escape. This is especially true when fans are placed incorrectly and blowing in opposite directions. As a rule of thumb, you want air to pull in from the front and exit through the top and/or back.

A CPU fan is a crucial component that actively cools the central processing unit. It generally sits on top of the heat sink, as described earlier, to help dissipate heat even more effectively. Remember, as the CPU performs calculations, it generates significant heat. Without proper cooling, this heat can lead to overheating, causing performance degradation, system instability, and even permanent damage to the CPU. The CPU fan works by dissipating this heat, ensuring the CPU operates within safe temperature limits, thereby maintaining system reliability and longevity.

ExamAlert

Remember that the two components that could cause the system to shut down are the power supply and the CPU fan. Check the CPU fan settings and temperature in the BIOS/UEFI first before opening the computer. If those are fine, you most likely need to replace the power supply.

Liquid Cooling Systems

Although this method is not as common as the typical CPU/heat sink/fan combination found on a typical computer, you will see liquid-cooled systems used in high-end PCs. As the TDPs of CPUs have increased over

time, many builders are opting for liquid-cooled systems. And newer water-cooling kits can be used not only to cool the CPU but to cool the chipset, storage drives, video cards, and more. A kit might come with a CPU water block, pump, radiator/fan, PVC tubing, and, of course, coolant; there are more simplified versions of liquid cooling systems as well. The advantages of such systems are improved heat dissipation (with proper installation), potential for higher overclocking rates, and support for the latest, hottest CPUs. Some of the disadvantages include the risk of a leak that can damage components; pumps becoming faulty over time; air being trapped in the lines, which can cause the system to overheat; and the need for maintenance in the form of inspecting the lines and replacing the coolant every few years. However, many off-the-shelf, prebuilt liquid-cooling systems are closed looped—meaning they are prefilled within a sealed environment. These systems are usually much easier to install and minimize the need for regular maintenance. Liquid cooling has traditionally been employed by enthusiasts (such as gamers), but as modern CPUs have become increasingly hotter, it is becoming more common for this solution to be used. You might see it in other CPU-intensive systems, such as virtualization computers and audio/video editing systems. Regardless of cost, installation complexity, and maintenance, liquid cooling systems can help dissipate heat the most efficiently.

ExamAlert

Of all PC cooling methods, liquid cooling systems can dissipate heat the most efficiently.

Installing CPUs

As with most other computer components, installing a CPU is easy. But you must be careful because it can be damaged easily. Go slowly and employ proper safety measures. Let's break down the installation into some simple steps:

1. **Select a CPU:** If you build a new computer, the CPU needs to be compatible with the motherboard. Consider the type of CPU, speed,

and socket type. If you upgrade a CPU, be sure that it is on the motherboard's compatibility list (which can be found at the manufacturer's website).

Power down the PC, disconnect the power cable (or turn off the kill switch), open the PC, and get your boxes of components ready!

2. **Employ ESD prevention methods:** Use an antistatic strap and mat. Remove the CPU and heat sink from the package, inspect them, and then place the CPU back in its plastic holder or inside an antistatic bag until you are ready to install it. (An antistatic bag usually comes with the motherboard, but you should have extra ones handy.) To prevent damage, make sure that the CPU's lands or pins are facing up if it is in an antistatic bag. Never touch the lands or pins of a CPU. Before touching any components, place both hands on an unpainted portion of the case chassis. For more information on ESD prevention measures, see Chapter 59, "Safety Procedures."
3. **Ready the motherboard:** Some technicians prefer to install the CPU into the motherboard and then install the motherboard into the case. If you do this, place the motherboard on the antistatic mat. (The mat should be on a hard, flat surface.) If you install the CPU directly into an already installed motherboard, clear away any cables or other equipment that might get in the way or that could possibly damage the CPU, heat sink, or fan.
4. **Install the CPU:** Be careful with the CPU! It is extremely delicate! Always touch the case chassis before picking up the CPU. Hold it by the edges and do not touch any pins, lands, or other circuitry on the CPU. Most of the time, a CPU will be installed to either an LGA socket or a PGA socket. The following two bullets show how to install a CPU into each type of socket. Be sure to refer to the installation guide that comes with your particular CPU and motherboard.

   - If you install to an LGA socket, unlock the socket by releasing the retaining arm(s) and swinging it open as far as it can go. Open the socket hatch, unhook it if necessary, and remove any plastic cover. Next, place the CPU into the socket. One corner of the CPU has an arrow that should be oriented with either a white corner or other similar marking on the motherboard or the socket's missing pin(s);

both of these corresponding corners indicate pin 1, as shown in Figure 17.2. Carefully place the CPU into the socket with zero force insertion. *Zero force insertion* means do not press down! (Imagine setting a very delicate piece of glass on a hard surface. You don't drop it, and you don't press down on it. You just gently set it down.) If it is oriented correctly, the lands on the CPU match up with the lands on the socket. Make sure it is flush and flat within the socket. Close the cap and secure the retaining arm underneath the tab that is connected to the socket, thus securing the CPU. Install thermal paste if necessary. Next, install the heat sink/fan assembly. (If the heat sink came with the CPU, it might have thermal paste applied already.) LGA sockets usually have four plastic snap-in anchors. Carefully press each of these into and through the corresponding motherboard holes. Don't use too much force! Then turn each of them to lock the heat sink in place. Make sure the heat sink is installed flush with the CPU by inspecting the assembly from the side. You want to be positive of this before turning on the computer because the thermal paste will begin to expand and fill the imperfections right away. Plug the fan into the appropriate motherboard power connector. (These connectors are usually labeled directly on the motherboard; if they're not labeled, see your motherboard documentation for details on where to plug in the fan.) Install the entire motherboard assembly into the case (if that is your method of choice).

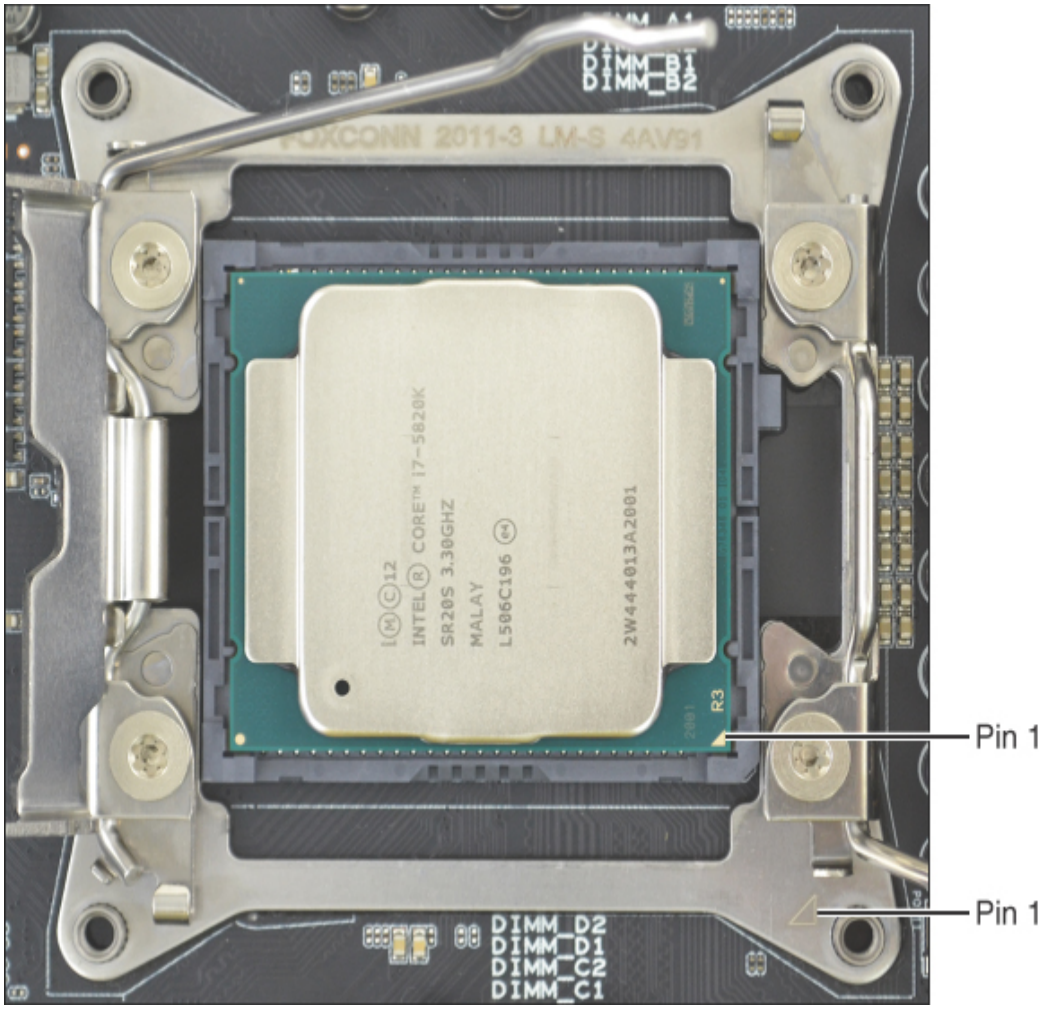


FIGURE 17.2 **Orientation Markings on a CPU and an LGA Socket**

- If you install to a PGA socket, unlock the socket by moving the retaining arm(s) out and upward until it is open as far as it will go, without forcing it. Then gently place the CPU into the ZIF socket. There will be an arrow on one corner of the CPU that should correspond to a missing pin (or arrow) on the socket. Don't use force; sometimes it is useful to very gently apply pressure from side to side on the edges of the CPU to see if it falls into place after you set it down on the socket. Look at the CPU from the side and make sure it is flush with the socket. Lock down the retaining arm to keep the CPU in place. Then attach the heat sink/fan assembly to the metal clips that are on the sides of the socket. Make sure that the

heat sink is installed flush with the CPU by inspecting the assembly from the side. You want to be positive of this before turning on the computer because the thermal paste will begin to expand and fill the imperfections right away. Attach the fan's power cable to the motherboard. (See your motherboard documentation for details on where to plug in the fan.) Install the entire motherboard assembly into the case (if that is your method of choice).

5. **Test the installation:** With the case still open, boot the computer to make sure that the UEFI/BIOS POST recognizes the CPU as the right type and speed. Enter the BIOS and view the CPU information to verify this. If the BIOS doesn't recognize the CPU properly, check whether a BIOS upgrade for the motherboard is necessary. Also make sure that the CPU fan is functional. Then view the details of the CPU within the BIOS. Be sure that the voltage reported by the BIOS is within tolerance. Then access the operating system (after the OS is installed) and make sure it boots correctly. Complete several full cycles and warm boots. Finally, view the CPU(s) within Windows and/or third-party tools (such as CPU-Z).

   For example, check in the Device Manager to make sure the CPU is identified correctly. This can be accessed within Settings, the Control Panel, within Computer Management, or by pressing Windows+R to open the Run prompt and typing **devmgmt.msc** and pressing Enter. You should see a category named Processors; expand it, and the CPU that is installed should be listed. Remember, it will show up as multiple *logical* processors, equal to the number of threads the CPU can run simultaneously.

> **Note**
>
> You can view basic CPU information in Windows on the System Information window, which can be accessed by opening the Run prompt and typing **msinfo32**.

6. **Close the case and monitor the system:** Finally, if everything looks okay, close the case and consider monitoring the clock rate, voltage,

and heat during the first few hours of operation. Voltage and heat can usually be monitored within the BIOS. All three can be monitored within Windows and by using third-party applications or by using monitoring utilities that accompany the motherboard. If all went well, congratulate yourself on a job well done!

Cram Quiz

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

1. What does multithreading do?

   - ○ **A.** It gives you multiple cores within the CPU.
   - ○ **B.** It enables four simultaneous threads to be processed by one CPU core.
   - ○ **C.** It enables two simultaneous threads to be processed by one CPU core.
   - ○ **D.** It provides a high-speed connection from the CPU to RAM.

2. What seals the tiny gaps between the CPU cap and the heat sink?

   - ○ **A.** Grape jelly
   - ○ **B.** Plumber's putty
   - ○ **C.** 3-in-1 house oil
   - ○ **D.** Thermal paste

3. Which of the following can be defined as the amount of heat generated by the CPU, which the cooling system is required to dissipate?

   - ○ **A.** GPU
   - ○ **B.** TDP

- ○ **C.** PSU
- ○ **D.** 140 watts

4. When you're deciding on a CPU for use with a specific motherboard, what does it need to be compatible with? (Select all that apply.)

- ○ **A.** Case
- ○ **B.** Socket
- ○ **C.** Chipset
- ○ **D.** PCIe slots

5. Which kind of socket incorporates "lands" to ensure connectivity to a CPU?

- ○ **A.** PGA
- ○ **B.** Chipset
- ○ **C.** LGA
- ○ **D.** Copper
- ○ **E.** AM4

6. Which of the following enables the user to increase the base clock within the BIOS, thereby increasing the clock speed of the CPU?

- ○ **A.** Overclocking
- ○ **B.** L3 cache
- ○ **C.** Integrated GPU
- ○ **D.** Heat sink

7. Which of the following would you use if you needed a typical CPU for a PC that can access 16 GB of RAM?

- ○ **A.** ARM
- ○ **B.** x86-64

- **C.** RISC
- **D.** x86

8. A technician needs to install a new server system in a data center that can run more than one physical CPU at a time. Which configuration will support this requirement?
   - **A.** Single-core
   - **B.** Multicore
   - **C.** Multithreading
   - **D.** Multisocket

Cram Quiz Answers

1. **C.** Multithreading allows for an operating system to send two simultaneous threads to be processed by a single CPU core. The OS views the CPU core as two virtual processors. Multiple cores would imply multicore technology, which means there are two physical processing cores within the CPU package. HyperTransport is a high-speed connection used by AMD from the CPU to RAM; it is roughly the same as Intel's Hyper-Threading.

2. **D.** Thermal paste is used to seal the small gaps between the CPU and the heat sink. It is sometimes referred to as thermal gel or jelly (among a variety of other names), but not *grape* jelly. (While grape jelly can be great on toast, it's not a good idea for CPUs.) Note: Never use petroleum-based products (such as 3-in-1 oil or WD-40) inside a computer; the oils can damage the components over time.

3. **B.** TDP (thermal design power) is the amount of power required to cool a computer and is linked directly to the amount of heat a CPU creates. Some CPUs come with a built-in graphics processing unit (GPU). This means that with a compatible motherboard, no separate video card is necessary. PSU stands for power supply unit, and 140 watts is a potential TDP rating but does not define what TDP is.

4. **B. and C.** The CPU needs to be compatible with the socket of the motherboard. In addition, the CPU needs to be compatible with the chipset of the motherboard. The case doesn't actually make much of a difference when it comes to the CPU, but it does matter for the motherboard! PCI Express (PCIe) slots don't actually play into this scenario at all because there is no direct connectivity between the two.

5. **C.** LGA (Land Grid Array) is the type of socket that uses "lands" to connect the socket to the CPU. PGA (Pin Grid Array) sockets have pinholes that make for connectivity to the CPU's copper pins. AM4 is a PGA socket that accepts AMD CPUs such as the older Ryzen 7. Newer AM5 AMD sockets use LGA.

6. **A.** Overclocking enables the user to increase the clock speed of the CPU within the BIOS. Level 3 (L3) cache comes in the largest capacities of the three types of cache and has the most latency; therefore, it is the slowest. If the CPU can't find what it needs in L1, it moves to L2 and then to L3. An integrated GPU is a video adapter that is built into the motherboard. The heat sink helps to dissipate heat from the CPU and is usually aided by a fan or liquid cooling system.

7. **B.** You would want an x86-64 CPU. This 64-bit CPU architecture can go beyond the 32-bit limitation of 4 GB of RAM and access as much as 256 TB of RAM (theoretically). Also, that is normally the type of CPU you would use in a PC. ARM-based CPUs are more often used with smartphones, tablets, and other mobile devices. Reduced instruction set computing (RISC) is a highly optimized technology used in ARM CPUs to make them more efficient. x86 is the older 32-bit version of PC-based CPUs. It is unlikely that you will see an x86 CPU, but you never know!

8. **D.** Some computers (such as servers) have multiple sockets, allowing them to run more than one CPU at the same time. Each of these physical CPUs will also incorporate multicore and multithreading technologies. Get ready for 64 simultaneous

threads or more! This is the kind of stuff that makes the cloud work.

Phew, this was a pretty intense chapter. Give yourself a high five for getting through it. Now, take a picture of yourself giving yourself a high five; it'll make for levity later. Stretch, hydrate, and let's move on!

"The human brain starts working the moment you are born and never stops until you stand up to speak in public." —George Jessel

Chapter 18

Power

This chapter covers the following A+ 220-1201 exam objective:

- **3.6** – Given a scenario, install the appropriate power supply.

Clean, well-planned power is imperative in a computer system. Power requirements should always be in the back of your mind when designing a computer. After the components of a computer have been selected—especially the CPU and GPU—the power supply needs to be chosen carefully. Not enough power, and the system might become unstable or might not work at all. Too much power, and it becomes expensive and wasteful.

The power supply unit (PSU) in a PC is in charge of converting the alternating current (AC) drawn from the wall outlet into direct current (DC) to be used internally by the computer. The power supply makes use of a transformer and a rectifier, working together to convert AC over to DC. The power supply feeds the motherboard, storage drives, optical drives, and any other devices inside the computer. Talk about a single point of failure! Many higher-end workstations and servers have redundant power supplies to protect against that single point of failure taking down the entire system. In this chapter, we focus on PC power supplies. For more information on power as it relates to laptops, see Chapter 1, "Monitoring, Maintaining, and Replacing Mobile Device Hardware."

You Have the Power!

Luckily, after some pretty heavy chapters so far, this one is much shorter. You've done great so far, so let's get underway!

ExamAlert

Objective 3.6 focuses on the following: input 110-220 VAC versus 220-240 VAC, output 3.3 V versus 5 V versus 12 V, 20+4 pin motherboard connector, redundant power supply, modular power supply, wattage rating, and energy efficiency.

Planning Which Power Supply to Use

It is important to use a reliable brand of power supply that is approved for use by organizations such as the International Electrotechnical Commission (IEC), Federal Communications Commission (FCC), UL, and so on, and that meets directives such as the Restriction of Hazardous Substances (RoHS). Adherence to appropriate standards reduces the risk of fire and allows for safer products in general.

You also must consider the following factors when planning which power supply to use in your computer:

- Type of power supply and compatibility
- Wattage and capacity requirements
- Number and type of connectors
- Energy efficiency

Types of Power Supplies and Compatibility

The most common form factor used in PCs today is Advanced Technology Extended (ATX). Depending on the type of ATX, the main power connector

to the motherboard will usually have 24 pins (or 20+4 pins). Today's systems use power supplies that adhere to one of the ATX 12V 2.x standards, or the newer ATX 3.x standards, which specify 24 pins. For backward compatibility with 20-pin connections, many power supplies' 24-pin connectors come with 4 pins that can be detached and moved out of the way.

Note

In 2022, Intel introduced a major update to power supplies: the new ATX 3.0 standard. This first major update after almost 20 years includes a new 12+4-pin power connector named 12VHPWR. This new power connector is specifically for modern GPUs. This one connector can deliver up to 600 watts for any PCIe 5.0 GPU! That's a big upgrade from the 6-pin, which could deliver 75 watts, and the 8-pin, which could deliver 150 watts. This new standard also increases the power threshold and increases efficiency.
Unfortunately, this new power connector had a rocky start because many users had issues with melted connectors on the graphics card side. This issue was addressed by informing users not to bend the end of the connector too sharply when plugging in. The issue was widespread enough that in September 2023 a new ATX specification was released: ATX 3.1. The main difference between ATX 3.0 and the ATX 3.1 standard is a redesigned 12VHPWR connector that is now noted as a 12V-2x6 connector. This new 12V-2x6 connector is backward compatible with the 12VHPWR connector and includes upgraded safety features to prevent the issues that plagued the 12VHPWR connector.

The key here is compatibility. If a computer is proprietary, you can go to the computer manufacturer's website to find out the exact form factor and possibly get a replacement power supply for that model computer. Some third-party power supply manufacturers also offer replacement power supplies for proprietary systems. However, if a computer is custom-built, you need to find out the form factor used by the motherboard and/or case, and you should open the computer to take a look at all the necessary power

connections. Then you need to find a compatible power supply (according to those specifications) from a power supply manufacturer.

Most of today's motherboards have an additional 4-pin or 8-pin 12 V power port for the CPU (referred to as EATX12V). A typical power supply offers one or two 4-pin connectors or one 8-pin connector for this extra power. Note that some high-end PSUs might even include a second 8-pin connector for extra power delivery if the motherboard supports it! If the motherboard and power supply don't match up, there are 4- to 8-pin adapters available. Figure 18.1 shows an example of a 24-pin ATX connector and an example of an 8-pin CPU connector.

ExamAlert

Be able to identify the main 24-pin power port/connector and the CPU's EATX12V 8-pin port/connector.

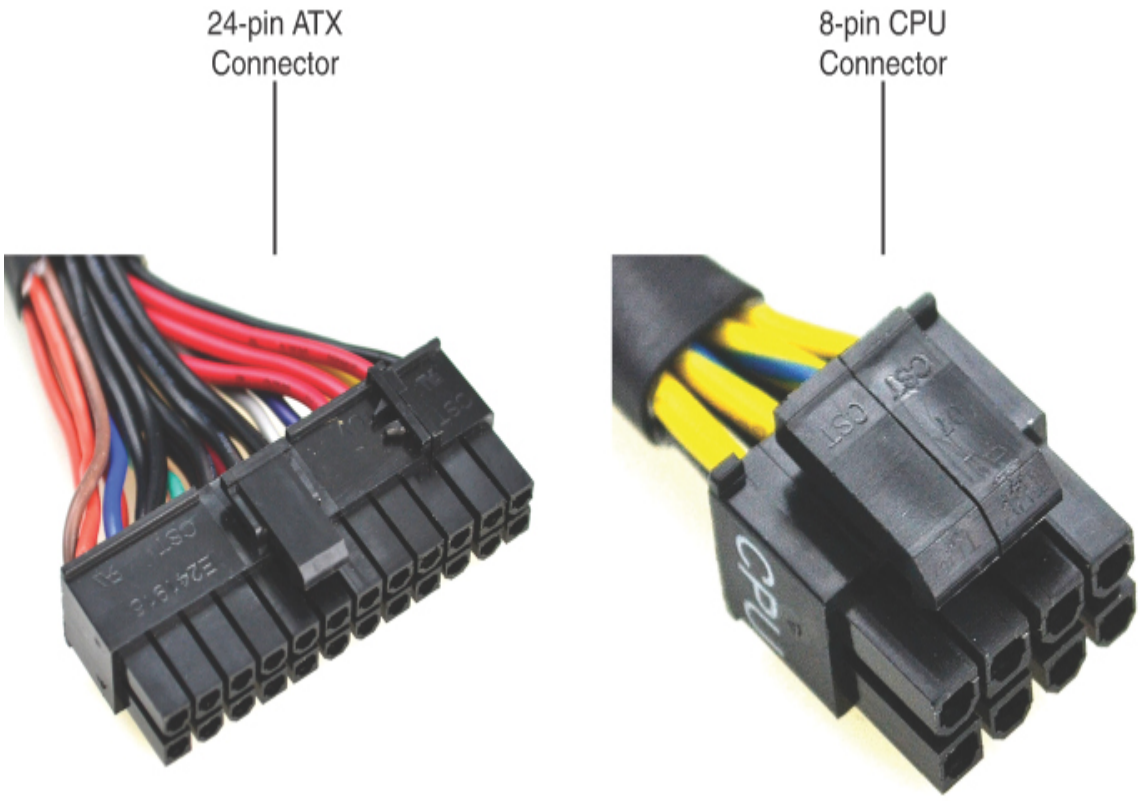


FIGURE 18.1 **24-Pin ATX and EATX12V 8-Pin CPU Connectors**

A quick word about rails: Remember that the ATX specification requires the power supply to produce +3.3 V, +5 V, +12 V, and –12 V outputs, as well as a 5 V standby output. These are known as *rails* (for example, the +12 V rail). You might have heard of *dual-rail* or *multi-rail* power supplies, such as multiple 12 V rails. This technology is a way of monitoring power circuits individually instead of collectively (single-rail) and helps to prevent overheating and possibly fire by shutting down the PSU if a certain point is reached (for example, more than 18 amps on a single 12 V wire). However, because of the extensive power that many components draw now—looking at your GPU—most modern PSUs have reverted back to single-rail PSUs. This allows more power, current specifically, to be diverted to one component if it needs it because the whole power distribution is on one power circuit. On dual-rail/multi-rail systems, that power is divided up and capped. Of course, the downside to this move back to single-rail is that if one component goes over the cap, the whole system will fail.

ExamAlert

The purpose of dual-rail PSUs is to separate and limit the current through each wire to avoid overheating.

Also, remember about case fans. If they have 4-pin connectors, they can connect directly to the motherboard. You can also connect a 3-pin fan connector to a motherboard 4-pin fan header, leaving one pin open. The fourth pin allows the motherboard to regulate the speed of the fan through pulse-width modulation (PWM). If you don’t have the fourth pin, the motherboard will most likely run the fan power at 100 percent, which is okay. Some motherboards, though, can still regulate the fan speed by changing the fan voltage if only using 3-pin connectors. If you don’t have enough fan headers on the motherboard, additional case fans may connect directly to the power supply feeds. What you use depends on how many fans you need and the configuration of the power connections.

Finally, case connectors for the power button and the reset button are usually located toward the front of the motherboard. When you’re connecting these, the colored wire normally goes to positive (+), if

necessary. Some case connectors can be connected either way, and it won't make a difference. But connectors like the power LED and the hard-drive activity LED need to be connected properly for the LEDs to display. Quite often, the motherboard will be color-coded; the fold-out instruction sheet (or manual) will show exactly where to plug in each case connector, and the case connectors themselves are normally labeled. Make sure you plug the case connectors into the correct motherboard headers and orient them properly. If you see an arrow on these front-panel connectors, it indicates positive, which can be extremely helpful when you're hooking these up.

Wattage and Capacity Requirements

Power supplies are usually rated in watts. They are rated at a maximum amount that they can draw from the wall outlet and pass on to the computer's devices. Remember that the computer will not always use all that power. And the amount of power used depends on how many devices work and how much number crunching your processor does! In addition, when computers sleep or suspend, they use less electricity. What you need to be concerned with is the maximum amount of power all the devices need collectively. Most power-supply manufacturers today offer models that range from 300 watts all the way up to 2000 watts! Devices use a certain amount of power, defined in amps and/or watts. By adding together the power consumption of all the devices, you can get a clearer picture of the power supply you need. Consult the manufacturer's web page of the device for exact requirements. Then consider using a power supply calculator on the Internet to find out how many watts you might need. Many desktop and tower computers can typically get away with using a power supply that is rated between 500 and 700 watts. But if you decide to add devices—especially video cards—you might find that the current power supply will not meet your needs anymore, and an upgrade will be necessary. So, plan for the future as well. (Apparently, technicians need to be prescient!)

ExamAlert

Remember that the PSU wattage rating refers to the maximum amount of power the PSU can output under 100 percent load capacity. Having a power supply that doesn't provide sufficient

wattage to system components may result in undervoltages (brownouts), intermittent reboots, or even the system failing to power up.

Number and Type of Power Connectors

It is important to know how many of each type of power connector you need when planning which power supply to use. You must be familiar with each type of power connector for the A+ exam. Be prepared to identify them by name and by sight. Table 18.1 defines the usage and voltages for some typical power connectors. Figure 18.2 shows these connectors.

TABLE 18.1 **Power Connectors**

Power Connector	Usage	Pins and Voltages
SATA	Serial ATA storage drives	15-pin, 3.3 V, 5 V, and 12 V
Molex	Case fans, IDE storage drives	4-pin, 5 V (red), 12 V (yellow), two ground wires
PCIe	PCI Express video cards	6-pin, 12 V (ATX12V version 2.1) 8-pin, 12 V (ATX12V version 2.2 and higher) 12+4-pin 12 v (ATX12 version 3.0 and higher)

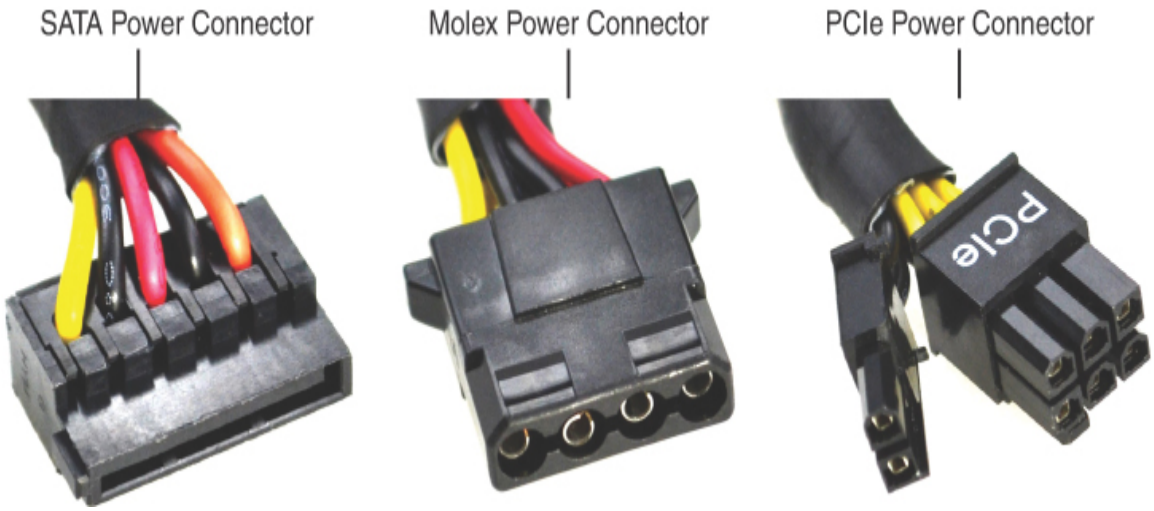


FIGURE 18.2 **SATA, Molex, and PCIe Power Connectors**

ExamAlert

Be able to identify SATA, Molex, and PCIe power connectors, know their associated voltages, and know their number of pins.

Note

Don't confuse 8-pin PCIe power connectors with 8-pin CPU connectors! To tell the difference, look for the label! Also, the PCIe video connector will usually separate two of the pins so that you can use it in 6-pin or 8-pin scenarios. Also know that PCIe cards can get power from the slot itself, and like PCIe, M.2 devices derive power from the motherboard connector.

Older PATA hard drives and optical drives used a thicker 4-pin power connector called a Molex connector. Some older PSUs still came with a Berg connector for backward compatibility. It's a smaller 4-pin connector used with the venerable 3.5-inch floppy drive.

Energy Efficiency

Remember, a PSU's primary job is to convert AC power to DC power to deliver it to the components. There is always some loss of power when converting AC to DC or vice versa. When a large percentage of power is converted from AC to DC, the PSU is considered energy efficient. Virtually all PSUs have the 80 Plus certification. If they don't, you might not want to buy one! This means that 80 percent or greater of the power is converted from AC to DC with the rest lost to heat. Of course, there's a big swing in efficiency even within the 80 Plus certification. Therefore, those 80 Plus certification PSUs are broken into levels of efficiency. Table 18.2 lists the 80 Plus certification levels and their respective efficiency ratings at 100 percent load.

TABLE 18.2 **80 Plus Certification Levels**

80 Plus Certification Level	Efficiency Rating at 100% Load
80 Plus (often labeled as White)	80%
80 Plus Bronze	82%
80 Plus Silver	85%
80 Plus Gold	87%
80 Plus Platinum	89%
80 Plus Titanium	90%

As you can see in Table 18.2, there is a large increase in efficiency with the higher-certified PSUs. Of course, this means a larger price tag as well. Often, you will find the best efficiency rating per cost ratio with the 80 Plus Gold PSUs. The difference between a White-rated PSU and a Gold-rated PSU is a 7 percent increase in efficiency and often a difference of $40 to $50. This initial cost difference will often be made up in energy savings over the lifetime of this PSU. If you're thinking that you might as well go for a Platinum or Titanium, then, well, you can, but these are often much more expensive for less gain in efficiency.

ExamAlert

Know what energy efficiency is in relation to power supplies and that the 80 Plus certification is a measure of that efficiency.

Modular and Redundant PSUs

In older times, PSUs had all of the power cables coming out in a single bundle from the unit; a person had little control over the connections available. Newer PSUs fix this problem by being modular. To accomplish this, a modular PSU has a variety of ports that you can plug power cables into (some also come with a bundle of standard power connections and are called *semi-modular PSUs*). This modularity allows a person to add more connections as needed; for example, Molex-to-SATA power connections or PCIe connections for video. For added flexibility and tidiness, go modular!

Redundant PSUs are very common on servers and some other high-end systems. To allow for true redundancy, the computer case must have two or more PSUs. (*Redundant* simply means more than one of a particular component.) When you have multiple PSUs, there is a separate IEC cable for each. For example, a rackmount server might come with two power supplies. Each one requires an AC outlet. They both are powered on at all times. Typically, if one fails, the other is ready to take over the electric load without any downtime because it is already running. In this case, it is not only redundant but able to tolerate a PSU failure (also known as *fault tolerant*). These power supplies are often removable, so if one fails, it can be slid out the back of the case and replaced. Some are even hot-swappable, meaning that you wouldn't even have to turn off the server to switch out the PSU. But you should always check the documentation first to be sure!

ExamAlert

Remember that a modular power supply is a power supply unit where the power cables are detachable. This modularity offers flexibility in cable management by allowing users to connect only the cables they need for their specific system, instead of having all

cables permanently attached like in a nonmodular power supply. A redundant power supply can help keep a system up and running in the event of a PSU failure.

Installing the Power Supply

When the power supply arrives, you can install it. But first take a look at the back of the power supply to identify the components, which are shown in Figure 18.3.

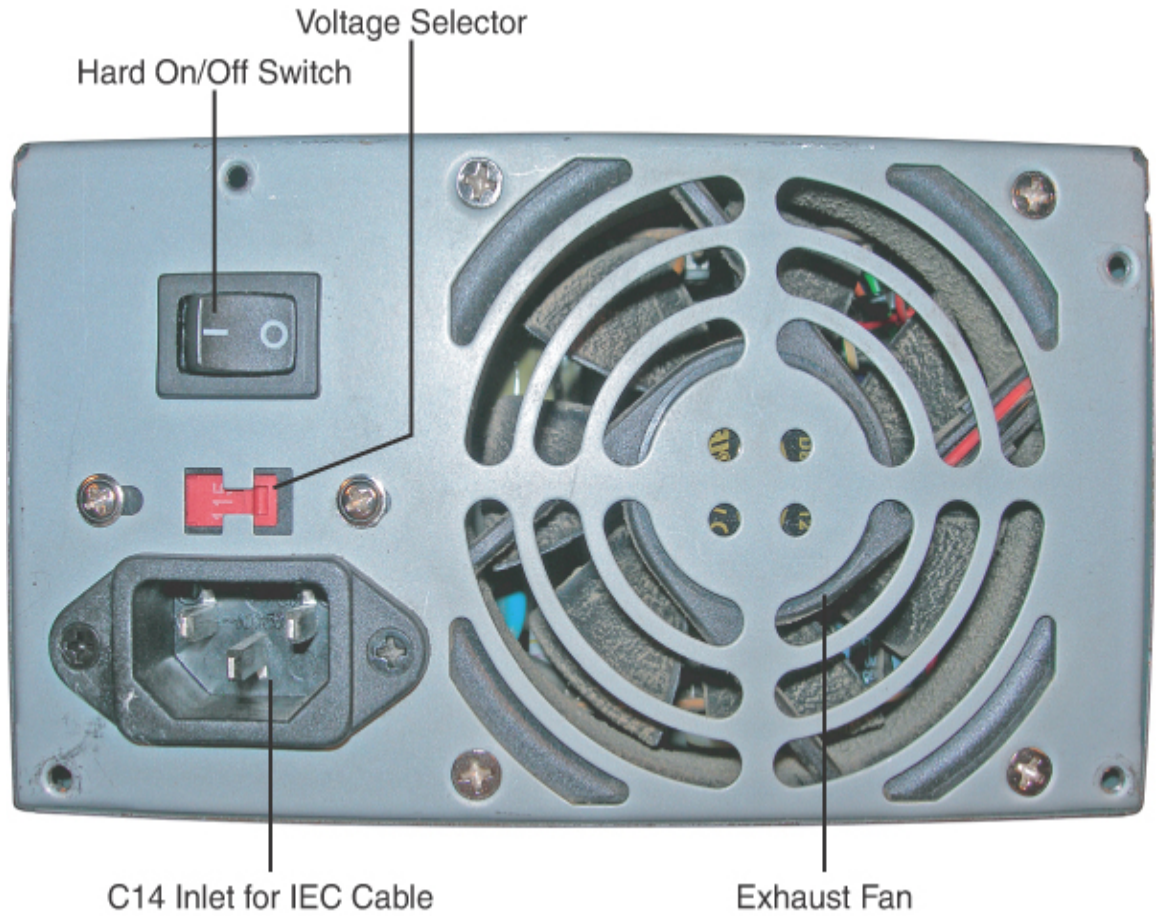


FIGURE 18.3 **Rear View of a Power Supply**

In the top-left portion of Figure 18.3 is a hard on/off switch, sometimes referred to as a kill switch. This switch is a helpful feature when you're troubleshooting PCs. Instead of disconnecting the power cable, you can

shut off this switch. It works effectively in emergencies as well. Below that, you see a (red) voltage selector switch. This switch indicates that this is a dual-voltage power supply. It should be set to 115 VAC in the United States. It also has a 230 VAC option to be used in other countries. (An additional adapter might be necessary for the different wall outlets you might encounter.) Always shut down the computer and disconnect the power cable before changing the voltage selector switch. Be sure to check this setting before initially using the power supply. This selector switch indicates an older, or atypical, power supply. Newer power supplies are equipped with a universal input, enabling you to connect the power supply to any AC outlet between 100 VAC and 240 VAC without having to set a voltage switch; the power supply "auto-detects" the voltage. To determine if a PSU without a voltage switch is truly dual-voltage, look for the phrase "100-240 VAC input" or something similar.

ExamAlert

In the United States, the power grid supplies anywhere from 110 VAC to 120 VAC. However, in Europe, for instance, the voltage supplied is double, ranging from 220 VAC to 240 VAC.

In Figure 18.3, below the voltage selector, you see the power cable inlet; this is known as a C14 inlet and is where you attach your power cord to the power supply. These inlets and the cables that connect to them are defined by the long-standing IEC 60320 specification and, because of this, some techs refer to the power cord as an *IEC cable*. This cord actually has a standard three-prong connector suitable for an AC outlet on one end and a C13 line socket on the other to connect to the power supply. To the right, you see the power supply fan that is of great importance when troubleshooting power supplies. We'll discuss troubleshooting in Chapters 23 through 28.

Back to our power supply installation! For new computer builds, we usually install the power supply at the beginning. This may or may not be possible, depending on your configuration, but it is a good rule of thumb. The power supply is a bulky unit, so installing it at the beginning of the build can

reduce chances that you might bump or hit another sensitive component when installing it. If this is a repair or an upgrade, and a power supply is currently connected to the computer, turn off the computer and unplug the power supply. ATX motherboards are always receiving 5 volts, even when they are off (if the computer is plugged in). Be sure that you use antistatic methods. Remove the old power supply and prepare to install the new one.

Note

Most custom-built computers have the power supply mounted on the bottom of the case. There is usually a fan on the bottom of the PSU. If your case has a vent on the bottom of the case, then point the PSU fan facing down. This will draw cool air from the bottom area below your case and exhaust it out the back of the PSU. Just remember that to mount it like this, you need to make sure your case has sufficient case feet and clearance below it so that air can be drawn up. In other words, don't set your computer tower on tall shag carpeting that could block the intake of air on the bottom! You'll overheat your PSU.

You might want to test the new power supply before installing it. You can do this by connecting a power supply tester, plugging in the power supply to the AC outlet, and turning on the hard on/off switch. (We'll show this in Chapter 23, "Troubleshooting Motherboards, CPUs, RAM, and Power.") Or you can test the power supply after it is installed by simply turning on the computer.

The power supply is placed inside the case and is often mounted with four standard screws that are screwed in from the back of the case. Make sure that there are no gaps between the power supply and the power supply opening in the case. Next, connect the main ATX 24-pin power connector to the motherboard. It can only be plugged in one way: a locking tab prevents a wrong connection and keeps the plug in place. Then, connect the 8-pin CPU power connector—again, tabbed for easy orientation. After that, attach the SATA and PCIe connectors as necessary to their corresponding devices. You might also have Molex connections to make for additional fans or

legacy devices. Most connectors are molded in such a way as to make it difficult to connect them backward or upside down. If you need a lot of strength to plug in the connector, make sure that it is oriented correctly. Don't force the connection. Afterward, remove any antistatic protection and, finally, plug in the power supply to the AC outlet, turn on the hard on/off switch (if the power supply has one), and turn on the computer. Check to see if the fan in the power supply is working and if the computer boots correctly. Do a final check of the CPU fan, case fans, internal/external indicator lights, and POST code readout—if the motherboard has one. If all systems are go, then close up the case and chalk up one more successful install!

Cram Quiz

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

1. Which power connector should be used to connect directly to a SATA storage drive? (Select the best answer.)

   - ○ **A.** Molex
   - ○ **B.** 6-pin
   - ○ **C.** 24-pin
   - ○ **D.** 15-pin

2. Which voltages are supplied by a SATA power connector?

   - ○ **A.** 12 V, 5 V, and 3.3 V
   - ○ **B.** 5 V and 3.3 V
   - ○ **C.** 3.3 V and 1.5 V
   - ○ **D.** 24 V and 12 V

3. A company salesperson just returned to the United States after three months in Europe. Now the salesperson's PC, which worked

fine in Europe, won't turn on. What is the best solution?

- **A.** Install a new power supply.
- **B.** The computer will not work in the United States due to European licensing.
- **C.** Install a power inverter to the power supply.
- **D.** Change the voltage from 230 to 115.

4. Which of the following can have 8 pins? (Select all that apply.)

- **A.** PCIe
- **B.** SATA
- **C.** ATX main power
- **D.** CPU
- **E.** Molex

5. A gaming enthusiast is building a new system that requires a powerful power supply unit. Which of the following would most likely help the gamer purchase the correct PSU for the system? (Select three.)

- **A.** Wattage rating
- **B.** Manufacturer's website
- **C.** Power supply calculator
- **D.** Redundancy

6. Which offers flexibility in cable management by allowing users to connect only the cables they need for their specific system?

- **A.** Nonmodular power supply
- **B.** Redundant power supply
- **C.** Dual-rail PSU
- **D.** Modular power supply

Cram Quiz Answers

1. **D.** The 15-pin connectors power SATA storage drives and other SATA devices (such as optical drives). That said, you might see a Molex power port on an older, modular PSU that can ultimately be connected to a SATA drive (with a Molex-to-SATA cable), but not directly; the SATA drive will have a 15-pin power connection on it. Molex connectors are also typically used to power older fans that don't connect directly to the motherboard, older IDE devices, and other secondary devices. The 6-pin power connectors are used for video cards (as are 8-pin connectors and the newer 12+4 connectors). 24-pin refers to the main power connection for the motherboard.

2. **A.** SATA connectors provide 12 volts, 5 volts, and 3.3 volts. There are four wires and 15 pins: if color-coded, yellow is 12 V, red is 5 V, orange is 3.3 V, and the one black wire is ground.

3. **D.** Most likely, the voltage selector was set to 230 V so that it could function properly in Europe (for example, in the UK). It needs to be changed to 115 V so that the power supply can work properly in the United States. Make sure to do this while the computer is off and unplugged. While most modern PSUs automatically set the voltage input, older PSUs have to be manually changed. Note: For shorter trips, a person will most likely use a laptop, which would require the right adapter to convert the voltage properly.

4. **A and D.** PCIe power can be 8-pin or 6-pin. CPU power (EATX12V) can be 8-pin or 4-pin. SATA power is 15-pin (and data is 7-pin). ATX main power is typically 24-pin. Molex is a 4-wire connector; it is sometimes also referred to as a *peripheral*. Remember, PCIe power that is 8-pin is often in the 6+2-pin configuration, whereas 8-pin CPU power is often in the 4+4-pin configuration. It's an easy way of differentiating the two.

5. **A, B, and C.** What the gamer needs to be concerned with is the maximum amount of power all the devices need collectively,

especially the GPU (or GPUs), CPU, and RAM. The PSU wattage rating refers to the maximum amount of power the PSU can output under 100 percent load capacity. By adding all the devices' power consumption together, the gamer can get a clearer picture of how powerful a power supply is needed. The gamer should also consult the PSU manufacturer's website for exact requirements. A power supply calculator on the Internet can be used to find out how many watts the gamer might need. Redundant PSUs are very common on servers and some other high-end systems but not as often on gaming systems.

6. **D.** A modular power supply is a power supply unit where the power cables are detachable. This modularity offers flexibility in cable management by allowing users to connect only the cables they need for their specific system, instead of having all cables permanently attached, as in a nonmodular power supply. A redundant power supply can help keep a system up and running in the event of a PSU failure. They are very common on servers and some other high-end systems. The purpose of dual-rail PSUs is to separate and limit the current through each wire to avoid overheating.

To-do list? More like "to-done" list! Just kidding…almost. On to the next adventure.

Chapter 19

Multifunction Devices/Printers

This chapter covers the following A+ 220-1201 exam objective:

- **3.7** — Given a scenario, deploy and configure multifunction devices/printers and settings.

A small office/home office (SOHO) multifunction device is usually a printer that can do other things, such as scan and save documents, copy documents, fax information, and more. However, for the A+ exam, the most important function of these multifunction devices is printing, so that is our main focus in this chapter.

Some printers connect via USB, but you will also encounter printers that connect directly to a network (via wires or wirelessly). Those that do connect via USB mostly connect with USB Type-B—a square-shaped connector that is usually used to connect larger peripherals to a computer.

Although there is a worldwide initiative to reduce the use of paper, printers are still an important part of the business world. Be ready to install and troubleshoot them.

ExamAlert

Objective 3.7 concentrates on the following concepts: properly unboxing a device, setup location considerations, use of appropriate drivers for a given OS, firmware, device connectivity, public/shared

devices, configuration settings, security, network scan services, and automatic document feeder (ADF)/flatbed scanners.

Setup Considerations

New printers and multifunction devices should be given some consideration prior to installation and configuration. People often say: “It’s all in the planning.” And it’s true; for most jobs, we spend more time on planning than we do on anything else. To ensure a smooth, easy printer or multifunction device installation, proper planning is imperative.

Before you purchase any equipment, it is important to define exactly what the equipment will be used for and by whom. Defining the amount of workload that you expect will help narrow down what type of printer to purchase and can save your organization money. Determine what client operating systems will be accessing the printer and what applications are being used by those clients.

For a printer, the “where” is also very important. You want a printer to be accessible to users, and you also want the printer to be able to access the network. If it is to be connected to a PC and shared, then some type of community area should be set up near the PC that it is to be connected to. However, it is more likely that a printer or a multifunction device will be connected directly to the network. If it is to be wired to the network, then it needs to be near a working RJ-45 jack. If it will connect wirelessly, then you should do a wireless site survey to see if your desired printer location will be well within the Wi-Fi area.

Remember: safety first. When working on a printer, be sure to work in a secure area, away from any other employees. Also, use proper lifting techniques (bend at the legs and avoid straining the back), and don’t move anything by yourself that requires two people. Finally, use proper safety protocols when working with tools. We’ll discuss safety in more detail in Chapter 59, “Safety Procedures.”

When unboxing a new printer, allow for some time and be sure to have your toolkit ready! A box cutter, screw gun, and work gloves are recommended.

Some printers are shipped in a protective wooden structure, and some are sent in hard foam. Either way, you will find that you have to remove and/or disassemble a lot of materials. You may want to save the box and the materials just in case the device has been damaged and needs to be returned. Be kind to the environment and dispose of any cardboard, wood planks, and plastic wrapping according to proper waste and recycling regulations. Inspect the device for any signs of damage. Remove any blue security tape, safety bars, or other securing mechanisms. Install any paper trays, platens, or other physical devices that are part of the printer. Collect and properly store any manuals, extra toner, USB cables, Ethernet cables, software, power converters, and anything else that might come with the multifunction device. And make the time to READ THE MANUAL!

ExamAlert

Exam Objective 3.7, "Given a scenario, deploy and configure multifunction devices/printers and settings," specifically wants you to be able to properly unbox the device and consider setup location.

If the multifunction device passes inspection, you can verify functionality of the device in your test environment (if you have one). Be sure to check for any protective tape that would prevent the multifunction device from printing. Sometimes this tape will be in the device or come as part of a toner cartridge or other printer consumable. Some higher-end inkjet printers require that you fill all ink cartridges yourself, using a funnel and a syringe. Depending on the printer, printer unboxing and setup can be quite a time-consuming process, so plan wisely. For example, typically, people tend to print (and printers tend to fail) between 3 and 5 p.m. on workdays, so that might not be the best time to perform new installations.

Next on the list is to update firmware for the device (if necessary) and install the proper software driver. We'll discuss firmware a little later. The driver might be software that came with the device in the form of an optical disc or a USB flash drive, or it might be software that you need to download from the Internet. Or, the device might be seen automatically by the operating system, and if you and your organization are okay with it, you

can use that generic driver. Usually, it is best to download the correct latest driver from the manufacturer's website. Either way, it's important to understand the difference between PCL, PostScript, and Microsoft Universal Printer drivers. For some printer models, there are separate drivers for each:

- **Printer Command Language (PCL) drivers:** These drivers are more commonly used. PCL is used for general office applications: printing typical documents, spreadsheets, and so on.
- **PostScript drivers:** These drivers are used for professional graphics and presentations. They are designed for higher-end printers but can be supported by lesser models as well.
- **Microsoft Universal Printer Driver (Unidrv):** While this generic driver has been in the works for several years, there is a large push in Windows 11 to utilize it or, even more, the IPP inbox class driver. This is part of Microsoft's modern print platform that uses an IPP inbox class driver along with print support apps. Basically, if your printer supports it, you won't install a third-party driver anymore. Instead, you will utilize the Windows in-house IPP class drivers.

When you install a driver, you might see whether it is PCL or PostScript within the name of the printer driver (for example, HP LaserJet 9065 PCL6 Class Driver). Be sure to use the correct driver type for your work environment.

ExamAlert

Know the differences between the printer driver types: PCL (more common, used for typical office printing) and PostScript (less common, used for professional graphics). Also know what the Unidrv is and the IPP inbox class driver.

Next, run any multifunction device/printer self-tests that are required by the manufacturer. Color laser printers, inkjet printers, and multifunction printers might need to be calibrated before use. Calibration involves aligning the

printing mechanism to the paper and verifying color output. Usually, the software that accompanies the printer guides you through this process. In some cases, you can perform these calibration tests by using the small display on the printer.

Make sure that the device can successfully print, scan, copy, and perform any other jobs that you need it to. You can do this, for example, by using the Print a Test Page feature in Windows. If the device has a scanner—flatbed, automatic document feeder (ADF), or other—be sure to test whether the system can properly scan items and send them via email, store them to a Windows Server Share via the Server Message Block (SMB) protocol, route them to the cloud, or provide any other network scanning services necessary. At this time, you can also configure additional printer settings (which we'll cover in just a bit), and network settings (such as TCP/IP) from your test environment. When the device passes all tests, install it to the destination of your choice, test one more time, and celebrate another job well done!

Note

Server Message Block (SMB) is an application-layer network protocol used primarily for providing shared access to files, printers, and ports as well as miscellaneous communications between nodes.

Firmware

Printer firmware is the embedded software that controls the printer's hardware and functions. Think of the printer firmware as a motherboard's BIOS. Updating firmware is crucial for optimal performance because it can improve print speed and image quality, and add new features like mobile printing. Furthermore, firmware updates address bugs and security vulnerabilities, enhancing the printer's overall reliability and security.

To update firmware, download the latest version from the manufacturer's website. Follow the manufacturer's instructions, which typically involve connecting the printer to your computer and using the provided update

utility. Some printers also allow firmware updates directly through their control panels; however, this would require the printer to be connected to the Internet or a USB flash drive with the firmware plugged in. Always refer to the manufacturer's documentation for specific instructions and to avoid potential damage to the printer during the update process.

Note

To update your printer's firmware, you can often use the printer's control panel, the printer's embedded web server, or the printer's update utility if available. Also, you should download the printer's firmware from the printer manufacturer's website.

Printer Configuration Settings

Printers can be configured in one of three places:

- **The operator control panel (OCP):** These small displays are most common on laser printers. They are menu-driven displays and are usually user-friendly and intuitive.
- **The printer's web interface (for a network printer):** This is often accessed through a web browser.
- **Within Windows:** This is the option we'll focus on in this section. To open a printer in Windows, use **Settings > Bluetooth & devices > Printers & scanners** or **Control Panel > Devices and Printers**. If you work with printers often, consider placing a shortcut to the printer or printers on the desktop or pin it to the taskbar. Several items can be configured in Windows, including managing print jobs, setting the priority of the printer, configuring the print spooler, and managing permissions.

Basic Printer Configuration Settings

A typical print job is simple—one printed page, printed on one side, on 8.5-by 11-inch paper in portrait mode, and at the standard 600 DPI resolution. For example, you might print a typical document (such as a résumé) this way. However, on many occasions the typical settings are not enough. There are some basic printer configuration settings you should know for the exams: duplexing, collating, orientation, tray settings, and print quality. They are generally found in the Printing preferences or Printer properties section of Windows. Let's briefly examine each one now.

Duplexing means printing on both sides of the paper, and it might simply be called "print on both sides." Some organizations require duplexing (for most print jobs) in their policies related to reducing paper consumption; however, most printers are not set to duplex by default. You might also see an option for duplexing on the main print screen when you go to perform a print job; it might be called "manual duplex."

If you print a single job, *collating* is not an issue. But when you print multiple copies of the same job, collating might become necessary. Historically, multiple copies of the same print job would print out all of page 1, then all of page 2, then all of page 3, and so on. It was up to the user to manually arrange, or collate, these pages. However, as printers became more sophisticated, they were equipped with the processing power to collate jobs, sorting them as page 1, page 2, page 3, and so on, and then moving on to the next copy of the entire job. This capability, of course, saves a lot of time for users. Some printers are set this way by default. Others have to be configured to collate.

Orientation is the method of positioning a printed page and is based on whether the page is going to be viewed vertically (portrait) or horizontally (landscape). This option can be set permanently from the Printing preferences page, and it can also be set manually when you go to print a single document. Often, it will be found in the layout section. Most documents are printed in portrait mode (such as reports or résumés created in a word processor), but sometimes you need to print a spreadsheet or a slide presentation, which is best done in landscape mode.

Now on to *tray settings*. A printer's paper tray can be physically configured to work with the standard size paper mentioned before (8.5 × 11 inches) or other sizes, such as 8.5 × 14 inches. Or you might have more narrow guides

that accept envelopes. More importantly, tray settings can be configured in the operating system. In Windows, this can also be done in Printing preferences, and most likely in the Advanced section. From there, you can modify the default paper size to be used (for instance, standard letter size, legal size, or a particular envelope type). From Advanced, you can also specify the number of copies to be made, enable a built-in stapler (if the device has one), and configure several other options.

Finally, *quality* is the print resolution, which is measured in dots per inch (DPI). A setting of 600 DPI or higher is considered to be "letter quality" and acceptable for professional documents. But you might want an even better quality (1200 or 2400 DPI), especially for a document that includes graphics. A specific DPI setting can usually be configured within the Advanced section of the Printing preferences, but it can also be configured from the Print window, often using more generic terms (such as draft, normal, and best).

Take a look at your Printing preferences, Printer properties pages, and the main Print screen (when you go to print a document) and view the configuration settings just discussed. Even if you don't have a printer, you can set up a false printer on your system by adding the printer in the Devices and Printers window in the Control Panel. Typically, we suggest selecting any one of the newer HP laser printers from the list as a fake printer. You can then access its properties just as you would on a printer that is actually installed to the computer or network.

ExamAlert

Know the following printer configuration settings: duplex, collate, orientation, tray settings, and quality.

Sharing Printers and Managing Permissions

A printer that is connected to a Windows PC must first be *shared* before users of other computers can send print jobs to it. There are two steps involved in sharing printers in Windows. First, printer sharing in general

must be enabled. To enable printer sharing in Windows, open the Network and Sharing Center. Then click the **Change advanced sharing settings** link. Click the down arrow for your network type and then select the radio button labeled **Turn on file and printer sharing**.

> **Note**
>
> You can also make a computer's devices visible when Windows is first installed. We'll discuss this and network discovery in the Windows networking section of this book.

Next, the individual printer needs to be shared. You can do this in the Sharing tab of the Printer properties window. Check the **Share This Printer** checkbox and give the printer a share name. Note that the share name does not need to be the same as the printer name. Click **OK**, and the printer should show up as shared in the Printers window.

Permissions can be set for a printer in the Security tab of the Printer properties window. Users and groups can be added in this window, and the appropriate permission can be assigned, including Print, Manage Printers, and Manage Documents. Standard users normally are assigned the Print permission, whereas administrators get all permissions, enabling them to pause the printer or cancel all documents (Manage Printers) and pause, cancel, and restart individual documents. For more information on permissions, see Chapter 45, "Windows Security Settings."

> **Note**
>
> Although printer sharing was once common before the ubiquitousness of networked printers, it is less common today. A major downside to printer sharing within Windows—meaning a USB connected printer to a desktop that is shared—is that the connected computer must always be on! With today's networked printers, most people do not use printer sharing anymore. If you need more granular control over printer permissions on a networked printer, you might need a print server.

Local vs. Network Printers

A local printer is a printer that connects directly to a computer, normally by USB. When a user works at a computer, that computer is considered to be the local computer. So, when a printer is connected to that computer, it is known as the local printer.

A network printer is a printer that connects directly to the network (usually via Ethernet) or to a print server device. Network printers are shared by more than one user on the computer network. Usually, a network printer is given an IP address and becomes yet another *host* on the network. If a printer connects directly to the network, it is usually by way of a built-in RJ-45 port on the printer, just as a computer's network card connects to the network. A print server could be a computer or a smaller black box device. Many SOHO routers offer integrated print server capabilities. With such devices, the printer connects via USB to the print server/router, and a special piece of software is installed on any client computers that want to print to that printer (that is, if the client OS doesn't automatically find the printer).

Network printing can also be accomplished wirelessly—via Wi-Fi or by Bluetooth—on most of today's printers. Remember that Wi-Fi typically has greater range than Bluetooth.

Note

Some printers separate Wi-Fi into two distinct offerings: a connection to the existing Wi-Fi or Wi-Fi Direct. Wi-Fi Direct is where the printer creates its own Wi-Fi signal that the user connects directly to. Unfortunately, this Wi-Fi signal is usually not very strong. In order of most stable to least connected to your networked printer, you will find hardwired (that is, the printer is plugged directly into an RJ-45 port); Wi-Fi (the printer is connected directly to the Wi-Fi network of your LAN); Bluetooth (this connection can have interface issues because it shares the 2.4 GHz spectrum of Wi-

Fi); and Wi-Fi Direct (this is one of the least reliable connections unless you are very close to the printer).

Then there is cloud-based printing. It is possible to harness the power of the cloud to print remotely. You might have a document you need printed to a printer in a network in another city. If your organization has implemented a cloud-based solution, you can print remotely simply by selecting the printer from a drop-down menu. We'll discuss cloud-based technologies further in Chapter 22, "Cloud Computing Concepts."

If a network printer is being controlled by Windows, you generally rely on direct TCP/IP connections. However, printers that are controlled by macOS might also make use of the networking service Bonjour and use AirPrint to automatically locate and download drivers for printers. Bonjour, which is a type of zero-configuration networking, enables automatic discovery of devices and services on a local network using industry-standard IP protocols. AirPrint is an Apple technology that helps you create full-quality printed output without the need to download or install drivers.

Basic Printer Security

Regardless of how a printer is connected and how a user connects to the printer, data privacy concerns should be addressed. An insecure printer can retain copies of information that could be accessible to anyone who has a little know-how. A printer might cache information to memory or to a print server's storage drive. This cache should be cleared at least every day and perhaps more often, depending on your organization's policy. A printer can also be audited—in Windows or elsewhere. Audit logs can show exactly who printed what, as well as when and where it was done. We say "can" because auditing normally needs to be enabled and configured properly. We'll discuss auditing briefly in Chapter 48, "Workstation Best Practices."

As an administrator, you can also consider implementing user authentication for a printer or print server, ultimately requiring a person to present credentials of some kind. For example, in Windows, you can enable Secure Print, which requires the user to enter a passcode before printing to a printer. As administrator, you set up this option beforehand within Printing

preferences by changing the printer's default job type from Normal to Secure and setting a passcode. While this approach can help to secure a printer from unauthorized use, a single static passcode is somewhat unmanageable. A more effective and more manageable approach is to rely on networkwide multifactor authentication—combining different factors such as username/password, biometrics, and an ID card or access badge that the user carries. We'll discuss authentication further in Chapter 43, "Physical Security," and Chapter 44, "Logical Security." For now, remember that personal and confidential data can be stored in many places and that those locations should be organized and secured accordingly.

ExamAlert

Printer security can be implemented through user authentication and policies, badging, and Secure Print. Audit logs can be used to see what was printed, where it was printed, and who printed it.

Cram Quiz

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

1. Where would you go in Windows to enable printer sharing?

   - ○ **A.** Network Connections
   - ○ **B.** Network and Sharing Center
   - ○ **C.** The printer's OCP
   - ○ **D.** Bonjour

2. Your printer supports printing to both sides of a piece of paper. What should you enable in the Printing preferences to print on both sides?

   - ○ **A.** Collate

- **B.** Orientation
- **C.** Duplex
- **D.** Quality

3. Which of the following address printer data privacy concerns? (Select the two best answers.)

- **A.** Implementing user authentication on the device
- **B.** Using PCL
- **C.** Using AirPrint
- **D.** Clearing the cache

4. When you are finished installing a new printer and print drivers, what should you do? (Select all that apply.)

- **A.** Calibrate the printer.
- **B.** Install the print drivers.
- **C.** Check for compatibility.
- **D.** Print a test page.

5. A technician is setting up a printer for a customer who prints professional graphics and presentations. Which print driver should be installed?

- **A.** PCL
- **B.** ADF
- **C.** SMB
- **D.** PostScript

6. A large company with several printers and Windows print servers located throughout the enterprise hires you to implement printer security measures. What industry-standard recommendations should you consider? (Select all that apply.)

- ○ **A.** Turn off all file and printer sharing
- ○ **B.** User authentication
- ○ **C.** Policies
- ○ **D.** Audit logs

Cram Quiz Answers

1. **B.** The Network and Sharing Center in Windows is the place where printer sharing is enabled. Network Connections is the window that shows the Ethernet and Wi-Fi connections that a system has to the network. Windows sharing has to be done in Windows; it can't be done from the printer's operator control panel (OCP). Bonjour is a macOS service that enables automatic discovery of devices on the LAN; it can also be run on Windows.

2. **C.** Duplexing (as it relates to printers) means printing on both sides of the paper. Collating means printing multiple copies of a document's pages in sequence instead of printing all of the copies of one page at a time. Orientation refers to how the print job is displayed on the paper; it could be portrait (vertical orientation—the default) or landscape (horizontal orientation). Quality refers to the clarity of the print job and is usually measured in dots per inch (DPI), where the higher the DPI setting, the better the quality.

3. **A and D.** Implementing user authentication for the printer or print server (PIN or password) and clearing the cache on the printer both address printer data privacy concerns. Printer Command Language (PCL) (sometimes referred to as Printer *Control* Language) is a type of driver for printers typically used for standard office application printing. AirPrint is an Apple technology for macOS and iOS that is used to automatically locate and download drivers for printers.

4. **A and D.** After the printer is installed (meaning it has been connected and the drivers have been installed), you should calibrate the printer (if necessary) and print a test page. You should

also consider updating the firmware for the printer. Before starting the installation, you should check for compatibility with operating systems, applications, and so on.

5. **D.** Know the difference between printer driver types: PostScript (less common, used for professional graphics and presentations) and PCL (more common, used for typical office printing). ADF, which stands for automatic document feeder, refers to a wonderful contraption that allows you to scan, copy, or fax multiple page documents without having to feed each page individually. SMB, which stands for Server Message Block, is a network file-sharing protocol.

6. **B, C, and D.** Printer security can be implemented through user authentication and policies, badging, and Secure Print. Audit logs can be used to see what was printed, where it was printed, and who printed it. Turning off all file and printer sharing will most likely be counterproductive for an organization that has several printers that customers need to access. As you've seen, some questions have a "throw-away" answer option. This is one of them.

Another chapter complete. Great work!

Chapter 20

Printer Maintenance

This chapter covers the following A+ 220-1201 exam objective:

- **3.8** – Given a scenario, perform appropriate printer maintenance.

Businesses use several types of printers. The most common business-oriented printer is the laser printer. Inkjet printers are more prevalent in homes due to their lower cost and their capability to print in color with excellent resolution. That said, organizations sometimes use high-end inkjet printers as well. A technician might also encounter thermal and impact printers. This chapter describes these four types of printers, how they function, and the materials they consume.

ExamAlert

Objective 3.8 focuses on the following: laser printers, inkjet printers, thermal printers, and impact printers.

Each type of printer has unique characteristics that affect how a technician installs, configures, and troubleshoots it. The most common type of printer used in businesses is the laser printer; this type of printer also happens to be the most complicated and difficult to troubleshoot. We'll discuss troubleshooting later in the book, but to be a good troubleshooter, you should know the technology well. Let's examine printer technology now.

Laser Printers

Laser printers can produce high-quality text and graphics on cut sheets of paper; printers that print to individual pieces of paper are known as *page printers*. The bulk of laser printers print in black, but there are also color laser printers (which, of course, are more expensive). Such printers are called laser printers because inside the printer is a laser beam that projects an image of the item to be printed onto an electrically charged drum; this image is later transferred to paper. Text and images that are shown on paper are created from electrically charged toner, which is a type of powder stored in a replaceable toner cartridge. The type of toner used can vary from one printer brand to the next, but they all work essentially the same way.

The laser printer drum, known also as a photoelectric or photosensitive drum, is at the center of the whole laser printing process, but there are a few other important components, including the primary corona wire, the transfer corona wire, the fuser assembly, and, of course, the laser itself. Figure 20.1 shows these components.

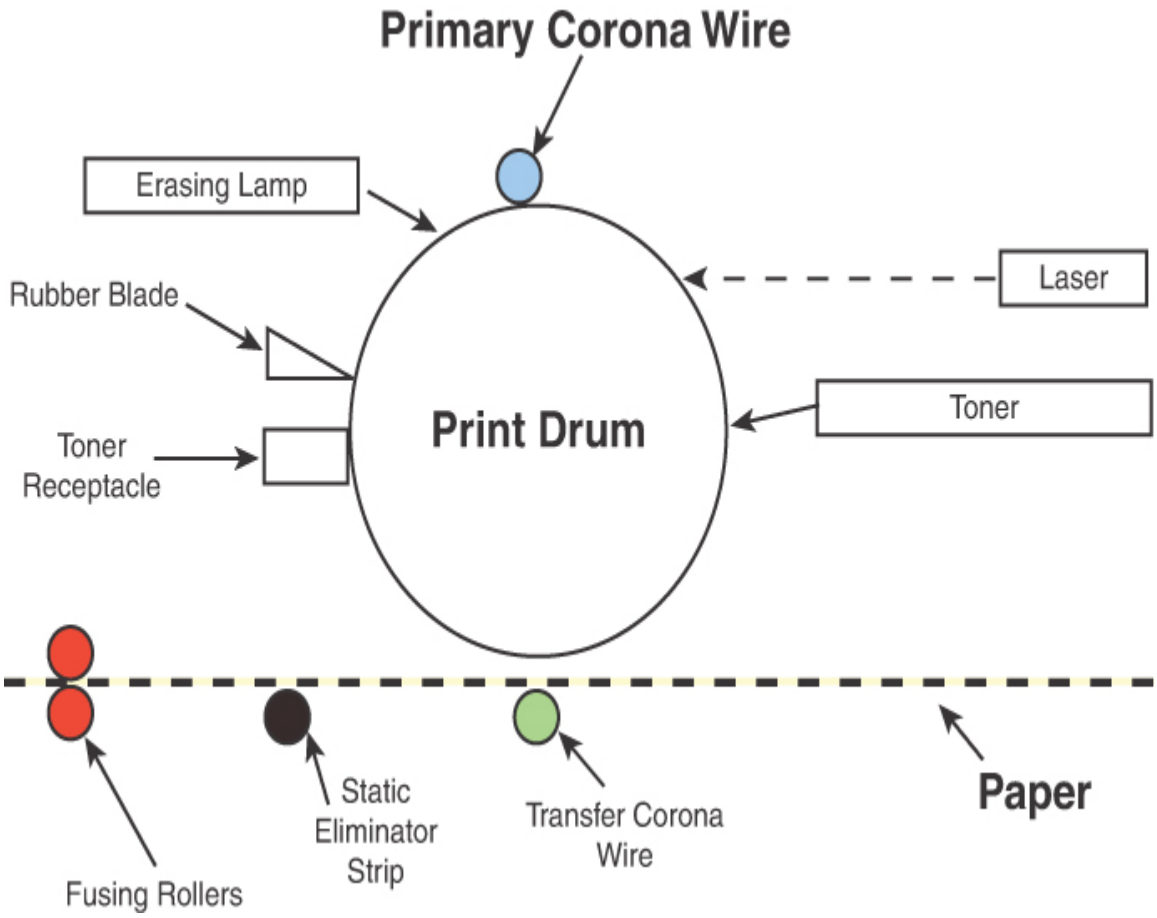


FIGURE 20.1 **Components Involved in the Laser Printing Process**

The laser printing process that a laser printer goes through is sometimes referred to as an imaging process. Knowledge of this process can help you when it comes time to troubleshoot and/or maintain a laser printer.

Note

Although the details of the laser printing process are no longer tested on the newest version of the A+ exam, 1201/1202 (it was tested for years previously), knowing this printing process is still important in order to understand maintenance of laser printers.

The typical laser printing process is as follows:

1. **Processing:** The text or image to be printed is sent to the printer, where a processor recalculates it and stores it in RAM while the printer readies itself for the ordeal of laser printing. Additional processing may be done at the local computer that initiated the printing.
2. **Charging:** In this step, a negative charge is applied to the imaging drum by the primary corona wire, which is powered by a high-voltage power supply within the printer.
3. **Exposing:** In this step, the laser is activated and "writes" to the drum as it spins. Where the laser hits the drum, it dissipates the negative charge toward the center of the drum that is grounded. The "exposed" areas of the drum now have a lesser negative charge. (By the way, the drum is also known as an imaging drum.)
4. **Developing:** The surface of the drum that was previously exposed to the laser is now applied with negatively charged toner. This toner has a higher charge than the areas of the drum that were written to.
5. **Transferring:** The toner, and therefore the text or image, is transferred to paper as the drum rolls over it. The movement of the paper is assisted by pickup rollers (for feeding the paper) and transfer rollers (to move it through the rest of the printer). Separation pads are used to make sure only one page is picked up at a time. On many laser printers, the paper slides between the drum and a positively charged corona wire (known as the transfer corona wire). The transfer corona wire applies the positive charge to the paper. Because the paper now has a positive charge, and the toner particles on the drum have a negative charge, the toner is attracted to the paper. (For voltages, opposites attract.) In many printers, the paper passes by a static elimination device (often a strip), which removes excess charge from the paper. Some color laser printers use a transfer belt to apply the various layers of colors to the paper. Some printers use a duplexing assembly that allows the paper to be printed on both sides.
6. **Fusing:** The toner is fused to the paper. The paper passes through the fuser assembly, which includes pressurized rollers and a heating element that can reach approximately 400 degrees F (or about 200 degrees C).

7. **Cleaning:** A rubber blade removes excess toner from the drum as it spins. An erasing lamp removes any leftover charge on the drum, bringing it to zero volts. The printer is now ready for another print job.

Note

Here's one example of why it's important to know the laser printing process. Your paper comes out of the laser printer, but you can wipe your finger and smudge the writing. The reason is most likely that the fuser assembly is going bad and is not able to heat up the paper to melt the plastic in the toner. Toner is composed of pigments, metal particles, plastic, and other materials. Understanding this process helps you to see how the toner could be charged: It has metal particles. The plastic allows it to be melted in the fusing step. It's also why you should not breathe in toner!

In some laser printers, the drum, laser, and primary corona wire are contained within the toner cartridge. Issues that are caused by these components can usually be fixed just by replacing the toner cartridge.

Note

Toner cartridges are replaceable; they are known as *consumables*. Whatever material it is that actually prints onto paper is usually considered a consumable, regardless of the type of printer.

Laser printers have a couple of advantages over other types of printers:

- **Speed:** A laser printer can print anywhere from 10 to 100 pages per minute (ppm), depending on the model and whether it is a color or black-and-white laser printer.
- **Print quality:** A laser printer commonly prints at 600 dots per inch (DPI), which is considered letter quality, but 1200 DPI and 2400 DPI printers are also available.

Maintenance of laser printers is vital. You should periodically inspect a laser printer and replace the toner cartridge if necessary. The toner cartridge usually slides into a compartment in the laser printer. Instructions on how to insert it accompany the cartridge. Be cautious of a couple of issues:

- Toner can potentially spill or leak out of the cartridge; it's messy and potentially hazardous. When you remove a cartridge, put it in a box or bag for transport to wherever it will be recycled. Carry it horizontally in the same position that it was taken out of the printer. Don't shake it!
- Remove the protective tape strip from the new toner cartridge. It is there to prevent toner spill, but the printer won't be able to print (and can even be damaged) if the tape is not removed.

Many laser printers have a counter that can be set to notify you when the printer has printed a particular number of pages, such as 50,000. Once the printer gets to that point, you should perform maintenance or, at the very least, carefully inspect the internals of the printer. Most laser printer manufacturers offer maintenance kits that include a variety of components, which we will discuss further in Chapter 28, "Troubleshooting Printers." If you do use the maintenance kit, reset the counter when you are finished. You will find that this is similar to the maintenance counter of a vehicle.

Another Automotive Parallel

A manufacturer will often set a relatively low number for the laser printer's counter, similar to how an automobile manufacturer will set the mileage maintenance counter to a number on the low end of the maintenance range. To put it nicely, the manufacturer is assuming the worst conditions for your printer. While this might be suitable for dirty environments, the average office printer can often last longer than the manufacturer's recommended time between maintenance. The beauty of this is that you can set the counter to a higher number if you think it is appropriate, which ultimately can save time and money for your organization. Keep a log of when printers were maintained and when failures occur. If failures occur earlier than expected on the whole, consider decreasing the counter once again.

During your maintenance of the printer, you should clean it up, including the outside cover, the trays, the bin where the cartridge sits, and possibly the rollers. After maintenance is complete, be sure to calibrate the printer. This

is usually a subroutine that is built into the printer's firmware; you might also be able to initiate it from Windows. Calibration allows you to set the horizontal and vertical printing coordinates and margins so that text and images appear clear and straight.

ExamAlert

Remember that maintenance for laser printers includes replacing toner, applying a maintenance kit, calibrating, and cleaning.

Inkjet Printers

Inkjet printers are common in small offices/home offices (SOHOs) and for personal use. They can print documents but more commonly print photographs and graphical information in color; most of the time, they connect to a computer by way of USB or Wi-Fi.

An inkjet printer works by propelling ink onto various sizes of paper. Many inkjet printers store ink in multiple ink cartridges that are consumable; they have to be replaced (or refilled) when empty. Some inkjet printers stop operating if just one of the ink cartridges is empty. Two common types of inkjet printers are the thermal inkjet and the piezoelectric inkjet:

- **Thermal inkjet printers:** These account for the bulk of consumer inkjets and are the more recognizable type of inkjet printer. To move the ink to the paper, heat is sent through the ink cartridge, forming a bubble (known as a thermal bubble) that pushes the ink onto the paper; immediately afterward, another charge of ink is readied. The reservoir of ink is within the ink cartridge; this is where the heat transfer occurs. HP and Canon develop many models of thermal inkjet printers. Don't confuse thermal inkjets with thermal printers.
- **Piezoelectric inkjet printers:** These account for the bulk of commercial inkjets. The printing processes within a piezoelectric inkjet printer and a thermal inkjet printer are similar; however, a piezo inkjet printer applies current to the ink material, causing it to change shape and size and

forcing the ink onto the paper. The reservoir of ink is in another area, outside where the current is applied. This process enables longer print head life than you get with thermal inkjet printers. Epson develops many models of piezoelectric inkjet printers. Piezoelectric inkjets can also be found in manufacturing assembly lines.

The inkjet print process is fairly simple:

1. The paper or other media is pulled or moved into position by a roller and feeder mechanism, or it's moved into position by an assembly line's conveyor belt (as with some piezoelectric inkjets).
2. The print head, located on a mechanical arm, moves across the paper, assisted by a carriage and belt system. The print head delivers black and colored ink from the ink cartridges as directed by the print driver.
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. In printers that allow for duplexing, a duplexing assembly refeeds the paper into the printer for printing on the other side.
4. When the page is complete, the paper or other media is ejected.

ExamAlert

Know that inkjet printer components include ink cartridge, print head, roller, feeder, duplexing assembly, carriage, and belt.

Maintenance of an inkjet printer is often much simpler than with a laser printer. Check the ink cartridges periodically by using the printer's onscreen display (OSD) or within Windows (if possible); you can also physically inspect them if necessary. If one or more cartridges are low, be prepared to replace them. Some higher-end inkjet printers require that you fill the cartridges using a syringe (and a funnel to protect against overspill). If you find that there is a buildup of residue on the print cartridge, clean it with a manufacturer-supplied solution or consider using a 50/50 mix of isopropyl

alcohol and water. (A box of cotton swabs would be a handy addition to your toolkit!) Inkjet printers should periodically be calibrated so that horizontal and vertical imagery lines up properly and so colors are blended appropriately. Calibration should always be done after cartridges are removed and replaced. While inspecting and maintaining an inkjet printer, look for any bits of paper that might have been caught up in the rollers or feeder and remove them. Clear any paper jams that might have occurred.

ExamAlert

Remember that inkjet printer maintenance includes cleaning print heads, replacing cartridges, calibrating, and clearing jams.

Thermal Printers

Thermal printers produce text and images by heating specially coated thermal paper. It is typical to see thermal printers used in point-of-sale (POS) systems, gas station pumps, and so on. Thermal printers consist of the following parts:

- **Thermal head:** This generates the heat and takes care of printing to the paper.
- **Platen:** This is the rubber roller that feeds the paper past the print head.
- **Spring:** This applies pressure to the print head, which brings the print head into contact with the paper.
- **Circuit board:** This controls the mechanism that moves the print head.

To print, special thermal paper is run through the feed assembly and then inserted between the thermal head and the platen. The printer sends current to the thermal head (heating element), which, in turn, generates heat. The heat activates the thermosensitive coloring layer of the thermal paper, which becomes the image.

Maintenance of a thermal printer includes inspecting the paper tray and replacing the paper, cleaning the heating element, and removing any debris

that can be left behind by the thermal printing process. It's also important to store any extra heat-sensitive paper away from direct sunlight and, of course, heat.

Note

To see why it is important to keep thermal printer paper away from the heat, try sticking a gas station receipt on your car's dash during a hot summer day. It'll turn dark! That's the thermal printer paper reacting to heat. Pretty cool, right?

ExamAlert

Thermal printers use a feed assembly, heating element, and special thermal paper. Maintenance includes replacing paper, cleaning the heat element, and removing debris.

Impact Printers

Impact printers use force to transfer ink to paper (for example, a print head striking a ribbon with paper directly behind it—similar to an old typewriter). This type of printer is somewhat deprecated, although certain environments might still use it, such as auto repair centers, warehouses, and accounting departments.

One type of impact printer, the daisy wheel, uses a wheel with many petals, each of which has a letter form (an actual letter) at the tip of the petal. These strike against the ribbon, impressing ink on the paper that is situated behind the ribbon. But by far the most common type of impact printer is the dot matrix.

Dot-matrix printers are also known as line printers because they print text one line at a time and can keep printing over a long roll of paper, as opposed to page printers, which print to cut sheets of paper. This paper can also be multipart paper. The paper is often used as carbon copy paper,

meaning the impact of the printer can cause the printer to print on the top sheet and the bottom sheet under it through the use of carbon paper in between or No Carbon Required (NCR) technology. Multipart paper is unique to impact printers because an actual physical force is applied to the paper to allow for carbon copy–type applications. Inkjet and laser printers have no physical force against the paper, so they can't use multipart paper.

The paper is fed into the printer using a tractor-feed mechanism; many dot-matrix printers use paper that has an extra perforated space with holes on each side that allow the paper to be fed into the printer. Dot-matrix printers use a matrix of pins that work together to create characters, instead of using a form letter. The print head that contains these pins strikes the ribbon, which, in turn, places the ink on the paper. Print heads come with either 9 pins or 24 pins; the 24-pin version offers better quality, known as *near letter quality (NLQ)*. Dot-matrix printers are loud and slow but are inexpensive to maintain.

Maintenance of an impact printer includes replacing the ribbon, replacing the print head, replacing the paper, and checking for bits of the perforated paper along the tractor feed mechanism and elsewhere in the printer.

ExamAlert

Know that impact printer components include the print head, ribbon, and tractor feed. Also know that impact paper is used and that maintenance includes replacing the ribbon, printhead, and paper. The use of multipart paper is also key in impact printers.

Cram Quiz

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

1. What consumable in laser printers actually makes the text and graphics on the paper?

- ○ **A.** Toner
- ○ **B.** Ink
- ○ **C.** Thermal paper
- ○ **D.** Ribbon

2. What types of printers should include calibration as a maintenance step? (Select all that apply.)

- ○ **A.** Laser
- ○ **B.** Inkjet
- ○ **C.** Thermal
- ○ **D.** Impact

3. What type of printer uses special heat-sensitive paper in lieu of traditional ink?

- ○ **A.** Laser
- ○ **B.** Inkjet
- ○ **C.** Thermal
- ○ **D.** Impact

4. What type of printer can use multipart paper?

- ○ **A.** Laser
- ○ **B.** Inkjet
- ○ **C.** Thermal
- ○ **D.** Impact

5. You are preparing to perform laser printer maintenance. Which of the following should you consider?

- ○ **A.** Replace toner, apply maintenance kit, calibrate, and clean.
- ○ **B.** Replace paper, clean heating element, and remove debris.

- **C.** Replace ribbon, replace print head, and replace paper.
- **D.** Clean printheads, replace cartridges, calibrate, and clear jams.

Cram Quiz Answers

1. **A.** Toner is a mix of plastic, silica, and organic compounds. This concoction is what fuses to the paper during the fusing step and produces the text and graphics on the paper. Ink is typically associated with inkjet printers. Thermal paper is heat-sensitive paper and is used with thermal printers, while a ribbon contains the ink that an impact printer strikes to produce the text and graphics.

2. **A and B.** Both laser and inkjet printers should have calibration done after consumables are replaced. This helps to make sure the alignment of the X- and Y-axes is correct. Thermal and impact printers do not need this step.

3. **C.** Thermal printers use a thermal head that heats up and forms text on heat-sensitive paper. Laser and inkjet use regular single-page paper. Impact printers use continuous feed paper or multipart paper.

4. **D.** Multipart paper is a type of paper that is used to create multiple copies of a document simultaneously. Because impact printers have actual pins that strike the paper through the inked ribbon, they can utilize the carbon/carbonless features of multipart paper. Inkjet and laser printers use no physical force striking the paper, so they won't activate the dye transfer of multipart paper. This is also true of thermal printers because they merely heat up special paper.

5. **A.** Laser printer maintenance includes replacing toner, applying a maintenance kit, calibrating, and cleaning. Thermal printer maintenance includes replacing paper, cleaning the heating element, and removing debris. Impact printer maintenance includes replacing the ribbon, replacing the printhead, and replacing paper. Inkjet printer maintenance includes cleaning the print head, replacing cartridges, calibrating, and clearing jams.

Time flies when you're having fun! That closes out Domain 3.0: Hardware. Woo-hoo! Be sure to review the chapters in this domain before continuing.

"The answer to the great question...of Life, the Universe and Everything...is...forty-two."—Douglas Adams, *The Hitchhiker's Guide to the Galaxy*

Core 1 (220-1201)

Domain 4.0: Virtualization and Cloud Computing

CHAPTER 21 Virtualization Concepts

CHAPTER 22 Cloud Computing Concepts

Chapter 21

Virtualization Concepts

This chapter covers the following A+ 220-1201 exam objective:

- **4.1** – Explain virtualization concepts.

Virtualization is the creation of a virtual entity, as opposed to a true or actual entity. The most common type of entity created through virtualization is the virtual machine—usually housing an operating system.

In this chapter, we'll discuss the types of virtualization, identify their purposes, and define their requirements. We'll also examine containers and the types of hypervisors you should know for the exam. However, we will focus mostly on client-side virtualization in this chapter.

ExamAlert

Objective 4.1 concentrates on the following concepts: the purpose of virtual machines, requirements, desktop virtualization, containers, and hypervisors.

Purpose of Virtual Machines

Many types of virtualization exist, from network and storage to hardware and software. The CompTIA A+ exam focuses mostly on virtual machine

(VM) software. The VMs created by this software run operating systems or individual applications. A virtual operating system—also known as a guest—is designed to run inside a real OS. So, the beauty of a VM is that you can run multiple various operating systems simultaneously from just one computer. This capability has great advantages for programmers, developers, and system administrators, and it can facilitate an excellent testing environment. VMs can also be used to run legacy software and operating systems such as Windows 7 or older. Today, many VMs are also used in live production environments as servers (and possibly as clients).

Desktop Virtualization

Desktop virtualization, by definition, separates the desktop environment from any application software. However, there is a bit of a gray area when it comes to virtual desktop technology, and there is also some overlap, so be ready to accept different terminology from different vendors. The virtual desktop can act as part of a user's computing system, or it can be the only place where users perform their work. It can be as simple as a browser window with a single application inside it, or it can include everything from a virtual OS to virtual hardware such as a virtual network interface card (virtual NIC) on down to all the required individual virtual applications.

When multiple virtual desktops for multiple users are hosted by a service (either in the cloud or on-premises), this is referred to as a *virtual desktop infrastructure (VDI)*. The idea with VDI is that users can use any system to connect to their virtual desktop and applications via a browser window or third-party application. Several companies offer virtual desktops and VDI, including Citrix (Managed Desktops), VMware (Horizon Cloud), Microsoft (Windows Virtual Desktop), and AWS (Workspaces). Some of these are offered solely in the cloud, and others can be implemented on-premises. Most desktop virtualization technology is dependent on *Platform as a Service (PaaS)*.

Note

Platform as a Service (PaaS) is a cloud computing service model in which the provider supplies the operating system and the user is

responsible for the stack above it. We'll cover cloud computing service models in more detail in Chapter 22, "Cloud Computing Concepts."

ExamAlert

Remember that virtual desktop infrastructure (VDI) is a server-based virtualization technology that hosts and manages the virtual desktops. Functions include creating the desktop images, managing the desktops on the servers, and providing client network access for the desktop.

Know this: Anything can be run virtually—from individual apps (in what is known as application virtualization) to complete operating systems—and in some cases, it can be hard to tell what's virtual and what's not. Today, anything that runs an OS virtually is generally referred to as a virtual machine, and that's what we will be focusing on the most during the rest of this chapter.

Virtualization vs. Emulation

The terms *virtualization* and *emulation* are often used interchangeably, but they are not quite the same. There are a couple of main differences between a virtual machine and an emulator. First, a VM is designed to create an isolated environment, whereas an emulator is designed to reproduce the behavior of some type of hardware and/or firmware. Second, VMs make use of a CPU's built-in virtualization capabilities, but emulators imitate hardware without relying on the CPU; they can even be coded to mimic an entire processor that is wholly different from the one in the programmer's computer. An example of an emulator is a small office/home office (SOHO) router's firmware that you can access online for testing purposes. It doesn't really control a SOHO router, and it has no connectivity to anything. Another example is an emulated BIOS/UEFI that some motherboard manufacturers offer on their websites for testing purposes. An example of a VM is a virtualized Windows operating system that runs within your computer's main operating system, makes use of the hardware of that computer, and can connect to other systems internally or externally. Developing an emulator usually requires a programmer, whereas any tech can create a VM. Another way to differentiate between the two is that an emulator does not use a hypervisor, but a VM does.

Note

Virtualization is a technology that uses software to create virtual versions of physical machines, such as servers, storage devices, networks, and operating systems. The software simulates the hardware's functionality to run multiple virtual machines on a single physical machine.

Hypervisors

Have you ever wished that you had another two or three extra computers lying around so that you could test multiple versions of Windows, Linux, and possibly a Windows Server OS all at the same time? Well, with virtual software, you can do this by creating a virtual machine for each OS.

A virtualization system uses what is known as a *hypervisor*, which allows multiple virtual operating systems (guests) to run at the same time on a single computer (host). But there are two different kinds:

- **Type 1: Native:** This means that the hypervisor runs directly on the host computer's hardware. Because of this, it is also known as *bare metal*. Examples of type 1 hypervisors include VMware ESXi, Microsoft Hyper-V (for Windows Server), and KVM.
- **Type 2: Hosted:** This means that the hypervisor runs within (or "on top of") the operating system. Guest operating systems run within the hypervisor. Guests are one level removed from the hardware, and therefore a type 2 hypervisor runs less efficiently than a type 1 hypervisor. Examples of this type include VirtualBox, VMware Workstation, and Hyper-V for Windows.

Remember that a type 1 hypervisor is faster than a type 2 hypervisor, but it requires a proper server, requires more knowledgeable administration, and is sometimes costlier. The A+ exams focus on both types of hypervisors and the virtualization software that utilizes that technology. These can be run on typical client operating systems such as Windows. Table 21.1 reviews the two types of hypervisors.

TABLE 21.1 **Hypervisor Types**

Type	Description	Examples
Type 1 (native or bare metal)	The hypervisor runs directly on the host computer's hardware.	VMware ESXi, Microsoft Hyper-V (Windows Server), KVM
Type 2 (hosted)	The hypervisor runs within the operating system. Guest VMs are one step removed from the hardware.	VMware Workstation, VirtualBox, Hyper-V for Windows clients

ExamAlert

Know the difference between type 1 and type 2 hypervisors!

Examples of Virtual Machine Software

Let's look at a couple of examples of virtualization software that make use of a type 2 hypervisor on a typical Windows client computer. First on the list is Microsoft Hyper-V. For this to work, you must first enable virtualization in the BIOS/UEFI (see Chapter 16, "Motherboards and Add-on Cards"). Then, you need to turn on Hyper-V in Windows Features, as shown in Figure 21.1. You can get to Windows Features by navigating to **Control Panel > All Control Panel Items > Programs and Features** and clicking the **Turn Windows features on or off** link, or simply search for "Turn Windows features" with the search tool to go directly there.

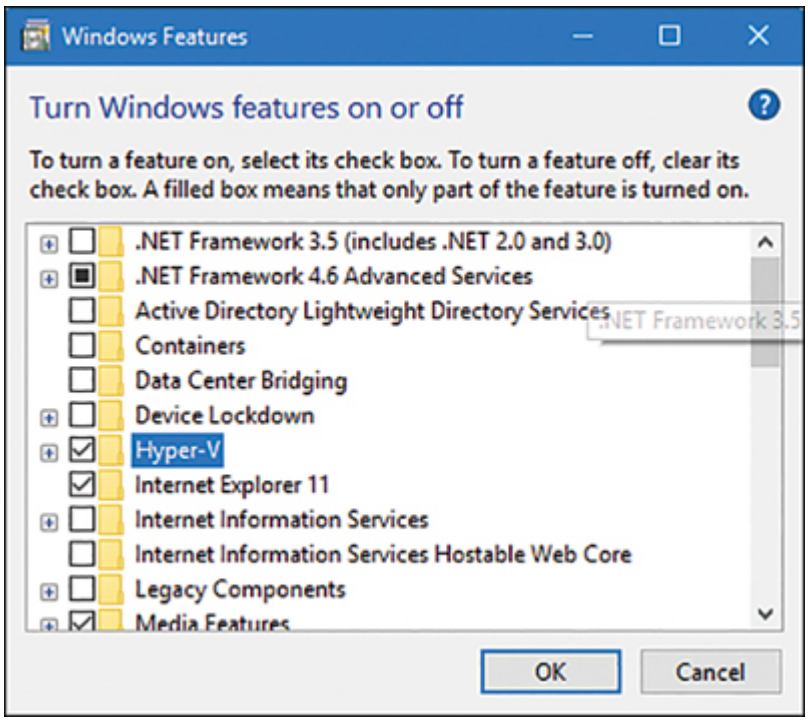


FIGURE 21.1 **Hyper-V Enabled in Windows Features on a Windows System**

Enabling Hyper-V requires a system restart, and it works only on certain editions of Windows. For example, it works on Windows Pro and Enterprise editions but not Windows Home editions. If you are not sure whether Hyper-V will be compatible with your system, you can open the Command Prompt or the PowerShell and type **systeminfo**. At the bottom of the results, you will see the Hyper-V Requirements section and details.

Attention, PowerShell Users!

Skip the GUI! Enable Hyper-V directly within PowerShell (run as administrator) with the following command:

```
Enable-WindowsOptionalFeature -Online -FeatureName
Microsoft-Hyper-V -All
```

To turn it off, change **Enable** to **Disable** and omit the **-All**.

After you have performed those actions, you can create VMs in Hyper-V Manager. During the creation process, you will be prompted to create a virtual hard drive and install an operating system, which you will need to obtain in .iso format or in a virtual format. The virtual hardware for the VM can be configured in the Settings section. The networking connections can be configured in the Virtual Switch Manager. Figure 21.2 shows an example of a VM that was installed to Hyper-V Manager.

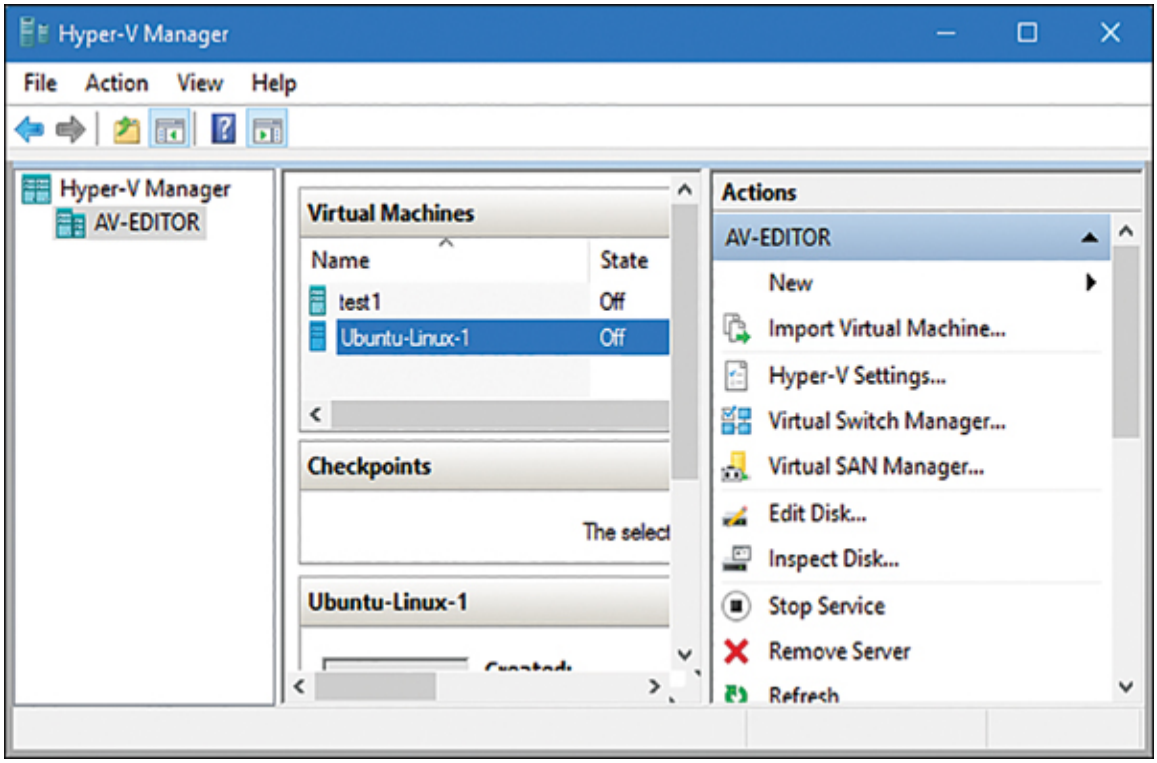


FIGURE 21.2 **An Ubuntu Linux Virtual Machine Created in Hyper-V Manager**

Another popular type 2 hypervisor is VMware Workstation. For an example of that, see Figure 21.3. Note that it has a variety of virtual machines inside, such as Windows 10 Pro (running), Windows Server, and Ubuntu Linux.

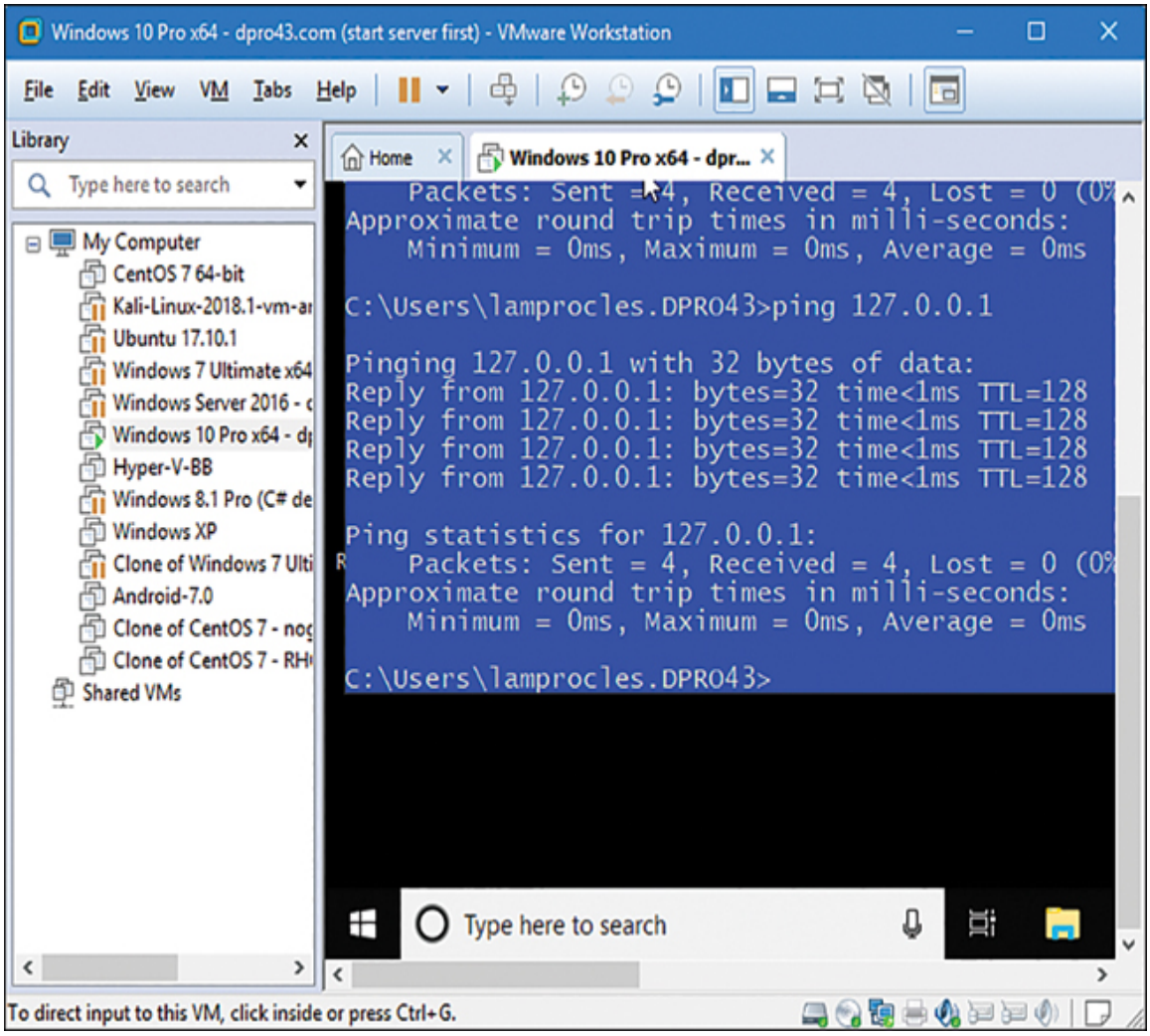


FIGURE 21.3 **VMware Workstation**

The concept is essentially the same across virtualization vendors, but of course, navigation and names will be slightly different. One difference is the type of file extensions used. For example, VMware uses the .vmdk file extension for the virtual hard disk of a virtual machine, whereas Hyper-V uses the .vhdx extension. The two types of VMs are not compatible by default, meaning you can't run a VM from VMware in Hyper-V or vice versa.

A third well-liked offering is Oracle VirtualBox, which provides a free and easy way to test operating systems. Admins have been using it for years and years. Figure 21.4 shows an example of a VM that was created in VirtualBox. The default virtual storage file extension for VirtualBox VMs is

.vdi; however, you can also use .vmdk for compatibility with VMware. That is the extension that was chosen for the VM shown in Figure 21.4.

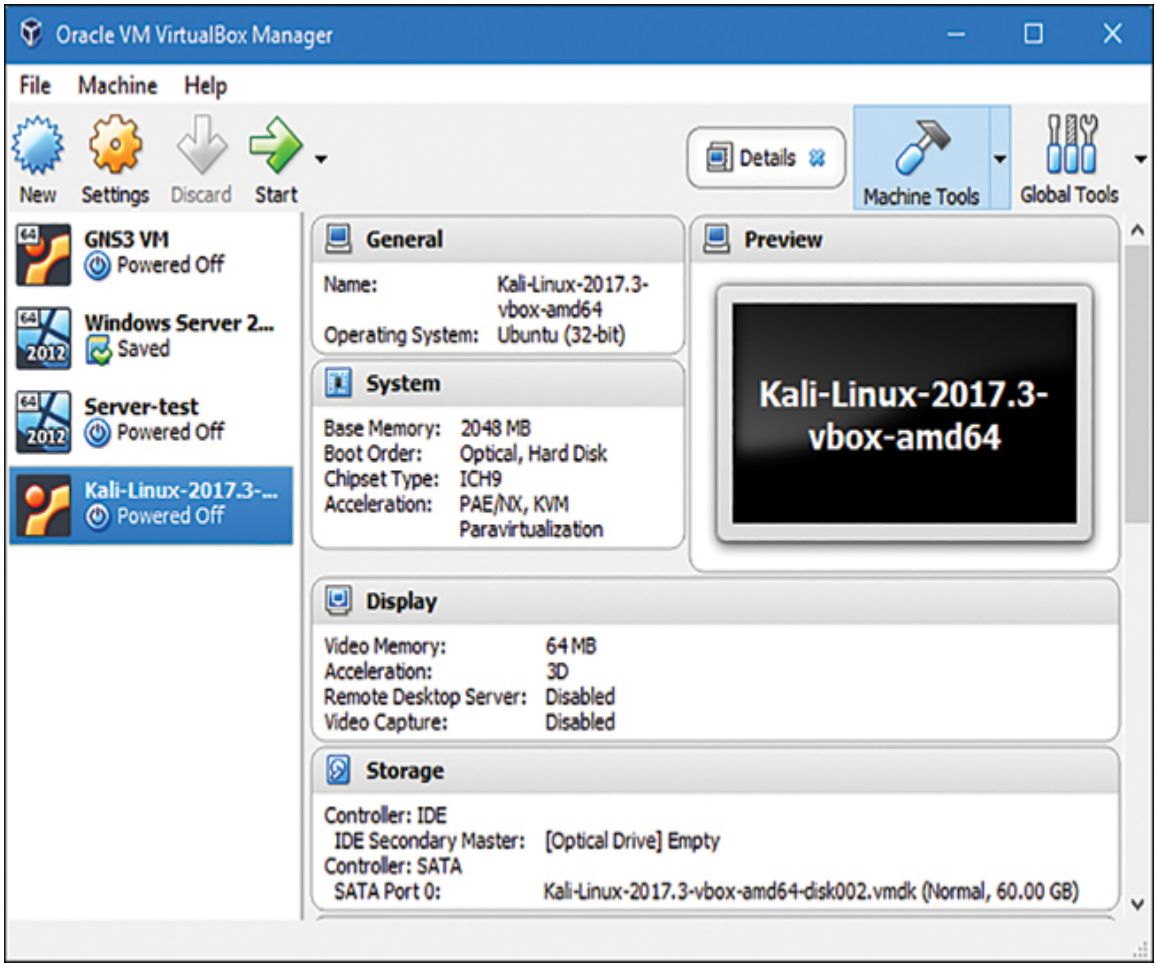


FIGURE 21.4 **A Kali Linux Virtual Machine Created in VirtualBox**

Note

For a video demonstration on how to install VirtualBox in Windows, see https://www.geeksforgeeks.org/how-to-install-virtualbox-on-windows.

If at all possible, try out the different types of virtualization software so that you can learn more about them and support customers who may have different products.

One more thing, and we can't stress this enough: Be sure to update your virtualization software! Bugs and vulnerabilities are constantly being found in all the major vendors' software, and updates are frequently available. Get in the habit of checking for updates!

Virtual Machine Requirements

There are a couple of requirements that you have to consider when installing a virtual machine: virtualization hosting software requirements and virtual machine requirements. Generally, most computers built in the past five years can run the latest version of virtualization software—as long as the BIOS/UEFI can support virtualization—but the VMs themselves can be very power hungry, especially with newer operating systems. For example, to install an operating system as a virtual machine, you will need to assign virtual resources—CPU, RAM, network connection, storage drive, and so on.

The CPU is the first of the virtual resources. The VM might run okay with one virtual processor (a single core, which is the default), but multiple cores are often recommended. Some virtualization platforms go by threads instead of cores. So, if you have a 6-core CPU, it will have 12 threads available. Be aware of this when selecting the virtual CPU usage for a VM. Also, be careful not to use more than 50 percent of the actual host's CPU power for a VM; doing so can cause the VM and the host to compete for the CPU. Ultimately, the amount of CPU resources you allocate will be dictated by the minimum requirements of the operating system you plan to install. And know this: Sometimes the minimum requirements for a VM installation can be higher than for a physical installation.

Commonly, a VM requires 2 GB to 4 GB of RAM, but again, more is suggested. The setting you select will depend on the physical hardware of the host. If you have a computer that is five years old with limited cores and RAM, then assigning more virtual RAM to the VM will simply bog down the main host system even more. But the beauty of the VM is that you can change the virtual resources at any time, as long as you shut down the VM first. You can test, tweak, and find the right balance.

Note

The Hyper-V role can be enabled on the following versions of Windows 11: Windows 11 Enterprise and Windows 11 Pro.

Hyper-V is available only in the 64-bit version of these operating systems. To enable Hyper-V on Windows 11, your system must also meet the following requirements:

- A 64-bit processor with Second Level Address Translation (SLAT)
- A minimum of 4 GB of RAM
- BIOS/UEFI-level hardware virtualization support

To learn more about Hyper-V Windows requirements, visit https://learn.microsoft.com/en-us/virtualization/hyper-v-on-windows/reference/hyper-v-requirements.

Network Requirements

For the network connection, you generally have three or four options. The following example is based on VMware:

- **Bridged networking:** This option gives the VM (also known as the guest) direct access to the hosting computer's network connection. It allows external access, but in this case, the VM must have its own IP address on the external IP network. Because of the direct connectivity to the external network, this can be a security concern. In most cases, some type of NAT is preferred.
- **Network Address Translation (NAT):** Often the default, this option gives the guest access to the external network, but by using NAT, the guest gets a separate IP address on a private network.
- **Host-only networking:** This option creates a private virtual network for the guests, and they can communicate with each other but not with the external network.

- **No networking:** This option disables networking for the VM altogether, which might be required for users who are working on confidential systems, testbeds, applications, and so on.

ExamAlert

Know the virtualization network connection options.

Networking is usually required for VMs. Just remember that any network connection (mapped network drive, browsing connection, and so on) can be a security concern. If there is a connection from the VM to the hosting OS, and the VM has a vulnerability that is exploited, the exploit could carry over to the host. Be ready to monitor for and disable any unused or unnecessary network connections between VMs and between the VMs and the host. Conversely, the host should be updated and secured vigilantly. If the hosting OS fails, then all guest VMs will go offline immediately.

ExamAlert

Because VM network connections can be security vulnerabilities, you will need to monitor and disable them as necessary, and in some cases you will have to disable networking altogether.

Different providers use different names for the types of networking connections, but they are similar; for example, Hyper-V uses external, internal, and private. You have the ability to create and configure virtual switches for the various VMs and to allow or disallow connectivity between them (and between the VMs and the host) as you see fit. This process can get pretty complex, so it is wise to create network documentation that diagrams the various virtual machines and switches using software such as Microsoft Visio.

Storage Requirements

You can select different virtual storage drive connections such as SCSI, SSD, SATA, and IDE that emulate those technologies. Then you choose the size of virtual drive (for instance, 60 GB). A VM can be configured to use all of that space right from the beginning; this is a static configuration. Or it can be configured to use only what it needs; this is a dynamic configuration. The size of the virtual drive can grow, as needed, up to the maximum that was selected. This ultimately saves space on the host computer's drive.

Security Requirements

We have mentioned security concerns a couple of times already. Take a look at Table 21.2 for some additional pointers and a review of basic virtualization security. The first bullet says to configure the hosting computer securely. This is easily said but not so easily done! We'll discuss system security further in Chapter 45, "Windows Security Settings," and Chapter 48, "Workstation Best Practices."

TABLE 21.2 **Virtualization Security Basics**

Best Practice	Methods
Updates	▶ Configure the hosting computer securely. ▶ Update the virtualization platform software. ▶ Update the VM operating system and applications. ▶ Monitor common vulnerabilities and exposures (CVEs).*
Disable unnecessary hardware in the VM's settings	▶ USB ports ▶ Optical drives ▶ Peripherals (mouse, tablet, and so on) ▶ Extra storage drives and NICs

Best Practice	Methods
Secure networking connections	▶ Use appropriate network connectivity for VMs (such as NAT). Disable bridged connections if not used. ▶ Remove unnecessary network shares between VMs and the host, as well as between VMs. ▶ Consider secure VLANs.
Other security precautions	▶ Configure the virtual BIOS/UEFI boot priority for the hard drive first. ▶ Limit the resources (CPU and RAM) used by a VM. ▶ Protect and monitor VM files with permissions, logging, and auditing. ▶ Secure VM files with encryption and digital signing. ▶ Preserve the entire state of VMs with snapshots. ▶ Use cross-platform virtualization management tools.

*Common vulnerabilities and exposures (CVEs) are a publicly available list of known cybersecurity vulnerabilities. To learn more, see https://cve.mitre.org/.

Cross-Platform Virtualization

Some organizations run multiple virtualization platforms. Studies show that an average company runs two different type 1 hypervisors in its data centers and at least two type 2 hypervisors across its various client systems. For example, some developers might work with VirtualBox, and others might work with VMware Workstation, while a third group might use Hyper-V.

Running these different platforms can lead to some problems, including application instability (when moving from one virtualization platform to the next) and incompatibilities between the virtualization systems on a resource level. It can also lead to VM sprawl, where the number of virtual machines on all systems goes beyond the control of the system owner or the administrator of the network.

Many organizations have some sort of cross-platform virtualization, so how do they make it run more smoothly? For one thing, they can attempt to use common file formats whenever possible. For example, let's say one developer is using VMware Workstation and another developer is using VirtualBox. The first developer saves VMs with the default file extension (.vmdk). The second developer could make sure that the VirtualBox VM is configured to use the same type of extension (instead of the default VirtualBox extension). To avoid application instability, both developers should have VMs that run the same OS at the same version level.

While those are good short-term options, a couple of long-term options are to have all developers use the cloud or to work in a container-based system. However, in a working environment, using these long-term options is easier said than done due to cost, decision-making processes, and administrative overhead.

VM sprawl can be reduced by consolidating the hypervisors used as much as possible, creating an organized library of VM images (possibly with third-party software), and using a virtual machine life-cycle management tool that can enforce how VMs are created, used, deployed, and archived.

In general, when it comes to working with virtual machines, proper type 1 hypervisors are the better option if at all possible. When these are combined with virtualization management software packages such as Microsoft System Center Virtual Machine Manager, Azure Arc-enabled System Center Virtual Machine Manager, or VMware vCenter Server, an organization can better organize and secure its virtual machines.

Note

Virtual machine sprawl occurs when the number of VMs expands beyond the manageable control of the administrator and they are omitted from change/life-cycle management processes. VM sprawl can be prevented by implementing policies, automated reporting, and life-cycle management tools. VM escape happens when the virtual machine breaks out of or escapes from isolation and can interact with the host operating system. The best ways to prevent VM escape are to keep up to date on VM CVEs and immediately apply patches and contact cloud service providers to inquire about patching affected products.

Containers and Sandboxes

Now let's discuss some more virtualization topics, including containers and sandboxes. You don't have to always run a full-blown virtual machine with a complete operating system and all the virtualized hardware. In some cases, especially for programming/developing, and even in production, you will want something much more trimmed down and simplified. Let's look at a couple of examples.

OS-Level Virtualization (Containers)

One type of operating system–level virtualization, known as *containerization*, allows you to run multiple isolated systems on a single OS kernel.

Now, a statement like that can cause some confusion, so let's put it into context and simplify it somewhat. A *container* is much simpler than a full virtual machine. First, it requires only a basic OS kernel. Second, it doesn't require much in the way of virtual hardware. Finally, in most container systems, you can run multiple containers on top of a single OS. Another important difference between a container and a virtual machine is usage. As mentioned previously, a virtual machine is used to run an entire operating system. A container is typically used to run a single application (and, less commonly, a couple of applications). Out of the box, container technology creates excellent isolation between applications.

Examples of container technology include Docker, Podman, and LXC. Docker is the most common of these. A Docker container is an open-source software development platform. Its main benefit is that it packages applications in containers, allowing them to be portable from one system to another. A system such as Docker has to be installed on the host computer. After it is installed, you can create containers and download basic OS images that you can house in those containers. Ultimately, if a container is configured properly, it can be far less resource intensive than a virtual machine.

Note

Docker as a whole is a group of Platform as a Service (PaaS) products.

Let's compare two scenarios: one that requires a virtual machine and one that works just fine with a container.

In the first scenario, imagine that you need to run a server that will have multiple services running, including DHCP, DNS, a file server, and some monitoring software for those services. In this case, it would usually be better to have a full virtual machine, where you have access to a complete set of virtualized hardware and perform a complete installation of an operating system (such as Windows Server or Linux). When you are running multiple services that can be taxing, a more powerful virtual machine with a complete OS is usually the best solution.

In the second scenario, say that you need to run a single web server with an individual web application that is being developed in-house. In this case, a container would be a better option because you don't necessarily need a lot of power, access to virtualized hardware, or even a complete operating system. The beauty of containers is that you can download premade OS kernels for them. These kernels are basic, take up little space, and use little processing and RAM power. They are simplified versions of operating systems.

In addition, containers can be run on just about any system, by anyone, and they are portable: You can move them to any other computer running the same containerization system. Finally, you can have one app that is being developed in one container, and another in a separate container, and so on, but they can all use the same OS kernel (or separate ones if you wish). This can be great for development, testing, training, and other purposes.

By now you should see the potential of containers, and you should understand their relevance for the field. We highly recommend that you investigate container technology more (Docker in particular) and test it for yourself to see how it works.

ExamAlert

Containers are technologies that allow the packaging and isolation of applications with their entire runtime environment; this includes all of the files necessary to run. Therefore, you can easily move the contained application between environments—for example, development, test, and production—while retaining full functionality.

Sandboxes

The term *sandbox* can be applied to software development and to computer security, and in both cases, virtualization can be involved. The term is somewhat open-ended, but in this section, we'll refer to it mostly from a software development perspective.

A sandbox can be any environment created for development, testing, or training that is isolated from any production servers and isolated from the rest of the operating system that the sandbox is running on.

Before we proceed any further, it's important to understand the difference between production and development. By *production server*, we mean any server that is distributing applications and/or files to customers. Such servers are considered to be "live" and are critical to an organization's operations. A *development server* is a server that is used during the process

of developing, programming, and testing software; it is not normally used by customers. To be safe, a development server shouldn't even be on the same network as a production server. Sandboxes should be run in a development environment, not in a production environment.

A sandbox could be run on a physical server, in a virtual machine, as a container, or as specially programmed software, depending on the scope of the project and the size and budget of the organization.

Many sandboxes are temporary. Every time a sandbox runs, it is pristine, meaning that it runs clean and new; any programming or testing that was done previously in the sandbox is discarded. You could say that the sand is smoothed out and the toys are removed after each use. This allows for a consistent environment every time a sandbox runs.

Let's consider an example. A developer designs a web-based application called *Asteroid Blaster*. It's a game where—yup, you guessed it—you blast asteroids to smithereens. After a time, the developer decides that the game is lacking in real physics and attempts to apply additional mathematics to make the game more realistic. However, the developer doesn't want to test it out on the live server where the website is hosted. So, the developer uses a sandbox. The developer can make slight modifications to the code, test them in the sandbox, and repeat until the outcome is what the developer wants. The developer could achieve this within third-party sandboxing software, a custom sandbox, a container, or a VM. As you can see, there are several options when it comes to sandboxing. The key is to make sure that the code or program is isolated from the rest of the system in a secure manner.

ExamAlert

Sandboxing allows programs and processes to be run in an isolated environment, to limit access to files and the host system.

Revision Control

When multiple developers are working on a project, you need to incorporate revision control software. This way, the group of developers can keep a "stable" set of source code somewhere that is accessible to everyone involved. If one developer wants to propose a change, that person can download ("check out," or "pull") a copy of the source code. That developer would then make the necessary changes to the code within their own sandbox. After testing is complete, the code can be merged back ("checked in," or "pushed") to the original source code. Ideally, it would be placed in a "testing" source code section for other developers to look at first before it is merged with the stable code. One common example of revision control software is Git, which tracks all changes made to the code. Developers can upload and download the code to and from a platform such as GitHub or GitLab and work in their own local sandboxes to keep their code isolated and tracked.

Also, for security purposes, a specific area of an operating system can be sandboxed (that is, isolated from the rest of the system) to allow the application to be isolated so that any malicious code can't travel from the application to the rest of the system. There are a variety of ways to do this in Windows and especially Linux systems. (Some sandboxing technologies are installed and running by default in Linux, such as SELinux and AppArmor.) In fact, just about anything can be sandboxed. So, as you can see, the term *sandbox* is somewhat ambiguous unless you know what the technician or developer is trying to accomplish. Ultimately, the best way to really understand a topic like this is to try it for yourself.

Challenge: Use a Sandbox

Try working with one or more sandboxes that are freely available on the Internet. Do a search for what you want to learn more about. Try any of the following Internet searches to locate a suitable sandbox: "Bash sandbox," "C++ sandbox," or "Linux sandbox" (for an entire Linux operating system). Make some changes to the code or system and then refresh the sandbox. You should see that it reverts back to its original state.

Note

In Windows 11, the Windows Sandbox feature enables you to create a lightweight virtualization environment to install and test untrusted programs or websites without altering or affecting the main setup. To learn more about the Windows Sandbox feature, visit https://www.windowscentral.com/software-apps/windows-11/how-

to-use-windows-sandbox-on-windows-11 or https://learn.microsoft.com/en-us/windows/security/application-security/application-isolation/windows-sandbox/windows-sandbox-overview.

Cram Quiz

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

1. Of the following listed technologies, which one should you select if you want to run an instance of Ubuntu Linux within your Windows 10/11 Pro workstation?

   - ○ **A.** Type 1
   - ○ **B.** Type 2
   - ○ **C.** Bare metal
   - ○ **D.** Cross-platform virtualization

2. Which of the following is the greatest risk with a virtual computer?

   - ○ **A.** If a virtual computer fails, all other virtual computers immediately go offline.
   - ○ **B.** If a virtual computer fails, the physical server goes offline.
   - ○ **C.** If the physical server fails, all other physical servers immediately go offline.
   - ○ **D.** If the physical server fails, all the virtual computers immediately go offline.

3. Which of the following file extensions is used by VMware by default?

   - ○ **A.** .vmdk

- **B.** .vdi
- **C.** .vhdx
- **D.** VT-x

4. Which of the following network connection types should be used to allow for connectivity to the external network but keep the VMs on a separate IP network?

- **A.** Bridged
- **B.** NAT
- **C.** Private
- **D.** No networking

5. A customer running Windows 10/11 Pro wishes to install a Linux VM in Hyper-V Manager. Which of the following requirements *must* be met in order for this to happen? (Select all that apply.)

- **A.** Update and secure the host system.
- **B.** Ensure that virtualization is enabled in the BIOS/UEFI.
- **C.** Ensure that Hyper-V is turned on in Windows Features.
- **D.** Restart the system.

6. A developer wants to test a custom web-based application in an isolated environment. Which of the following should be used?

- **A.** Sandbox
- **B.** Virtual machine
- **C.** NAT
- **D.** VirtualBox

7. Which statement best describes VDI?

- **A.** It occurs when the number of VMs expands beyond the manageable control of the administrator, and they are

omitted from change/life-cycle management processes.

- ○ **B.** They are technologies that allow the packaging and isolation of applications with their entire runtime environment.
- ○ **C.** It gives the VM (also known as the guest) direct access to the hosting computer's network connection.
- ○ **D.** It is the server-based virtualization technology that hosts and manages the virtual desktops.

Cram Quiz Answers

1. **B.** You would need to run virtualization software that includes a type 2 hypervisor such as Windows 10/11 Hyper-V, VMware Workstation, or VirtualBox. Type 1 hypervisors are used on servers; they are also known as *bare metal* because they allow virtual machines to access the computer hardware directly. With cross-platform virtualization, an organization uses multiple virtualization programs, such as VirtualBox and Hyper-V.

2. **D.** The biggest risk of running a virtual computer is that it will go offline immediately if the server that it is housed on fails. All other virtual computers on that particular server will also go offline immediately.

3. **A.** VMware uses the .vmdk file extension for the virtual hard drive file. VirtualBox uses .vdi by default (although it can use others). Hyper-V uses .vhdx. VT-x is the Intel virtualization extension that is incorporated into Intel-based systems and must be enabled in the BIOS/UEFI for virtualization software to work.

4. **B.** Network Address Translation (NAT)–based network connections are the most common default. NAT allows the VMs to have their own IP network but still connect to the external network and make use of the Internet. This is the same principle behind NAT used in a SOHO network. Bridged means that the VMs have access to the external network, but they must use IP addresses

from that external network. Private means that multiple VMs within a host can communicate with each other but not beyond the host. The no networking option disables any type of networking connectivity for the VM in question.

5. **B, C, and D.** Virtualization must be enabled in the BIOS/UEFI. Then, Hyper-V needs to be turned on in Windows Features. Finally, the system needs to be restarted. Updating and securing the host system are recommended but are not required.

6. **A.** The developer should run the custom application in a sandbox. A sandbox is designed to run code in an isolated way. It could possibly be done in a virtual machine, but the virtual machine is not secure by default; a container would usually be a better option. NAT stands for Network Address Translation, and while the sandbox could be located in a NAT network, that in itself is not enough. In addition, the developer might not want *any* network connectivity for the custom application. VirtualBox is a type of virtualization software. Again, the developer might choose VirtualBox as the tool to run a VM, but it has to be done in a secure way. A properly isolated sandbox would have to be set up within a VM on VirtualBox (which itself should be secured properly as well).

7. **D.** Virtual desktop infrastructure (VDI) is a server-based virtualization technology that hosts and manages the virtual desktops. Functions include creating the desktop images, managing the desktops on the servers, and providing client network access for the desktop. Virtual machine sprawl occurs when the number of VMs expands beyond the manageable control of the administrator, and they are omitted from change/life-cycle management processes. Containers are technologies that allow the packaging and isolation of applications with their entire runtime environment; this includes all of the files necessary to run. Bridged networking gives the VM (also known as the guest) direct access to the hosting computer's network connection. It allows external access.

Phew! Lots of data here. Have you been taking notes? If you have, excellent. If your notes are lacking, remember that note taking is one of the best ways to retain information—either on paper or within your favorite note-taking program. We recommend that you review this chapter, review your notes, take a nice break, and then move on to the next domain. Terrific work so far!

Chapter 22

Cloud Computing Concepts

This chapter covers the following A+ 220-1201 exam objective:

- **4.2** – Summarize cloud computing concepts.

Cloud computing and virtualization in general have grown by leaps and bounds in recent years. These technologies have become so popular for businesses, organizations, and home users that they are now commonplace. You're not likely to go a day without connecting to some kind of cloud-based service or virtualized system.

Two chapters are not nearly enough to even scratch the surface of the cloud and virtualization. You learned about virtualization in the previous chapter. Let's move on to an introduction to cloud computing.

ExamAlert

Objective 4.2 focuses on common cloud models and cloud characteristics.

Introduction to Cloud Computing

Cloud computing can be defined as a way of offering on-demand services that extend the capabilities of a person's computer or an organization's network. These might be free services, such as browser-based email from

providers such as Gmail and Yahoo!, and personal storage from providers such as Microsoft (OneDrive); they might also be offered on a pay-per-use basis, such as services that offer data access, data storage, infrastructure, and online gaming. A network connection of some sort is required to make the connection to the "cloud" and gain access to these services in real time.

Some benefits that cloud-based services provide for organizations include reduced costs, reduced administration and maintenance, greater reliability, increased scalability, and possibly increased performance. A basic example of a cloud-based service is browser-based email. A small business with few employees definitely needs email, but it might not be able to afford the costs of an email server and perhaps might not want to have its own hosted domain and face the costs and work that go along with that. By connecting to a free (or inexpensive) browser-based service, the small business can benefit from nearly unlimited email, contacts, and calendar solutions. However, keep in mind that with cloud computing, you lose administrative control, and there are some security concerns as well.

Common Cloud Models

Cloud computing services are generally broken down into a few categories of services, including

- **Software as a Service (SaaS):** The most commonly used and recognized of the three categories is SaaS, in which users access applications provided by a third party over the Internet. The applications need not be installed on the local computer. In many cases, these applications are run within a web browser; in other cases, a user connects with a screen-sharing program or remote desktop program. A common example of this is webmail such as Gmail. Other examples include Dropbox and Microsoft 365. SaaS can potentially offer lower hardware, software, and maintenance costs because the provider houses the hardware and software.
- **Infrastructure as a Service (IaaS):** IaaS is a service that offers computer networking, storage, load balancing, routing, and virtual machine (VM) hosting. The cloud provider hosts the network infrastructure hardware components that are normally present in a

traditional on-premises data center. Through a subscription service, you access hardware only when you need it. The potential benefits include scalability, minimized hardware maintenance and support, and reduced downtime. Common examples of IaaS providers include Amazon Web Services (AWS) and Microsoft Azure. More and more organizations are seeing the benefits of offloading some of their networking infrastructure to the cloud.

- Platform as a Service (PaaS): PaaS is a service that provides various software solutions to organizations, especially the ability to develop and test applications in a virtual environment without the cost or administration of a physical platform. It is also used on a subscription basis to reduce costs and increase collaboration. PaaS is used for easy-to-configure operating systems and on-demand computing. Often, PaaS users utilize IaaS as well for an underlying infrastructure to the platform. Cloud-based virtual desktop environments are often considered to be part of this type of service, but they can be part of IaaS as well. PaaS works well for serverless environments also—where the programmer/developer doesn't want or need a server to host applications or code. Examples of PaaS providers include the usual suspects: Azure, AWS (Lambda), and Google (App Engine). There are also private tools, such as OpenShift and Docker.

ExamAlert

Know what SaaS, IaaS, and PaaS are.

Organizations use different types of cloud models: public, private, hybrid, and community. Let's look at each briefly:

- **Public cloud:** A service provider offers applications and storage space to the general public over the Internet. A couple of examples of this are free, web-based email services and pay-as-you-go business-class services. The main benefits of a public cloud include low (or zero) cost and scalability. Providers of public cloud space include Google, Microsoft, Rackspace, and Amazon.

- **Private cloud:** A private cloud is designed with the needs of an individual organization in mind. The security administrator has more control over the data and infrastructure than is the case with a public cloud. A limited number of people have access to a private cloud, and they usually must be located behind a firewall of some sort to gain access to the private cloud. Resources might be provided by a third party or could come from the security administrator's server room or data center. Some companies incorporate broad network access—meaning that resources are available to a wide range of devices, including PCs, Macs, laptops, tablets, and smartphones. While a private cloud creates increased availability for clients, it also intensifies the level of security concerns.
- **Hybrid cloud:** A hybrid cloud is somewhere between public and private. Dedicated servers located within the organization and cloud servers from a third party form the collective network. In a hybrid scenario, confidential data is usually kept in-house.
- **Community cloud:** A community cloud is another mix of public and private, but multiple organizations can share the public portion. Community clouds appeal to organizations that usually share a common form of computing and a way of storing data.

ExamAlert

Know what public, private, hybrid, and community clouds are.

Cloud Computing Characteristics

Cloud computing is all about shared resources—data, devices, and network resources that can be accessed from a remote location. Generally, if resources are stored internally within an organization, users will get faster and more efficient access to them; but this is not always true. Sometimes, externally stored resources can be just as effective, especially if they have a small footprint and don't use much in the way of networking and processing power. One example of this is off-site email and email applications. Email has been so streamlined over the years that it can now be accessed from

almost any device from just about anywhere. Even an email application itself can be run in a way so as to tax the client less and the server more; this is the case with web-based email clients and email clients that run virtually—a form of virtual application streaming. Or perhaps the entire desktop, including the email application, is virtual, running either within a browser or from a thin client. In such a case, having externally shared resources is a viable option, although it might not integrate well with an organization's security policy. Also, for the enterprise environment, email technologies are often simply too immense and complex to be stored in any way except privately.

Note

In cloud computing, *shared resources* means that multiple users share the same pool of computing resources, such as power, storage, and network bandwidth on a single server. Compare with *dedicated resources*, which means a single user has exclusive access to a server's entire capacity.

Another consideration is the types of applications that will be run from the cloud, the types of devices that will use them, and how they will synchronize. Basic email applications from major providers have one version for desktops/laptops and another version for mobile devices, such as smartphones and tablets. Complex applications are more difficult to port to more than one type of device, but you don't want to have a PC version of an application running on a mobile device such as a smartphone because it would put additional strain on the end user. However, the more versions of software you offer, and the more types of endpoint devices that connect to them, the greater the need for more resources within the cloud.

So, ultimately, the type of cloud an organization uses will be dictated by the organization's budget, the amount and type of resources to be supplied to users, the level of security the organization requires, and the amount of humanpower (or lack thereof) it has available to administer its resources. While a private cloud can be very appealing, it is often beyond the means of an organization, and the organization must instead use a public or

community-based cloud. Whatever an organization chooses, the provider will measure the services supplied. *Measured services* means the provider monitors the services rendered in order to properly bill the customer and make sure the customer's use of services is being handled in the most efficient way. This can work in conjunction with a pay service called *metered utilization*, in which an organization has access to virtually unlimited resources and pays only for the resources that are used. This is also known as *metered services* or software metering. It should be measured carefully, and the details of the resources should be stated clearly every month. In metered utilization, there is ingress and egress data. *Ingress* refers to the data transferred into the cloud from external sources, such as uploading files to cloud storage or syncing on-premises systems with cloud-based platforms. *Egress*, on the other hand, refers to the data transferred out of the cloud to external destinations, such as downloading files or streaming data to users. While many cloud providers do not charge for ingress traffic, egress traffic is often metered and can significantly affect costs, especially for organizations with high outbound data requirements.

ExamAlert

Know the difference between measured services and metered utilization.

ExamAlert

Ingress refers to the data transferred into the cloud from external sources, such as uploading files to cloud storage or syncing on-premises systems with cloud-based platforms. Egress, on the other hand, refers to the data transferred out of the cloud to external destinations, such as downloading files or streaming data to users.

There are some other cloud-based terms you should be familiar with for the A+ 220-1201 exam. For example, *rapid elasticity* is the ability to build or extend a cloud-based network quickly and efficiently. Choosing a provider

that can provide you with a scalable model is important for an organization's growth. You also want to have *high availability (HA)* for any on-demand services; this means the cloud should be available in real time and whenever you need it (24/7); that is, it should be always on. In a community cloud scenario, the provider usually implements *resource pooling*, which is the grouping of servers and infrastructure for use by multiple customers but in a way that is on demand, highly available, and scalable. As you can imagine, *file synchronization* is of paramount importance when dealing with the cloud. This could mean something basic, such as email or basic document synchronization with SaaS, or something a little more in depth, such as database synchronization, or perhaps even more complex, such as synchronization of entire virtual desktops across the cloud with PaaS. Whatever the resource, synchronization methods should be monitored and tested periodically to make sure that end users are getting what they expect. Also, a key characteristic of cloud computing is *multitenancy*, where multiple customers or tenants share the same underlying cloud infrastructure, including hardware, storage, and networking resources, while maintaining isolation between each tenant's data and operations. *Multitenancy* enables cloud providers to optimize resource utilization and reduce costs by allowing multiple customers to share the same physical resources efficiently.

ExamAlert

Be familiar with these cloud-based concepts: rapid elasticity, high availability, file synchronization, and multitenancy.

Here's a last thought for the chapter: All of this cloud technology might seem a bit beyond what an A+ technician will be routinely called upon to do. However, you should have a basic knowledge of cloud types, cloud technologies, cloud terminology, and desktop virtualization so that you can better facilitate users in your role as a help desk specialist or other tech support position. Later, if you decide to specialize in one of the cloud/virtualization providers, you will find that it really is a technology

specialty all its own, with a lot of competition in the market and certifications to prove your worth.

Tip

CompTIA Cloud+ certification maps to real-world demands of cloud operations job roles, validating the essential skills necessary for excelling in the cloud environment. To learn more, visit https://www.comptia.org/certifications/cloud.

Cram Quiz

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

1. Which of the following types of cloud services offers email through a web browser?

   - ○ **A.** SaaS
   - ○ **B.** IaaS
   - ○ **C.** PaaS
   - ○ **D.** Community cloud

2. Your organization requires more control over its data and infrastructure. Money is apparently not an issue. There are only 2 admins and about 30 users who will have access to the data in the cloud. Which of the following cloud types is the best option?

   - ○ **A.** Public
   - ○ **B.** Private
   - ○ **C.** Hybrid
   - ○ **D.** Community

3. You require the ability to quickly and efficiently add to your cloud-based network whenever necessary. What is the term for this?

   - ○ **A.** Measured services
   - ○ **B.** Metered utilization
   - ○ **C.** Rapid elasticity
   - ○ **D.** On-demand service

4. What is the term for multiple customers sharing the same underlying cloud infrastructure while maintaining data and operational isolation between tenants?

   - ○ **A.** Resource pooling
   - ○ **B.** Multitenancy
   - ○ **C.** High availability (HA)
   - ○ **D.** Rapid elasticity

Cram Quiz Answers

1. **A.** Software as a Service (SaaS) is the most commonly recognized cloud service; it allows users to use applications to access data that is stored by a third party on the Internet. Infrastructure as a Service (IaaS) is a service that offers computer networking, storage, load balancing, routing, and VM hosting. Platform as a Service (PaaS) is used for easy-to-configure operating systems and on-demand computing. A community cloud is a mix of public and private clouds, but one where multiple organizations can share the public portion.

2. **B.** The best option listed is a private cloud. This option gives the most control over data and resources in an environment where there are limited users (and a healthy budget). These resources could be entirely internal, or a portion of them could also be provided by a third party. Public cloud technology is used for the general public to access applications over the Internet. Hybrid is a

mixture of public and private, but it is not necessary in this situation because of the healthy budget and the limited number of users. Community cloud is similar to hybrid but is meant for multiple organizations that share data, which is not necessary in this scenario.

3. **C.** Rapid elasticity is the ability to build a cloud-based network or extend an existing one quickly and efficiently. Measured services refers to a provider monitoring a customer's service usage in order to properly bill the customer. Metered utilization (or metered services) refers to a customer being able to access as many resources as needed and be billed only for what was accessed. On-demand service means that the cloud service is available at all times. Also, it allows a user to store data to the cloud when necessary but remove that data from the cloud when space is freed up at the local system. The leaders of a successful organization don't care what it takes; they simply want high-speed, secure access to services 24/7.

4. **B.** Multitenancy is a key characteristic of cloud computing where multiple customers or tenants share the same underlying infrastructure, such as hardware, storage, and networking resources. This model allows cloud providers to optimize resource utilization and reduce costs while ensuring that tenants' data and operations remain isolated from one another. Resource pooling refers to the provider's ability to dynamically allocate and reassign resources as needed. High availability (HA) focuses on ensuring continuous service availability through redundancy and failover, and rapid elasticity describes the ability to quickly scale resources up or down in response to demand.

Continue on! You are doing just great!

Core 1 (220-1201)

Domain 5.0: Hardware and Network Troubleshooting

CHAPTER 23 Troubleshooting Motherboards, CPUs, RAM, and Power

CHAPTER 24 Troubleshooting Storage Drives and RAID Arrays

CHAPTER 25 Troubleshooting Video Issues

CHAPTER 26 Troubleshooting Mobile Devices

CHAPTER 27 Troubleshooting Wired and Wireless Network Problems

CHAPTER 28 Troubleshooting Printers

A+ Core 1 (220-1201) Practice Exam

Chapter 23

Troubleshooting Motherboards, CPUs, RAM, and Power

This chapter covers the following A+ 220-1201 exam objective:

- **5.1** – Given a scenario, troubleshoot motherboards, RAM, CPUs, and power.

Let's continue on our troubleshooting quest. This chapter gets into the guts of the PC. Sometimes it can be a bit difficult to figure out which component is causing a problem. In this chapter, we'll give some tips to help you identify whether a problem comes from the motherboard, the CPU, the RAM, or whether it is a power issue.

If you are new to computers, we suggest reviewing the corresponding hardware chapters as well—Chapters 12 through 20.

This chapter refers to only one exam objective, but it is a pretty massive one. We're basically talking about the entire core of a PC. We could fill a book on this subject, but alas, our time and space are limited. So, we've condensed as much as possible. Consider acquiring and breaking down older systems to help develop your troubleshooting skills.

ExamAlert

Objective 5.1 concentrates on troubleshooting common symptoms related to motherboards, RAM, CPUs, and power, such as lack of

power, proprietary crash screens, power-on self-test (POST) beeps, blank screen, no power, sluggish performance, overheating, burning smell, random shutdown, application crashes, unusual noise, capacitor swelling, and inaccurate system date/time.

Troubleshooting Motherboards

Seeing a motherboard fail is uncommon, but if it does, the problem may be due to a few different issues. Let's look at several of them now.

First and probably the most common of these rarities are UEFI/BIOS firmware issues. We'll refer to this as *BIOS* for simplicity. Remember that you might need to flash the motherboard's BIOS to the latest version. For example, a new CPU or RAM might not be recognized at the correct clock speeds. An adapter card might not be seen properly. Or perhaps the operating system isn't working as it should be with the hardware in the system. Updating the BIOS can fix many of these issues. On a separate note, you might encounter a PC that, instead of booting normally, accesses the BIOS. A drained or faulty CMOS battery could be the culprit. Change out the battery, and the system should boot normally. Often, this is a CR2032 lithium battery. If you are not sure whether the battery is discharged, test it with a multimeter. CR2032 batteries normally have an output of 3 volts. Such a battery is only usable down to 2 V, so if it measures 2.5 V or less, it should be replaced. Also, if the battery is discharged, then the time and date of the system will revert to a default (such as January 1, 2012; note that different systems can have different default dates). Also, any other settings you configured will be lost. After a new battery is installed, the time/date and any other required settings will have to be reconfigured or imported from a backup.

ExamAlert

If the time and date on a system have reset, there is a good chance that the rest of the settings have also reset to defaults. Review the BIOS configuration settings, compare them with your organization's

documentation, and make any modifications necessary. Remember to save your work!

Note

A multimeter is a measuring device used to test electrical properties, including resistance (ohms), current (amps), and voltage (volts). You should have a multimeter in your toolkit!

If the system attempts to boot to an incorrect device, then the reason could be that the intended boot device is new; again, a BIOS flash could fix the problem. Of course, it could also be due to a configuration error. You should know how to change the BIOS boot order and many other settings in the BIOS. You should also know where to go in the BIOS to view log entries and error messages. The BIOS log can help describe various system problems (though it might require a bit of translation, with the aid of the motherboard manual). We discuss the BIOS further in Chapter 16, "Motherboards and Add-on Cards."

Electrostatic discharge (ESD) and other electrical issues might present intermittently. If you find some intermittent issues (for example, the computer reboots out of nowhere) or you receive random proprietary crash screens, such as blue screens of death (BSODs) in Windows or the spinning pinwheel in macOS, ESD could be the culprit. Or a power surge could cause the problem. A particular wire, circuit, or capacitor on the motherboard could have been damaged. Document when failures occur. Swap out the motherboard with a known good one to see if the issue happens again when running through the same processes. If the issue doesn't recur, chances are the original motherboard is headed for the bit bucket (meaning it is to be disposed of). There are lots of circuits on a motherboard; electrical damage to any one circuit could cause the system to behave "irrationally" at best and trigger intermittent device failure. Beyond this, electrical damage can go right through the power supply to the motherboard, disabling it permanently. Be sure to use a surge suppressor or

an uninterruptible power supply (UPS) to protect your equipment and, of course, implement antistatic measures whenever you work inside a system.

ExamAlert

A surge suppressor, also known as a surge protector, is an inexpensive and simple device placed between a power outlet and a network component to protect the component from spikes and surges. An uninterruptible power supply (UPS), also called a battery backup, is a system that provides protection against power surges and power outages. During a total power outage, a UPS gives you limited time to safely shut down systems or devices on the network before the temporary power interruption becomes permanent.

Note

Antistatic measures such as using an antistatic wrist strap and mat are crucial when working on systems. We'll cover these measures in depth in Chapter 59, "Safety Procedures."

Another issue is component failures. It is possible for a single component of the motherboard (for example, the SATA controller) to fail and for the rest of the motherboard to work fine. This can be verified by doing a power-on self-test (POST) analysis. The POST process starts when the computer first boots. It can result in visible codes or *audible beeps*. The visible codes could be on the screen or could be part of a two-digit digital readout that is incorporated into the motherboard. Either way, the visible codes or the beep codes can be deciphered with the help of the motherboard manual or the motherboard manufacturer's website.

Note

Keep in mind that different BIOS manufacturers (AMI BIOS, Award BIOS, and Dell) have different beep codes. For example, two or

three beeps sounded by a motherboard with AMI BIOS means a memory issue.

To fix a problem such as a SATA controller failure, you can purchase a separate PCIe SATA controller card. Then you can connect the hard drives to the new controller and disable the original integrated SATA controller in the BIOS. A good bench or lab will have extra controller cards of all kinds so that you can test these types of problems. In some cases, a failed controller can be symptomatic of a bigger problem; the entire motherboard might need to be replaced. Some component failures can cause system lockups, where the OS freezes and the keyboard and mouse become nonfunctional. Such failures could be due to controller issues, chipset issues, or faulty hard drives. Check all connections and consider flashing the BIOS. Worst-case scenario: Replace the motherboard. We'll discuss hard drive troubleshooting in Chapter 24, "Troubleshooting Storage Drives and RAID Arrays."

Finally, manufacturing defects and failed motherboard components often occur. Printed circuit boards (PCBs), such as motherboards, are mass-produced at high speed. Problems might be found immediately when receiving a motherboard. In general, defects are uncommon but can occur due to mechanical problems in the machinery or due to engineering errors. If you suspect a manufacturing defect, you should return the motherboard.

Motherboard component failure can also manifest over time. For example, a distended capacitor is one that becomes swollen and possibly leaks electrolytic material; this bulging can cause the system to unexpectedly restart or shut down, cause BSOD, or cause other errors. If possible, the affected capacitor(s) should be replaced right away. If that does not work, the motherboard should be replaced. In the early 2000s, capacitor swelling, or "swollen caps," was somewhat prevalent due to raw material issues; the problem was even dubbed the "capacitor plague." However, the problem is much less common today. In fact, motherboards that are received in a dead-on-arrival (DOA) state are uncommon with reputable manufacturers.

ExamAlert

Remember that capacitor swelling is when a motherboard capacitor fails and expands due to gas generation. This causes the capacitor to rupture and damage the motherboard.

Troubleshooting CPUs

The most common issue with a CPU is when it isn't installed properly or securely. An improperly installed CPU could possibly cause a complete failure when you try to turn on the system. This failure might be accompanied by a series of beeps from the POST. If this happens, always check the power first, just in case. Then check the main power connections and then the 8- or 4-pin CPU power connection. Another possibility is that the system might turn on and power might be supplied to the system, but nothing else happens: no POST, no display (meaning a blank or black screen), and no drive activity. In any of these situations, after checking power, make sure of the following:

- **Ensure that the fan is connected and functional:** Some motherboards have a safeguard that disables booting if the fan is defective or not plugged in. Or you might get a message on the screen or another type of warning, depending on the motherboard. Be sure that the fan is plugged into the correct power connector on the motherboard (or elsewhere) and verify whether it turns on when the computer is on. If the fan has failed, purchase a replacement fan; just make sure that the new fan is compatible with the heat sink and motherboard.
- **Check other major components:** Remember that the CPU is a part of a bigger system—one in which other components are more likely to be the cause of many problems. These components include the video card, RAM, and motherboard. Be sure to check these other components for simple connectivity problems, which could be the actual culprit. Always check connections first before taking apart the CPU assembly.
- **Make sure the heat sink is connected properly:** Make sure that the heat sink is flush with the CPU cap and that it is securely fastened to the motherboard (or socket housing).

- **Ensure that the CPU is installed properly:** Make sure it was installed flush into the socket and that it was oriented correctly. Of course, this means removing the heat sink. If you do so, you should clean off excess thermal compound and reapply thermal compound to the CPU cap before reinstalling the heat sink.

ExamAlert

When troubleshooting the CPU, be sure to first check all connections and then make sure the fan, heat sink, and CPU are secure and installed properly.

Following are a few more possible symptoms of a failing CPU:

- Unexplained crashes (shutdowns) occur during bootup or during use.
- The system locks after only a short time of use.
- Voltage is near, at, or above the top end of the allowable range.

Sometimes a CPU is just plain defective. It could have been received this way, or maybe it overheated. Perhaps there was a surge that damaged it, or maybe someone overclocked it too far, and it was a victim of overvoltage (and subsequent overheating). Regardless of the culprit, the CPU needs to be replaced. Now, by default, CPUs come with a heat sink and fan, and you can install the CPU as you normally would. But in some cases, you can save money by purchasing only the CPU and using the existing heat sink. In this case, remember to clean excess thermal compound and then reapply thermal compound; but reapply it to the CPU cap and not to the heat sink. If the CPU was installed properly, users don't usually have many problems with it (unless they are overclockers). Keep this in mind when troubleshooting the CPU or when troubleshooting an issue that *appears* to be a CPU issue but that might actually be something else altogether.

On a lighter note, sometimes you might get reports from customers about unusual noises coming from inside a PC—a buzzing of sorts (or perhaps even a grinding noise). The noise could be caused by a wire or cable that is

brushing up against the CPU fan (or other case fan). Be sure to reroute cables inside the computer so that they are clear of the CPU and any other devices. This will also aid with airflow in the PC and keep the PC cooler. The CPU fan might also make noise due to being clogged with dust, especially in dirtier environmental conditions. If the fan is still functional, you can use compressed air to clean it out. But be careful because too much air movement could cause a static discharge. For example, if the CPU fan (or case fan) is moved due to the air flow of a compressor, it could cause ESD. Use a piece of foam or other plastic stopper to keep the fan(s) in place while you use compressed air. Keep a computer vacuum handy to clean up the mess, if necessary; we've seen computers that had so much dust and dirt inside it could fill a garden! But be careful with computer vacuums and air compressors. Use a plastic nozzle or tip (never metal) and don't actually touch any of the components.

Troubleshooting RAM

It's not common, but RAM modules can cause intermittent issues, or they can fail altogether. Always make sure that the RAM is fully seated within the RAM slot and that the plastic ears are locking the RAM into place. An unstable system can be caused by several components, including RAM. Remember to check other components in the system as well, including the video card, motherboard, and CPU.

A lot of the issues you see occur because a user has purchased and installed a memory stick that is not compatible, or is semi-compatible, with the motherboard: wrong speed, incorrect capacity, improper configuration, and so on. Be ready for this; check the RAM compatibility against the motherboard, even if the user swears it has been checked already. Remember, a good technician has documentation available, has access to the Internet, and knows how to use both.

ExamAlert

Verify compatibility of RAM with the motherboard when troubleshooting!

Perhaps there was some kind of surge inside the computer; maybe the computer is not protected by a surge suppressor or UPS. Another possibility is that the RAM was damaged by ESD, and this damage manifests in intermittent problems. There are expensive hardware-based RAM testers that can tell you if the RAM is electrically sound and if it can process data correctly. If your company owns one, or if you can get your hands on one for a short time, you might narrow the problem. However, we have rarely needed to use these.

Here are some possible symptoms of a RAM issue and corresponding troubleshooting techniques:

- **Computer will not boot/or randomly shuts down:** If there is no RAM in the computer, or if the RAM is damaged or is not installed securely, it can prevent the computer from doing anything at all (aside from draining electricity from your AC outlet). For example, the power supply fan turns but nothing else happens—no beeps and no displays. First, if the RAM was just installed, make sure that the RAM is compatible. Next, and in general, try reseating the RAM before you attempt to troubleshoot a CPU or motherboard. Add RAM if none exists. (Sounds silly, but we've seen this!) If you suspect faulty RAM, corroded contacts, or a faulty RAM slot, you can try taking the RAM out, cleaning the RAM and RAM slot, and putting the RAM back in, being sure to seat the memory module properly. (For cleaning, use contact cleaner on the RAM contacts and use compressed air on the slot.) Next, try moving memory modules to different slots; check your motherboard documentation for proper orientation. As mentioned, a POST analysis can be helpful in these situations as well. If necessary, replace the memory module with an identical one (if you have an extra one handy) or purchase a new one if you have identified the memory module as the source of the problem. In some cases, RAM can overheat and cause random shutdowns. To prevent this, purchase a heat sink for RAM. These are made of aluminum or copper, just like CPU heat sinks, and are sometimes referred to as heat spreaders. You can also purchase RAM with heat sinks preinstalled. This type of RAM might be necessary for high-end systems.

- **BIOS indicates a memory error:** The BIOS can indicate a memory error through a message on the screen and a flashing cursor or by beeping. If it beeps, you need to reference the motherboard documentation for the specific beep codes. Sometimes a BIOS setting can be incorrect. If the computer has a saved version of the BIOS settings, you can try reverting to them, or you can try loading the BIOS defaults; we can't tell you how many times this has worked for me! Sometimes the BIOS indicates the wrong amount of RAM. If this is the case, check the RAM, as explained in the first bullet. Finally, a BIOS update can be the cure; perhaps the BIOS just doesn't have the programming necessary to identify the latest type of RAM that was installed.
- **An application crashes:** If an application crashes, it could be due to faulty RAM (or, uncommonly, a CPU issue). Make sure that the RAM is compatible with the motherboard and use memory testing programs to verify if there is any damage to the RAM. (More on memory testing in just a bit.)
- **A stop error, aka BSOD (blue screen of death), occurs:** This is a critical system error that causes the operating system to shut down. Most of the time, these errors are due to device driver errors (poor code), but they can be associated with physical faults in memory. One example of this would be a non-maskable interrupt (NMI). An NMI can interrupt the processor to gain its attention regarding nonrecoverable hardware errors, resulting in a BSOD. The BSOD usually dumps the contents of memory to a file (for later analysis) and restarts the computer. If you don't encounter another BSOD, it's probably not much to worry about. But if the BSOD happens repeatedly, you should write down the information you see on the screen and cross-reference it to the Microsoft Support website, at https://support.microsoft.com. Again, if you suspect faulty RAM, try the troubleshooting methods in the first bullet.

Note

We'll cover BSODs in more depth in Chapter 53, "Troubleshooting Microsoft Windows."

Chances are you won't need them often, but memory testing programs such as MemTest86 (https://www.memtest86.com) are available online. In fact, a whole slew of testing and benchmarking software is freely available to you. Search around! Plus, you can use the Windows Memory Diagnostics tool, which you can access by typing **mdsched.exe** in the Run prompt or from the Windows Recovery Environment (more on that in Chapter 53). These steps can help diagnose whether a memory module needs to be replaced. But in general, trust in your senses. Look at and listen to the computer as you try to diagnose any RAM issues that might occur.

Troubleshooting Power Supply Issues

Many types of power problems can happen. We discuss power in general in Chapter 18, "Power," and Chapter 60, "Environmental Controls," but for now let's focus on power issues related to the power supply within a computer.

Many issues that occur with power supplies are intermittent. This makes the troubleshooting process a little tougher. Your best friends when troubleshooting power supplies are a power supply tester and your eyes and ears.

Of course, always make sure that the power supply cable connects from the power supply to a properly wired AC outlet before troubleshooting further. Next, check all of the internal power connections. Make sure they are connected firmly. To *test* these connections, use a power supply tester.

A power supply tester (or PSU tester) is a tool every computer tech should have in their toolkit. Figure 23.1 shows an example of a PSU tester. These testing devices normally test for 12 V, 5 V, and 3.3 V for most of the connections within the computer, including the main 24-pin ATX power connector, 8- and 4-pin CPU connectors, PCI Express 8-pin and 6-pin connectors, SATA power connector, and Molex power connector. If there are error readings, error lights, no lights, or missing lights for specific voltages on the tester, you should consider replacing the power supply; or if

it is modular, you should replace that particular power cable. If all the lights and indicators are normal, then the issue resides somewhere else.



FIGURE 23.1 **PSU Tester Testing a 24-Pin ATX Power Connector**

Here are several of the issues you might encounter with power supplies:

- Fan failure
- Fuse failure
- Quick death
- Slow death

Fan failure can be due to the fact that the power supply is old, the fan is extremely clogged with dirt, or the fan is of a cheaper design (without ball bearings). However, for the A+ exam, the reason doesn't make a difference.

As far as the A+ exam is concerned, if the fan fails, the power supply needs to be replaced (and that strategy makes sense). Chances are, if the fan has failed, other components of the power supply are on their way out also. It is more cost-effective to a company to simply replace the power supply than to have a technician spend time opening it and trying to repair it. More importantly, although it is possible to remove and replace the fan by opening the power supply, this can be a dangerous venture because the power supply holds an electric charge. So, the A+ rule is to never open the power supply.

ExamAlert

Do not open a power supply! If it has failed, replace it with a working unit.

Fan failure can sometimes cause a loud noise to emanate from the power supply; it might even sound as though the noise is coming from inside the computer. Any fan in the computer (power supply fan, case fan, or CPU fan) can make unusual noises over time. If a customer reports a loud noise coming from the inside of a PC, consider the power supply fan as a suspect.

On the other hand, sometimes the fans spin but no other devices receive power, and the computer doesn't boot. This could be due to improper installation (or failure) of the motherboard, CPU, or RAM.

Fuse failure can occur due to an overload or due to the power supply malfunctioning. Either way, the proper course of action is to replace the power supply. Do not attempt to replace the fuse. If the fuse is blown, chances are that the power supply is faulty.

If the power supply dies a quick death and provides no power, the reason might be several issues, ranging from an electrical spike to hardware malfunction. First, make sure that the IEC power cable is connected properly to the power supply and to the AC outlet. Sometimes it can be difficult to tell whether the power supply has failed or whether the problem is something else inside or outside the computer system. You should check the AC outlet with your trusty receptacle tester, make sure that a circuit

hasn’t tripped, and verify that any surge protectors and/or UPS devices work properly. Depending on what you sense about the problem, you might decide to just swap out the power supply with a known good one.

A power supply that is dying a slow death may cause intermittent errors or frequent failure of hard drives and other devices, and this can be tough to troubleshoot. If you suspect intermittent issues, first make sure the power cord is connected securely and then try swapping out the power supply with a known good one. Boot the computer and watch it for a while to see if the same errors continue to occur.

Note

If a system was recently upgraded, the power supply could cause the system to reboot intermittently because the new components are causing too much power drain. When upgrading components, be sure to check whether you need to upgrade the power supply as well!

Remember that connections sometimes can be jarred loose inside and outside a computer. Check the IEC cord on both ends and all power connections inside the computer, including the main motherboard connector as well as the CPU, Molex, SATA, and PCIe connectors. Any single loose connector can have “interesting” results on the computer!

Heating and Cooling

Another issue to watch for is the system overheating. This can happen for several reasons:

- Power supply fan failure
- Auxiliary case fan failure
- Inadequate number of fans
- Missing or open slot covers
- Case not being tightly closed and screwed in

- Location of the computer

Air flow is important on today's personal computers because their processors can often operate at hundreds of billions of instructions per second or more (referred to as 100 giga-instructions per second [GIPS]). They typically use 50 to 150 watts of power, and that creates a lot of heat! Add to that the video card and other cards that have their own on-board processors, and you quickly realize it can get *hot* inside the computer case. Plus, environmental factors and higher-temperature areas (such as warehouses and cafeterias) can cause heat to be trapped in the case, producing random shutdowns. Circulation is the key here. Air should flow in the case from the front and should be exhausted out the back. Any openings in the case or missing slot covers can cause circulation to diminish. If you have a computer that has a lot of devices, does a lot of processing, or runs hot for any other reason, your best bet is to install a case fan in the front of the case (which pulls air into the case) and a second case fan in the back of the case (which, with the power supply fan, helps exhaust hot air out the back). Standard sizes for case fans are 80 and 120 mm. Also, try to keep the computer in a relatively cool area and leave space for the computer to expel its hot air! Of course, there are other special considerations and options, such as liquid cooling and special processor cooling methods, such as oversized tower heat sinks; however, for typical workstations, these options will most likely not be feasible.

You should also train your nose for smells and watch for smoke. If a power supply starts to emit a burning smell, or if you see any smoke emanating from it, you should turn off the computer and disconnect the power right away. The power supply is probably about to fail, and it could short out, trip the circuit, or, worse yet, start a fire. Be sure to replace it. In some cases, a power supply has a burn-in period of 24 to 48 hours, during which time you might smell some oils burning off, but it's best to be safe and check/test the power supply if you smell something that seems wrong.

Troubleshooting Questions in the A+ Exams

Hardware and software troubleshooting make up at least a quarter of the A+ exam objectives. For bench techs, help desk people, and other tech support personnel, it makes up a much larger

percentage of work. When we really get down to it, we technicians are here to solve problems, and troubleshooting is a key component of problem solving. So, we have included a lot more cram quiz questions for these troubleshooting chapters than for other chapters. It seemed the proper way.

Cram Quiz

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

1. What is the best way to tell if a CR2032 lithium battery has been discharged?

   - ○ **A.** Use a power supply tester.
   - ○ **B.** Check within Windows.
   - ○ **C.** Use a multimeter.
   - ○ **D.** Plug it into another motherboard.

2. A PC reboots without any warning. You rule out any chance of viruses. When you look at the motherboard, you see that some of the capacitors are swelling and appear distended and out of shape. What should you do?

   - ○ **A.** Replace the motherboard.
   - ○ **B.** Replace the hard drive.
   - ○ **C.** Remove and replace the capacitors.
   - ○ **D.** Reconfigure the BIOS.

3. A computer you are troubleshooting won't boot properly. When you power on the computer, the video display is blank, and you hear a series of beeps. What should you do?

   - ○ **A.** Check power supply connections.
   - ○ **B.** Consult the vendor documentation for the motherboard.

- ○ **C.** Remove all memory and replace it.
- ○ **D.** Unplug the speakers because they are causing a conflict.

4. You are troubleshooting a CPU and have already cut power, disconnected the power cable, opened the case, and put on your antistatic strap. What should you do next?

- ○ **A.** Check the BIOS.
- ○ **B.** Check connections.
- ○ **C.** Remove the CPU.
- ○ **D.** Test the motherboard with a multimeter.

5. What is a possible symptom of a failing CPU?

- ○ **A.** CPU is beyond the recommended voltage range.
- ○ **B.** Computer won't boot.
- ○ **C.** BIOS reports low temperatures within the case.
- ○ **D.** Spyware is installed in the browser.

6. You are repairing a computer that has been used in a warehouse for several years. You suspect a problem with a memory module. What should you do first?

- ○ **A.** Replace the module with a new one.
- ○ **B.** Install more eRAM.
- ○ **C.** Clean the RAM slot.
- ○ **D.** Install RAM heat sinks.

7. You are investigating a computer that is suffering from random shutdowns. You note that the RAM modules are overheating. What is the best solution?

- ○ **A.** Install a heat sink on the memory controller.
- ○ **B.** Install more CPU fans.

- ○ **C.** Install heat sinks on the RAM modules.
- ○ **D.** Install a heat sink on the chipset.

8. You just installed new, compatible RAM into a motherboard, but when you boot the computer, it does not recognize the memory. What should you do?

   - ○ **A.** Flash the BIOS.
   - ○ **B.** Replace the RAM.
   - ○ **C.** Upgrade the CPU.
   - ○ **D.** Add more RAM.

9. You are troubleshooting a computer that won't power on. You have already checked the AC outlet and the power cord, which appear to be functioning properly. What should you do next?

   - ○ **A.** Test the computer with a PSU tester.
   - ○ **B.** Plug the computer into a different outlet.
   - ○ **C.** Check that the RAM is seated correctly.
   - ○ **D.** Install a UPS.

10. A computer you are troubleshooting shuts down without warning. After a few minutes, it boots back up, but after running for a short time, it shuts down again. Which of the following components could be the cause? (Select the two best answers.)

    - ○ **A.** Power supply
    - ○ **B.** SATA hard drive
    - ○ **C.** RAM
    - ○ **D.** CPU fan
    - ○ **E.** Video card

Cram Quiz Answers

1. **C.** Although there might be a Windows application that monitors the battery, the surefire way is to test the voltage of the lithium battery with a multimeter. A CR2032 lithium battery is designed to run at 3 volts (and they often ship at approximately 3.3 volts). Some UEFI/BIOS programs can also monitor the voltage of the battery.

2. **A.** You should replace the motherboard if it is damaged. It would be much too time-consuming to even attempt replacing the capacitors and probably not cost-effective.

3. **B.** You should check the BIOS version and consult the documentation that accompanies the motherboard. You might need to go online for this information. You can also try performing a POST analysis to discern the problem. The issue could be video based, or RAM based, but the beep code should help identify the problem.

4. **B.** Check connections first as they are a common culprit.

5. **A.** If the CPU is running beyond the recommended voltage range for extended periods of time, it can be a sign of a failing CPU. If the computer won't boot at all, another problem might have occurred, or the CPU might have already failed. Low case temperatures are a good thing (as long as they aren't below freezing). Spyware is unrelated in this case.

6. **C.** Because the computer is being used in a warehouse (and a warehouse is often a fairly dirty environment), you should use compressed air on the RAM slot and clean the memory module with contact cleaner. Clean out all of the dust bunnies within the entire computer. Using MemTest86 or another memory diagnostic tool is another good answer.

7. **C.** The best thing to do in this situation is to install heat sinks on the RAM modules. On older computers, the memory controller in a northbridge doesn't usually overheat because it already has a heat sink; on newer computers, it is within the CPU. A CPU can

have only one fan. You can't install more (although an additional case fan might help). The chipset also usually has a heat sink.

8. **A.** If you are sure that the RAM is compatible and the system doesn't recognize it during POST, try flashing the UEFI/BIOS. It could be that the RAM is so new that the motherboard doesn't have the required firmware to identify the new RAM.

9. **A.** You should test the computer with a PSU tester. This can tell you whether the power supply functions properly. You already know that the AC outlet is functional, so there is no reason to use another outlet. The computer would still turn on if the RAM wasn't seated properly. A UPS won't help the situation because it is part of the power flow before the power supply.

10. **A and D.** The two components that could cause the system to shut down are the power supply and the CPU fan. Check the CPU fan settings and temperature in the BIOS first before opening the computer. If those are fine, you most likely need to replace the power supply. The RAM, video card, and hard drive should not cause the system to suddenly shut down.

Now we are getting deep into troubleshooting. This was a longer chapter (for this book at least), and we recommend that you review it carefully. Great work so far!

Chapter 24

Troubleshooting Storage Drives and RAID Arrays

This chapter covers the following A+ 220-1201 exam objective:

- **5.2** – Given a scenario, troubleshoot drive and RAID issues.

Storage drives contain the data that we need, so we depend on our drives and RAID arrays to run efficiently every day. For this to happen, the drives need to be healthy. We can keep our drives healthy by carrying out a variety of precautionary measures. But sometimes, our systems can be affected by powers outside our control and beyond our planning. Then, they can potentially fail—and then, we have to troubleshoot.

ExamAlert

Objective 5.2 focuses on troubleshooting common symptoms in storage drives; hard disk drives (HDDs) and solid-state drives (SSDs); and RAID issues.

Preventive Maintenance and Troubleshooting of Storage Drives

Storage drives will fail. It's not a matter of if; it's a matter of when, especially when it comes to mechanical drives. The moving parts are bound to fail at some point. Storage drives have an average warranty of three years, as is the case with the SATA drives used in the examples in this book. But many of us want our drives to last longer than that. So, to quote Benjamin Franklin, "an ounce of prevention is worth a pound of cure" or, for those of you using the metric system, 29 grams and .45 kg—but that just doesn't seem to roll off the tongue quite so well! Either way, by implementing good practices, you can extend the lifespan of a storage drive. So, before we get into troubleshooting storage drives, let's consider some examples of prevention.

Storage Drive Preventive Maintenance

Always the pessimists, we are constantly on the lookout for ways to *prevent* problems before they happen. By taking preventive measures, you, as a technician, can reduce the risk of catastrophic failure. Here are a couple of ways to prevent storage drive issues.

- **Turn off a computer when not in use:** This can help increase the lifespan of a magnetic-based drive (or hard disk drive). Turning off the computer tells the hard disk drive to spin down and enter a "parked" state. It's kind of like parking a car or placing a record player's arm on its holder. Turning off a computer when not in use increases the lifespan of just about all its devices (except for the lithium battery). You can also set the computer to hibernate, sleep, or standby, or you can simply set your operating system's power scheme to turn off hard disks after a certain amount of inactivity, such as five minutes. The less the drive is in motion, the longer the lifespan it will have. Of course, if you want to take the moving parts out of the equation, you can opt for a solid-state drive, as discussed later in this chapter.
- **Clean up the disk:** Use a storage drive cleanup program to remove temporary files, clean out the Recycle Bin, and so on. Microsoft includes the Disk Cleanup program (cleanmgr.exe) in Windows. And there are free cleanup programs available on the Internet. (Just be careful what you download.) When you remove the "junk" from the

drive, there is less data that the drive must sift through, which makes it easier on the drive when it is time to defragment.

- **Defragment the drive:** Defragmenting, also known as *defragging*, rearranges the data on a partition or volume so that it is laid out in a contiguous, orderly fashion. Defragmentation is most commonly performed on a hard disk drive. Consider defragmenting the disk every couple of months or perhaps more often if you are a power user. Don't worry: The operating system tells you if defragging is not necessary during the analysis stage. Over time, data is written to the drive and subsequently erased, over and over again, leaving gaps in the drive space. New data is sometimes written to multiple areas of the drive, in a broken or fragmented fashion, filling in any blank areas the drive can find. When this happens, the drive has to work much harder to find the data it needs. Logically, data access time is increased. Physically, the drive spins more, and it starts and stops more; in general, there is more mechanical movement. It's kind of like changing gears excessively with the automatic transmission in your car. The more the drive has to access this fragmented data, the shorter its lifespan becomes due to mechanical wear and tear. But before the drive fails altogether, fragmentation can cause intermittent read/write failures. You can defragment the drive by using Microsoft's Disk Defragmenter (dfrgui.exe), the command **defrag**, or other third-party programs. If using the Disk Defragmenter program, you need 15 percent free space on the volume you want to defrag. If you have less than that, you need to use the command-line option **defrag -f**. To summarize, the more contiguous the data, the less the drive has to work to access that data, thus decreasing the data access time and increasing the lifespan of the drive. While defragmenting works best on magnetic drives, it can also help with solid-state drives, but not to the same extent or in the same way because of the design differences between the two types of drives.

Note

Be careful with defragging; this process can wear out a drive if it is done too much, especially when performed on SSDs.

ExamAlert

Know how to troubleshoot failures such as read/write errors using tools such as Optimize Drives/Disk Defragmenter and the **defrag** command.

- **Leave at least 10 percent of the drive free:** If you use up all the space on a drive, its performance and lifespan will decrease greatly. Consider leaving between 10 and 25 percent of the space on a drive free of data. Some manufacturers add a 10 percent buffer by design, and some companies have a policy that states drives should never go past 50 or 60 percent of capacity. This preventive measure applies to HDDs and SSDs.
- **Make sure that high-performance drives have good airflow:** NVMe drives (such as M.2 and PCIe-based drives), as well as RAID arrays, can generate a lot of heat. Be sure to have good airflow and adequate cooling, and if at all possible, don't cramp the drives too much.
- **Scan the drive with antimalware:** Make sure the computer has an antimalware program installed. Also known as an endpoint protection platform, this program should include antivirus/antimalware and antispyware at the very least. Verify that the software is scheduled to scan the drive at least twice a week. (The manufacturer default is usually every day.) The quicker the software finds and quarantines threats, the lower the chance of physical damage to the drive.

Preventive techniques will save you time, save your users some heartache, and save your organization money. But as we've said, storage drives will fail. When failures happen, you troubleshoot.

Storage Drive Troubleshooting

Now, let's get into some of the problems you might encounter concerning storage drives:

- **Bootable device not found:** If the UEFI/BIOS doesn't recognize the drive you have installed, you can check a few things. First, make sure the power cable is firmly connected and oriented properly. Next, make sure SATA data cables are fully seated in the ports and weren't accidentally installed upside down; if you find one that was, consider replacing it because it might be damaged due to incorrect installation. An "OS Not Found" error message or another boot failure could also be caused by improperly connected drives or an erroneous BIOS boot order. Finally, check if there is a motherboard BIOS update; sometimes newer drives require new BIOS code to access the drive.
- **Windows does not "see" a second drive:** There are several reasons Windows might not see a second drive. Maybe a driver needs to be installed for the drive or for its controller. This issue is more common with newer drive technologies. Perhaps the secondary drive needs to be initialized within Disk Management. Or it could be that the drive was not partitioned or formatted. Also try the methods listed in the first bullet.
- **Slow reaction time:** If a drive is suffering from longer read/write times than usual, the issue could be due to several things. Perhaps the drive is full, or has become fragmented, or has been infected with malware. Sometimes it could be the fault of torrent-based software. Or perhaps there are bad sectors, indicating a damaged drive. In any of these cases, it is common to see that the drive's LED status indicator on the front of the computer is blinking more than usual, telling you that the drive is working harder than it normally would. Check for (and remove) undesirable software such as bit torrent clients, P2P software, and so on. Check the drive's properties in the OS; if it is full or nearly full, start offloading data. If it is not full, analyze and defragment the drive. If it is heavily fragmented, the drive can take longer to access the data needed, resulting in slow reaction time. You might be amazed at the difference in performance! If you think the drive might be infected, scan the disk with your antimalware program to quarantine any possible threats. It's wise to schedule deep scans of the drive periodically as well. You will learn more about viruses, spyware, and other malicious software in Chapter 46, "Wireless Security and Malware."

After you have worked on the drive, check it with some type of benchmarking software (CrystalDiskMark, ATTO, or a similar program). These programs can measure the data transfer capabilities of your storage drive, either in megabytes per second (MB/s) or in input/output operations per second (IOPS). Either of these measurements can be compared to the vendor's documentation for the drive to see if the drive is working within specifications. Note that vendor tests are usually done in an optimal environment and show the *maximums* for the drive. Your results will often be 10 to 20 percent lower, which is usually okay. However, if your results are 25 percent or more below the vendor's numbers, you should investigate the drive further.

ExamAlert

Input/output operations per second (IOPS) is a common metric used to measure the throughput or performance of storage devices, such as hard disk drives (HDDs), solid-state drives (SSDs), or other data storage systems. It is a key factor in determining how well storage systems perform and is especially useful for applications that require very fast response times.

In extreme cases, you might want to move all the data from the affected drive to another drive, being sure to verify the data that was moved. Then format the affected drive and, finally, move the data back. This is common in audio/video environments and when dealing with data drives, but it should not be done to a system drive (that is, a drive that contains the operating system).

- **Missing files at startup:** If you get a message such as "BOOTMGR Is Missing," the file needs to be written back to the drive. For more on how to do this, see Chapter 53, "Troubleshooting Microsoft Windows." In severe cases, this can mean that the drive is physically damaged and needs to be replaced. If this happens, the drive needs to be removed from the computer, and the data must be copied from the damaged drive to a known good drive (which might require a third-party program).

Then, a new drive must be installed to the affected computer. Afterward, the recovered data can be copied on the new drive.

- **Missing or corrupted files:** Missing or corrupted files could result from drive failure, operating system failure, malware infection, user error, and so on. If data corruption happens, be sure to back up the rest of the data on the drive and then use the preventive methods mentioned previously, especially defragmenting and scanning for malware. (Ultimately, you may have to replace the drive.) You can also analyze the drive's S.M.A.R.T. data. S.M.A.R.T., which stands for Self-Monitoring, Analysis, and Reporting Technology, is a monitoring system included with almost all drives that creates reporting data which, when enabled in the BIOS, can be accessed within the operating system. You can easily view some basic S.M.A.R.T.-based information in the Windows Command Prompt by using the command **wmic diskdrive get status**. Each (S.M.A.R.T.-enabled) drive will be analyzed; the message "OK" means that Windows didn't find any issues. A message of "Bad," "Unknown," or "Caution" should convince you to initiate more analysis. There are also plenty of third-party tools available that can be downloaded from the Internet and are very easy to use. The problem with S.M.A.R.T. data is that it can be unreliable at times due to a lack of hardware and driver support within the third-party S.M.A.R.T. application, lack of common interpretation, and incorrectly diagnosed data. Also, a drive might be diagnosed as a failing drive when in reality the problem is power surges or another issue.

Note

If a file is written during a power surge (whether the surge originates internally or externally), that file will most likely be placed on the drive in a corrupted fashion—with the associated sector being affected by the power surge. In this case, you should find out two things: (1) if the power supply has the right capacity for the equipment in the computer, and (2) if the proper power suppressing/conditioning equipment is being used. If a drive is making clicking sounds or other strange noises, analysis with

S.M.A.R.T. data is not recommended. See the following bullet for more information.

- **Noisy drive/lockups:** Watch out for clicking and grinding sounds! If your SATA magnetic disk drive starts getting noisy, it's a sure sign of impending drive failure. You might also hear a scratching or grating sound, akin to a record being scratched with a record player needle. Or the drive might intermittently just stop or lock up, with one or more loud audible clicks. You can't wait in these situations; you need to connect the drive to another computer immediately and copy the data to a good drive. Even then, it might be too late. However, some third-party programs available on the Internet might help you to recover the data.

Note

Storage drive issues can also result in proprietary crash screens: either a Windows blue screen of death (BSOD) or a macOS spinning pinwheel. Fixing these issues often requires using recovery environment tools and/or restoring the system to an earlier point in time. If these issues happen often and drive repair methods do not work, consider either a new installation of Windows or a new drive. We cover how to troubleshoot these problems further in the Core 2 (220-1202) portion of the book.

As mentioned, storage drives *will* fail, so it is important to make backups of your data. The backup media of choice will vary depending on the organization. It could be the cloud, a tape backup, a secondary system, optical discs, or USB flash drives, depending on the scenario. Know this: RAID arrays are not considered to be backups. They are fault-tolerant ways of storing data. Because they consist of storage drives, it stands to reason that you will have to troubleshoot them too.

Troubleshooting RAID Arrays

Sometimes, hardware RAID arrays fail. They might stop working, or the OS could have trouble finding them. If you see an issue like this, check whether the storage drives are securely connected to the controller and ensure that the controller (if an adapter card) is securely connected to the motherboard. Also, if you use a RAID adapter card or an external enclosure and the motherboard also has built-in RAID functionality of its own, make sure you disable the motherboard RAID within the BIOS because it could cause a conflict. Verify that the driver for the RAID device is installed and updated. Finally, check whether any of the drives or the RAID controller has failed. If a RAID controller built into a motherboard fails, you will either have to purchase a new motherboard or a RAID adapter card.

When a RAID array is missing, it may manifest as a complete loss of access to the data stored within the array or an inability to boot the operating system if it resides on the array. The system might display error messages like “Array Not Found,” “Missing RAID Volume,” or “No Bootable Device.” These symptoms could be caused by several issues, such as disconnected drives, a disabled RAID setting in the BIOS, a failed RAID controller, or firmware corruption. Begin troubleshooting by verifying physical connections, checking BIOS settings for RAID configuration, and ensuring the RAID controller is functioning properly. If a RAID adapter card is in use, ensure the card is securely installed and its firmware is up to date. Additionally, consider using RAID management utilities to identify any discrepancies or missing drives within the array.

Many RAID controllers, particularly those in enterprise environments, are equipped with audible alarms to alert users to potential issues. These alarms may indicate problems such as a degraded array, a missing drive, or a failing RAID controller. If an alarm sounds, consult the RAID controller’s documentation to interpret the specific alert tone or code. Common steps to troubleshoot include checking the RAID utility for detailed error messages, verifying the physical status of all drives, and replacing any failing components. It’s important to address audible alarms promptly to minimize the risk of data loss and ensure system reliability. For silencing the alarm temporarily, most RAID controllers offer an option within their utility, but you must make sure to document and resolve the root cause of the issue.

Intel-based RAID setups are common as part of server and workstation motherboards and as separate RAID adapter cards. To configure Intel RAID, you need to press Ctrl+I when the system first boots up. From there, you can configure the RAID array as shown in Figure 24.1.

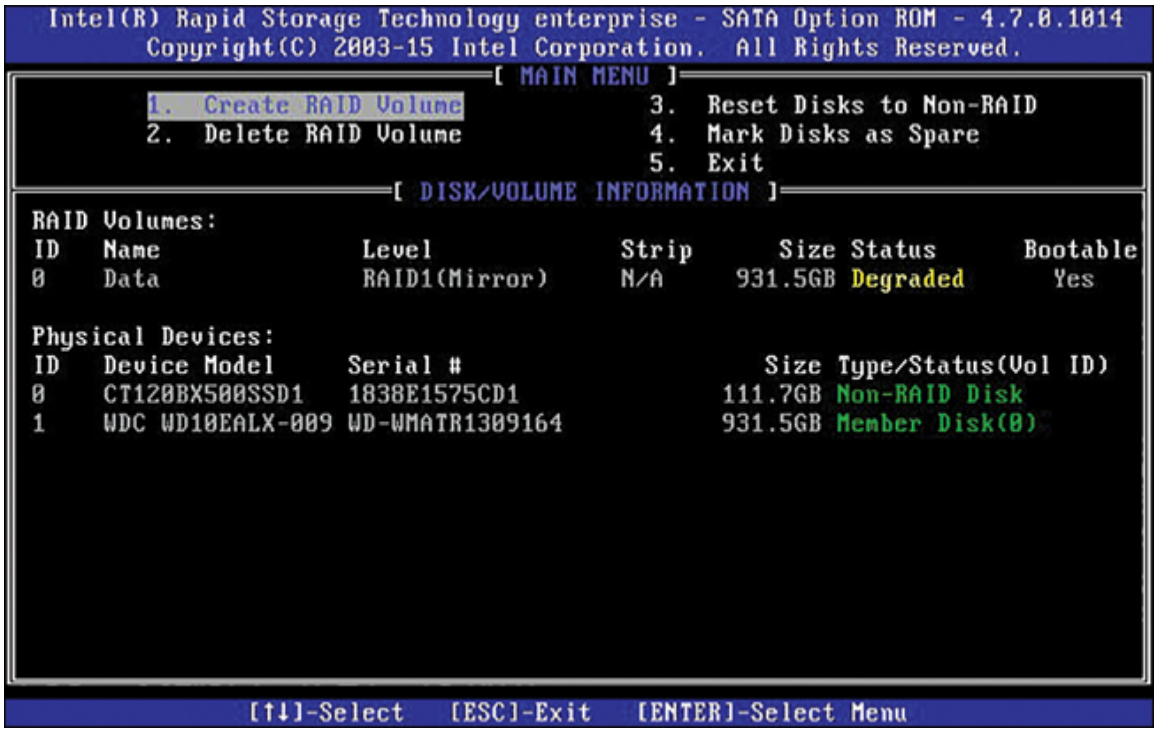


FIGURE 24.1 **Intel RAID Configuration Screen**

In Figure 24.1 you can see that there is a RAID 1 mirror, but the status is "Degraded." This means the array has failed or has been deconstructed in some way. The listed drive is part of a RAID 1 volume called Data, but the second drive of the mirror is missing, so the mirror is broken. (That's because we removed it from the system to show this very error.) Look in the listed physical devices for the drive that is 931.5 GB; you can see that it is listed as Member Disk, meaning that it is part of an array. A degraded RAID 0, 1, 5, 6, or 10 array can result in either a loss of access to data or—if the OS is installed to the array—failure of the OS to boot. Either way, the array would have to be repaired, or the data would have to be recovered from backup and placed on a new array. Repairing a RAID array could be as simple as reconnecting the physical drives, but it could also mean reconfiguring the array within the RAID utility. Some organizations have a rule that if a RAID array fails and it is more than three years old, the

organization should downgrade the array, create a new array with new drives, and recover the data from backup.

Now, let's say that that RAID functionality is indeed built into your motherboard, as it is on the system shown in Figure 24.1. To configure a RAID array, you first have to enable RAID in the BIOS. Quite often, that is done by accessing the SATA configuration screen and changing from AHCI to RAID. If you don't do this, you won't be able to access the RAID utility at bootup. Take it to the next level: If someone resets the BIOS to defaults, then that SATA setting will revert to AHCI, rendering the RAID array useless and nonbootable—ultimately leading to various error messages. This could also happen after a BIOS flash update. Yet another reason to know the BIOS of your systems!

Note

AHCI stands for Advanced Host Configuration Interface, which is the default setting for SATA drives in many BIOS programs. However, AHCI is being gradually replaced by Non-Volatile Memory Express (NVMe) which offers significantly higher performance for modern solid-state drives.

One way to check the status of a RAID array is to use S.M.A.R.T. For example, in Figure 24.2, you can see the S.M.A.R.T. information screen for one of the disks in a RAID 1 mirror of a network-attached storage (NAS) device. This screen gives some meaningful data that requires some analysis, but for quick peace of mind, just check the Status column. OKs are good; anything else requires further attention and could be a precursor to a RAID failure. Also note in the figure the S.M.A.R.T. Test page, where you can do additional testing of the drive, drives, or array. Just be sure to run tests of this nature off-hours!

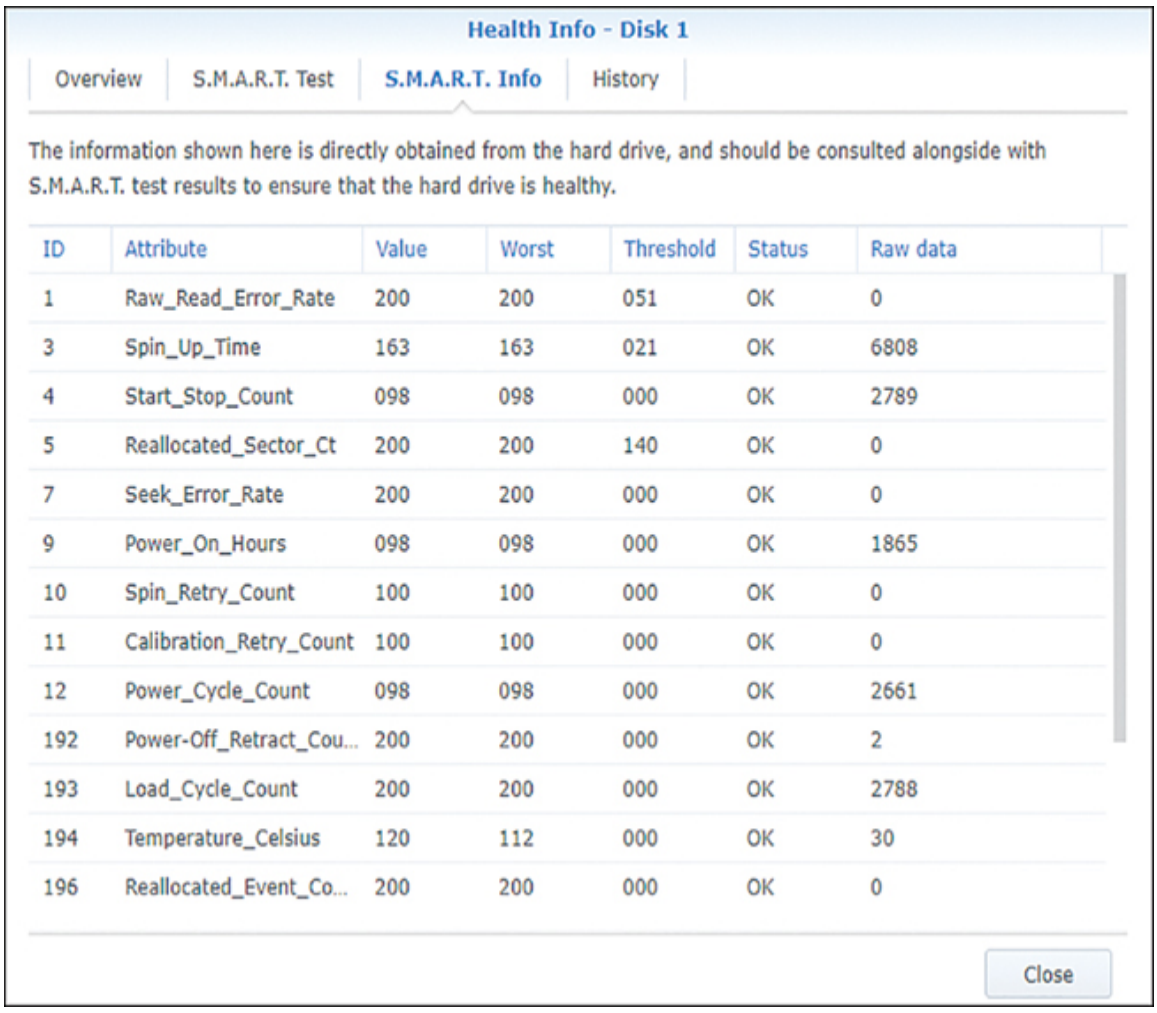


FIGURE 24.2 **S.M.A.R.T. Information and Status of a NAS Drive**

RAID Is Not Backup!

Remember, in the workplace, RAID is generally used for fault tolerance; it is not a backup of data, even if you are using RAID 1 (mirroring). A RAID array's data should be properly backed up to a *separate* system, according to your organization's procedures. The backup should be tested thoroughly and documented.

Cram Quiz

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

1. What should you do first to repair a drive that is acting sluggish?

   - ○ **A.** Remove the drive and recover the data.
   - ○ **B.** Run Disk Cleanup.
   - ○ **C.** Run Disk Defragmenter.
   - ○ **D.** Scan for viruses.

2. Which of the following are possible symptoms of storage drive failure? (Select the two best answers.)

   - ○ **A.** System lockup
   - ○ **B.** Antivirus alerts
   - ○ **C.** Failing bootup files
   - ○ **D.** Network drive errors
   - ○ **E.** BIOS doesn't recognize the drive.

3. You just replaced a SATA drive that you suspect failed. You also replaced the data cable between the drive and the motherboard. When you reboot the computer, you notice that the SATA drive is not recognized by the BIOS. What most likely happened to cause this?

   - ○ **A.** The drive has not been formatted yet.
   - ○ **B.** The BIOS does not support SATA.
   - ○ **C.** The SATA port is faulty.
   - ○ **D.** The drive is not jumpered properly.

4. You are troubleshooting a SATA drive that doesn't function on a PC. When you try it on another computer, it works fine. You suspect a power issue and decide to take voltage readings from the

SATA power connector coming from the power supply. Which of the following readings should you find?

- **A.** 5 V and 12 V
- **B.** 5 V, 12 V, and 24 V
- **C.** 3.3 V, 5 V, and 12 V
- **D.** 3.3 V and 12 V

5. You are troubleshooting a Windows server that normally boots from a SATA-based RAID 0 array. The message you receive is "missing operating system." As it turns out, another technician has been updating the BIOS on several of the servers in your organization, including this one. What configured setting needs to be changed? (Select the best answer.)

- **A.** RAID 1
- **B.** AHCI
- **C.** S.M.A.R.T.
- **D.** NVMe

6. What should you do *first* if your SATA magnetic disk begins to make loud clicking or grinding noises? (Select the best answer.)

- **A.** Copy the data to another drive.
- **B.** Replace with a new SATA drive.
- **C.** Update the UEFI/BIOS.
- **D.** Replace the SATA power cable.

7. Which are performance measurements for storage drives that measure data transfer capabilities every second? (Select two.)

- **A. wmic**
- **B.** MB/s
- **C.** RAID

- **D.** IOPS

Cram Quiz Answers

1. **C.** Attempt to defragment the disk. If defragmentation is not necessary, Windows lets you know. Then you can move to other options, such as scanning the drive for viruses.

2. **A and C.** System lockups and failing bootup files or other failing file operations are possible symptoms of storage drive failure. Antivirus alerts tell you that the operating system has been compromised, viruses should be quarantined, and a full scan should be initiated. Sometimes drives fail due to heavy virus activity, but usually if the malware is caught quickly enough, the drive should survive. Network drives are separate from the local drive; inability to connect to a network drive suggests a network configuration issue. If the BIOS doesn't recognize a drive, consider a BIOS update.

3. **C.** Most likely, the SATA port is faulty. It might have been damaged during the upgrade. To test the theory, you would plug the SATA data cable into another port on the motherboard. You can't format the drive until it has been recognized by the BIOS, which, by the way, should recognize SATA drives if the motherboard has SATA ports! SATA drives don't use jumpers unless they need to coexist with older IDE drives. Most of today's drives do not come with jumpers.

4. **C.** If you test a SATA power cable, you should find 3.3 V (orange wire), 5 V (red wire), and 12 V (yellow wire). If any one of these doesn't test properly, try another SATA power connector.

5. **B.** When the BIOS was updated, the SATA setting in the BIOS probably reverted to AHCI. That caused the RAID 0 array to be ignored, and so the OS would not boot because it is stored on that array. The setting should be changed from AHCI to RAID (or a similar name). Now, if this was a RAID 1 mirror, a copy of the OS would be on each drive, and it *might* still boot (though you would

probably receive a message about the state of the mirror being degraded or broken). But with RAID 0, the OS is *striped* across two or more drives; all drives need to be present and accessed via RAID in order for the OS to boot. That's one of the reasons the golden rule for many years was to "mirror the OS and stripe the data." Phew! Anyway, on to the incorrect answers. RAID 1 is incorrect because there would be no option to set this; this scenario uses RAID 0. S.M.A.R.T. is the monitoring system included in HDDs and SSDs. NVMe (Non-Volatile Memory Express) is the specification for non-volatile storage used by M.2 drives, PCIe card–based drives, and so on. Remember to back up any and all BIOS configurations!

6. **A.** Don't hesitate! Copy the data to another drive. Afterward, update the UEFI/BIOS, replace the drive with a new one, and consider getting a new SATA cable while you are at it.

7. **B and D.** Megabytes per second (MB/s) and input/output operations per second (IOPS) are performance measurements for storage drives that measure data transfer capabilities every second. The **wmic** command enables you to view basic S.M.A.R.T.-based information in the Windows Command Prompt. Redundant array of inexpensive disks (RAID) is an array of storage drives; you can measure the performance of these in addition to individual drives.

Fantastic! Another chapter complete. You are getting closer to the halfway point of this book. Take a break, clear the mechanism, and continue.

Chapter 25

Troubleshooting Video Issues

This chapter covers the following A+ 220-1201 exam objective:

- **5.3** – Given a scenario, troubleshoot video, projector, and display issues.

Video is a technology that you will troubleshoot often. Video issues could be hardware based or software based. There are many types of video connectors, standards, and different output devices, and so there is plenty of work for techs. Be sure to refer to Chapter 13, "Cables and Connectors," for more information on video connections.

ExamAlert

Objective 5.3 concentrates on troubleshooting common symptoms of video issues, such as incorrect data input source, physical cabling issues, burned-out bulb, fuzzy image, display burn-in, dead pixels, flashing screen, incorrect color display, audio issues, dim image, intermittent projector shutdown, sizing issues, and distorted image.

PC Video Troubleshooting

Several parts, both hardware and software, make up a video system: GPUs, monitors, cables and connections, video drivers, video settings, and so on.

So, there is plenty to troubleshoot when it comes to video. We like to look at it as a system within the computer system, and we tend to follow the path of video when troubleshooting; for example, from the software, to the operating system and driver, to the video card itself, through the cables and connectors, and out to the display (or displays, whatever they might be). And let's not forget power: Many video cards require a power connection, and the monitor does as well. Also remember the types of video connections: HDMI, DVI, DisplayPort, and so on. Keep all these things in the back of your mind as you are troubleshooting video—and remember to write out your process. Document and write down (or type) as much as possible about what you see and what you try: Include pictures and illustrations to help in the troubleshooting process.

When you're troubleshooting video issues, there are a number of things to check, including the following:

- **Inspect connections:** If nothing is showing up on the display, first make sure the monitor is plugged into the video card properly (and to the correct video port) and then verify whether the monitor is connected to the AC outlet and is powered on. Poor connectivity of cables can also cause screen flicker. Inspect for damage along the length of cables and the plugs. Wear and tear can cause physical cable issues over time, which could lead to flicker, fuzziness, and other eye-straining issues.
- **Check the data/input source:** By *data/input source*, we mean what type of video connection the monitor is using. For example, if a PC is connected to a monitor by way of DisplayPort, and the monitor's onscreen display (OSD) is set to HDMI, the monitor won't receive any signal; the monitor will simply display a black screen. Always check which video port the monitor is configured to use by accessing the OSD with the appropriate button on the monitor.

ExamAlert

When troubleshooting video issues, check the data source (HDMI, DisplayPort, DVI, USB-C, VGA) within the OSD of the monitor!

- **Power cycle the computer, display, and any power protection equipment:** Power cycling the equipment can fix all kinds of problems and is an easy solution to implement. Problems such as video memory (image retention) and stuck pixels might be easily repaired by a power cycle of the display, the computer, and any surge suppressor that the equipment is plugged into. You might also need to leave a display off for a couple of hours to fix a video memory problem, such as the video memory/image retention issue that is sometimes referred to as *burn-in*. But burn-in is actually a *symptom* of the problem that occurs in the older (but still used) cathode ray tube (CRT) type of monitor. While image retention and flickering image issues are more common with CRTs, you might still see them with flat-panel monitors as well. If you use a KVM (keyboard, video, mouse) switch, power cycle that as well. Many KVMs need to be turned on first (and left on for 10 seconds or so) before a connecting computer can be turned on; otherwise, that computer won't display through the KVM properly.
- **Check for an onboard video setting in the UEFI/BIOS:** If you install a new video card in a computer that previously used onboard video, check that the onboard video setting is disabled in the UEFI or BIOS. It can conflict with the new video card. And, of course, be sure to plug the monitor into the new video card—not the old onboard connection.
- **Modify resolution and refresh settings:** If the resolution was set too high or was set to a resolution not supported by the monitor, you might get a distorted image, a fuzzy image, or no image at all. In Windows, boot into low-resolution VGA mode or Safe Mode. This starts the computer with a resolution of 640×480. Then modify the resolution setting in the Screen Resolution window. Lower resolutions will result in oversized icons and images that might be preferable to some but will make it difficult for the typical user to view all the information required on one screen (for example, within a spreadsheet or AV editing program). Simply increase the resolution to "resolve" the problem! For CRT monitors, an incorrect resolution setting could cause distorted geometry—where the image doesn't fit the display properly—although this might also be caused by poor horizontal or vertical settings on the monitor itself. The refresh rate can also cause issues if it is not set correctly (for example, screen flicker, flashing screen, or no display at

all). The refresh rate is the number of times that the screen image is refreshed per second; a common number is 60 Hz. The number it is set to should coincide with the monitor's capability. You'll learn more about resolution and refresh rate in Chapter 36, "Windows Control Panel Utilities."

- **Adjust screen sizing and scaling issues:** If the display resolution is misconfigured, it may result in oversized or undersized content on the screen. For instance, text, icons, and images may appear too large, extending beyond the screen's edges, or too small, making them difficult to read. These issues are commonly caused by incorrect resolution settings in the operating system or scaling settings on the monitor. To resolve this problem, ensure that the display resolution matches the monitor's native resolution. In Windows, go to **Display Settings** and adjust the scaling percentage to ensure elements are appropriately sized. Monitors with built-in scaling options might require adjustments via the OSD menu. Additionally, incorrect aspect ratios, such as using a 16:9 resolution on a 4:3 monitor, can also lead to sizing problems. Always verify that the resolution and aspect ratio align with the monitor's specifications.
- **Check the driver:** Maybe the driver failed, or perhaps the wrong driver was installed. Maybe an update is necessary, or perhaps an update to the driver is causing the problem. If there is nothing on the display, or if the image is distorted, or if the monitor only displays a lower resolution, boot into low-res mode or Safe Mode and update the driver from within Device Manager (in Windows) or consider "rolling back" the driver, which means reverting to the older driver that was installed previously. Driver failures can also be the cause of blue screens of death (BSODs).
- **Check the version of DirectX:** DirectX is a Windows technology that includes video, animation, and sound components. It helps a computer get more performance out of multimedia, games, and movies. The DirectX Diagnostic Tool (DxDiag) helps troubleshoot DirectX-related issues. This tool provides information about the installed version of DirectX and whether it is operating correctly, among other things. You can start the DirectX Diagnostic Tool by opening the Run prompt and typing **dxdiag**. By default, Windows 10/11 uses DirectX 12. However, it can be updated to newer versions if necessary.

> **Note**
>
> We've mentioned Windows several times in this chapter. We'll cover DirectX and other Windows utilities in depth in Chapters 32 through 37.

- **Check the temperature threshold of the video card:** High-end video cards are intensely used by gamers and designers, and such a card can be the hottest component in a computer. If the temperature surpasses the safeguards in place, it might cause the card to throttle back the GPU speed, or it might cause an overheat shutdown, where the video card might stop working altogether, causing the current application to close or, at worst, the display to go blank. If this happens more than once or twice, consider additional cooling fans or a liquid cooling system.
- **Use software to check and repair stuck or dead pixels:** When a single pixel fails, it can be irritating. But you can use third-party software programs to identify stuck pixels and possible dead pixels and attempt to fix them. (Search "LCD repair," "dead pixel repair," or similar terms.) Try power-cycling the device as well. If you can't repair a stuck or dead pixel, you might have to send the display to the manufacturer or an authorized repair center for repair or for replacement. If it is a laptop, replace the screen yourself!
- **Calibrate the monitor:** If you see artifacts (image distortions) or notice incorrect color patterns being displayed, or if the display just doesn't seem to look quite as good as it used to, try calibrating the monitor either by resetting it with the OSD or by adjusting the contrast, brightness, and color levels. Also try adjusting the color depth in Windows and check the screen resolution. You can also try using the built-in Windows Display Color Calibration tool, which can be accessed by going to Search and typing **color calibration** or by going to Run and typing **dccw**. Try to limit reflections on the screen. If you are using an older CRT monitor and the artifacts still appear, consider upgrading to an LCD display. Dim images could also be caused by misconfigured brightness and contrast. Always configure the brightness first, and once the optimal brightness level has been found, configure the contrast.

ExamAlert

If you see artifacts (image distortions) or notice incorrect color patterns being displayed, try calibrating the monitor either by resetting it with the OSD or by adjusting the contrast, brightness, and color levels.

- **Adjust distorted images:** This issue can manifest as stretched, compressed, or misaligned visuals on a screen. These distortions are often the result of resolution mismatches or improper monitor calibration. For example, running a widescreen resolution (16:9) on a standard 4:3 monitor can cause images to appear stretched or squished. Incorrect geometry settings, such as trapezoidal or pincushion distortions, are more common with CRT monitors but may still occur on certain flat-panel displays. To resolve these issues, ensure that the resolution and aspect ratio match the monitor's specifications. Additionally, check the video driver settings and verify that the GPU is outputting the correct signal for the connected display. If the problem persists, recalibrate the monitor using the OSD or built-in calibration tools, and adjust horizontal and vertical alignment if necessary. For external displays like projectors, verify that keystone correction settings are properly configured to eliminate image distortion.
- **Use a filter on the monitor:** Sometimes users will complain of eye strain. This might not be a video issue at all; it could be due to glare. Consider using an antiglare filter. Companies make these filters specifically for individual monitor models. They help reduce glare from fluorescent lights, sunlight, and so on. In a more secure environment, consider also using privacy filters. They reduce the viewing angle of the screen—so that only the person sitting directly in front of the screen can read it—and help reduce the chance of shoulder surfing. Privacy filters often reduce glare as well.
- **Check for newly installed applications:** New applications could cause the display to malfunction or stop working altogether. Check the application manufacturer's website for any known hardware compatibility issues.

- **Check inside the computer:** Unless we have a sneaking suspicion that one of the connections inside the computer is loose, we usually leave this check for last because it is time-consuming to open the system. If you decide to check inside the computer, check whether the video card is seated properly. In areas in which the temperature and humidity change quickly, the card could be unseated due to thermal expansion and contraction. (Some refer to this as chip creep or card creep.) Also, if the computer was moved recently, it could cause the card to come out of the slot slightly. Verify that the power connections and other cables are not loose. Check all other connections inside the PC to make sure it isn't a video problem. For example, if the system uses an onboard video controller and you start seeing garbled images, strange colors, or cursor trails, you might have defective RAM (or maybe you have been working on computers too long). Remember that onboard video controllers rely on the sticks of RAM in the motherboard, whereas individual video cards have their own RAM.

Again, verify that the problem is actually the video. Don't forget about the other major components of a computer system. When you can't see anything on the display and you know the computer is receiving power, you can narrow down the issue to video, RAM, processor, or the motherboard (what we sometimes refer to as the "big four"). But if the system appears to boot, and you can see storage drive activity from the LED light on the front of the case, and/or hear the drive accessing data, then it is most likely a video problem. Go back to the basics: Check power and connections. Check the data source at the OSD of the monitor. Try substituting a known good monitor in place of the current one. When it comes to video, as with most other things in life, the simple answers are usually the most common.

External Laptop Monitors and Projectors

We discussed laptops in the beginning of the book, but we should also include them here because we are talking about video troubleshooting. And you'll probably get your hands dirty with projectors as well. Let's briefly consider some usage and troubleshooting techniques for those now.

External Laptop Monitors

Most laptops have the capability of sending video signals to an external monitor. Some people refer to this technology as *screen switching* and/or extending the display.

Almost all laptops come with an external connection (for example, HDMI or DisplayPort) for a second monitor or for a projector. When such a monitor is plugged in, you can enable it by pressing the display toggle key (otherwise known as the secondary monitor button). On some laptops, you can do this by pressing Fn+F4 simultaneously. However, on other brands of laptops, this key might be different than F4. The icon on the key often looks like an open laptop with a monitor to its right. Normally, you have several options: Display the desktop to the laptop, display the desktop to the external monitor, display a copy of the desktop to both screens, or "extend" the desktop across both monitors. These last two options are also known as using *dual displays*. In addition to using the display toggle key, you can configure your video for any of these scenarios in Windows, macOS, or Linux, which we'll discuss later in the book.

If an external monitor won't display anything, make sure that the cable is firmly connected to the external port, verify that the external monitor is plugged in and is turned on, and then try cycling through the various video options by pressing the button several times, waiting a few seconds each time. Make sure you are holding down the Fn key while doing so. Finally, restart the computer if necessary.

By the way, HDMI and DisplayPort connections and cables have the ability to transmit video *and* audio. However, DVI does not. Understand this if you need to transmit audio over the video cable to an external monitor. Verify that the external monitor is set to the correct video standard and that audio is enabled (if necessary, within the OSD). You might need an adapter to change from one video standard to another—for example, if a laptop has a DisplayPort connection but the external monitor only has HDMI. In this scenario, DisplayPort can support video and audio transfer with the use of a proper adapter.

Also, know how to set the audio output from a laptop or PC so that it will output through the HDMI or DisplayPort cable properly. For example, in Windows, you can go to **Settings > System > Sound** or simply right-click the speaker icon in the notification area and select **Open Sound Settings**.

(Or, for the Control Panel option, go to Run and type **mmsys.cpl**.) From there, you can select the output device to use. Think about it: You don't want to display video on a 60-inch TV and have weak, tinny audio coming from a laptop somewhere else in the room, right? The attendees' focus should be on the display and the presenter. You might also need to adjust the volume for that connection with the volume mixer, which you can also get to by right-clicking the speaker icon. For a presentation to be great, you need audio!

ExamAlert

Know how to configure Windows to output sound to an external monitor via HDMI or DisplayPort!

Projectors

We haven't covered projectors yet, so let's talk about them briefly.

A video projector can be plugged into a computer's external video port to project the computer's video display to a projection screen. An extremely bright bulb is necessary to project this image to the screen. The light output is measured in *lumens*. A typical high-def projector might output 2000 to 3000 lumens. This is *really* bright, and you should never allow a person to look into the projector's lamp! Increased lumens are necessary for locations with higher amounts of ambient light (that is, existing light in the room).

Projectors are used for presentations and for teaching and are common in conference rooms and training centers. However, some schools and companies opt to use large, flat-screen TVs instead of projectors, even though projectors can usually project a larger image. Projectors are available in LCD, LED, and Digital Light Processing (DLP) versions. The LCD type works in a similar fashion to the monitor technology of the same name, whereas DLP uses light valves with rotating color wheels. Common high-definition display resolutions used by projectors include 1080p and 4K; the price of the projector increases with the resolution standard and with other characteristics, such as the brightness, contrast, and noise. You

can use a video projector with a laptop by using the display toggle button, or you can use a projector with a computer that has a video card with dual outputs.

Troubleshooting can get a little tricky when you are using a projector as the second display. A projector might need time to warm up or might need to be configured via its own OSD. You might also need a video adapter if your laptop's ports and projector's ports don't match up. Identify the projector's ports and consult the projector's documentation for more details.

Bulbs fail, and you should be prepared to encounter burned-out bulbs in projectors now and again. A failed bulb is evident because no light comes from the projector at all. (The device might even flash a message on an OSD.) Be sure to replace a bulb with the exact type for the model of projector in question; it's also wise to go with manufacturer bulbs or manufacturer-suggested bulbs because they usually work better out of the box and last longer. Before replacing a bulb, make sure to power down the unit and unplug it. Many projectors are mounted to the ceiling; so have a step ladder ready. A projector's bulb is usually behind an access panel. Watch the orientation of the bulb and consider taking a picture of it so that you know how to orient the new bulb. Make sure the bulb makes full contact inside the projector. Then, close the access panel securely, plug in the projector, and power it on. If all goes well, there should be light! Reset the lamp counter to zero hours. This counter can be found in one of the menus in the OSD of the projector.

You might also encounter intermittent projector shutdown. This issue could be due to several things, including environmental factors, poor installation (such as the projector not having any space to exhaust heat properly), or a faulty bulb. It usually means that the projector has overheated. Check for good airflow and check the bulb. As mentioned, bulb issues are less common if you use manufacturer-recommended bulbs. Also, ensure that the cooling fan is working and replace it if necessary.

ExamAlert

Remember that the reason for intermittent projector shutdown can be several things, including environmental factors, poor installation

(such as the projector not having any space to exhaust heat properly), or even a faulty bulb. It usually means that the projector has overheated.

Another intermittent issue is screen flicker or random display shutoff, which could be due to a faulty cable. (In fact, we see this often.) Use a quality cable, and make sure the plugs are intact and haven't been damaged. Also make sure that you are not exceeding the maximum length for any particular video standard. For example, as a rule of thumb, a practical limit for HDMI cables that are transferring 1080p signal is 25 feet (7.6 meters); higher resolutions allow shorter distances. HDMI cables are usually rated based on the number of feet in distance they can transmit signal. A cable rated for longer distance is usually a thicker, stronger cable. Use the right one for the resolution being passed by the laptop or other device. If you are in a situation where you don't know where a cable came from, try to decipher the writing on the cable to find out what it is rated for or simply replace it with the proper cable if it doesn't appear to work properly.

ExamAlert

Use quality cables that are rated for the distance you need and the resolution at which you wish to transmit!

If extenders are being used, make sure they are of good quality; it's recommended to use an active extender (meaning one that plugs into an AC outlet) as opposed to a passive one.

One last thought: *When troubleshooting, write it down*. A quick sketch, diagram, or even a photo can work wonders for your thought process, especially when you have a chain of devices, cables, and equipment to troubleshoot. This technique can also be helpful when you take the A+ exams.

Cram Quiz

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

1. A user set the resolution in Windows too high, resulting in a scrambled, distorted display. What should you do to fix the problem? (Select the best answer.)

   - ○ **A.** Upgrade the video driver.
   - ○ **B.** Boot into low-resolution mode.
   - ○ **C.** Press the monitor toggle key.
   - ○ **D.** Check the video connections.

2. You are troubleshooting a video issue. Which utility should you use?

   - ○ **A.** Regedit
   - ○ **B.** Msconfig
   - ○ **C.** DxDiag
   - ○ **D.** Task Manager

3. You receive a basic computer that has a broken onboard DVI connector. What should you attempt first?

   - ○ **A.** Replace the motherboard.
   - ○ **B.** Replace the DVI connector.
   - ○ **C.** Install a video card.
   - ○ **D.** Use an adapter.

4. You just replaced a video card in a PC with another card from a different manufacturer. However, the driver installation does not complete. What should you do first?

- ○ **A.** Install the driver again.
- ○ **B.** Locate the latest version of the driver.
- ○ **C.** Roll back the driver.
- ○ **D.** Install the original video card.

5. You are helping a project manager with a presentation using a laptop that feeds video to a projector. During your tests, the projector's image begins to flicker. The laptop's display does not have any problems. You attempt to change the resolution on the laptop, but the issue continues. Which of the following should you do next?

- ○ **A.** Change the projector settings.
- ○ **B.** Check the connectivity of the video cable.
- ○ **C.** Change the aspect ratio of the laptop.
- ○ **D.** Check the connectivity of the power cable.

6. A user needs to transmit video and audio to an external monitor. Which of the following technologies allows this? (Select two.)

- ○ **A.** OSD
- ○ **B.** HDMI
- ○ **C.** DisplayPort
- ○ **D.** DVI
- ○ **E.** VGA

7. What are common causes of distorted images or misaligned visuals being displayed on a monitor? (Select all that apply.)

- ○ **A.** Resolution mismatches
- ○ **B.** Burned-out bulb
- ○ **C.** Incorrect input source
- ○ **D.** Improper monitor calibration

Cram Quiz Answers

1. **B.** Boot into a low-resolution mode. In Windows, this is called Enable Low-Resolution Video. Safe Mode is another valid option, but keep in mind that Safe Mode loads Windows with a minimal set of drivers, and you can't access the Internet. Depending on the display configuration, pressing the monitor toggle key might actually fix the problem temporarily by displaying the screen on a secondary monitor, but it doesn't solve the root cause of the problem.

2. **C.** You should use DxDiag to troubleshoot video issues. The other three answers are not used to troubleshoot video. Regedit is used to perform advanced configurations in the registry. Msconfig is used to change how the system boots and to enable/disable services. The Task Manager is used to see the performance of the computer and view applications and processes that are running. We'll discuss the rest of those tools in more depth in the Windows portion of this book.

3. **C.** Try installing a video card first to see if the system will still work. Unless it is a specialized system, the video card should be less expensive than the motherboard. (In addition, it will take a lot less time to install.) PC techs usually do not replace connectors, and this step should be further down your troubleshooting list. An adapter cannot help if the DVI port is broken.

4. **C.** If the driver installation doesn't complete, you should roll back the driver. It could be that you have attempted to install the incorrect driver. After you roll back the faulty installation, find the correct latest version of the video driver from the manufacturer's website. Installing the driver again will most likely have the same result. Only reinstall the original video card temporarily if you cannot find a proper solution right away.

5. **B.** Check the connectivity of the video cable. If it is flickering, chances are that the cable is loose, or the cable's quality is lacking. Screen flicker is more common with older VGA cables, but it can

happen with just about any connection, depending on the age and quality of the cable. Remember, always check the basic stuff first: connectivity, power, and so on. It is unlikely that the projector settings will make a difference in this particular case. You cannot change the aspect ratio by itself on most laptops; however, when you change the resolution (which was already done, according to the question), you might be changing the aspect ratio as well, depending on the resolution selected. A loose or damaged power cable would probably result in more than just screen flicker; the projector might power off and power back on, which would prevent the image from being displayed for at least several seconds while the projector powers back up.

6. **B and C.** HDMI and DisplayPort connections and cables have the ability to transmit video *and* audio. However, DVI and VGA do not. An onscreen display (OSD) is a computer monitor control panel that allows you to adjust horizontal/vertical positioning, contrast, brightness, and other monitor settings. On a side note, keep in mind that USB-C can also transfer video, audio, *and* data.

7. **A and D.** Distorted images can manifest as stretched, compressed, or misaligned visuals on a screen. These distortions are often the result of resolution mismatches or improper monitor calibration. For example, running a widescreen resolution (16:9) on a standard 4:3 monitor can cause images to appear stretched or squished. To resolve these issues, ensure that the resolution and aspect ratio match the monitor's specifications. Burned-out bulbs are related to projectors. Bulbs fail, and you should be prepared to encounter burned-out bulbs in projectors now and again. A failed bulb is evident because no light comes from the projector at all. Be sure to replace a bulb with the exact type for the model of projector in question. If the monitor is using an incorrect input source (for example, if a PC is connected to a monitor by way of DisplayPort, and the monitor's onscreen display [OSD] is set to HDMI), the monitor won't receive any signal; the monitor will simply display a black screen. Always check which video port the monitor is configured to use by accessing the OSD with the appropriate button on the monitor.

We hope this chapter has been enlightening and that we have projected some of our experience on to your brain. Dad jokes aside, great work so far! Review your notes, take a short break, and continue!

Chapter 26

Troubleshooting Mobile Devices

This chapter covers the following A+ 220-1201 exam objective:

- **5.4** – Given a scenario, troubleshoot common mobile device issues.

It's time to think portable and mobile. Fixing mobile devices can be a life-long career. Just look at the abundance of mobile device repair shops: There seems to be no end to cracked screens, missing displays, overheated devices, and battery issues to sustain all these shops. And most mobile devices can be difficult to open and work on because of their small size.

There is some overlap between this objective and 220-1202 Objective 3.2. Some of the content (mostly hardware-based) we'll cover here, while the rest (mostly software-based) we'll cover in Chapter 54, "Troubleshooting Mobile Operating Systems and Applications."

ExamAlert

Objective 5.4 focuses on troubleshooting common symptoms of mobile device issues, such as poor battery health, swollen batteries, broken screens, improper charging, poor/no connectivity, liquid damage, overheating, digitizer issues, physically damaged ports, malware, cursor drift/touch calibration, inability to install new applications, stylus not working, and degraded performance.

Mobile Device Display Troubleshooting

The display is the cause of many user headaches. Lots of things can go wrong with it. Sometimes devices fail, but more often than not, such issues are due to user error or, more accurately, user ignorance.

For example, the display might look dim. The reason could be that the brightness level is too low in the display settings. Or it could be that automatic brightness was enabled, and perhaps it doesn't react well in highly lit areas. Or perhaps auto-brightness isn't calibrated properly; perhaps it was initially enabled in a very bright (or very dark) environment. To recalibrate the device's light sensor, turn off auto-brightness and then go to an unlit room and set the brightness to the lowest setting. Finally, turn auto-brightness back on and leave the unlit room. The device should now make better use of its light sensors, and auto-brightness should function better.

You might also encounter a situation in which there is no display whatsoever or in which there appears to be no display. The reason could simply be that the device is in sleep mode or turned off. Always check the simple solutions first; they work more often than you might expect! Another issue could be that the brightness (once again) is at the lowest setting and the user is working in a bright area. When taking a device out of sleep mode, the user might not be able to tell that the display is working because it might be barely visible. Take the device to a dark area to fix it or hold it under a desk or table so that you can see the screen until it is fixed. The brightness might have been turned down by accident, the user might have turned it down the night before (because it was dark out), or a virus could be affecting the slider that controls the brightness.

Brightness is definitely a common culprit. Let's just thank our lucky stars that there is no contrast setting on the majority of mobile devices! However, no display or a nonresponsive display could also mean that the device is turned off or that the battery has been discharged. It could also be that the display needs to be calibrated. Finally, the display connection might be loose, or the display might be damaged. In these last two scenarios, the device will have to be opened to repair or replace the display. If your organization uses an authorized repair center to perform these duties, and

the device is under warranty, document what the problem is and pack it securely to be shipped out right away. For disassembly tips, see the last section of this chapter, "Disassembling Processes."

Mobile Device Overheating

How many times have you heard a user say that a mobile device is running hot? How many times has your own device run hot? It's common. Overheating can be caused by a number of issues: poorly written applications, excessive use of applications, excessive browsing, old batteries, damaged batteries, and, of course, the simple fact that the device is very small, and there is an inherent lack of ventilation.

ExamAlert

Mobile devices can overheat when they're exposed to too much heat, like direct sunlight, or when running too many apps. Overheating can cause your phone to slow down, stop charging, or even disable the camera flash!

Some applications use a lot of power (CPU-wise and battery-wise). These applications tend to slow down a mobile device, eat up battery reserves, cause power drain, and make a device run hot. Certain GPS programs, games, and streaming media apps are among the top offenders, but just about any app could cause such issues. And then you have the aging effect; newer apps don't run very well on older devices because of the lack of resources, and they can overheat the device. Unfortunately, there isn't too much the user can do about this problem other than remove apps suspected to be the cause and disable unnecessary functionality on the device. Does the user need that live wallpaper? Has that user collected enough "coins" in that game? You know what we mean. Let's not forget about mobile OS updates; they can make a device feel like it was in an oven. This is normal, and the device should be plugged in and placed in a cool area, away from sunlight, while an update proceeds.

Degraded performance on mobile devices is often caused by resource-intensive applications, outdated software, or insufficient available storage. A common symptom is slower response times when launching apps or navigating menus. To troubleshoot, first close unnecessary background apps to free up RAM and reduce CPU usage. Check the device's available storage and delete unused apps, large files, or cached data to optimize performance. Verify that the operating system and apps are updated to their latest versions because updates often include performance improvements and bug fixes. If the device feels warm, overheating can also contribute to the issue. Refer to the section on overheating for additional steps. Last, consider restarting the device because doing so can clear temporary files and refresh system processes.

A device factory reset may be necessary if it's acting up or you want to start fresh, or you might need to reset your phone if you're selling it. To reset the device, you should

1. Back up your data.
2. Go to your phone's settings and find the Factory Data Reset option.
3. Select **factory data reset**.
4. Confirm that you want to erase all data.
5. Wait for the reset to complete.

A device's battery can get hot simply because it is old (or damaged). Battery manufacturers use the term *charging cycle* to refer to the process of charging a mobile device that is completely discharged up to 100 percent. Most battery manufacturers say that a typical battery can handle a maximum of several hundred charge cycles. This essentially means that a typical smartphone battery has a shelf life of about three to five years because most people charge their phone every day. Tablets usually last much longer because of the greater battery capacity and the fact that they aren't charged as often. So, it's mobile phones that we are most concerned with. A user can do the following to increase the lifespan of their battery:

- **Avoid draining the battery:** Charge the device often, before it gets too low. The more the battery is discharged below 50 percent, and

especially below 10 percent, the less shelf life it will have in general.

- **Conserve power:** Set sleep mode to 1 minute or less. Decrease brightness. Disable or remove unnecessary functions and apps. Restart the phone at least once a day to stop any running apps. (This is a big power saver.) Consider putting the device into airplane mode at night.
- **Keep the device away from heat sources:** For example, if the device is mounted near a vehicle's air vent during the dead of winter, it's bound to run hot. Sarcasm aside, this can actually cause battery wear and damage over time. Keep it out of direct sunlight too, if at all possible.
- **Turn off the mobile device when not in use:** Some people simply cannot do this, but we thought we'd mention it anyway!
- **Don't bang or throw the device:** It might seem crazy that we would have to say this, but it's good advice. Dropping, throwing, or banging a device can break the device completely, damage the battery and cause it to overheat, reduce the lifespan of the battery, or cause a battery leak, which is a toxic mess that you don't want to be a part of.
- **Select protective cases carefully:** Using a protective case is a very good idea (especially for a user who is prone to actions in the previous bullet), but make sure it has good airflow. Sometimes these cases can envelop the battery, causing it to overheat.

ExamAlert

Know how to increase the lifespan of a mobile device's battery.

More Mobile Device Troubleshooting

When it comes to mobile devices, batteries—and power in general—tend to account for a lot of troubleshooting.

For many users, mobile devices need to be charged daily. As you have probably experienced, charging issues are common. A mobile device not charging or charging improperly could be due to many things, but the cable is the first thing to check and is usually the culprit. Inspect the charging

cable for rips, bends, or cuts. Check the cable—especially the connector ends—for any discoloration or burn marks. If any of these things are identified, it's time for a new charging cable. Check the device's charging port for dust and debris. Clear it out with compressed air and clean it as well (following the cleaning recommendations below). Unfortunately, if the port(s) is damaged, the entire device may need to be replaced.

No power or failure to charge could be a sign that the battery needs to be replaced—either because it is simply too old and won't hold a charge anymore or because it is damaged. Battery damage can manifest internally (which can't be seen with the naked eye), or it could show up as a visibly swollen battery. As mentioned previously in the book, watch out for swollen batteries; they could be caused by damaging the battery, overcharging it, overvoltage, or a manufacturing problem. A damaged battery should be removed (if possible); use great care if you are the one handling the battery and make sure it is stored in a cool, dark place until it can be recycled. If it can't be removed, the device should be taken to an authorized repair center.

Be sure to clean your device. Every month or so, turn off the device, take it out of the case, and clean it (as well as the inside of the case) with a mix of half isopropyl alcohol and half water (applied to a dry, lint-free cloth). Take extra care when cleaning the charging port: Use a cotton swab and/or toothpick. This technique really works in situations when the device is not charging properly. Use that solution sparingly, though; a little goes a long way.

A battery issue could also cause a system to "freeze," or lock up, rendering it useless; however, a frozen system could also be caused by faulty applications or a problem with the mobile OS or a driver. If a system freezes, it might require you to force stop an application, perform a battery pull (if possible), or, more likely, a soft reset (again, if possible). You might need to initiate a hard reset, which you normally want to avoid if you can because it will wipe the system. We'll discuss force stops and resets in Chapter 54.

One common issue users face is being unable to install new applications on their mobile devices. This can happen for several reasons, such as insufficient storage space, operating system compatibility issues, or

restrictions on app installations. Begin troubleshooting by checking the device's available storage and deleting unnecessary files, applications, or cached data to free up space. Next, verify that the operating system is up to date because some apps require specific OS versions to run. Additionally, ensure that app installation permissions are correctly configured in the settings menu. For users trying to install apps from third-party sources, remind them to enable the Install from Unknown Sources option (if supported), but caution them about potential security risks. If the issue persists, suggest restarting the device and retrying the installation.

If a mobile device is the victim of liquid damage, remove the device from the liquid immediately. Turn off the device and leave it off until cleanup is complete. Remove any protective case and remove any microSD cards, SIM cards, and batteries (if possible). Use a clean cloth to dry the device as much as you can. If the liquid in question was not water, you can later attempt to clean the screen and charging port with the isopropyl alcohol solution mentioned previously. After the device is completely dry, return any microSD cards, the case, and so on, and see if it will boot. Because many devices are IP68 (or IP65) compliant, the device may still work because it has a certain level of protection against water and dust.

Sometimes the touchscreen (or digitizer) of a mobile device may become nonresponsive. There are several potential reasons for this:

- An application or the OS has failed.
- The system has frozen.
- The display connection is loose.
- The display needs to be replaced.
- User error has occurred.

If a stylus is not working with a mobile device, the issue could stem from several sources. First, check whether the stylus is compatible with the device; not all styluses work with all screens because some require specific technologies such as active digitizers or Bluetooth connectivity. If the stylus uses batteries, ensure that they are properly installed and have sufficient charge. Inspect the stylus tip for damage, and replace it if necessary. For

Bluetooth-enabled styluses, check the device's Bluetooth settings and ensure the stylus is paired correctly. If the stylus still does not work, try restarting the device or calibrating the touchscreen. In some cases, the issue could be due to a faulty digitizer, which may require repair or replacement.

The last reason in the preceding list should always be on your mind. A person might be wearing gloves that prohibit proper touchscreen response. Or perhaps the person is using the wrong type of stylus or the touchscreen doesn't accept stylus input. Perhaps the touchscreen needs to be calibrated; this is not very common with today's devices, but it is possible. Be ready for a variety of issues!

No sound from the speaker? Start with the easy stuff, such as checking whether the volume is muted or turned down. It is not always easy for some users to figure out sound issues because of the built-in mixer in most of today's smartphones: There are separate volumes for voice calls, media, notifications, and so on. So even though one volume might be up, another might be down. Or perhaps the speaker has been blocked by a protective case that doesn't fit quite right. Or maybe an app simply isn't registering sound correctly or has its own volume or mute option. It's unlikely, but another possibility is that the speaker connection is loose, or the speaker has failed. For such issues, a tech needs to open the device or send it out for repair.

Keep an open mind. When you are dealing with technology that can potentially fail often, combined with users who might not have been trained to use devices properly, you can expect to do *lots* of troubleshooting.

Disassembling Processes

You should try to disassemble mobile devices in a logical manner, so that when it comes time to put them back together, you will not be confused and can reduce the chance of making mistakes. The first and best way to do this is to document what you do. Just as with bigger computers such as PCs, you should write down as much as you can. Take notes and make little illustrations—even if your artwork is a bunch of chicken scratches! Organize any parts that have been removed. Document and label wires and cables and where they are supposed to connect. Record what types of

screws go where and store the screws temporarily in an organized manner. Some people put them all in a bowl or can. Another option is to use a large weekly pill box (which many healthcare organizations give away for free). In your documentation, mark which screws are where; for example, Monday has the #6-32 thumbscrews, and Tuesday has the T4 Torx screws, and so on. Chances are that you won't see both thumbscrews and Torx screws on the same device because they are for different devices (PCs and phones and similar devices, respectively). Take photos with your smartphone or another digital camera during the disassembly process. These are just some examples! Remember that good documentation aids in efficient planning, proper testing, and insightful troubleshooting.

Make use of manufacturer resources, such as tech support via phone, email, or website; help forums; downloadable manuals in PDF format; and information on removable media.

ExamAlert

Use manufacturer-supplied resources such as manuals, tech support, and forums to help troubleshoot issues.

Use appropriate hand tools when working with mobile devices. Of course, first make sure you are protecting against electrostatic discharge (ESD)—which means using proper antistatic equipment. Also, have your tools at the ready: miniature screwdrivers, shims, spudgers, magnifying glass, mini-flashlight, multimeter and other testing gear, SD and microSD card reader, and various USB, Lightning, and other cables and adapters for hooking up the mobile device to a testing PC or laptop. Take a look at Figure 26.1 for an example of some of the hand tools we use on mobile devices. The list goes on, and there are several manufacturers of mobile device toolkits that can help you on your way toward mobile device repair. Make sure that you are not using magnetically charged tools, and again, implement ESD prevention procedures before you start working.



FIGURE 26.1 **Mobile Device Hand Tools**

Cram Quiz

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

1. A user's mobile device is overheating. Which of the following could be the problem? (Select the two best answers.)

   - ❍ **A.** A damaged battery.
   - ❍ **B.** The brightness setting is too low.
   - ❍ **C.** Excessive gaming.

- ○ **D.** The device is not in a case.
- ○ **E.** The charging cable is defective.

2. You are troubleshooting a user's smartphone. The user is unable to see anything on the screen. Of the following, what should you do first?

- ○ **A.** Disassemble the device for proper reassembly.
- ○ **B.** Check the volume mixer sliders.
- ○ **C.** Verify the brightness setting.
- ○ **D.** Calibrate the screen.
- ○ **E.** Restart the phone.

3. When disassembling a mobile device, what should you *not* do?

- ○ **A.** Document everything you see.
- ○ **B.** Store screws in a logical manner.
- ○ **C.** Make use of manuals.
- ○ **D.** Implement antistatic procedures.
- ○ **E.** Use magnetic-tip screwdrivers.
- ○ **F.** Label cables.

4. Which of the following are common reasons that a mobile device might not charge properly? (Select three.)

- ○ **A.** Airplane mode is activated.
- ○ **B.** A cable is ripped or bent.
- ○ **C.** A port is dirty.
- ○ **D.** A port is damaged.
- ○ **E.** The user installed *Asteroid Blaster*.

5. What can cause a digitizer to become nonresponsive? (Select three.)

   - **A.** Application failure
   - **B.** Defective charging cable
   - **C.** Loose display connection
   - **D.** User error
   - **E.** Disabled audio

Cram Quiz Answers

1. **A and C.** The best answers listed are a damaged battery and excessive gaming. If the brightness setting is low, the device should use less power and run cooler. If the device is not in a case, it should not overheat; however, a poorly manufactured case could cause the device to overheat. A defective charging cable usually does not cause a device to overheat; if it is defective, it is likely not even charging the device.

2. **C.** Check the brightness slider first! Chances are that the brightness is turned all the way down, and in a bright environment, it might appear that nothing is on the screen. Or the device might simply need to be woken up, so use the side button or the home button or double tap the screen to wake up the device. If these measures are not successful, restart the device. Screen calibration has nothing to do with brightness, but on some rare mobile devices, it might be necessary. The volume sliders are not part of the problem. Don't open the device until you have exhausted every other known option—and do so only if you are qualified to work on this type of device; otherwise, send it to an authorized repair center.

3. **E.** Stay away from magnetically charged tools such as screwdrivers and bits. These can potentially damage circuitry and components. All of the other answers are valid procedures—things

you *should* do when working on mobile devices, and computers in general.

4. **B, C, and D.** A mobile device not charging or charging improperly could be due to many things, but the cable is the first thing to check and is usually the culprit. Inspect the charging cable for rips, bends, or cuts or damage to the connector. Check the device's charging port for dust and debris and use compressed air to clear it out. Unfortunately, if the port(s) is damaged, the entire device probably needs to be replaced. Placing the device in airplane mode actually conserves battery power and won't normally have an impact on the device's ability to charge properly. Installing apps on a mobile device will usually not have an effect on the device's ability to charge properly (unless a virus was unknowingly downloaded with the app). However, many apps (especially games) can drain the battery quickly.

5. **A, C, and D.** There are several potential reasons a digitizer might be nonresponsive, including failure of an application or the OS, a frozen system, a loose display connection, a failed display, and user error. For example, something might be interfering with the touchscreen; perhaps the user is wearing gloves that prohibit proper touchscreen response. A bad charging cable and disabled audio are not likely to cause a digitizer to become nonresponsive.

Chapter done. You're getting very close to the end of the 220-1201 material. Great job!

Chapter 27

Troubleshooting Wired and Wireless Network Problems

This chapter covers the following A+ 220-1201 exam objective:

- **5.5** – Given a scenario, troubleshoot network issues.

In this chapter, we'll discuss troubleshooting of network connectivity issues. Because you will have users who connect in a wired fashion and other users who connect in a wireless fashion—and some connecting both ways—you have to be ready to support a variety of network connectivity. The goal of this chapter is to explain some basic troubleshooting techniques in a generic sense and ensure you have the right troubleshooting mindset.

To perform their work, users need access to resources, and network connectivity enables this access. Network connectivity is crucial. A faulty network connection means little to no available resources and, consequently, little to no work getting done.

ExamAlert

Objective 5.5 concentrates on troubleshooting common symptoms of wired and wireless network problems, such as intermittent wireless connectivity, slow network speeds, limited connectivity, jitter, poor VoIP quality, port flapping, high latency, external

interference, authentication failures, and intermittent internet connectivity.

Troubleshooting Common Symptoms

Network troubleshooting? Oh yes, it could be one of the best ways to learn how networks operate. We recommend reviewing the networking chapters in this book (Chapters 4 through 11). And, most importantly for successful troubleshooting, remember to check the simple and obvious first. For example, physical power connections and network connections or disabled wireless connections are common culprits for network problems.

When you think about network troubleshooting, you should consider access to resources. If a resource—be it a data share, a printer, or something else—is unavailable, users won't be able to get their work done. Efficiency decreases, and the organization loses money.

Resources can be broken down into two types—local resources (those on the LAN) and remote resources (those beyond the LAN, possibly on the Internet or another external network):

- **Local resources:** You might find that a user can't browse the network or map network drives to network shares, or connect to network printers, or access an email server on the LAN. There are lots of examples, but the bottom line is that if a user can't access local resources, you need to troubleshoot the network connection. That's the bulk of what we discuss in this chapter. If multiple users can't access resources, you may be looking at a more centralized problem; for example, if a server is down, perhaps a DHCP server is not properly handing out IP addresses to clients or a domain controller has failed, and users cannot be authenticated to resources. This type of issue might go beyond the scope of your work as a technician with the A+ certification, so be prepared to escalate the problem if necessary.
- **Internet-based resources:** If remote resources—for example, websites, VPN connections, and streaming media services—are not available to a user, it could be that the IP configuration (especially the gateway and

DNS settings) needs to be inspected and possibly reconfigured. If multiple users are having connectivity problems, it could be that the gateway itself or the DNS server (among other things) needs to be fixed. Again, escalate the problem if necessary.

All of the following bullet points list symptoms you might encounter that could lead to unavailable resources, either locally or on the Internet, as well as how to troubleshoot the underlying problems:

- **No connectivity:** If a user complains of a problem connecting to the network and you verify that there is indeed a problem, check the patch cable first and verify that there is a link light. Make sure the user's computer is actually connected to the network. If it appears to be a cable issue, use a patch cable tester or cable certifier to test the cable. If it isn't a cable problem, make sure the network adapter is enabled. If it's a laptop (or other mobile device) and the user has a wireless problem, check the Wi-Fi switch or button. Next, run **ipconfig /all** and check the settings. Afterward, ping the local computer to see if TCP/IP works. If you haven't resolved the problem by now (and you probably will have), access the Network and Sharing Center in Windows and view the graphical connections to see if there is a red X anywhere, denoting a problem. Search for and use the network troubleshooter if necessary. You can also right-click the **Network** icon in the Notification Area and select **Troubleshoot problems**. This brings up the Windows Network Diagnostics program; follow the steps for a possible resolution. Don't forget to check for the latest drivers for the network adapter. You can also try rebooting the computer to find out if any programs were recently installed or updated. Sometimes antimalware software or firewall updates can cause connectivity issues. Some switches and routers have the capability to enable/disable specific ports; make sure the port in question is enabled in the firmware.

  If it's a network-wide problem, power down the network equipment (SOHO routers, cable modems, and so on), then disconnect the network and power cables and wait 10 seconds. Finally, reboot the network equipment. If users cannot find the wireless network that they need to connect to using Windows or the wireless adapter's software, find a good third-party Wi-Fi locator program that you can download for free

and perform a wireless site survey. Such programs can locate all wireless networks in the vicinity and display information such as SSID, signal quality, distance, and channel used (as long as the wireless network adapter is functional). If an SSID does not show up in Windows *or* in third-party software, you should enter the SSID manually.

> **Note**
>
> Site surveys use Wi-Fi and other wireless analyzers to understand and map out the wireless infrastructure. One output is a wireless heat map. This provides a visual method for understanding coverage and signal strength.

- **Authentication failures:** Authentication failures occur when a user cannot access network resources due to incorrect credentials or issues with the authentication system. These failures may present as error messages indicating incorrect username/password, account lockouts, or expired credentials. To troubleshoot, first verify the user's credentials and ensure that they are entered correctly. If the user reports their credentials are valid, check whether their account is locked or disabled in the authentication system (e.g., Active Directory). Verify that the authentication server (e.g., RADIUS or domain controller) is reachable, and inspect the user's network configuration to ensure their device is connecting to the correct network and domain. Time synchronization issues between the client and server can also cause authentication failures. Check and align the device's clock with the network time protocol (NTP) server. Lastly, ensure that any multifactor authentication (MFA) tokens are functioning correctly and synced with the server.
- **Limited and intermittent connectivity:** If the problem is limited connectivity, attempt some pings. First, ping the localhost (**ping 127.0.0.1**) to see if TCP/IP is functioning. If that works, ping the router or another system on the network. If that fails, the user has only local area network connectivity. Run **ipconfig /all** and check the rest of the IP settings. If pinging the router *does* work, try pinging a website by

domain name. If that fails, the DNS server address is probably not configured properly. Check it with **ipconfig /all** and modify it in the IP Properties dialog box, if necessary. Run **ipconfig /release** and **ipconfig /renew** if you suspect an issue with obtaining an address from a DHCP server. Intermittent connectivity could be caused by a faulty patch cable, a wireless network adapter that is too far away from the wireless access point (WAP), or a router that needs to be reset. In a larger environment, if a person can access some networks but not others, you might want to try using **tracert** with inaccessible networks to see where the problem lies. This type of network troubleshooting gets a bit more in depth, but the **tracert** program basically shows which router between you and the final destination has failed. We'll cover that command and more networking commands in the 220-1202 portion of this book.

Intermittent Internet connectivity can disrupt workflows and frustrate users. This issue often results from physical problems, such as loose or damaged cables, failing network adapters, or environmental interference in wireless networks. Begin by checking the physical connections, including patch cables and ports, and replace or repair any damaged components. For wireless connections, ensure that the device is within range of the WAP and that the signal is not obstructed by physical barriers or electronic interference. Intermittent connectivity can also be caused by network equipment, such as overloaded routers or switches, or outdated firmware. Restart or update these devices to resolve temporary glitches. On the client side, check for IP address conflicts, incorrect DNS settings, or misconfigured DHCP leases. If the problem persists across multiple devices, contact the ISP to determine whether external factors, such as service outages or signal noise, are affecting the connection.

- **Low RF signal:** A low radio frequency (RF) signal spells doom for wireless users. The first thing to check is the distance of the computer from the WAP. Make sure the computer is within the appropriate range. Take advantage of the network's potential! For instance, if the WAP uses 802.11ax and the wireless adapter is 802.11n, consider upgrading to an 802.11ax adapter. Update the software on the wireless adapter and WAP as well. Placement of the router is important; it should be central to all users and away from sources of electromagnetic interference

(EMI), such as microwave ovens and devices with electric motors. Try a different antenna placement on the router and the wireless adapter. Normally, a 90-degree angle is best, but a little tweaking can go a long way. Also, some routers can boost their wireless signals. Check for this setting in the firmware.

- **Slow network transfer speeds:** The type of Internet connection is the biggest contributor to speed. For example, if a user has dial-up and complains about slow transfer speeds, it's time to upgrade! Even though dial-up can be tweaked for speed, it's simply easier to move up to DSL, cable, or fiber-based services. Slow transfer speeds could also be related to network equipment, patch cables, and network adapters. The newer and faster the equipment and cables, the better the data transfer rate. Of course, slow speeds could also be caused by network-wide congestion. What exactly is running on the network? A detailed analysis of captured packets (via a tool such as Wireshark) can be very telling. Check the router as well. See what kind of traffic is passing through it. Update everything, clear all cache, and power cycle all equipment (off-hours), and you just might see an improvement. If necessary, invest in a newer, faster router.

  It could also be that the user simply has too many open network connections. Run **netstat -a** to see which types of connections the local computer has to the Internet. If you see dozens of established connections, the computer might be compromised by malware or might be part of a botnet. Or perhaps the user runs torrent software or just goes to a lot of websites for various reasons. Advise the user to close any unnecessary programs and limit the number of streams of data.

- **High latency:** Latency is the typical amount of time that it takes for packets of data to travel from one computer to the next. The higher the latency, the worse the experience when it comes to real-time video conferencing, webinars, gaming, and so on. (Another term used to describe latency is *lag*.) To reduce latency, use the techniques mentioned in the previous bullet, especially the part about closing any other programs and connections that are running. The most bandwidth-intensive culprits are video-sharing websites and movie-streaming sites and applications.

- **Jitter and poor VoIP quality:** Network congestion can cause *jitter*, which is an irregular time delay in the sending of certain data packets. Jitter is similar to latency, but the delay that is involved is inconsistent; you might call it "inconsistent latency." The connection might be good one minute and bad the next. This is a problem that can affect voice over IP (VoIP) and streaming video and audio connections, which may lose quality for a period of time (or get "jittery"). Jitter may be more common with wireless connections. If using wireless, consider moving closer to the WAP. Also consider the wireless channel being used and check for external interference from neighbors or electrical equipment. Next, configure quality of service (QoS). QoS is a feature that attempts to prioritize data for specific computers or for specific programs. Configure it at the router to prioritize the packets that are more important to the users (for example, VoIP or other packets). In addition, you might opt for a jitter buffer, which is a shared data area where voice packets are collected and sent out smoothly during times of network congestion. Consider also that wireless connections are still in many cases slower than wired connections and break out that trusty old Ethernet cable (if at all possible). Finally, see the earlier bullet about slow transfer speeds for additional techniques to reduce jitter and network congestion in general.

ExamAlert

Know the difference: Latency is the typical time it takes for packets to travel from source to destination; jitter is irregular latency that often affects VoIP connections. It is the variation in the delay of packet delivery within a network and represents the deviation in the arrival time of packets compared to their expected arrival time. Jitter is measured in milliseconds (ms).

- **Port flapping:** Port flapping (also known as link flapping) is an issue where a communications link periodically changes between up and down states. For example, a computer that is wired to a switch might experience a network connection that alternates between a working state

and a nonworking state. You can check this by viewing the LED light on the switch's port that corresponds to the affected computer. You could also run a continuous **ping** command (for example, **ping -t example.com**) to see if some of the packets are being dropped. Flapping could be caused by a bad patch cable, improper duplex settings, or power-saving features. Test cables and check settings!

ExamAlert

Port flapping involves a communications link alternating between up and down states.

- **IP conflict:** An IP conflict message will pop up on the displays of both Windows computers that are causing the conflict. Usually, the first computer that used the IP address will continue to function, and the second computer will not be able to access the network. The second computer will have to be reconfigured to a different IP address and rebooted. Reboot the first computer for good measure. IP conflicts usually happen only when static IP addresses are being used. Consider using DHCP for all client computers.
- **Link-local/APIPA address:** If a computer is showing an IPv4 link-local address such as 169.254.49.26 when you type **ipconfig /all**, it generally means that the computer is attempting to obtain an IP address from a DHCP server but is failing to do so. IPv4 link-local addresses always start with 169.254. Microsoft also uses the name Automatic Private IP Addressing (APIPA). Usually, a link-local address is assigned internally, so the real problem could be that the computer is not getting connectivity to the network. Check everything in the first bullet point. Also, consider using **ipconfig /release** and **/renew**. Finally, if these measures do not work, check the DHCP server to make sure it is functional and available.

ExamAlert

In Windows, use **ipconfig /all** to check whether a system is using an APIPA address on the 169.254.0.0 network.

- **Cannot connect to Internet websites:** There could be a DNS issue. Consider flushing the DNS cache. You can do this by issuing the command **ipconfig /flushdns**. Or you could reset the TCP/IP stack with the **netsh int ip** command. Resetting the TCP/IP stack and flushing the DNS cache can also be helpful if a client computer cannot connect to a network path by name on the LAN.

ExamAlert

Double-study your network troubleshooting techniques and common symptoms in this chapter! It's all about troubleshooting!

Cram Quiz

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

1. A user complains that the computer is not connecting to the network. Which of the following should be done first?

   - ○ **A.** Use **ipconfig /all**.
   - ○ **B.** Ping the router.
   - ○ **C.** Check the patch cable.
   - ○ **D.** Check the network drivers.

2. One of your customers received the following error message while trying to connect to a shared drive on the network at \\server1\datashare:

Network Path was Not Found

Which of the following should you perform to resolve the issue? (Select two.)

- **A.** Reset the TCP/IP stack.
- **B.** Configure the network interface card to full duplex.
- **C.** Disable the Ethernet adapter.
- **D.** Use static IP addressing instead of DHCP.
- **E.** Flush the DNS cache.
- **F.** Disable the local firewall.

3. One of your customers no longer has access to a frequently accessed website. You ping another computer and the router on the network successfully. Which of the following should be done next?

- **A.** Check the IP configuration.
- **B.** Ping the website.
- **C.** Update the OS.
- **D.** Update the AV software.

4. A user moves a laptop from one office to another. The patch cable and the network adapter do not appear to be working properly at the new office. The cable is plugged in correctly and tests okay when checked with a patch tester. Which of the following should be done first?

- **A.** Check whether the port on the switch is enabled.
- **B.** Update the network adapter driver.
- **C.** Replace the patch cable with a crossover cable.
- **D.** Make sure the network adapter is compatible with the OS.

5. A computer is experiencing a problem in which the network connection alternates between a working state and a nonworking

state. It affects all applications. What is most likely occurring in this scenario?

- ○ **A.** Jitter
- ○ **B.** Network congestion
- ○ **C.** Port flapping
- ○ **D.** High latency

6. A user is experiencing slow network transfer speeds. You suspect that the user's system has too many open network connections to the Internet. Which of the following commands should you run to see which connections the user's system has to the Internet?

- ○ **A. netstat -a**
- ○ **B. tracert**
- ○ **C. ipconfig /release**
- ○ **D. ipconfig /renew**

7. What is the first thing you should check for when experiencing low RF and intermittent wireless connectivity issues?

- ○ **A.** APIPA address
- ○ **B.** Configure QoS
- ○ **C.** The distance of the computer from the WAP
- ○ **D.** Outdated equipment and cables

Cram Quiz Answers

1. **C.** Check the super-obvious first: Make sure the computer has a physical cabled connection to the network. Then attempt things such as **ipconfig**, **ping**, and network driver updates.

2. **A and E.** The issue here is most likely related to name resolution (which means DNS). Try resetting the TCP/IP stack or flushing the DNS cache. You can reset the TCP/IP stack in PowerShell or the

Command Prompt by typing **netsh int ip**. Or you can disable *and* enable the Ethernet adapter in Windows (as disabling alone is not enough). The DNS cache can be flushed by issuing the **ipconfig /flushdns** command. Configuring the network interface to full duplex would allow it to send and receive data simultaneously. Chances are that this is not the problem in the scenario. Assigning a static IP address probably won't help because this issue is usually a name-based problem, and DNS is probably not functioning properly. Disabling the local firewall is a bad idea from a security standpoint because it would allow people to access the local computer. However, it wouldn't help in this scenario anyway because a firewall normally wouldn't stop the local system from connecting to a remote data share.

3. **B.** This is the concept of pinging outward. Start by pinging the localhost, then a computer, and then the router on the network. Then ping a domain name or website. If you can ping a website but the browser cannot get through, the browser might have been compromised. If you cannot ping the website, you should check the IP configuration; the DNS server address might be incorrectly configured. You should update the OS and AV software right away if you suspect that the browser has been compromised.

4. **A.** Some routers and switches can disable physical ports (which is a smart security measure). Check that first. Later, you can check whether the network adapter is compatible with the OS and update it if necessary. Do not replace the cable with a crossover cable; this type of cable is used to connect one computer to another.

5. **C.** It is most likely port flapping (aka link flapping), which involves a communications link alternating between on and off states, back and forth. Jitter is an irregular time delay for particular packets (such as VoIP packets). It can be caused by network congestion, which simply means there is too much traffic on the network! High latency means data packets take longer to travel between a client computer and another system, and it occurs all the time.

6. **A.** Run **netstat -a** to see which types of connections the local computer currently has to the Internet. Advise the user to close any unnecessary programs and limit the number of streams of data. The **tracert** command in Windows is used to determine the route or path taken to a destination. The **ipconfig /release** and **ipconfig /renew** commands release and renew the DHCP-obtained IP address on a Windows system.

7. **C.** The first thing to check is the distance of the computer from the WAP. Also, consider the wireless channel being used and check for external interference. An APIPA address is a self-assigned IP address in Windows (for example, 169.254.49.26). Configuring quality of service (QoS) on a router prioritizes the packets that are more important to the users. Outdated equipment is a potential culprit; perhaps the organization needs a new WAP. However, "outdated cables" is not correct because this is a wireless scenario!

You did it! Another piece of the puzzle in place. This chapter brought some serious brain gain, and you handled it like a pro. Take a moment to breathe, maybe do a little victory stretch, and get ready to tackle the next challenge. Onward!

Chapter 28

Troubleshooting Printers

This chapter covers the following A+ 220-1201 exam objective:

- **5.6** – Given a scenario, troubleshoot printer issues.

This chapter delves into a variety of common printer issues that you will face. They can happen in large organizations and small offices alike. A printer is a mechanical device, but it is controlled by embedded firmware and by computers that manage it. Be ready to get your hands dirty (perhaps literally) as you fix printer problems, and be ready to work in the operating system as well.

ExamAlert

Objective 5.6 focuses on troubleshooting common symptoms in printers, such as unwanted lines, garbled print, paper jams, faded print, paper failing to feed, and more.

Troubleshooting Printers

If a printer will not print or prints incorrectly, it has to be fixed. Sometimes companies hire paid consultants to manage all their printers and copiers, and sometimes the care of these devices is the job of the in-house IT technician. Even if your company pays consultants, it is a good idea to

know some of the basic issues that can occur with printers and how to troubleshoot them. Table 28.1 describes some of these issues and possible solutions. Some of these problems (for example, paper jams and resulting error codes) might be displayed on a printer's operator control panel (OCP).

TABLE 28.1 **Printer Problems and Solutions**

Printer Issue	Possible Solutions

Printer Issue	Possible Solutions
Paper jams or creased paper	1. Turn the printer on and off in the hope that the printer will clear the jam. This is known as *power-cycling* the printer. If this doesn't work, turn the printer off and unplug it and then open it. 2. Remove paper trays and inspect them for crumpled papers that can be removed by firmly grabbing both ends of the paper and pulling or rotating the rollers to remove it. In general, clear the paper path. 3. Verify that the right paper type is in the printer. Paper that is too thin or thick might cause a paper jam. Also, watch for paper that has been exposed to humidity. 4. Check for dirty or cracked feed rollers. A temporary fix for dirty rubber rollers is to clean them using isopropyl alcohol. A permanent fix is to replace the rollers. 5. Check whether the fusing assembly has overheated. Sometimes a printer just needs time to cool or perhaps it is not in a sufficiently ventilated area. In uncommon cases, the fuser might have to be replaced. Be sure to unplug the printer and let the printer sit for an hour or so before doing so, due to the high temperatures of the fuser. The fusing assembly can usually be removed by removing a few screws. 6. Check the entire paper path. Duplexing printers (those that print on both sides of the paper) have more complicated and longer paper paths, providing more chances for paper to get jammed.

Printer Issue	Possible Solutions
Blank pages printing	▶ Determine whether the toner cartridge is empty or has failed, and if so, install a new one. Toner cartridge failures may be associated with the developing and transferring stages of the laser printing process, with the developing stage being more common. ▶ Determine whether the toner cartridge was installed with the sealing tape still in place. If it was, remove the tape. ▶ Check whether the transfer corona wire has failed. If the transfer corona wire fails, there will be no positive (opposite) voltage to pull the toner to the paper. Replace the wire.
Paper not feeding	Check the type and condition of the paper. Check the rollers (and raise the humidity if possible). Clean the rollers. Reset the printer. Consider using a maintenance kit.
Multiple pages fed in at once (that is, multipage misfeed)	Check whether the separation pad is getting enough traction; it might need to be cleaned. Also check whether the paper is too thin; 20 lb. or heavier paper is usually recommended.
Error codes	If a specific error is shown on the printer's OCP, read it. It might tell you exactly what the error is and how to fix it (or at least what the error is). On some printers, the OCP displays error numbers. Check your printer's documentation to find out what an error code means.

Printer Issue	Possible Solutions
Out-of-memory or low-memory error message	Check whether the user's computer is spooling documents. The setting with the least chance of this error is the Start Printing Immediately spool setting. You might also need to restart the Print Spooling service. A user who tries to print a large image might need to change settings in the application in which the image was made. In some cases, the printer's RAM might need to be upgraded. Whenever installing RAM to a printer, take all the same precautions you would when working on a PC.
No image on printer display (OCP)	Check whether the printer is in sleep mode (or off altogether). Verify that the printer is plugged in. In rare cases, the internal connector that powers the display might be loose.
Vertical lines on page, streaks, smearing, speckling, toner failing to fuse to paper	Black lines or streaks (and sometimes faded print) can be caused by a scratch in the laser printer drum or a dirty primary corona wire. Usually, the toner cartridge needs to be replaced. White lines could be caused by a dirty transfer corona wire; this can be cleaned or replaced. Wide white vertical lines can occur when something is stuck to the drum. Smearing can occur if the fusing assembly has failed; in this case, you might also notice toner coming off the paper easily. If it is an inkjet, one or more ink cartridges might need to be replaced, or the printer might need to be calibrated. If toner is not fusing to the paper correctly, the fuser rollers might not be heating properly, likely due to mechanical fuser failure.
Faded prints	Replace ink or toner. Clean the ink cartridge head. Also, check the fuser and increase the humidity, if necessary.

Printer Issue	Possible Solutions
Garbage printout or garbled characters on paper	This issue can occur due to an incorrect driver. Some technicians like to try “close” drivers. This is not a good idea. Use the exact driver for the exact model of the printer that corresponds to the appropriate version of the operating system. A bad formatter board or printer interface can also cause garbage printouts. These can usually be replaced easily by removing two screws and a cover.
Ghosted image	Ghosted images or blurry marks can be a sign that the drum has some kind of imperfection or is dirty, especially if the image reappears at equal intervals. Replace the drum (or toner cartridge). Another possibility is that the fuser assembly has been damaged and needs to be replaced.
Double/echo images	The toner cartridge/print heads might be misaligned, or the drum or fuser unit may be faulty. The printer driver and even printer firmware might need to be reinstalled or updated. Administer printer maintenance according to the manufacturer’s documentation.
Grinding noise	Grinding or similar noises emanating from a printer could relate to a defective toner cartridge. (Always have backup cartridges near the printer!) The noise could also be due to a paper jam or carriage stall.

Printer Issue	Possible Solutions
No connectivity or connectivity issues	Check the following: ▶ The printer is plugged in to an AC outlet and is online. ▶ The printer is securely connected to the local computer or to the network. ▶ The computer has the correct print driver installed. ▶ The printer is shared to the network. ▶ The printer has a properly configured IP address. (This can be checked on the OCP of most networkable laser printers.) ▶ Remote computers have a proper connection over the network to the printer. ▶ The printer is set up as the default printer, if necessary.
Access denied	If an Access Denied message appears on the screen while attempting to print, the user doesn't have permission to use the printer. You (or the network administrator) will have to give the user account permissions for that particular printer. This message might also be displayed when a person attempts to install a printer without the proper administrative rights.
Multiple prints pending in the print queue	If the printer window shows several documents listed in the queue, but the printer is not currently printing anything, a document might have stalled and may need to be restarted. Also, the print spooler might need to be restarted in the Services console window, in the Task Manager, or in the Command Prompt. In less common cases, you might need to reinstall the printer driver.

Printer Issue	Possible Solutions
Color printouts are a different (wrong) color than shown on the screen or incorrect chroma display	A printout will always be *slightly* different from the screen. But if the difference is very noticeable, check the ink or toner cartridges and make sure none of the colors are empty. Run the calibration tool for the printer. Verify that the printer is a PostScript-capable printer that can do raster image processing (RIP). If this functionality is not built into the printer, look for it as a separate software solution.
Finishing issues such as staple jams or hole punches	Some printers can perform finishing tasks on print jobs, such as stapling and hole punching. Sometimes a printer might not staple all pages or might hole punch everything at once. Ensure the following: ▶ Paper guides are in the proper place and paper is being stacked properly by the printer. ▶ The printer has a supply of *quality* staples. ▶ The correct printer driver is installed. ▶ The stapler/punching settings in the OS or printing application or on the printer's OCP are correct. ▶ The tray settings are correct. ▶ The punch hole tray is not full.
Incorrect paper size or page orientation	Make sure the correct paper is in the printer. Then check the Windows settings for paper size (or envelope size) and orientation. We discuss these topics further in Chapter 19, "Multifunction Devices/Printers."
Multiple failed jobs in logs	Reset the printer, analyze the controlling operating system or print server, clear the print queue, and reconfigure the spooler.

Printer Issue	Possible Solutions
Unable to install printer	Check whether the printer is properly connected to the computer or network physically. Check whether it is getting an IP address. In Windows, start the Print Spooler service and update the driver. (Advanced: Define new printer keys in the registry.) More on the spooler and how to start it appears later in this chapter.

ExamAlert

Study the printer troubleshooting methods in Table 28.1.

A printer failing to recognize a paper tray can prevent users from completing print jobs. This issue is often caused by incorrect tray configuration, physical misalignment, or firmware/software bugs. Begin troubleshooting by checking that the tray is securely installed and correctly aligned with the printer's guides. Verify that the tray is loaded with the correct paper type and size, and ensure that paper size settings in the printer's operator control panel match the tray contents. If the tray is still not recognized, update the printer firmware and check for driver compatibility with the operating system. Some printers allow manual tray assignments in the settings or printer software. Confirm that the tray is not disabled or improperly configured. If these steps fail, inspect the tray for any mechanical damage or sensor issues that may require repair or replacement.

In general, when working with printers, keep them clean and use printer maintenance kits and always refer to manufacturers' instructions. As a car needs its oil changed periodically, printers also need maintenance. HP and other manufacturers offer maintenance kits that include items such as fusers, rollers, separation pads, and instructions on how to replace all these items. Manufacturers recommend that maintenance be done every once in a while (for example, every 200,000 pages printed). When you finish installing a maintenance kit, be sure to reset the maintenance count. You

should also have a toner vacuum available for toner spills. A can of compressed air can be helpful when you need to clean out toner inside a laser printer; remember to do this job outdoors. Vacuum any leftover residue.

Printer maintenance can be broken down into the following basic categories:

- **Laser:** Replace toner, apply maintenance kit, calibrate, clean.
- **Inkjet:** Clean heads, replace cartridges, calibrate, clear jams.
- **Thermal:** Replace paper, clean heating element, remove debris.
- **Impact:** Replace ribbon, replace print head, replace paper.
- **3D printer:** Clean the filament nozzle, resin reservoir, and anywhere there is a supply or distribution of plastic/resin. Also check the platform (print bed), check whether fans are working, and check the axis and gear movement.

When troubleshooting printers, don't forget to RTM (read the manual)! Most printers come with manuals, and these manuals often include troubleshooting sections. In some cases, the manual is in PDF format on the Internet or on the disc that accompanied the printer. In addition, manufacturers usually have manuals on their websites as well as support systems for customers. Use them!

Remember to check the printer's display, which is referred to as the operator control panel (OCP). Back in the day, messages were sometimes obscure—for instance, the famous "PC LOAD LETTER" error—but today they are much more human readable. Get to know your way around the OCP and use the displayed information in conjunction with the printer manual to troubleshoot issues.

Keep in mind that many products come with warranties, and customers sometimes purchase extended warranties. We once had to do some troubleshooting on two color-laser printers that were only two weeks old when they failed. When we described to the manufacturer the error code that was flashing on the printers' displays, the representative didn't need to hear anything else and simply sent out a tech the next day because the

devices were under warranty. Let the manufacturer help you. This help can save you a lot of time and aggravation, and it might not cost you or your company anything.

Print Jobs and the Print Spooler

It's a good idea to know how to work with printers in Windows. You should know how to manage printers and print jobs, and you should be able to configure the print spooler. Let's talk about those two concepts now.

Managing Printers and Print Jobs

To manage a printer or an individual print job in Windows, just double-click the printer to which the job was sent. This might open a proprietary screen designed by the printer manufacturer or a Microsoft window similar to the one in Figure 28.1.

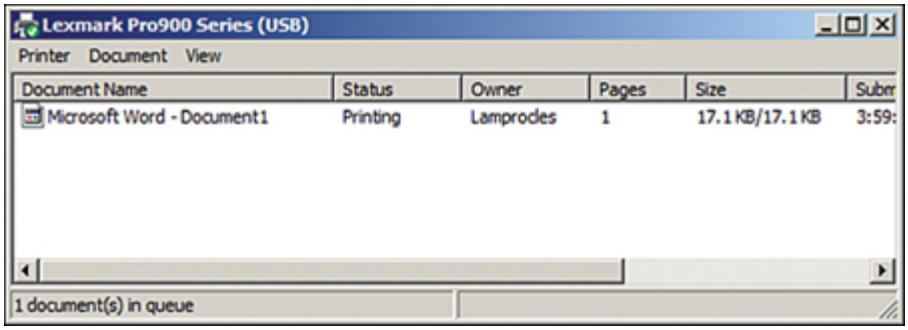


FIGURE 28.1 **A Typical Printer Window Showing One Print Job**

Figure 28.1 shows one print job, called Document1, listed. The job went to the printer properly; you can tell because it says Printing in the Status column. Any other message would mean that the job was either spooled, queued, stopped, or failed altogether. You can pause, restart, or stop a job completely if it is not printing properly. This can be done by right-clicking on the job in the window or by clicking the Document menu. Keep in mind that larger documents might take longer to spool before they start printing. (We'll discuss that topic in a little bit.) In addition, all documents can be paused or canceled, or the entire printer can be taken offline from the Printer menu. Use these tools to help troubleshoot printing issues.

A frozen print queue can prevent documents from printing and delay workflows. This issue often occurs when a print job becomes corrupted or the print spooler service malfunctions. To resolve it, first check the print queue in Windows by double-clicking the printer icon in the taskbar or accessing the printer settings. Identify any jobs stuck in the queue and attempt to cancel or restart them. If these steps fail, stop and restart the print spooler service. Open the Services console (services.msc), locate the Print Spooler service, and select **Stop**. Navigate to C:\Windows\System32\spool\PRINTERS and delete all files in this folder to clear the queue. Then, restart the print spooler service and reattempt the print job. If the issue persists, check for driver updates or reinstall the printer driver. Persistent frozen queues may indicate software conflicts, so ensure that the operating system and all printer-related software are updated.

Using the Windows Print Spooler

Spooling is page-by-page processing that is done at the local system before a print job goes to the printer.

Whenever a job goes to print, there are three options:

- **Print directly to the printer:** This means the print job goes right to the printer, without any delays. How well this works depends solely on the amount of memory in the printer (which can be increased, just as with computers). Of course, if the print job is larger than the amount of RAM in the printer, the job will probably fail. Usually, a better solution is to spool the document.
- **Start printing immediately:** This is the first of two spooling options. When this setting is selected, the document will be *spooled* to the storage drive one page at a time. When an entire page has been spooled, it is sent to the printer for printing. This repeats until all the pages of the document have been spooled and, ultimately, printed. This is the default setting in Windows and is usually the best option because it prints faster than other spooling options. Figure 28.2 shows an example of this.

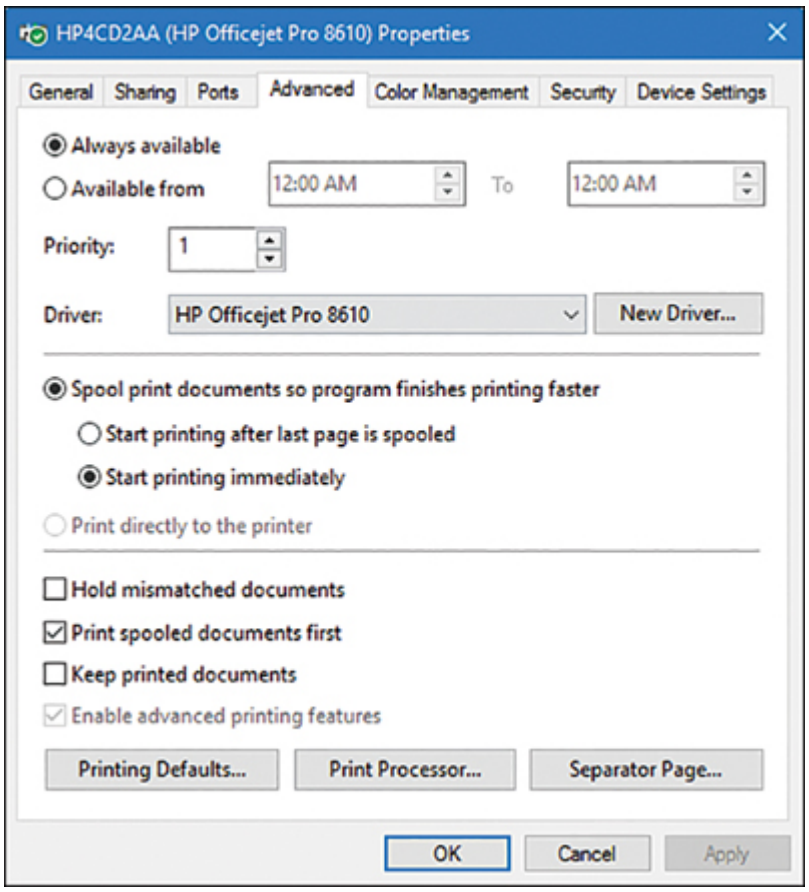


FIGURE 28.2 **Printer Spooling Options in Windows**

- **Start printing after last page is spooled:** This means the entire document will be spooled to the storage drive and then pages will be sent to the printer for printing. This is usually slower than the Start printing immediately option but might have fewer issues, such as stalls or other printing failures.

The print spooler is controlled by the Print Spooler service, which processes print requests and sends them to the printer. Not only can you experience issues in which print jobs or printers stop working, the Print Spooler service can fail. This service can be started, stopped, and restarted from the GUI and from the Command Prompt:

- **Adjusting the Print Spooler service in the Services window:** Open the Run prompt and type **services.msc** to open the Services console window. Scroll until you find the Print Spooler service. To start a

stopped service, right-click it and click **Start**. Alternatively, you can click the Start button or other buttons on the toolbar. Also, you can double-click the Print Spooler service to see its properties, where you can start and stop the service and make additional configurations (see Figure 28.3).

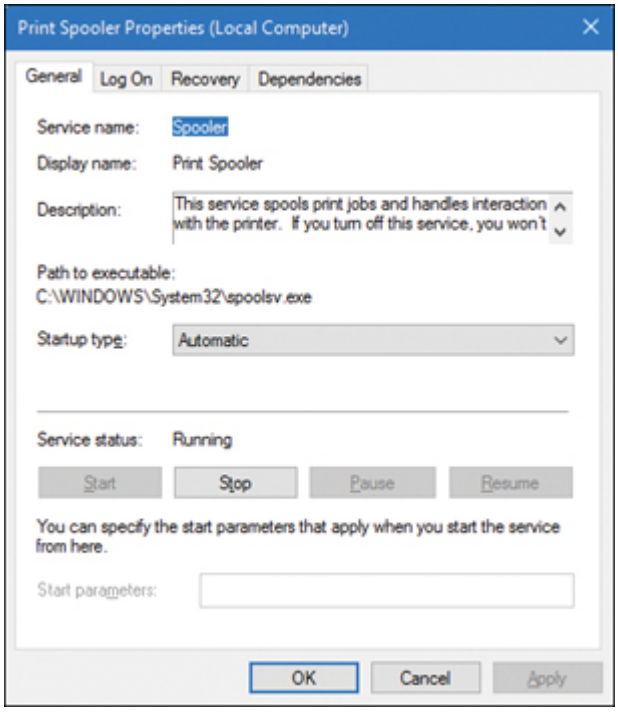


FIGURE 28.3 **The Print Spooler Properties Window**

- **Adjusting the Print Spooler service in Task Manager:** Open the Task Manager from the taskbar or Power User menu by pressing Ctrl+Shift+Esc or by going to Run and typing **taskmgr.exe**. Under the Services tab, right-click the **Spooler** service and select **Start, Stop, or Restart service**.
- **Adjusting the Print Spooler service in the PowerShell/Command Prompt:** When you open PowerShell or the Command Prompt (as an administrator), you can start the Print Spooler service by typing **net start spooler**. Typing **net stop spooler** stops the service. (This is a good one. We've actually heard of several companies asking how to do this during an interview!)

ExamAlert

Know how to configure spooling and how to start and stop the Print Spooler service within the services console window, the Task Manager, and especially in PowerShell.

Cram Quiz

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

1. How can a paper jam be resolved? (Select all that apply.)

   - ○ **A.** Clear the paper path.
   - ○ **B.** Use the right type of paper.
   - ○ **C.** Check for and replace damaged rollers.
   - ○ **D.** Check the OCP.

2. A user informs you that color printouts are noticeably different from what appears on their screen (incorrect chroma display). What actions should you take? (Select two.)

   - ○ **A.** Ensure that ink/toner cartridges aren't empty.
   - ○ **B.** Make sure the separation pad is getting enough traction.
   - ○ **C.** Ensure that the paper is not too thin.
   - ○ **D.** Run the printer calibration tool.

3. A technician is troubleshooting finishing issues with the company laser printer. Which of the following actions should the tech perform? (Select all that apply.)

   - ○ **A.** Clean the filament nozzle and platform (print bed).

- ○ **B.** Make sure the staple cartridge is full and free of jams.
- ○ **C.** Ensure that the hole punch tray is not full.
- ○ **D.** Change out the toner cartridge.
- ○ **E.** Ensure that the proper paper tray is specified in the printer settings.
- ○ **F.** Verify proper paper orientation.

4. Which of the following are usually included in a laser printer maintenance kit? (Select the two best answers.)

- ○ **A.** Rollers
- ○ **B.** Image drum
- ○ **C.** Toner
- ○ **D.** Duplexer
- ○ **E.** Fuser

5. One of your customers is connected to a standalone printer. The customer gets an "out of memory" error when printing large graphic files. What should you do?

- ○ **A.** Upgrade the storage drive on the computer.
- ○ **B.** Upgrade the RAM on the printer.
- ○ **C.** Upgrade the RAM on the computer.
- ○ **D.** Reinstall the printer drivers.

6. What should you do first when removing a paper jam?

- ○ **A.** Take the printer offline.
- ○ **B.** Clear the print queue.
- ○ **C.** Open all the doors of the printer.
- ○ **D.** Turn off the printer.

7. You have been called to a customer site to perform maintenance on an impact printer. Which should you consider?

- ○ **A.** Replacing paper, cleaning heating element, and removing debris
- ○ **B.** Replacing toner, applying maintenance kit, calibrating, and cleaning
- ○ **C.** Replacing ribbon, replacing print head, and replacing paper
- ○ **D.** Cleaning heads, replacing cartridges, calibrating, and clearing jams

8. Which is the faster option for spooling documents?

- ○ **A.** Print directly to the printer
- ○ **B.** Start printing immediately
- ○ **C.** Start printing after last page is spooled
- ○ **D.** Start printing after the separator page

9. How can you immediately stop the Print Spooler service? (Select the three best answers.)

- ○ **A.** Start printing immediately.
- ○ **B.** Type **sc config spooler start= disabled** in the Command Prompt.
- ○ **C.** Print directly to the printer.
- ○ **D.** Type **net stop spooler** in the Command Prompt.
- ○ **E.** Open the Services console window, right-click **Print Spooler**, and select **Stop**.
- ○ **F.** Open the Task Manager, click the **Services** tab, right-click **Spooler**, and select **Stop**.

10. You are configuring a new laser printer. Which laser printer configuration setting do you need to change if users want to have

both letter-sized paper and legal-sized paper automatically available?

- **A.** Duplex
- **B.** Orientation
- **C.** Tray settings
- **D.** Quality

Cram Quiz Answers

1. **A, B, and C.** There are several possible reasons a paper jam might occur. The paper could be stuck somewhere in the paper path, the paper could be too thick, or the rollers could be damaged. However, just checking the operator control panel (OCP) will not resolve anything. It will hopefully clue you in to why the paper jam has happened, though.

2. **A and D.** The printout will always be slightly different from what is shown on the screen, but if the difference is very noticeable, check the ink or toner cartridges and make sure none of the colors are empty. Run the calibration tool for the printer to adjust color output as necessary. Checking whether the separation pad is getting enough traction and whether the paper is too thin are proactive actions related to multipage misfeeds, not color issues.

3. **B, C, E, and F.** For finishing issues (such as stapling and hole punching), check the staple cartridge, hole punch tray, tray settings, and paper orientation. Cleaning the filament nozzle and platform are measures to take with 3D printers, not laser printers. The toner cartridge is very important for printing on a laser printer, but it is not important for finishing processes such as stapling and hole punching.

4. **A and E.** Maintenance kits usually include things like paper pickup rollers, transfer rollers, and a fuser. The duplexer, image drum, and toner are parts of the printer and/or toner cartridges. Toner cartridges are not included in maintenance kits.

5. **B.** You should upgrade the RAM on the printer. Large graphics files need a lot of memory (in both the PC and the printer). But if the PC can send the file to the printer, it has enough RAM and storage drive space. Printer drivers will not cause an "out of memory" error to display on the printer.

6. **D.** Turn off the printer before you start working inside it. You want to make sure it is off and unplugged before you put your hands inside it. Taking it offline is not enough in this case.

7. **C.** Impact printer maintenance procedures include replacing the ribbon, replacing the print head, and replacing paper. Laser printer maintenance includes replacing toner, applying a maintenance kit, calibrating, and cleaning. Thermal printer maintenance includes replacing paper, cleaning the heating element, and removing debris. Inkjet printer maintenance includes cleaning the heads, replacing cartridges, calibrating, and clearing jams.

8. **B.** The Start printing immediately option is faster than the Start printing after last page is spooled option when spooling documents. The Print directly to the printer option doesn't use the spooling feature. There is no option called Start printing after the separator page.

9. **D, E, and F.** To immediately stop (or turn off) the Print Spooler service, you have several options. You can stop it in the Command Prompt with the **net stop spooler** command or the **sc stop spooler** command. You can also do it in the Services console window or in the Task Manager. (By the way, the answers listed are based on Windows 11 Pro.) Note that in Services you look for "Print Spooler," and in the Task Manager you look for "Spooler."

   The answers Start printing immediately and Print directly to the printer are options for how (or whether) documents will be spooled. While printing directly to the printer does not use the spooler, it doesn't turn off the spooler either. Finally, **sc config spooler start = disabled** *disables* the service but doesn't turn it off —immediately, that is. However, the service won't start the next time the computer is restarted. Try that command and then the **net**

stop spooler command to see what we mean. Then, to set everything back to run as normal, type the following:

```
sc config spooler start= auto
net start spooler
```

10. **C.** Having multiple paper trays in a laser printer allows the printer to automatically supply different paper sizes. To configure which tray has which type of paper, change the tray settings configuration options. Duplex is for two-sided printing. Orientation is for portrait or landscape, and Quality affects options such as resolution.

Congratulations! This is the end of the 220-1201 chapters of this book. Following, you will find a practice exam that is designed to test your knowledge of the 220-1201 objectives. Good luck!

If you are planning on taking the actual CompTIA A+ 220-1201 exam, be sure to go through the 220-1201 checklist in "Introduction to Core 1 (220-1201)," just before Chapter 1. However, keep in mind that we recommend going through this *entire* book before attempting either of the A+ exams.

A+ Core 1 (220-1201) Practice Exam

The multiple-choice questions provided here help you to determine how prepared you are for the actual exam and which topics you need to review further. Write down your answers on a separate sheet of paper so that you can take this exam again if necessary. Compare your answers against the answer key that follows this exam. Read through the explanations and also the incorrect answers very carefully. If there are any concepts that you don't understand, go back and study them more.

Exam Questions

1. Which of the following components can be considered the "brains" of a computer?

   - **A.** RAM
   - **B.** Storage drive
   - **C.** CPU
   - **D.** Motherboard

2. You are attempting to load an operating system from a USB flash drive at computer startup. Which of the following settings should you modify in the UEFI/BIOS?

   - **A.** Enable a BIOS password

- **B.** Boot sequence
- **C.** Enable TPM
- **D.** Disable TPM

3. Which of the following is the most common type of networking connector used in a PC's network interface card?

- **A.** RJ-11
- **B.** F-type connector
- **C.** ST
- **D.** RJ-45

4. Which of the following is the bus width of quad-channel RAM?

- **A.** 64-bit
- **B.** 128-bit
- **C.** 288-pin
- **D.** 256-bit

5. Which of the following should be reset during normal printer maintenance?

- **A.** Page count
- **B.** Job queue
- **C.** Print job cache
- **D.** Tray settings

6. You are a technician for an accounting company. You are helping a user who is unable to access websites and is reporting connectivity issues as well as pop-ups on the screen. You discover and remove malware. After rebooting the system, you are able to ping the gateway and access the Internet.

Which of the following next steps should you take while troubleshooting this issue? (Select the two best answers.)

- **A.** Reboot the computer and verify that it works.
- **B.** Research the problem based on the symptoms you found.
- **C.** Perform a virus scan.
- **D.** Verify TCP/IP settings with **ipconfig**.
- **E.** Document findings, actions, and outcomes.
- **F.** Reconnect the system to the network.

7. A laptop's battery fails to charge. Which of the following should be checked first?

- **A.** DC-in jack
- **B.** AC-in jack
- **C.** CMOS battery
- **D.** AC circuit breaker

8. One of your coworkers has opened a trouble ticket concerning paper jams on a laser printer. The paper jams have become more frequent of late. You attempt to re-create the problem and then check the printer log for more information. Which of the following are the most likely solutions to the problem? (Select the two best answers.)

- **A.** Clean and inspect the entire paper path.
- **B.** Clean the fuser roller and verify fuser operation.
- **C.** Clean and replace the paper-out sensor.
- **D.** Use a printer maintenance kit to replace parts.
- **E.** Replace the paper exit assembly switch.
- **F.** Clean and inspect the print drum.

9. What should you do after you have located a device for pairing during the Bluetooth connection process?

- **A.** Test the connection.

- **B.** Turn both devices off and then back on.
- **C.** Enter the PIN code.
- **D.** Enable Bluetooth on both devices.

10. The power supply fan and case fans spin, but there is no power to other devices. Which of the following is the most likely cause of this?

- **A.** Failed boot drive
- **B.** Improper connectivity
- **C.** Drive not recognized
- **D.** Failed RAM

11. One of the desktop computers at a customer site is randomly rebooting several times per day. You have checked for overheating issues, but everything seems okay with the case fans, CPU fan, and power supply. What should you check next?

- **A.** Make sure the integrated network adapter has the latest drivers.
- **B.** Ensure that the storage drive is defragmented.
- **C.** Check the motherboard for signs of swollen capacitors.
- **D.** Check the RAM and confirm that it is the right type.

12. Which of the following cable types should be used to connect a cable modem to a SOHO router?

- **A.** Coaxial
- **B.** Ethernet
- **C.** USB
- **D.** Thunderbolt
- **E.** SATA

13. Which of the following is an example of a MAC address?

- **A.** 10.1.1.255
- **B.** 4410:FF11:AAB3::0012
- **C.** https://greencurtaintraining.com
- **D.** 00-1C-C0-A1-55-21

14. Your client has three business locations within the city limits. All three locations need to be networked. The vendor's network requirements for all three locations include a minimum data transfer rate of 1 Gbps. Which of the following network types should you most likely use for the internal office communications and the office-to-office network communications? (Select the two best answers.)

- **A.** SAN
- **B.** WAN
- **C.** LAN
- **D.** MAN
- **E.** PAN

15. Which of the following best describes the most likely reason for connecting a tone generator to an RJ-45 cable drop?

- **A.** To confirm continuity of the conductors
- **B.** To locate the position of the cable on a patch panel
- **C.** To test the transmission quality of the connection
- **D.** To validate proper wiring of the network jack

16. When a mobile device is put into airplane mode, which of the following features are typically disabled? (Select the two best answers.)

- **A.** Cellular data
- **B.** Wi-Fi
- **C.** Multitouch capability

- ○ **D.** Data encryption
- ○ **E.** Camera

17. One of your coworkers has asked for a cable for an Apple iPhone 16 that can charge it and transfer data to and from it. Which of the following connection types would meet your coworker's requirements?

- ○ **A.** USB-C
- ○ **B.** Micro-USB
- ○ **C.** Lightning
- ○ **D.** Mini-USB

18. A client is having a problem printing a specific type of document. The main network printer operator control panel (OCP) shows that the printer is online and that there are no errors. No other users are having issues printing to that printer. You ask the person to send the same document to another printer, and the document prints fine. Which of the following should you do first when troubleshooting this problem?

- ○ **A.** Stop and start the print spooler service.
- ○ **B.** Stop and start the print server queues and have the user resend the document.
- ○ **C.** Verify that the user is sending the document to the correct printer queue.
- ○ **D.** Have all users send the same document to the correct printer queue.

19. A desktop computer (named workstation22) can't connect to the network. A network card was purchased without documentation or driver media (disc or thumb drive). Which of the following is the best way to install the network card driver?

- ○ **A.** Purchase the media online and install the drivers.

- **B.** Run Windows Update to install the driver.
- **C.** From the desktop computer (workstation22), download and install the driver.
- **D.** Copy the driver to a flash drive and install it.

20. You are working in a command line and see the following results:

```
example.com = 93.184.216.34
```

Which of the following server types has most likely helped supply this information to you?

- **A.** DHCP server
- **B.** DNS server
- **C.** Authentication server
- **D.** Syslog server
- **E.** Print server

21. Which of the following features allows users to store files in cloud-based storage when needed but can be removed when space is freed up locally?

- **A.** Shared resources
- **B.** Metered utilization
- **C.** On-demand
- **D.** Resource pooling

22. You are the system administrator for a medium-sized enterprise organization. You configure a server to host several virtual machines (VMs). Now, you are ready to begin provisioning the VMs. Which of the following should you implement to perform this task?

- **A.** Remote Desktop Services
- **B.** Hypervisor
- **C.** Virtual LAN

- **D.** Disk Management
- **E.** Device Manager

23. You are part of a team that has decided to make use of a cloud provider for some of your organization's technology needs. Your top priority is to offload some of your networking, storage, and VM hosting to the cloud. Which of the following services best suits your needs?

- **A.** SaaS
- **B.** IaaS
- **C.** PaaS
- **D.** Hybrid cloud

24. Your guest virtual machines get direct access to the hosting computer's network connection. What is another name for this?

- **A.** NAT
- **B.** Private virtual network
- **C.** Host-only networking
- **D.** Bridged networking

25. Your office printer was working earlier in the day but is no longer printing any documents. Preexisting workstations are manually configured to print to the printer directly over the network. You begin troubleshooting the problem and determine that the printer is still visible when browsing the network directory. You also verify, at the physical printer, that the printer can print test pages successfully. Which of the following is the most likely cause of the problem?

- **A.** The print spooler was restarted.
- **B.** Two users sent print jobs at the same time, and a collision occurred.
- **C.** The printer's IP address has changed.

- **D.** The message “perform printer maintenance” is displayed on the printer’s display panel.

26. Which of the following is an advantage of UDP over TCP?

- **A.** It uses flow control.
- **B.** It transfers packets faster.
- **C.** It uses connection handshakes.
- **D.** It is connection based.

27. John is a PC technician for an organization that has a computer network with 12 computers. All the computers contain vital information, so they use static IP addresses (on the 192.168.50.0 network). John just finished troubleshooting a Windows computer that could not access the network. He ascertained (correctly) that the computer needed a new network card. He purchased a plug-and-play card and physically installed the card. He then turned on the computer and noted that the network card’s LED link was lit and that there was activity. He then rebooted the computer to Windows and documented the whole process. Later, his boss tells him that the user is complaining that there is no Internet access. Which step of the A+ troubleshooting methodology did John forget to perform?

- **A.** Identify the problem.
- **B.** Establish a theory of probable cause.
- **C.** Test the theory to determine cause.
- **D.** Establish a plan of action to resolve the problem.
- **E.** Verify full system functionality.
- **F.** Document findings, actions, and outcomes.

28. On your server, two drives of a RAID 5 array have failed. What should you do?

- **A.** Replace one of the drives and run RAID repair.

- **B.** Replace the failed drives and format the RAID array using the quick option.
- **C.** Replace one of the failed drives and repair the RAID array using system utilities.
- **D.** Replace the failed drives and restore the data from tape backup to the repaired RAID array.

29. Which of the following could be used for two-factor authentication?

- **A.** IMEI and IMSI
- **B.** Password plus biometric
- **C.** GPS and location services
- **D.** PRL and baseband updates

30. Which of the following types of printers requires a maintenance kit that contains a fuser, a transfer roller, and pickup rollers?

- **A.** Thermal
- **B.** Laser
- **C.** Inkjet
- **D.** Impact

31. You are tasked with fixing a laptop that is not booting. You have analyzed the system and can't see any system lights or display, and you can't hear any sounds when the power button is pressed. Which of the following should be attempted first when troubleshooting the problem?

- **A.** Boot the system from a flash drive.
- **B.** Disconnect the AC and the battery and press and hold the power button for several seconds.
- **C.** Remove storage drives and optical drives, RAM, and USB devices from the laptop.

- **D.** Connect an external monitor to the laptop to determine if the LCD has failed.

32. You are planning to build a computer that will be used at trade shows on several different continents. Part of your planning includes specifications such as maximum RAM and a typical video card, CPU, and storage drive. Which of the following specifications is the most important for you to consider when you select a power supply unit?

- **A.** Efficiency
- **B.** 12 V rail amperage
- **C.** Input voltage
- **D.** Number of SATA connectors

33. You are a technician for a small organization of 50 employees. You are tasked with replacing a damaged LED screen on a mobile computer. After installing a new LED screen, you find that the OS can be seen on the screen, but the touchscreen is not working. Which of the following are the most probable root causes of this failure? (Select the three best answers.)

- **A.** The touchscreen needs to be calibrated after replacement.
- **B.** Touchscreen drivers must be installed.
- **C.** The hardware replacement in the scenario is not touchscreen capable.
- **D.** A grounding screw is not attached securely.
- **E.** The digitizer cable is not attached to the motherboard properly.
- **F.** The LCD panel firmware should be updated.

34. A monitor's onscreen display (OSD) indicates that the proper video source has been selected, yet no image is displayed. Which of the following are the most likely causes? (Select the two best answers.)

- **A.** The monitor's brightness setting is too low.

- **B.** The monitor's backlight has failed.
- **C.** There is no device sending video.
- **D.** The source cable has been disconnected.
- **E.** The monitor's contrast setting is too high.

35. A computer you are working on randomly reboots. Which of the following should be checked first when troubleshooting the computer? (Select the two best answers.)

- **A.** Memory integrity
- **B.** Video card integrity
- **C.** CMOS battery
- **D.** PSU integrity
- **E.** Optical drive integrity

36. Which of the following mobile phone technologies is responsible for contactless pay like Apple Pay?

- **A.** IMSI
- **B.** NFC
- **C.** RFID
- **D.** Bluetooth

37. You are setting up a network for a small office with 30 computers and 1 server. The server will be used as a file-sharing device and a print server, and it will act as the domain controller. What kinds of addresses should you assign to the server? (Select the two best answers.)

- **A.** DHCP
- **B.** MAC
- **C.** Static IP
- **D.** Dynamic IP

- **E.** Subnet mask
- **F.** FTP

38. Which protocol does Active Directory rely on most? (Select the best answer.)

- **A.** SMB
- **B.** HTTPS
- **C.** LDAP
- **D.** DHCP

39. As you are building a new PC, you notice that the motherboard has eight DIMM sockets that are labeled 0 through 7. Four of them are gray, and the other four are a darker shade of gray. Which of the following should be performed first?

- **A.** Install the memory into the gray slots.
- **B.** Install the memory into the dark gray slots.
- **C.** Install the memory into slots 0 through 3.
- **D.** Fill all the slots with memory.
- **E.** Consult the motherboard documentation.

40. Which of the following printer technologies uses piezoelectric pressure pads to produce small bubbles that are moved to the paper?

- **A.** Laser
- **B.** Inkjet
- **C.** Thermal
- **D.** Impact

41. You need to describe RAID to a nontechnical customer. Which of the following is the best description to use for this customer?

- **A.** RAID stands for redundant array of independent disks.

- **B.** RAID utilizes multiple disks to increase performance and/or enable protection against data loss.
- **C.** RAID is a dynamic disk management system.
- **D.** RAID uses striping to reduce the amount of storage drive write time and utilizes parity bits to reconstruct the data from a failed drive.

42. You just completed a CPU installation. When you turn on the computer, the POST sounds a series of beeps, and the system won't boot. What is the most likely cause?

- **A.** The mouse is not plugged in.
- **B.** The operating system is corrupted.
- **C.** The CPU is not properly seated.
- **D.** The fan is running too fast.

43. Which of the following devices should be configured to block specific ports on a network?

- **A.** Firewall
- **B.** Gateway
- **C.** Router
- **D.** Bridge
- **E.** Access point

44. Which connector is necessary to supply power to a graphics expansion card? (Select the best answer.)

- **A.** 8-pin EATX12V
- **B.** PCIe 8-pin
- **C.** 24-pin ATX
- **D.** SATA 15-pin

45. Which of the following monitor types provide for the widest viewing angle, along with rich colors and consistent backlighting? (Select the two best answers.)

- **A.** VA
- **B.** TN
- **C.** IPS
- **D.** LED

46. You replaced a bad internal WLAN card in a Windows laptop. You completed the installation and verified that the new WLAN card is listed in the Device Manager as enabled. What should you do next to actually use the card?

- **A.** Type the security passphrase.
- **B.** Update the firmware of the WLAN card.
- **C.** Configure encryption on the router.
- **D.** Add the SSID of the network to the connection.

47. You need to connect external peripherals to a typical PC. Which of the following connector types will allow you to do this? (Select the two best answers.)

- **A.** SATA
- **B.** SAS
- **C.** EIDE
- **D.** eSATA
- **E.** USB 3.0

48. Look at the following list of wires. What wiring standard is being used here?

```
1. White/orange 2. Orange 3. White/green 4. Blue
5. White/blue   6. Green 7. White/brown 8. Brown
```

- **A.** RJ-45
- **B.** T568B
- **C.** T568A
- **D.** TIA

49. You need to make a patch cable to connect a computer to an RJ-45 wall jack. Which of the following tools should be used to attach the RJ-45 plugs to the patch cable?

- **A.** Crimper
- **B.** Punchdown tool
- **C.** Loopback plug
- **D.** Cable tester

50. Four people share a connection to a SOHO router that connects to the Internet. When a single user starts streaming media over the Internet, browsing slows down for the rest of the users. Which setting should be configured to alleviate the problem?

- **A.** QoS
- **B.** DSL
- **C.** WAN
- **D.** VPN

51. A user with an inkjet printer states that all color printouts are missing red ink. The printer has cartridges for each of the CMYK colors, and the user has recently replaced the magenta cartridge. Which of the following steps should be performed next?

- **A.** Verify that the printer cables are connected.
- **B.** Perform printhead cleaning.
- **C.** Purchase a maintenance kit.
- **D.** Use paper of a different weight.

52. A user calls you and says that their computer won't boot and that there is a faint smell of something burning. Which tool should be used to identify the problem?

- ○ **A.** Loopback plug
- ○ **B.** Cable tester
- ○ **C.** PSU tester
- ○ **D.** ESD strap

53. Which of the following describes the function of a switch in a network?

- ○ **A.** Converts a packet for transmission from one network to another network
- ○ **B.** Transmits packets it receives to specific connections (ports)
- ○ **C.** Broadcasts packets it receives to all connections
- ○ **D.** Determines whether a packet belongs on an internal or an external network

54. You are troubleshooting a user's system that connects to the network and disconnects from the network in an alternating fashion. The system is connected via an Ethernet cable. Which of the following is the most likely cause?

- ○ **A.** Port flapping
- ○ **B.** High latency
- ○ **C.** Jitter
- ○ **D.** External interference

55. Which of the following cable types is prone to EMI?

- ○ **A.** Fiber optic
- ○ **B.** STP
- ○ **C.** UTP

- **D.** Multimode

56. You are troubleshooting a projector in a conference room. The training manager tells you that it flickers during presentations. As you investigate the problem, you verify the flicker on the projector screen but notice that the laptop display does not yield the same issue. You modify the resolution on the laptop, but the issue continues. Which of the following is the next step that you should take to fix the problem?

- **A.** Check power cable connectivity.
- **B.** Check video cable connectivity.
- **C.** Modify settings on the projector.
- **D.** Change the aspect ratio on the laptop.

57. A workgroup of five PCs uses a shared printer. A customer is not able to print to the printer but can access shares on another PC used for common files. The printer appears to be powered on. Which of the following would be the most likely cause?

- **A.** The PC with the connected printer is off the network.
- **B.** The printer needs to be restarted.
- **C.** The printer is low on toner.
- **D.** Device drivers are corrupted.

58. What is the term for devices that have an integrated CPU and RAM and are part of the Internet of Things (IoT), such as smart security systems and fire alarms, medical sensors, and appliances?

- **A.** Embedded systems
- **B.** Syslog servers
- **C.** Web servers
- **D.** IDS/IPS systems

59. You just set up a printer in the company training room. The trainer wants to be able to print multiple copies of the training

documentation for class, and to comply with the company's new green policy, the trainer needs to conserve paper by printing on both sides of the documents. To comply with the policy, which feature should they be primarily concerned about?

- **A.** Orientation
- **B.** Print quality
- **C.** Duplexing
- **D.** Sharing
- **E.** ADF

60. Which of the following voltages are normally supplied by a PSU's rails? (Select the two best answers.)

- **A.** 1.5 V
- **B.** 3.3 V
- **C.** 5 V
- **D.** 9 V

61. You are troubleshooting a printer. Which of the following are common symptoms of printer failure or other printer issues? (Select the three best answers.)

- **A.** Vertical lines down the printed pages
- **B.** Garbled print
- **C.** Faded print
- **D.** Failure to document screw and cable locations

62. Which of the following cable types would most likely experience degraded video signal quality over long distances?

- **A.** VGA
- **B.** HDMI
- **C.** DVI

- **D.** DisplayPort

63. You are building a high-performance workstation. You are required to select a boot drive with the highest performance available. Which of the following is the best option?

- **A.** NVMe
- **B.** 15K rpm HDD
- **C.** MicroSD
- **D.** USB flash

64. You are tasked with fixing a client's PC that hasn't booted after the latest test of the building's backup generator. As you analyze the computer, you notice that once it is powered on, there is no display and there are no beep codes. After 15 seconds, the fans inside the computer start spinning faster and making more noise. The computer was working fine before the test, and you verify that no one has opened the computer. Which of the following is most likely the problem?

- **A.** The RAM was damaged by ESD.
- **B.** The motherboard was damaged by the power test.
- **C.** The storage drive was erased due to the power test.
- **D.** The power supply was damaged and is nonfunctional.

65. Which of the following memory technologies enables protection against random inconsistencies when storing data?

- **A.** Quad-channel
- **B.** Parity
- **C.** Dual-channel
- **D.** ECC
- **E.** RAID 5

66. You are servicing a small office's network. One PC's network adapter has a link light that is lit, but the PC can't access internal network resources located on other PCs on the LAN. Which of the following is the most likely cause of the issue?

- ○ **A.** IP address conflict
- ○ **B.** High latency
- ○ **C.** Jitter
- ○ **D.** Limited connectivity
- ○ **E.** APIPA
- ○ **F.** Slow network transfer speed

67. A workstation fails to boot. The POST found an error, and the computer beeps twice. This happens again and again. Which of the following is the most likely issue?

- ○ **A.** Power supply failure
- ○ **B.** Video adapter failure
- ○ **C.** Memory failure
- ○ **D.** CPU failure

68. You are attempting to install Hyper-V on a Windows computer. However, you receive an error saying that the software cannot be installed. Which of the following CPU characteristics should be checked?

- ○ **A.** Number of cores
- ○ **B.** Virtualization support
- ○ **C.** Hyper-threading
- ○ **D.** Cache size

69. You are a technician working on a problem with a projector. While investigating, you find that the lamp turns off for brief periods during longer demonstrations. You replace the lamp, but the problem

continues, and now you get a message that appears just before the lamp turns off. Which of the following should you perform? (Select the two best answers.)

- **A.** Replace the cooling fan.
- **B.** Change the video resolution.
- **C.** Install a more powerful lamp.
- **D.** Adjust the brightness.
- **E.** Reset the lamp counter.
- **F.** Update the laptop's video driver.

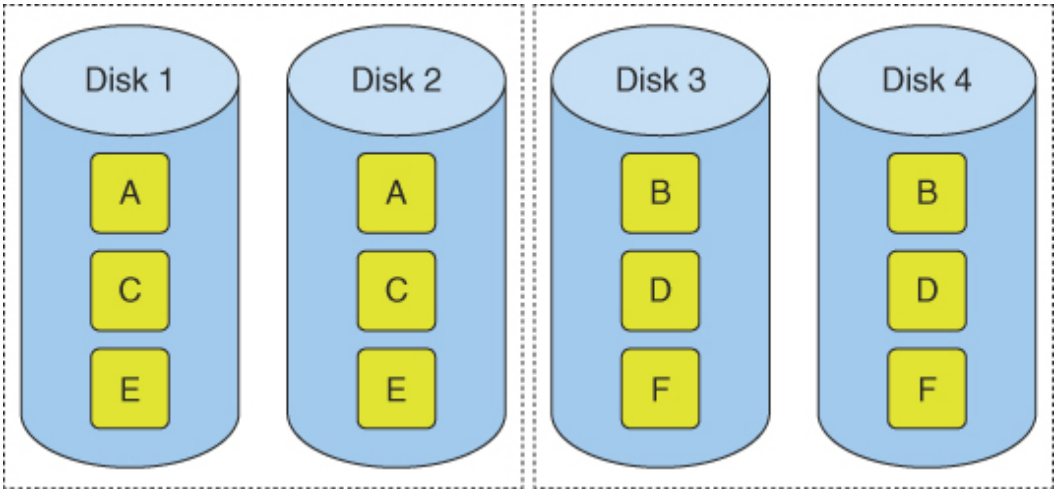
70. Which of the following are commonly found in electrical power grids, water treatment plants, gas/oil pipelines, hydroelectric systems, sewage systems, and traffic systems and must be heavily secured because they are often used in protected environments and infrastructures?

- **A.** SCADA systems
- **B.** Routers
- **C.** Load balancers
- **D.** Spam gateways

71. Which of the following ports can be used for audio, video, and storage?

- **A.** Thunderbolt
- **B.** DisplayPort
- **C.** HDMI
- **D.** DVI

72. Which RAID configuration is displayed in the figure?



- **A.** RAID 0
- **B.** RAID 1
- **C.** RAID 5
- **D.** RAID 6
- **E.** RAID 10

73. Which of the following protocols is used to perform file sharing between Apple computers running macOS and PCs running Windows on a LAN?

- **A.** RDP
- **B.** SSH
- **C.** POP3
- **D.** SMB

74. You have been hired to install a network cable in a crawl space that runs the length of a hallway. You are required to meet fire code specifications. Which of the following types of cable should you run?

- **A.** Shielded
- **B.** Coaxial
- **C.** Fiber

- **D.** Plenum

75. You replace a failed storage drive with a new one. You then boot to a special preinstallation environment media so that you can install a custom operating system build that is meant for deployment to the network. The storage drive is recognized in the UEFI/BIOS, but once you have booted to the preinstallation environment, the storage drive is not recognized, the process fails, and the drive can't be imaged. Which of the following statements best describes the most likely problem?

- **A.** The PC's power supply cannot provide enough power for the new drive.
- **B.** The boot media has failed and needs to be replaced.
- **C.** The storage drive has not been partitioned correctly.
- **D.** The storage drive must be configured in the UEFI/BIOS.

76. Which of the following LAN hosts would most likely provide the services needed to allow multiple clients access to cached Internet web pages?

- **A.** File server
- **B.** Proxy server
- **C.** Web server
- **D.** DNS server

77. Your organization has paid access to virtually unlimited cloud resources but pays only for the resources that are used. What is this called?

- **A.** Rapid elasticity
- **B.** Community cloud
- **C.** Metered services
- **D.** High availability

78. One of the workstations at your organization was just moved to a new work location in the same building. The new location does not have a surge suppressor. The workstation was working the day before, but today the system will not power up, the fans do not spin, and there are no other signs of activity. Which of the following should you do first?

- **A.** Check the voltage of the PSU with a multimeter.
- **B.** Check for swollen capacitors.
- **C.** Check the voltage switch on the PSU.
- **D.** Check the power cable connection.

79. You are planning a secure screened subnet (DMZ) that will incorporate several servers, including a web server, an FTP server, and a mail server. Which inbound ports will need to be opened at the firewall so that the servers can securely communicate with users on the Internet? (Select the four best answers.)

- **A.** 21
- **B.** 22
- **C.** 23
- **D.** 53
- **E.** 80
- **F.** 110
- **G.** 143
- **H.** 443
- **I.** 587
- **J.** 995
- **K.** 3389

80. You need to run a diagnostic program by booting to a USB flash drive on a laptop running Windows. You modify the boot order in the

UEFI/BIOS and set it to the flash drive first. However, the laptop still boots into Windows. What do you need to adjust to boot to the USB flash drive?

- **A.** Secure Boot
- **B.** TPM
- **C.** UEFI/BIOS password
- **D.** Virtualization

81. Which Wi-Fi standard was the first to introduce support for the 6 GHz frequency band, significantly reducing interference from legacy devices?

- **A.** Wi-Fi 5
- **B.** Wi-Fi 6
- **C.** Wi-Fi 6E
- **D.** Wi-Fi 7

82. Why is Network Time Protocol (NTP) considered a critical service in network environments?

- **A.** It ensures timestamp accuracy for security policies and log correlation across systems.
- **B.** It automatically adjusts firewall rules based on time-sensitive threat levels.
- **C.** It coordinates scheduled updates and software rollouts across multiple devices.
- **D.** It helps enforce time-based access control for users on shared systems.

83. Which of the following best explains why **multitenancy** is a cost-effective approach for cloud providers?

- **A.** It allows providers to assign each customer a dedicated virtual server, increasing billing efficiency.

- **B.** It enables multiple customers to share the same physical resources while maintaining secure data isolation.
- **C.** It reduces the need for synchronization services by consolidating all client data into a single database.
- **D.** It improves network availability by routing each tenant's traffic through separate, physical network interfaces.

84. A technician powers on a server and receives the error message "RAID Array Not Found." The system previously booted from a RAID 0 configuration. Which of the following is the most likely cause of this issue?

- **A.** The RAID controller firmware was corrupted or reset to default.
- **B.** One of the drives was accidentally reformatted during maintenance.
- **C.** The system was infected with ransomware that deleted the array.
- **D.** The boot order in Windows Disk Management is incorrect.

85. A user complains that icons and text on a new 4K monitor appear too small, making them difficult to read. Which of the following is the best solution to this problem?

- **A.** Decrease the refresh rate in the monitor's OSD menu.
- **B.** Change the monitor's color depth to 16-bit.
- **C.** Increase the display scaling percentage in the operating system.
- **D.** Lower the resolution to 1024×768.

86. A user reports that their smartphone has become noticeably slower when launching apps and navigating menus. Which of the following is the most appropriate initial step to troubleshoot this degraded performance?

- **A.** Update all apps to the latest versions.
- **B.** Perform a factory reset of the device.
- **C.** Close unnecessary background applications.
- **D.** Clear the system cache partition from recovery mode.

87. A user is unable to log in to their domain account despite entering the correct username and password. Which of the following should a technician check first to identify the cause of the authentication failure?

- **A.** Confirm the user's password has not expired.
- **B.** Ensure the workstation is not infected with malware.
- **C.** Check if the workstation's antivirus definitions are up to date.
- **D.** Verify that the authentication server is reachable and the user's account is not locked.

88. A user reports that nothing is printing and multiple jobs are stuck in the queue. Canceling the jobs does not work. What is the next best step a technician should take to clear the print queue?

- **A.** Reboot the printer and the computer.
- **B.** Change the printer's default paper tray.
- **C.** Lower the printer's print quality setting.
- **D.** Stop and restart the print spooler service.

89. Why would a network administrator configure DHCP exclusions within a DHCP scope?

- **A.** To ensure specific IP addresses are not dynamically assigned, typically because they are reserved for devices with static IPs
- **B.** To prevent DHCP servers from responding to requests from unauthorized MAC addresses

- ○ **C.** To block specific clients from obtaining any IP address through DHCP
- ○ **D.** To permanently assign the same IP address to a client using its MAC address

Answers at a Glance

1. C
2. B
3. D
4. D
5. A
6. C, E
7. A
8. A, D
9. C
10. B
11. C
12. B
13. D
14. C, D
15. B
16. A, B
17. A
18. C

19. D

20. B

21. C

22. B

23. B

24. D

25. C

26. B

27. E

28. D

29. B

30. B

31. B

32. C

33. B, C, E

34. C, D

35. A, D

36. B

37. C, E

38. C

39. E

40. B

41. B

42. C

43. A

44. B

45. C, D

46. D

47. D, E

48. B

49. A

50. A

51. B

52. C

53. B

54. A

55. C

56. B

57. A

58. A

59. C

60. B, C

61. A, B, C

62. A

63. A

64. B

65. D

66. A

67. C

68. B

69. A, E

70. A

71. A

72. E

73. D

74. D

75. C

76. B

77. C

78. D

79. B, H, I, J

80. A

81. C

82. A

83. B

84. A

85. C

86. C

87. D

88. D

89. A

Answer Explanations

1. **Answer: C.** The central processing unit (CPU), otherwise known as the processor, is often considered to be the "brains" of the computer because it performs the bulk of the calculations for the system. See Chapter 17, "CPUs," for more information.

   Incorrect answers: Random-access memory (RAM) stores calculated data over the short term; it is often called volatile memory because its contents are lost when the computer is shut down. A storage drive stores data over the long term; it is often called non-volatile memory, or simply "storage," because it retains data when the computer is shut down. The motherboard is the central connecting point for all components and connections within the computer, including the CPU, RAM, and storage drive.

2. **Answer: B.** Most of the time a computer's BIOS (or UEFI) is configured to boot to the storage drive first. To boot from a USB flash drive, an optical disc, or other removable media, you might need to change the boot sequence—also known as the boot order or boot priority—and place the removable media first. However, if the drive is brand new and blank, you still might be able to boot from the removable media, even if it is not first on the list. This will depend on the system, but essentially, the BIOS will see that the drive is blank and move on to the next boot media on the list. Keep in mind that you might boot to removable media with an operating system for other reasons than installing the OS (for example, recovering an existing system). See Chapter 16, "Motherboards and Add-on Cards," for more information.

Incorrect answers: Enabling a BIOS/UEFI password is not necessary, but there should be a password. If there is, you need to know it to access the BIOS. If there is not a password, you should create one while you are there. TPM (Trusted Platform Module) deals with the encryption of data on the storage drive and should be enabled or disabled before an operating system is installed; it won't have any bearing on the boot sequence.

3. **Answer: D.** The RJ-45 connector is the most common type of networking connector. It is used in Ethernet twisted pair networks. See Chapter 13, "Cables and Connectors," for more information.

   Incorrect answers: RJ-11 is the connector used by landline-based phones (POTS connections) and DSL connections in households. The F-type connector is a type of coaxial connector used for cable TV and cable Internet connections. ST stands for straight tip, and it is a type of fiber optic connector that is not common on a PC's network interface card.

4. **Answer: D.** The data channel (bus width) of quad-channel RAM is 256-bit. In this environment, you can have four separate modules of RAM (or possibly eight or more) working together. See Chapter 14, "RAM," for more information.

   Incorrect answers: Single-channel is 64-bits wide, dual-channel is 128-bits. Triple-channel is 192-bits. 288-pin is different; it refers to the connection type for DDR4 and DDR5 RAM (though they are not compatible with each other).

5. **Answer: A.** The page count counter should be reset whenever you perform normal, scheduled printer maintenance. For example, a laser printer can print about 200,000 pages before it needs scheduled maintenance. By resetting the page count after a successful maintenance, you will know when the next maintenance should occur. This is reset on the printer itself. See Chapter 20, "Printer Maintenance," for more information.

   Incorrect answers: The job queue and cache should reset automatically; the reason is that you would normally turn off the printer before maintaining it. Any print queue located on a computer

is not reset automatically, but jobs in the queue will probably have to be re-sent. The tray settings do not have to be reset.

6. **Answers: C and E.** You should perform a virus scan and then document findings, actions, and outcomes.

   Incorrect answers: The computer was already rebooted in the scenario, and you already verified that it can now access the Internet. If you can ping the gateway (router) and access the Internet, then the TCP/IP settings should be fine, and using **ipconfig** isn't necessary. If you can connect to the Internet, then the system was already reconnected to the network previously. However, it is important to note that any system that you are troubleshooting for malware should indeed be taken off the network right away until the malware is removed.

Note

Yes, be ready for questions that might traverse the 220-1201 *and* 220-1202 objectives. This question covers virus scans and AI, which aren't covered until the 220-1202 portion of this book. We suggest going through this entire book before attempting either of the exams. Read the whole book and then revisit the concepts and objectives for each exam—and take one exam at a time.

Also, be sure to read the entire question. Questions such as these are much more in-depth than questions 1–5. Not all the questions you see will be this wordy (or have as many potential answers), but you need to be prepared for the tougher ones. In addition, when you see questions that require multiple answers, you will see checkboxes instead of the typical radio buttons. Use the process of elimination when you encounter these and any other questions.

7. **Answer: A.** Of the listed answers, you should check the DC-in jack on the laptop first. However, the *very* first thing you should do is check the basics: See if the power brick is connected to the AC outlet and to the DC-in jack and verify that the battery is connected

properly. See Chapter 1, "Monitoring, Maintaining, and Replacing Mobile Device Hardware," for more information.

Incorrect answers: Laptops don't have an AC-in jack; the power adapter takes care of converting AC power to DC power for the laptop to use. Of course, you should always check the laptop battery first, to ensure that it is not missing and make sure it is connected properly. Next, make sure the power adapter is plugged into the DC-in jack and that the jack is not damaged. A damaged DC-in jack can also cause the laptop to occasionally shut off. Users often damage the DC-in jack because they leave the power adapter plugged in while they are in transit. On most laptops, a new one has to be soldered on to the board. The CMOS battery is inside the laptop. It retains UEFI/BIOS settings and has nothing to do with charging the main laptop battery. The AC circuit breaker might have tripped, but this is less likely than the previously listed reasons. Also, a good indication of a failed AC circuit is that all of the devices on that circuit stop working.

8. **Answers: A and D.** You should clean and inspect the entire paper path first. This costs nothing; plus, by clearing out any papers in the path, you will often solve the problem, at least temporarily and perhaps permanently. Also, use the correct printer maintenance kit to replace worn parts. The parts from these kits should be installed every 100,000 to 200,000 pages printed (depending on the printer). Older worn parts can often lead to paper jamming, especially if the problem has been getting worse lately. See Chapter 28, "Troubleshooting Printers," for more information.

   Incorrect answers: Paper jams don't usually occur in the fusing assembly, but it is a possibility. Of course, you should wait 10 to 15 minutes for the fuser to cool before cleaning or replacing it. (Don't forget to make sure the printer is turned off and unplugged.) Replacing other components such as sensors and switches (if they exist) is less common. It is also uncommon to clean and inspect the print drum; instead, you simply replace the toner cartridge. However, this concerns problems such as streaking, marks, and ghosting more than it does paper jams.

9. **Answer: C.** CompTIA lists the Bluetooth connection process in the following order: Enable Bluetooth, enable pairing, find a device for pairing, enter the appropriate PIN code, and, finally, test connectivity. See Chapter 3, "Mobile Device Network Connectivity and Application Support," for more information.

   Incorrect answers: Testing connectivity is the final step and should be completed after you have entered the appropriate PIN code. You don't have to turn the connecting devices off and then back on during the connection process. Enabling Bluetooth is the recommended first step in the Bluetooth connection process.

10. **Answer: B.** If the power supply fan and the case fans are spinning but there is no power to other devices, chances are that the main 24-pin power connection was not made from the power supply to the motherboard. In this scenario, the case fans would have been connected by way of Molex or SATA power connectors directly to the power supply. Although it's usually better to connect case fans to the motherboard, if they are connected to the motherboard, they do not spin because the motherboard is not receiving power. If this scenario were to occur, no other devices would get power, including the CPU, RAM, motherboard, storage drives, optical drives, and so on. See Chapter 18, "Power," for more information.

    Incorrect answers: If the boot drive fails, the operating system will fail to boot up. If the drive cannot be repaired, it will have to be removed and replaced. If the drive is not recognized, again, the OS will not boot. It would have to be reconnected properly, configured in the BIOS/UEFI, or partitioned and formatted properly in Windows, depending on the specific situation. Failed RAM could cause a boot failure and will definitely be registered by the POST, but it doesn't necessarily mean that the RAM (or any other device) is not receiving power.

11. **Answer: C.** The best answer listed is to check the motherboard for swollen capacitors. A swollen (or distended) capacitor could cause the system to reboot intermittently. The capacitor (or entire motherboard) needs to be replaced. See Chapter 23, "Troubleshooting Motherboards, CPUs, RAM, and Power," for more information.

Incorrect answers: It is unlikely that the network adapter or fragmented storage drive would cause the system to sporadically reboot, but you should check for the latest drivers and firmware for the network adapter anyway and analyze whether the storage drive has been defragmented of late (especially for magnetic disks). RAM could cause the system to periodically reboot, mainly if the RAM is overheating. (RAM heat sinks could fix that.) But the wrong type of RAM will usually result in a POST failure instead.

12. **Answer: B.** Use an Ethernet patch cable to connect a cable modem to a SOHO router. Consider Cat 5e, Cat 6, or better. This is the same kind of patch cable that is used to connect a computer to an RJ-45 jack, as well as connect a patch panel port to a switch port. This is a shorter question (and perhaps a bit easier than the last few) but could still be a little tricky if you are not reading the question carefully. See Chapter 13, "Cables and Connectors," for more information.

    Incorrect answers: Use an RG-6 coaxial cable to connect the cable modem to the coaxial jack. USB cables can be used to connect a plethora of devices to PCs, laptops, and mobile devices or can be used to charge devices (depending on the type of USB cable). Thunderbolt can be used to transmit data to devices or video to displays. SATA cables are used to connect storage drives to a motherboard.

13. **Answer: D.** The only answer listed that is an example of a MAC address is 00-1C-C0-A1-55-21. The MAC address is the address burned into the ROM chip of a network adapter that uniquely identifies it. This address is composed of six hexadecimal numbers, each between 00 and FF. The decimal equivalent of this is 0 through 255. The first three numbers are the OUI (organizationally unique identifier); 00-1C-C0 is an Intel OUI. The last three numbers are the individual address of the particular network adapter. You might also encounter MAC addresses separated by colons instead of hyphens. See Chapter 8, "Network Devices," for more information.

    Incorrect answers: 10.1.1.255 is an IPv4 address. 4410:FF11:AAB3::0012 is a truncated IPv6 address. https://greencurtaintraining.com is a web address (or URL). It

includes the protocol used (HTTPS) and the domain name (greencurtaintraining.com).

14. **Answers: C and D.** You would most likely use LAN (local area network) and MAN (metropolitan area network) network types. The LAN is for internal office communications, and the MAN is for office-to-office network communications (which will require a data communications provider). Both of these can handle 1 Gbps network communications. See Chapter 10, "Network Types," for more information.

    Incorrect answers: A SAN (storage area network) is used to connect NAS devices and RAID arrays at high speed. A WAN (wide area network) is used to connect multiple LANs but over large geographic distances—and perhaps at speeds lower than 1 Gbps. A PAN (personal area network) is used to connect Bluetooth devices in an ad hoc manner.

15. **Answer: B.** A tone generator is often used to locate cables, especially if there are a bunch of them in a small area. In the scenario, the technician is connecting the tone generator to an RJ-45 port, perhaps near a person's desk. Then the technician uses the probe (an inductive amplifier) to locate the other end of that cable at the patch panel either in a wiring closet or in the server room. Collectively, the two tools are known as a tone and probe kit, or toner probe. See Chapter 11, "Networking Tools," for more information.

    Incorrect answers: The other answers require a cable tester/cable certifier. Although a cable tester can often act as a tone generator, a tone generator is not a cable tester; it can only generate a tone across the cable. Cable certifiers are used to confirm continuity, validate proper wiring, and test the transmission quality of a given connection.

16. **Answers: A and B.** Cellular connections are disabled when a mobile device enters airplane mode, and so are other wireless connections, such as Wi-Fi, Bluetooth, GPS, and NFC. However, on some devices, some of these other wireless technologies can be turned on individually after the device has been placed in airplane mode. See

Chapter 3, "Mobile Device Network Connectivity and Application Support," for more information.

Incorrect answers: The display's multitouch capabilities will work as normal, but web browsers, email programs, and other apps that require Internet access will appear not to function properly when tapped on and navigated through—because, indeed, they are not functioning at all due to airplane mode. Data encryption will still function, though you won't be able to send that encrypted data anywhere. The camera will work, but posting images and video to a remote source will not function.

17. **Answer: A.** USB-C is a universally accepted standard that enables charging, syncing data, and playing audio and video. From the iPhone 15 on, Apple switched over to USB-C. See Chapter 2, "Mobile Device Accessories and Connectivity Options," for more information.

    Incorrect answers: Apple devices do not use Micro-USB or Mini-USB, although adapters may be available depending on the device used. Micro-USB is common on Android-based devices. The Lightning connector is a proprietary connector that was used by Apple mobile devices. The iPhone 14 was the last iPhone to use the Lightning connector.

18. **Answer: C.** Verify that the user is sending the document to the correct printer (printer queue). When there are multiple printers on a network, it's easy to mistake one name for another. Remember that OCP stands for operator control panel, which is the display on the printer. See Chapter 28, "Troubleshooting Printers," for more information.

    Incorrect answers: You should not need to stop and start the print spooler service (which would undoubtedly be at the user's PC) because the user is able to print exactly the same document to other printers. Stopping and starting the printer queues could cause some angst among employees and won't do anything to help the problem either. It's never wise to ask *all* employees of an organization to do anything—in this case, sending the same document to the printer—

especially when you already know that the other users can print to the printer in question.

19. **Answer: D.** You need to go to another computer, download the driver from the manufacturer's website, copy that to a flash drive, and bring it back to the affected computer. See Chapter 27, "Troubleshooting Wired and Wireless Network Problems," for more information. "What's a disc?" you say? For that, you will need to review Chapter 15, "Storage Drives."

    Incorrect answers: If you have access to another computer, it would be silly to wait for a media (disc or USB thumb drive) from the manufacturer. And any manufacturer that charges for drivers (or a driver media) should be ashamed, as should the user who actually purchases the media! You can't run Windows Update or download drivers from the computer in question because the computer has no network connection; and remember, Windows Update is used to download Microsoft drivers, not other vendors' specific drivers.

20. **Answer: B.** The Domain Name System (DNS) server is the server that is in charge of resolving domain names (such as example.com) to their corresponding IP addresses (such as 93.184.216.34 or another IP address). So, in other words, it maps user-friendly names to network resources. The DNS server can supply this information to you when you make use of various commands at the command line, such as **ping**, **tracert**, **nslookup**, and **dig**. See Chapter 8, "Network Devices," and Chapter 7, "Network Configuration Concepts," for more information.

    Incorrect answers: A DHCP server takes care of handing out IP addresses to client computers automatically. An authentication server —such as a domain controller running LDAP—is in charge of verifying the identity of users who attempt to log in. A syslog server is used to gather the logs from network devices and present the information in a manageable way to an admin's workstation. A print server is a computer that is in charge of one or more printers on the network.

21. **Answer: C.** On-demand means a cloud service is available when the user needs it, 24/7. It allows a user to store data to the cloud, when necessary, but can be removed when space is freed up at the local system. See Chapter 22, "Cloud Computing Concepts," for more information.

    Incorrect answers: Shared resources means that different customers share server space, infrastructure, and so on in a public cloud setting. With metered utilization, an organization has virtually unlimited cloud resources but only pays for what is needed. Resource pooling is the grouping of servers used by customers in a highly available and scalable way.

22. **Answer: B.** Use a hypervisor! This is the software that hosts virtual machines (for example, VirtualBox, which is a Type 2 hypervisor). However, if you are working for a medium-sized enterprise organization, you might want to consider a Type 1 hypervisor, such as ESXi or Hyper-V for Windows Server. See Chapter 21, "Virtualization Concepts," for more information.

    Incorrect answers: Remote Desktop Services is a Microsoft utility that lets you connect to and remotely control other Windows systems or use applications from those systems. (It is also known by its older name: Terminal Services.) A virtual LAN allows you to regroup systems virtually within a LAN; it is done at the switch or with special software. A virtual LAN is not required to have *virtual* machines. Disk Management is a Windows utility used to configure storage drives. Device Manager is a Windows utility used to configure the various devices on a PC or laptop.

23. **Answer: B.** The best answer listed is Infrastructure as a Service (IaaS). This allows for networking services, storage, load balancing, routing, VM hosting, and more. See Chapter 22, "Cloud Computing Concepts," for more information.

    Incorrect answers: Software as a Service (SaaS) provides common applications such as Gmail or Microsoft 365 to clients over the Internet. Platform as a Service (PaaS) provides software solutions such as the ability to develop and test applications within the cloud. A

hybrid cloud is a mixture of public and private clouds that combines dedicated on-premises servers with servers from a cloud service provider.

24. **Answer: D.** With bridged networking, virtual machines can get *direct* access to the hosting computer's network connection and access other systems on the LAN and the Internet. You might also see this referred to as "external," or "public." See Chapter 21, "Virtualization Concepts," for more information.

    Incorrect answers: With Network Address Translation (NAT), the guest can access the external network but not directly. Instead, the guests using NAT get IP addresses on a separate private IP network. Host-only networking creates a private virtual network for the guests, and they can communicate with each other, but not out to the external network or Internet.

25. **Answer: C.** In this scenario, it is possible that the printer's IP address has been changed, and it is the best choice of the listed answers. The workstations were manually configured (most likely via IP address), which means that an IP address change on the printer would cause any print jobs from those workstations to fail. The IP address could have been configured manually by another tech, or if it was set to DHCP, the printer might have received a new address from the DHCP server. Because of this exact scenario, it is always a good idea to configure a static IP address at the printer itself (within the LCD display). Remember, in the scenario, the printer can be seen in the network directory, which usually searches by printer *name* as opposed to printer IP address. Also, test pages are printing successfully. All these are clues that point to a potential IP problem. See Chapter 28, "Troubleshooting Printers," for more information.

    Incorrect answers: Restarting the print spooler service is a troubleshooting technique used when the spooler service is hung up for some reason. It generally doesn't cause problems but can fix a lot of spooling issues. Two print jobs can't be sent at the same time; collisions are a concept related to networking. It is possible that packets or frames can collide, but not the actual print jobs. The print jobs are placed into a queue either at the printer or at the print server.

The need to perform printer maintenance doesn't usually cause print failures, but if you see that message, you should attend to it right away.

26. Answer: B. The main advantage of UDP (User Datagram Protocol) over TCP (Transmission Control Protocol) is that it can transfer data packets faster. Because it is a connectionless protocol, it doesn't require the overhead of synchronization or sequencing that TCP does. This makes it a faster option for streaming services, VoIP, and so on. See Chapter 4, "TCP and UDP Ports and Protocols," for more information.

Incorrect answers: UDP does not have an option for flow control. Also, it does not use a handshaking process. (TCP uses the three-way handshake: SYN, SYN-ACK, ACK.) As mentioned, UDP is connectionless, whereas TCP is connection based. However, even though UDP can transmit packets faster, you will find that TCP is used for most services and applications you will deal with.

27. Answer: E. John forgot to verify full system functionality. We can't stress it enough: Always *test!* And by "*test*," we mean verify functionality—make sure it works—not "test the theory." With a default installation of a plug-and-play network card, the card will, by default, be set to obtain an IP address automatically. If the computers need to be configured for static IP addresses, this will most likely cause a problem. There might not even be a device or server that is handing out IP addresses on the network. If that is the case, the Windows computer would attempt to self-assign an IP address (an APIPA address starting with 169.254). If that happens, the computer will most definitely not be able to communicate with the gateway—or the Internet, for that matter. And even if there is a DHCP server on the network, the chances are very slim that it is handing out addresses on the 192.168.50.0 network. Most SOHO routers will hand out addresses on the 192.168.0.0 or 192.168.1.0 networks, and that is only if DHCP is enabled.

John should have logged in to Windows, checked the system with **ipconfig /all**, run a ping test, tried to connect to websites with one or

more browsers, and so on. Verifying full functionality is very important. Always remember to test every repair thoroughly.

Incorrect answers: John performed all basic troubleshooting steps (the other options listed) except for verifying full system functionality.

ExamAlert

Know the A+ troubleshooting methodology like the back of your hand for both exams!

28. Answer: D. You will need to replace both failed drives (which causes a total RAID 5 array failure, by the way) and restore the entire set of data from tape backup, from the cloud, or elsewhere. See Chapter 15, "Storage Drives," and Chapter 24, "Troubleshooting Storage Drives and RAID Arrays," for more information.

Incorrect answers: In a RAID 5 array, one drive can fail, and you can still recover from the issue without tape backup (using the RAID parity information), but no more than one drive can fail. If more than one drive fails—as in the question's scenario—you need to restore all data from a previous backup. However, in RAID 6, two drives can fail, and it can still recover. Formatting the RAID array is a good idea if you have to recover from backup but not a good idea otherwise because it will make the current data inaccessible. However, *quick option* is a Windows term, implying that the RAID array was created in Windows and is therefore a software-based array. It is recommended that you create hardware-based arrays that connect to a RAID adapter card (or RAID-enabled motherboard). In a hardware-based system such as this, you could repair the array with the system utilities, but again, in this scenario (with RAID 5), only if one drive has failed.

29. Answer: B. Using a password and some kind of biometrics is an example of two-factor authentication, or 2FA. See Chapter 3, "Mobile

Device Network Connectivity and Application Support," for more information.

Incorrect answers: The rest of the answers do not deal with authentication directly. Some deal with identification, but none offer two-factor authentication solutions. The IMEI identifies a mobile device, and the IMSI is used to identify the user of a device. GPS technology is a mobile tracking service that can help a user navigate while driving (among other things). PRL updates help you get better coverage by keeping your device on preferred networks. Baseband updates are necessary to communicate properly with GSM cell towers.

30. **Answer: B.** The laser printer is the one that is most associated with maintenance kits. Common components of a laser printer maintenance kit include a fuser assembly, a transfer roller, and pickup rollers. See Chapter 28, "Troubleshooting Printers," for more information.

    Incorrect answers: Common components of a thermal printer include the feed assembly and heating element. The inkjet printer normally includes the ink cartridge, print head, roller, feeder, duplexing assembly, carriage, and belt. An impact printer's components include the print head, ribbon, and tractor feed.

31. **Answer: B.** Although you could try several things, the best of the listed answers is to disconnect the AC connection and the battery and press and hold the power button for several seconds. This approach effectively discharges the laptop (capacitors and such) and may also clear the BIOS, either one of which could potentially fix the problem. Exactly what happens will depend on the model of laptop, and the length of time you will need to hold down the power button will vary (it could be up to 30 seconds). Afterward, reconnect the battery and AC connection and continue troubleshooting from there, if necessary. The key in this question is that you cannot hear or see anything happening. In most cases, something will happen, but in this case, the laptop may have had a voltage overload or other similar problem. Discharging it in this fashion can fix the problem, but you might have

to reconfigure your BIOS. See Chapter 1, "Monitoring, Maintaining, and Replacing Mobile Device Hardware," for more information.

Incorrect answers: Booting the system to a flash drive will probably result in nothing. If you can't see or hear anything, you need to take stronger measures than that. Sometimes, removing drives and USB devices can help when troubleshooting, but again, in this scenario, where you can see and hear nothing, it probably won't help. Connecting an external monitor is a good idea if you can see LED lights blinking when you press the power button but get no main display. In this case, the result will probably be no image on both displays.

32. **Answer: C.** One of your most important considerations should be the input voltage. For example, in the United States (and some other countries), this is 120 volts. However, in many other countries, it is 240 volts. (These are also represented as 115 VAC and 230 VAC.) It's better to avoid voltage converters if at all possible, so you will need a power supply unit (PSU) that can handle both. That means one of two things: an auto-selecting PSU or a PSU with a voltage switch. The former is preferable, so that the person setting up the computer at trade shows does not need to remember to check the switch. However, keep in mind that you might still need an adapter for the actual three-prong connection used in other countries. See Chapter 18, "Power," for more information.

Incorrect answers: The efficiency rating tells you how effectively the PSU uses energy. For example, the 80 Plus program promotes energy efficiency of more than 80 percent. While this is important for most computers—because we all want to conserve energy, right?—it is not as important for this particular system because the PC will be relying on power that is provided by the trade show venues. Rail amperage is important for resource-intensive computers such as gaming PCs, design systems, and so on, where an individual rail (such as the 12 V) can overheat if driven too hard. Of course, we don't want our devices (such as GPUs) to draw too much current from the PSU (which generally can max out at about 30 amps or so); however, the system is using typical components, so current should not be a factor. As long as the PSU meets the wattage requirements, it

should be okay. Maximizing the RAM shouldn't cause the computer to go beyond the maximum current or wattage (as long as you don't overclock it—but even then, it is unlikely). Almost all PSUs come with several SATA power connectors, and you are only using one storage drive, so that should not be a factor either.

33. **Answers: B, C, and E.** Potential root causes include the following: The touchscreen drivers need to be installed; the hardware replacement is not touchscreen capable; and the digitizer cable is not attached to the motherboard. Always make sure you install drivers, or the functionality on the system will be limited. Be sure to get the exact model screen that you need. And always verify that cable and connections are secure before closing up a system. See Chapter 12, "Device Display Components," for more information.

    Incorrect answers: There's nothing to calibrate yet because the touchscreen is not working at all. If it were working, and if the cursor (or touch sensitivity and positioning) were a little bit off, then calibration would be a good idea. A missing or insecure grounding screw shouldn't affect the touchscreen capabilities *only*; however, it might cause the entire system to fail to boot. You normally wouldn't have to update the panel's firmware (it should be done at the manufacturer), and also, the panel in question is an LED panel, not an LCD panel—splitting hairs, we know—but it is always important to purchase the correct replacement parts.

34. **Answers: C and D.** The most likely answers here are that there is no device (such as a video card) sending video or that the source cable has been disconnected (for example, from the computer's video card to the monitor). Always check the connections on both ends and make sure that the computer (the video source) is on and booting properly. See Chapter 25, "Troubleshooting Video Issues," for more information.

    Incorrect answers: The brightness and contrast settings are not likely to cause a no-image issue. On most monitors, you can reduce the brightness to 0 but still see the image on the screen. Likewise, you can increase the contrast to 100 (or whatever maximum number is used) and still see the image on the screen. It is not possible for the

monitor's backlight to have failed because you can see in the OSD that the proper video source has been selected. The OSD would not be visible (or would only be barely visible with a flashlight) if the backlight had failed. Again, it is much more likely that there is a connectivity or source video problem. Always check the connections first!

35. **Answers: A and D.** Check the memory and the power supply unit (PSU) first. Both of these can fail intermittently, causing random reboots. Try reseating and cleaning RAM (and replacing it, if necessary). Test the PSU with a PSU tester or multimeter and replace it if necessary. The PSU can also cause the computer to quickly shut down immediately after it was started. See Chapter 23, "Troubleshooting Motherboards, CPUs, RAM, and Power," for more information.

    Incorrect answers: If the video card fails, the computer simply won't display to the monitor. If the CMOS battery fails (or discharges), the time and date will reset to an earlier date (for example, to January 1, 20XX.) Other settings in the BIOS will be lost as well. If the optical drive fails, you won't be able to read optical media, but the optical drive should not cause the computer to reboot.

36. **Answer: B.** Near-field communication (NFC) is the short-ranged technology that contactless payment systems like Apple Pay and Google Wallet use. See Chapter 2, "Mobile Device Accessories and Connectivity Options," for more information.

    Incorrect answers: IMSI, which stands for International Mobile Subscriber Identity, is a unique 64-bit field used to identify the user of a cellular network. By the way, don't confuse IMSI with IMEI. IMEI, which stands for International Mobile Equipment Identity, identifies the phone. RFID stands for radio-frequency identification, a technology that uses tags and radio-frequency scanning to identify those tags. Bluetooth is a technology primarily used to allow for peripherals' access to a computer, such as using a Bluetooth headset with a smartphone.

37. **Answers: C and E.** Unless a company has a lot of servers, the servers will usually be assigned static IP addresses, as opposed to having them dynamically assigned by a DHCP server. When you manually configure the TCP/IP properties of a computer, you are required to enter the IP address and a subnet mask (for example, IP address 192.168.1.100 and subnet mask 255.255.255.0). Often, you will also configure a gateway address and a DNS server address, although they might not be required. The great thing about the static IP address is that you know what it is because you assigned it; you can enter it into your network documentation, knowing that it will not change. DHCP-assigned addresses can change from time to time, depending on how the DHCP scope was configured. See Chapter 9, "SOHO Network Configuration," for more information.

Note

There is one glaring issue in this question's scenario. Ever heard of the phrase "Don't put all your eggs in one basket"? That's exactly what is happening here. The server is doing everything: It's a domain controller, a file server, a print server, and who knows what else. Talk about a single point of failure! While small companies sometimes have to make do with the resources at hand, it would be wise to separate one or more of these services and either place them on a second server or use virtual machines or containers to achieve that goal.

Incorrect answers: Dynamic Host Configuration Protocol (DHCP) is not typically used for servers in a small company. Dynamic IP addresses are handed out by the DHCP server to client computers. The MAC address is the hexadecimal address that is programmed into the firmware of the network adapter at the manufacturing plant; it is not (normally) set by the administrator. A File Transfer Protocol (FTP) address is rather vague. Does that mean an IP address or a name? Either way, the scenario doesn't mention anything about FTP.

38. **Answer: C.** Of the listed answers, Lightweight Directory Access Protocol (LDAP) is relied upon most by Active Directory. LDAP deals with directory lists (such as the users within a Microsoft Active Directory domain) or the users' email addresses listed within a Microsoft Exchange server. See Chapter 4, "TCP and UDP Ports and Protocols," for more information.

    Incorrect answers: Server Message Block (SMB) is a protocol that allows shared access to files; it is important to any computer running Windows, not just computers that are in charge of, or connect to, a Microsoft Active Directory domain. SMB is also known as the Common Internet File System (CIFS). HTTPS (Hypertext Transfer Protocol Secure) is used to transfer data from a web server to a client computer's web browser. DHCP (Dynamic Host Configuration Protocol) is used to provide IP address information to clients automatically.

39. **Answer: E.** Always check the motherboard documentation before you begin installing components. You need to know what type of memory you should be using, what type of channel configuration (most likely dual- or quad-channel) to use, and where the sticks of RAM should be installed, depending on the configuration you will use. The motherboard documentation will have a table or matrix explaining all the different possibilities. A single motherboard might allow one stick of RAM, plus configurations for dual-channel, tri-channel, and quad-channel. You need to know what is allowed and plan for the right type of RAM before you purchase it. In this scenario, there are eight slots in total (0–7). If you install the memory into all the gray slots, then you are probably setting up the system for a multichannel configuration, but you must get the correct RAM. Note that the colors of the slots can be different, depending on the manufacturer; for example, they might be blue and black, and the first slots you should use are the blue ones. Check documentation! See Chapter 14, "RAM," for more information.

    Incorrect answers: Installing the memory to the dark gray slots might work, but it might not if those are the secondary slots for each channel. Going by the first four numbers might not be correct either, depending on the motherboard. In fact, a motherboard often uses the

numbering system A1, A2, B1, B2, C1, C2, D1, D2, with each letter corresponding to a different channel. Filling all the slots might work, perhaps if you get quad-channel-compliant memory (and a lot of it), but it is not the recommended choice because it can be expensive and probably is not necessary. The main lesson here is that there are a lot of possibilities, depending on the motherboard and depending on what you as the user wish to accomplish. So always RTM (read the manual) and plan your purchases wisely.

40. **Answer: B.** The inkjet printer uses piezoelectric pressure pads to produce small bubbles that are moved to the paper. See Chapter 20, "Printer Maintenance," for more information.

Incorrect answers: The laser printer applies toner to the paper in the electro-photographic imaging process. A thermal printer uses heat to create text and images on specially coated thermal paper. Impact printers use a print head to hammer the letters through a ribbon and on to the paper.

41. **Answer: B.** RAID uses multiple disks to increase performance and/or enable protection from data loss. RAID 0, 5, and 10 are often used to increase read performance, while RAID 1, 5, 6, and 10 can be used to enable protection from data loss. See Chapter 15, "Storage Drives," for more information.

Incorrect answers: Telling a customer that RAID stands for redundant array of independent (or inexpensive) disks is technical jargon that you should try to avoid. RAID is not a dynamic disk management system. However, in Microsoft operating systems, you need to set disks to dynamic in the Disk Management utility if you wish to add them to RAID arrays. Regardless, this is more information that the customer does not need to know. Finally, the statement "RAID uses striping to reduce the amount of storage drive write time and utilizes parity bits to reconstruct the data from a failed storage drive" is not altogether correct. RAID can also be mirroring. In addition, not all versions of RAID can use parity bits to reconstruct data from a failed storage drive. RAID 0, 1, and 10 do not. However, RAID 5 and 6 do. Remember that the customer needs to know how

the technology will make their business more efficient; they do not need to know the technical details or jargon.

42. **Answer: C.** Of the listed answers, the most likely cause is that the CPU needs to be reseated. This will result in a series of beeps from the power-on self-test (POST) as the BIOS searches for the CPU and can't find it. If a computer were being built in this scenario, then it's also possible that the RAM was not seated properly or there is some RAM compatibility issue. See Chapter 23, "Troubleshooting Motherboards, CPUs, RAM, and Power," for more information.

    Incorrect answers: No other answer choice would cause the POST to issue a series of beeps. The mouse would not, but a lack of a keyboard would result in beeps. (Always make sure the keyboard is securely connected!) Also, the POST doesn't look for operating system corruption; it is relegated to hardware only. However, it can display messages such as "no operating system found" if the storage drive is missing, not formatted, or not in the correct location in the BIOS/UEFI boot order. "The fan is running too fast" is subjective; regardless, its maximum speed is usually governed by the BIOS/UEFI settings and shouldn't affect how the system boots.

43. **Answer: A.** The firewall is the device that prevents outside intrusion by blocking ports and protocols. In many networks it is the first line of defense. See Chapter 6, "Networked Hosts," for more information.

    Incorrect answers: A gateway (usually a router) is a device that allows multiple clients on one network access to another network (for example, computers on the LAN that want to gain access to the Internet). A router connects two networks together. A bridge separates a LAN into two distinct network sections. An access point allows wireless connectivity to the network for Wi-Fi-enabled computers.

44. **Answer: B.** PCIe 8-pin is the best answer. Don't confuse this with 8-pin CPU power connectors. 6-pin PCIe power connectors are also common on older cards while some newer cards are using the 12VHPWR connectors. See Chapter 18, "Power," for more information.

Incorrect answers: The EATX12V 8-pin connector is used for CPUs. 24-pin ATX refers to the main power connection from the PSU to the motherboard. SATA power connectors are 15-pin and are used for storage drives and optical drives.

45. **Answers: C and D.** IPS (in-plane switching) monitor technology offers the widest viewing angle, and LED (light-emitting diode) monitors offer rich colors and consistent backlighting. See Chapter 12, "Device Display Components," for more information.

    Incorrect answers: Vertical alignment (VA) screens are significantly better than TN screens but not quite as good as IPS for viewing angle. TN (twisted-nematic) monitors are less expensive monitors that do not have as good a viewing angle as IPS. Note that LED also performs well when it comes to use in an area with a lot of natural light.

46. **Answer: D.** The next thing you need to do is connect to a wireless network, the first step of which is to scan for network names (SSIDs) or to add them manually. See Chapter 27, "Troubleshooting Wired and Wireless Network Problems," for more information.

    Incorrect answers: You won't type the security passphrase until you connect to a wireless network. The firmware and/or drivers for the WLAN card (Wi-Fi adapter) should be updated as part of the installation of that card. If the router is set up to accept wireless connections, encryption should have already been configured on that router as well.

47. **Answers: D and E.** External SATA (eSATA) is a SATA port that is meant for use with external devices. It is sometimes found as a port on the back of a PC or can be added with an adapter card. Of course, USB (3.0, 2.0, and so on) is another external port that is used to connect to audio and video equipment as well as external storage drives. See Chapter 13, "Cables and Connectors," for more information.

    Incorrect answers: Normally, SATA (without the *e* preceding it) is used for internal devices, not external devices. Serial Attached SCSI (SAS) is a type of storage drive technology that is used in servers and

power workstations rather than in typical PCs. Enhanced IDE (EIDE, also known as Parallel ATA) is an older storage drive standard that you won't see often—unless you are recovering data!—and it is internal by default.

48. **Answer: B.** White/orange, orange, white/green, blue, white/blue, green, white/brown, brown is the correct wiring sequence for the T568B wiring standard. You might also see this shown as WO, O, WG, B, WB, G, WBr, Br. It's the same thing, just abbreviated. See Chapter 13, "Cables and Connectors," for more information.

    Incorrect answers: The T568A standard, which switches the orange and green pins, is the older standard that was replaced by T568B. But to stay within electrical code and municipal guidelines, use the wiring scheme defined by the T568B standard on each end for straight-through cables. To create a crossover cable, use T568B on one end and T568A on the other. RJ-45 is a type of plug (or jack) that network cards, switches, and network jacks use. The TIA (Telecommunications Industry Association) developed the T568 standards and other wiring standards.

49. **Answer: A.** Use an RJ-45 crimper to crimp those RJ-45 plugs on the ends of a patch cable. See Chapter 11, "Networking Tools," for more information.

    Incorrect answers: Use a punchdown tool to terminate individual wires to the RJ-45 wall jack and to patch panels. Use a loopback plug to test a network adapter by plugging it into the card's RJ-45 port. Use a cable tester to test patch cables or longer LAN cable connections.

50. **Answer: A.** Quality of service (QoS) refers to the performance of user connections over the network, particularly connections to the Internet. On some small office/home office (SOHO) routers, QoS can be configured to allow for equal data transfers among all users, or it can be used to configure special traffic (such as streaming media) to transfer faster. See Chapter 27, "Troubleshooting Wired and Wireless Network Problems," for more information.

Incorrect answers: DSL (Digital Subscriber Line) is a family of technologies used to transfer data over the Internet. A WAN (wide area network) is a network that spans a large geographic area and connects two or more LANs. A VPN (virtual private network) allows for secure (tunneled) connections over the Internet.

51. Answer: B. You should clean the printhead! Most printers come with an onscreen utility that will do this, or you can manually clean the printhead (delicately!). Similarly, printers might need to be calibrated if colors are slightly off. See Chapter 28, "Troubleshooting Printers," and Chapter 20, "Printer Maintenance," for more information.

Incorrect answers: If the printer cables weren't connected, the printer wouldn't print anything at all. Maintenance kits are used more often for laser printers and are unnecessary in this case. The weight of the paper will not affect what colors are printed by an inkjet printer.

52. Answer: C. Use a power supply unit (PSU) tester to check whether the power supply is malfunctioning. If you ever smell something burning, even if it is a faint smell, turn off the power to any associated computers or devices and disconnect them from the AC outlet. Then test the affected PSU. Sometimes there is a burn-in period for new PSUs, and there might be a very faint smell for the first 24 to 48 hours. This is possible if the PSU was newly installed, but you should still test and monitor the PSU until the smell goes away. However, if the computer was working previously but suddenly doesn't work anymore, and you smell something burning, then you should most likely replace the PSU after testing it. Only test the PSU in your lab and make sure you have all the necessary fire prevention tools and technologies available. See Chapter 23, "Troubleshooting Motherboards, CPUs, RAM, and Power," for more information.

Incorrect answers: A loopback plug is used to test a switch port or the RJ-45 port on a computer. There are many cable testers, but the term is often associated with network cabling, such as cable certifiers for Cat 6 or greater cable. An ESD strap, or, more accurately, antistatic strap, is used to protect components from electrostatic discharge (ESD).

53. **Answer: B.** A switch is a network device that transmits packets it receives to specific connections (ports). It does this by mapping systems' MAC addresses to physical ports on the switch. See Chapter 8, "Network Devices," for more information.

    Incorrect answers: A router converts a packet for transmission from one network to another network. It also determines whether a packet belongs on an internal or an external network, though this process can be augmented by other devices. A hub broadcasts packets it receives to all connections.

54. **Answer: A.** With port flapping, a communication link alternates between on and off states in a short period, causing instability and intermittent connectivity issues. See Chapter 27, "Troubleshooting Wired and Wireless Network Problems," for more information.

    Incorrect answers: High latency means that the typical time for packets to get from the local computer to a remote source is higher than you desire (for example, an average ping of 130 ms instead of 50 ms). Jitter is inconsistent latency and often associated with VoIP. External interference could cause issues with connectivity on a wireless connection (which could appear similar to port flapping if the issue is severe), but the scenario implies a wired connection when it says the system "is connected via an Ethernet cable."

55. **Answer: C.** Unshielded twisted pair (UTP) cable is prone to electromagnetic interference (EMI). See Chapter 13, "Cables and Connectors," for more information.

    Incorrect answers: Fiber optic cable is not prone to EMI because it uses light as the medium instead of electricity. Multimode cable is a type of optical fiber. STP stands for shielded twisted pair, and as the name indicates, it incorporates an aluminum shield around the wires to prevent EMI.

56. **Answer: B.** The best answer listed is to check the video cable connectivity. A loose connection or an older or damaged cable could cause the projected video to flicker. This is especially the case with VGA connections. Use a quality cable and make sure it is properly

secured to the projector and the laptop. See Chapter 25, "Troubleshooting Video Issues," for more information.

Incorrect answers: The power cable wouldn't cause video flicker, but it could cause the projector to randomly shut down if it isn't connected securely. There aren't any projector settings that should produce flicker, so modifying them probably won't help. Changing the aspect ratio is along the lines of changing the resolution (which the scenario says was already performed). For example, a 16:9 aspect ratio is used for HD video (such as a 1920×1080 resolution). A 16:10 aspect ratio (such as 192×1200 resolution) might be used by graphics workstations.

57. **Answer: A.** The most likely listed cause is that the PC to which the printer is connected is currently off the network. It would appear from this scenario that the printer is connected to a PC by way of USB and is shared at the PC itself, which is offline. If the customer can connect to other shares on other PCs, you know that that particular computer is functional on the network. Another possibility in this scenario is that the Share this Printer checkbox in Printer Properties in Windows is unchecked. See Chapter 19, "Multifunction Devices/Printers," for more information.

Note

In this scenario, the user is accessing shared files from another PC. Remember that this is a *shared printer*. That means that the printer is connected to another PC on the network, not directly to the network. The answer "PC is off the network" means the PC that has the printer connected to it.

The key here is that the customer can access shares on other PCs, which indicates that there is an issue with the computer that has the printer connected to it.

Incorrect answers: The printer is on, and restarting a printer can fix some issues, but it will most likely return the printer to the same state

it was in previously. The printer being low on toner should have no effect on whether it can be accessed. But a message would probably appear on one of the computer's screens, stating that the toner cartridge should be changed soon. If device drivers are corrupted, the printer should still be accessible and might print, but it will probably print garbled information.

58. Answer: A. *Embedded systems* are devices that have integrated CPU and RAM and can process information internally without the need for a controlling system. They are commonly found in home appliances, office automation, thin clients, security systems, telecommunications, automotive, medical, assembly systems, and much more. They make up a large percentage of that nutty Internet of Things! See Chapter 6, "Networked Hosts," for more information.

Incorrect answers: Syslog is a protocol that can take logged event information from a router or other network device and send it to a logging server—also known as a *Syslog server*. The *web server* is the server that houses the website of an organization. An *intrusion detection system (IDS)* can determine whether an unauthorized person has attempted to access the network and then alert the system administrator of its findings. Building on this concept, an *intrusion prevention system (IPS)* not only detects unauthorized access to the network but attempts to thwart it, making the admin's job somewhat easier.

59. Answer: C. The functionality that the trainer desires is duplexing, which means printing on both sides of the paper. Some organizations require this (for most print jobs) in their policies related to reducing paper consumption; however, most printers are not set to duplex by default. See Chapter 19, "Multifunction Devices/Printers," for more information.

Incorrect answers: Orientation is the method of positioning a printed page and is based on whether the page is going to be viewed vertically (portrait) or horizontally (landscape). Print quality is the print resolution, which is measured as dots per inch (DPI). A printer that is connected to a Windows PC must first be *shared* before other users at other computers can send print jobs to it. An ADF (automatic

document feeder) is a wonderful contraption that allows you to scan, copy, and fax multiple-page documents without having to feed each page individually. Although this may be an important feature, the trainer should first be concerned about the duplex settings!

60. **Answers: B and C.** The voltages a power supply unit (PSU) typically supplies include 3.3 V, 5 V, and 12 V (as well as their negatives) to components in the computer. See the section "Power Supplies" in Chapter 18, "Power," for more information.

    Incorrect answers: 1.5 is a common voltage for AA and AAA batteries. 9 V is usually associated with batteries used by handheld devices such as power supply testers and multimeters. PSUs do not supply a 9 V rail or a 1.5 V rail.

61. **Answers: A, B, and C.** A common symptom of printer trouble is vertical lines on the page, which would indicate a print drum issue, likely fixed by a toner cartridge replacement or inkjet cartridge calibration. Garbled print can occur due to an incorrect driver. Some technicians like to try "close" drivers. This is not a good idea. Use the exact driver for the exact model of the printer that corresponds to the appropriate version of the operating system. For faded print, replace ink or toner. Clean the ink cartridge head. Also, check the fuser and increase the humidity, if necessary. See Chapter 28, "Troubleshooting Printers," for more information.

    Incorrect answers: Failure to document cable and screw locations and failure to organize parts could make reassembly of a printer or laptop difficult. These failures could possibly even be reasons the printer or laptop fails, but they wouldn't be symptoms of the problem. When troubleshooting, be sure to understand the difference between a symptom of a problem and a cause of a problem. And, of course, think carefully about the best solution to the problem!

62. **Answer: A.** VGA is an older standard that outputs analog signals to a monitor. Of the listed answers, it is the most susceptible to signal degradation. See Chapter 13, "Cables and Connectors," for more information.

Incorrect answers: HDMI, DVI, and DisplayPort are designed to work by sending digital signals and can send them over longer distances than can analog cables (such as VGA). Digital is inherently better in terms of distance and signal quality.

63. Answer: A. The best answer listed is NVMe (Non-Volatile Memory Express)—for example, an M.2 drive. This technology can transfer the most data and provides the highest performance of the listed answers. See Chapter 15, "Storage Drives," for more information.

Incorrect answers: A 15K rpm HDD means a hard disk drive (or magnetic-disk drive) that can revolve 15,000 times per minute. While that is one of the fastest speeds of an HDD, it will be lucky to move one-quarter as much of the data as an NVMe drive. A MicroSD card is meant for mobile devices as a means of secondary storage (for photos, videos, music, and so on); it is not a good candidate for a boot drive. Neither is a USB flash drive, unless you are testing a new operating system or troubleshooting an existing system.

64. Answer: B. The most likely option of the listed answers is that the motherboard was damaged by the power test. This causes a failure to power-on self-test (POST) and causes the fans to function improperly. There was probably some kind of surge or spike of electricity, which could have overloaded the motherboard in a variety of ways. Perhaps a capacitor burst, or maybe one of the circuits burned out. You might be able to repair it, but chances are you will need to replace the motherboard. You should notify your manager or your building facilities department about the issue. Also, to protect systems against this kind of problem in the future, consider upgrading the surge suppressor, installing a new one, or using a line conditioner or an uninterruptible power supply, or UPS (depending on the type of system). See Chapter 23, "Troubleshooting Motherboards, CPUs, RAM, and Power," for more information.

Incorrect answers: If no one opened the computer, then it is unlikely that the RAM was damaged by electrostatic discharge (ESD). Internal components are usually affected by ESD only when someone handles them improperly. You don't know yet, but the storage drive could experience data corruption or be erased due to a power surge. But that

isn't the cause of the problem in the scenario; it is simply another potential result. It's another reason to have good protective power equipment to plug the computer into. If the power supply were damaged and nonfunctional, the fans wouldn't spin at all. However, the power supply might also be partially damaged. You need to do a lot of testing of the computer to make sure it is fully functional before putting it back into its normal work environment.

65. Answer: D. ECC (error correction code) memory can detect and correct common types of data corruption. It is often used in servers. It is not typically installed in desktops but might be used if data corruption cannot be tolerated. It provides for error correction and, therefore, protection while storing data in RAM. See Chapter 14, "RAM," for more information.

Incorrect answers: Quad-channel means that the RAM can send data over four 64-bit channels at the same time—and four sticks of RAM are required to take advantage of that. Parity support in RAM means that the memory can *detect* errors, but it cannot correct them the way ECC does. Dual-channel RAM uses two 64-bit data channels at the same time. RAID 5 is not a memory technology; rather, it is a redundant storage drive array technology. While RAID 5 does use parity, it is not the same type of parity that RAM might use.

Note

You may have heard of *unbuffered memory* and *buffered memory*. While these terms are not in the A+ objectives, as a tech, you should know what they mean: Unbuffered memory is standard RAM that you would install to a typical PC. Buffered memory (also known as registered memory) places less electrical load on the memory controller, making a system that has a lot of sticks of RAM more stable. It is sometimes found in servers.

66. Answer: A. An IP address conflict is a possible cause of the problem. This happens when two computers are assigned the same IP address

(usually when at least one was configured statically). When this happens, the link light on the network adapter will still work as usual because the system has a physical link to a central connecting device such as a switch, and bits (and frames) of data are still being sent back and forth between that computer and that switch. It's the IP layer that is nonfunctional due to the IP conflict. IP conflicts are most common in smaller networks where the clients might use static IP addresses, but they are not common in larger enterprise networks that use DHCP. See Chapter 27, "Troubleshooting Wired and Wireless Network Problems," for more information.

Incorrect answers: Latency is the typical amount of time that it takes for packets of data to travel from one computer to the next. The higher the latency, the worse the experience.

Network congestion can cause *jitter*, which is an irregular time delay in the sending of certain data packets. Jitter is similar to latency, but the delay that is involved is inconsistent; you might call it "inconsistent latency."

Limited connectivity means that a system can connect some of the time. This is different from what you would see with an IP conflict in that the system will have periodic connectivity.

APIPA (Automatic Private IP Addressing) is a type of link-local addressing. The OS gives itself (self-assigns) an IP address, such as an address on the 169.254.0.0 network. If that happens, the system will probably not be able to access network resources. However, this is just a symptom and not a cause of the problem. In a typical network, an APIPA address usually occurs because there is no DHCP server to obtain proper IP addresses from.

Although slow transfer speeds could cause the system to take a while to connect, the system should still connect at some point to internal network resources. You can tell if the system has sent or received data in the current session by going to the network icon in the notification area or by running the **netstat -e** command in the Command Prompt (in Windows); this shows packets that were transceived (that is, transmitted and received).

67. **Answer: C.** The most likely cause is a memory failure. Two beeps often means a problem with memory. Of course, this depends on the type of BIOS or UEFI. For example, two beeps in some Dell systems means that no memory has been detected, causing a RAM failure. Two short beeps in AMI BIOS systems means a memory parity error. See Chapter 23, "Troubleshooting Motherboards, CPUs, RAM, and Power," for more information.

    Incorrect answers: If the power supply were to fail, the system wouldn't even POST because the motherboard doesn't receive power. If the video adapter failed, you would get a different set of beeps. For example, in Award/Phoenix Technologies BIOS systems, one long and two short beeps (or three short beeps) means some kind of video error. In some Dell systems, six beeps means a video card failure. Read the motherboard documentation to find out what the beep codes mean. If the CPU fails, the system will not boot or go through the power-on self-test (POST).

68. **Answer: B.** You need to check whether the CPU has virtualization support enabled in the UEFI/BIOS. If it is not enabled, Windows will not allow the installation of Hyper-V to continue. You may receive an error message, or Windows might simply have a grayed out area where you want to select Hyper-V in Programs and Features. See Chapter 16, "Motherboards and Add-on Cards," and Chapter 21, "Virtualization Concepts," for more information.

    Incorrect answers: The number of cores, hyper-threading, and cache size will not cause an error in Windows. However, you should make sure that the system meets the minimum requirements to run Hyper-V. In most cases, if a system can run Windows, then it *should* be able to run Hyper-V. According to Microsoft, the general requirements to run Hyper-V are a 64-bit processor with second-level address translation (SLAT), at least 4 GB RAM (though more is better!), and virtualization support turned on in the UEFI/BIOS.

69. **Answers: A and E.** The scenario most likely is depicting an overheating issue. This is causing the lamp to turn off periodically until the projector cools down. Perhaps the cooling fan failed and needs to be replaced. The message that appears is most likely about

resetting the lamp life counter to zero because the system "sees" that a new lamp was involved. See Chapter 25, "Troubleshooting Video Issues," for more information.

Incorrect answers: Because this is most likely an overheating issue (which is common), changing the resolution or brightness won't help. Neither will updating the laptop's video driver. The scenario doesn't even mention what kind of system is being used, but it is *usually* a laptop (or another mobile device). A more powerful lamp might not even work in the projector and would probably worsen the problem because it would require more power and therefore create more heat.

70. Answer: A. Supervisory control and data acquisition (SCADA) systems are found in electrical power grids, water treatment plants, gas/oil pipelines, hydroelectric systems, sewage systems, traffic systems, building controls, and so on. Compared to typical home offices/small offices, SCADA solutions must be heavily secured because they are often used in protected environments and infrastructures. See Chapter 6, "Networked Hosts," for more information.

Incorrect answers: A router is a device that allows access from one network to another. A load balancer is a hardware or software solution that monitors the servers in question and routes client requests to servers in a uniform fashion, making sure that no servers are overloaded and that no servers are idle. A spam gateway is a software solution that is either incorporated into an email server or installed as a virtual appliance—generally, just behind an organization's firewall to protect the network to a certain extent from spam email.

71. Answer: A. Thunderbolt is the only answer listed that can be used for audio, video, and storage. See Chapter 13, "Cables and Connectors," for more information.

Incorrect answers: DisplayPort and HDMI can transfer audio and video data but are not used for storage. DVI is used for video only.

72. Answer: E. RAID 10 combines the advantages of RAID 1 and RAID 0. It requires a minimum of four or more disks. The system contains

at least two mirrored disks that are then striped; it is also known as a "stripe of mirrors." See Chapter 15, "Storage Drives," for more information.

Incorrect answers: RAID 0 is striping. It is not fault tolerant and does not incorporate mirroring. RAID 1 is mirroring and does not use striping the way RAID 10 does. RAID 5 is striping with parity. Data is striped across multiple disks. RAID 6, a double-parity RAID level, offers enhanced data protection by tolerating up to two drive failures, using block-level striping with two parity blocks distributed across all member disks, requiring a minimum of four drives. It does not include mirroring the way RAID 10 does.

73. **Answer: D.** SMB (Server Message Block) can be used to facilitate file sharing between Windows computers and computers running macOS. It is sometimes referred to by its older name, CIFS (Common Internet File System). See Chapter 4, "TCP and UDP Ports and Protocols," for more information.

    Incorrect answers: RDP (Remote Desktop Protocol) is used to view or take control of remote computers from a central workstation. SSH (Secure Shell) is a protocol used to make secure connections to other systems; it replaces protocols such as Telnet. POP3 (Post Office Protocol version 3) is used for downloading email. For the A+ exam, you should remember that SMB/CIFS uses port 445, RDP uses port 3389, SSH uses port 22, Telnet uses port 23, and POP3 uses port 110. Remember your port numbers!

74. **Answer: D.** You should run plenum-rated cable, which has a special outer covering that will not burn (or will not burn as quickly as other cable) in a fire. It should be used in areas that cannot be accessed by a fire suppression system. (In some cases, it needs to be used throughout a municipal installation.) See Chapter 13, "Cables and Connectors," for more information.

    Incorrect answers: Shielded cable (for example, shielded twisted pair, or STP) is used to reduce electromagnetic interference (EMI). It does not meet fire code for plenum areas. Unless specified as plenum-rated, coaxial cable will not work, especially because you are

running a network cable (which implies twisted pair cable). Fiber optic cable is a high-speed cable but by default is not rated for plenums.

75. **Answer: C.** Of the listed answers, the most likely problem is that the storage drive has not been partitioned correctly. In this scenario, the point of the preinstallation environment (PE)—which is often located on removable media such as a USB flash drive or boot disc—is to boot the system and partition the storage drive, readying it for the image to be obtained over the network. If the drive is not partitioned properly, the process will fail because the image will expect to be installed to a specific partition. See Chapter 24, "Troubleshooting Storage Drives and RAID Arrays," for more information.

> **Note**
>
> In some scenarios, a drive can be fully unpartitioned, and you can have the image install properly. This depends on several factors, including the local system hardware, what type of network installation is being done, and what software is being used for the imaging process.

Incorrect answers: Storage drives don't vary much from one to the next in regard to power, so the power supply should provide plenty of power. If it didn't, you wouldn't see the drive in the UEFI/BIOS. The boot media has not failed; the scenario says that you have accessed the preinstallation environment, and that is only possible if the PE boot media was booted to successfully. Today, it is uncommon for a drive to be configured in the BIOS or UEFI (unless it is part of a RAID array, which is controlled by the motherboard). Normally, the drive is either seen or not. If not, you might need to perform a flash of the BIOS or UEFI.

76. **Answer: B.** A proxy server provides the services needed for multiple clients to access Internet web pages. It is a server that is normally located on the LAN, or the internal computer network, and as such is

known as a LAN host or a network host. See Chapter 6, "Networked Hosts," for more information.

Incorrect answers: A web server does provide web pages, but the web server is not normally on the LAN. Web servers normally exist on the Internet, on an intranet, or in a DMZ or screened subnet, so they cannot be considered network hosts or LAN hosts. File servers simply store files for multiple clients to access; Word documents and Excel spreadsheets are examples. A DNS server is used to resolve hosts' domain names to their corresponding IP addresses. They are very common on the Internet, though they can exist on a LAN as well. However, they don't deal with *cached* web pages the way that a proxy server does.

77. **Answer: C.** With metered services, an organization has access to virtually unlimited resources but pays only for the resources that are used. This is also known as metered utilization. See Chapter 22, "Cloud Computing Concepts," for more information.

    Incorrect answers: With rapid elasticity, a provider offers a scalable cloud-based network that can grow as the organization needs it to. On-demand is the ability for customers to gain access to resources 24 hours a day, 7 days a week. A community cloud is a mix of public and private where multiple organizations can share the public portion. High availability (HA) means the cloud should be available in real time and whenever needed (24/7); it should be "always on."

78. **Answer: D.** You should first check the power cable connection. Remember to check the simple stuff first! If there are no signs of life from the computer at all, then it's most likely a power problem. Make sure the cable is connected securely to the PSU and to the AC outlet. See Chapter 18, "Power," for more information.

    Incorrect answers: Checking the voltage of the PSU means opening the system. Try to avoid doing that until after you have checked the obvious and easy things first. Also, while you can use a multimeter, consider using a proper PSU tester. Checking for capacitor issues on the motherboard shouldn't be necessary in this scenario. However, distended capacitors—physically bulged or swollen—are common on

motherboards and should be checked. If the PSU has a voltage switch, it is something that you could check (after checking the power cable). However, it should not have been changed if the system was moved within the office.

79. **Answers: B, H, I, and J.** In this scenario, the screened subnet/DMZ needs to have several inbound ports open to the servers. To do this in a secure way, one possibility would be to use SFTP on port 22, HTTPS on port 443, SMTP on port 587 (for outbound mail), and POP3 on port 995 (for inbound mail). That would meet the requirements for the secure FTP server, web server, and mail server. Besides SFTP—which rides on Secure Shell (SSH)—the rest of the secure solutions use SSL/TLS by default. See Chapter 4, "TCP and UDP Ports and Protocols," for more information.

    Incorrect answers: While you can use any port and secure it with the appropriate protocols, there are default security port numbers that you will usually work with. For example, when configuring FTP, you use SFTP (port 22) or FTPS (ports 989/990) but not port 21, which is used with standard FTP. As for the rest of the incorrect answers, port 23 is used with Telnet (which is considered insecure). Port 53 is used by DNS, which can be secured in a variety of ways, but the scenario does not require a DNS server. Port 80 is HTTP (which is insecure and rarely seen today). Port 110 is POP3 without security. Port 143 is IMAP without security. Port 3389 is used by Remote Desktop Protocol (RDP). By the way, you probably won't get a question with 11 possible answers, but we are just trying to stress that you should know your ports and protocols!

80. **Answer: A.** You need to adjust the Secure Boot setting. Secure Boot uses encryption in conjunction with operating systems such as Windows to make sure that only a particular operating system will boot. Secure Boot blocks devices from booting from external media such as bootable USB sticks or optical discs. In this scenario, to boot off the flash drive, you not only need to change the UEFI/BIOS boot order but most likely also need to disable Secure Boot. See Chapter 16, "Motherboards and Add-on Cards," for more information.

Incorrect answers: TPM, which stands for Trusted Platform Module (and is located on the motherboard), is used to encrypt an entire storage drive. The UEFI/BIOS password most likely refers to the administrator password of the UEFI/BIOS. See Chapter 16, "Motherboards and Add-on Cards," for more information. You already knew this password; otherwise, you would not have been able to modify the boot order. Virtualization refers to the ability for the CPU to work with virtual machine software (such as Windows Hyper-V). It has to be enabled for Hyper-V and other virtualization machine managers to work properly.

81. Answer: C. Wi-Fi 6E is the first Wi-Fi standard to extend Wi-Fi 6 (802.11ax) capabilities into the 6 GHz frequency band. This new band adds more spectrum and reduces congestion from older devices operating on the 2.4 GHz and 5 GHz bands. Wi-Fi 6 (without the E) only supports 2.4 GHz and 5 GHz. Wi-Fi 5 (802.11ac) supports 5 GHz only. Wi-Fi 7 (802.11be) also uses the 6 GHz band, but it was introduced after Wi-Fi 6E. See Chapter 5, "Wireless Technologies," for more information.

Incorrect answers: Wi-Fi 5, also known as 802.11ac, operates exclusively in the 5 GHz frequency band. While it provided higher throughput than previous generations, it does not support the 6 GHz band and predates the introduction of Wi-Fi 6 technology. Wi-Fi 6 (802.11ax) does improve network efficiency and performance using technologies like OFDMA and MU-MIMO, but it is still limited to the 2.4 GHz and 5 GHz bands; it does not extend into 6 GHz. Wi-Fi 7, also referred to as 802.11be, does support the 6 GHz band and introduces enhancements like multilink operation and higher data rates. However, it was introduced after Wi-Fi 6E and is not the first standard to leverage the 6 GHz spectrum.

82. Answer: A. NTP ensures timestamp accuracy for security policies and log correlation across systems. NTP's main role is to synchronize the clocks of devices across a network. Accurate timekeeping is crucial for maintaining consistent logs, coordinating time-based authentication, and ensuring secure operations. See Chapter 6, "Networked Hosts," for more information.

Incorrect answers: Firewall rules do not automatically adjust based on time-sensitive threat levels through NTP. While some firewalls support time-based rules, it is the firewall software—not NTP—that controls this behavior. NTP's role is limited to providing accurate time. Software updates and rollouts are typically coordinated by patch management or systems management tools, not by NTP. While synchronized time can help ensure updates occur uniformly, NTP itself does not handle update scheduling. Time-based access control policies rely on accurate clocks, but enforcing those access controls is the responsibility of authentication or policy management systems—not NTP. NTP simply ensures the time reference is correct across devices.

83. Answer: B. Multitenancy enables multiple customers to share the same physical resources while maintaining secure data isolation. It is a foundational concept in cloud computing where a single instance of the infrastructure (servers, storage, network) supports multiple customers (tenants). This shared environment optimizes resource utilization, improves scalability, and lowers costs for providers. Each tenant's data and operations remain securely isolated, despite being on shared hardware. See Chapter 22, "Cloud Computing Concepts," for more information.

Incorrect answers: Assigning each customer a dedicated virtual server increases isolation but defeats the purpose of multitenancy, which is about shared infrastructure. Consolidating all client data into a single database poses serious security risks and contradicts the principle of data isolation. Routing each tenant's traffic through separate physical interfaces is inefficient and unnecessary; cloud providers typically use virtual network segmentation to ensure secure traffic flow without duplicating hardware.

84. Answer: A. A "RAID Array Not Found" error after POST is a common sign that the RAID configuration is missing, disabled, or corrupted. The most likely cause is that RAID was disabled or reset in the BIOS, such as when a technician flashes or resets the BIOS, causing the SATA mode to revert from RAID to AHCI. This prevents the RAID utility from loading at boot and causes the system to see

the drives as individual, nonbootable disks. See Chapter 24, "Troubleshooting Storage Drives and RAID Arrays," for more information.

Incorrect answers: Reformatting a single drive in a RAID 0 array would result in data loss, but it would not typically trigger a "RAID Array Not Found" error. The array would still be detected, though broken. Ransomware rarely deletes RAID configurations; it typically encrypts data, and such an attack would be accompanied by ransom notes or encryption warnings, not hardware-related boot errors. The Windows Disk Management utility cannot control boot order at the hardware level and does not affect whether a RAID array is detected during POST, making it irrelevant to this specific startup error.

85. **Answer: C.** On high-resolution monitors like 4K displays, text and icons may appear too small due to the high pixel density. Adjusting the display scaling percentage in the operating system enlarges UI elements without lowering the resolution, ensuring content remains sharp and properly proportioned. See Chapter 25, "Troubleshooting Video Issues," for more information.

    Incorrect answers: Decreasing the refresh rate in the monitor's OSD affects how often the image is redrawn but has no impact on the size of text or icons. Changing the color depth to 16-bit reduces image quality and color range but does not affect the scaling or size of on-screen elements. Lowering the resolution to 1024×768 would enlarge text and icons but significantly degrade image clarity and make poor use of a 4K display's capabilities, resulting in a blurry and stretched appearance.

86. **Answer: C.** Closing background apps is the recommended first step when troubleshooting degraded performance, as it quickly frees up system memory and reduces CPU load. While updating apps, clearing cache, or performing a factory reset may help in some cases, those steps are generally secondary or more drastic. Start with the least invasive option that targets common causes of slowdowns. See Chapter 26, "Troubleshooting Mobile Devices," for more information.

Incorrect answers: Updating all apps to the latest versions can improve performance over time, but it's not the most immediate or targeted fix for a slow device and may even increase background activity during the update process. Performing a factory reset is a last-resort solution that erases all data and settings; it's far too drastic as an initial step. Clearing the system cache partition can help in some cases, particularly after system updates, but it's a more advanced step and less commonly needed than simply closing background apps, which directly addresses RAM and CPU usage.

87. **Answer: D.** Authentication failures may be due to server availability issues or account status (locked or disabled). These should be the first things checked when a user reports login issues, especially if they're sure the credentials are correct. See Chapter 27, "Troubleshooting Wired and Wireless Network Problems," for more information.

    Incorrect answers: Checking whether the user's password has expired may be helpful, but if the account is locked or the authentication server is unreachable, the login would still fail even with a valid password. Investigating malware infections or outdated antivirus definitions is important for overall system health but unlikely to cause an immediate domain authentication failure. These steps are more appropriate after confirming that the server and account status are not the root cause.

88. **Answer: D.** When jobs are stuck and cannot be cleared through the interface, the most effective way to reset the queue is to stop and restart the print spooler service. This also allows the technician to clear the spool folder and remove any corrupted jobs. See Chapter 28, "Troubleshooting Printers," for more information.

    Incorrect answers: Rebooting the printer and computer may sometimes resolve basic communication issues, but it often does not clear a stuck print queue caused by a malfunctioning spooler. Changing the printer's default paper tray addresses paper selection problems, not job processing or queue-related issues. Lowering the printer's print quality setting may help with speed or print clarity but has no effect on clearing or releasing stalled print jobs in the queue.

89. **Answer: A.** DHCP exclusions are used to reserve specific IP addresses *within* the DHCP scope so that they are *not* handed out dynamically. This prevents conflicts with devices that are assigned static IPs manually, like servers, printers, or firewalls.

    Incorrect answers: Preventing DHCP servers from responding to unauthorized MAC addresses is a security function typically handled by MAC filtering or network access control (NAC), not DHCP exclusions. Blocking specific clients from obtaining any IP address requires access control measures or DHCP deny lists—not exclusions, which are used to reserve unused addresses. Permanently assigning the same IP address to a client based on its MAC address is called a DHCP reservation, not an exclusion. While both exclusions and reservations operate within the DHCP scope, they serve different purposes. See Chapter 7, "Network Configuration Concepts," for more information.

A Final Word About the 220-1201 Exam

After taking this practice exam, if you are unsure or unconfident in any way, we urge you to step back and continue studying the 220-1201 objectives before attempting the real exam. And don't forget, if you purchased the print version of this book, you have a bonus practice exam waiting for you on the companion website (as well as other bonus materials). See the Introduction of this book for details. For even more practice questions, check out the A+ Exam Cram *Practice Questions* book.

Be ready for anything! We can't tell you *exactly* what will be on the exam because that would violate the CompTIA NDA and, more importantly, the questions can change at any time! But the bottom line is this: If you know the concepts, you can pass any test. Use the official CompTIA A+ objectives as your guide. Review this book thoroughly. Finally, we challenge you to study in a hands-on manner on real computers and investigate all the concepts to the best of your ability. This will help you not only for the exam but also for the real world!

Part II

Introduction to Core 2 (220-1202)

Welcome to the Core 2 (220-1202) section of this book. This portion of the CompTIA A+ certification focuses on operating systems, computer and network security, software troubleshooting, and operational procedures. Sound like a lot? It is—but you can do it. Study hard, stay confident, and you will prevail.

The Core 2 content of this book comprises Chapters 29 through 65. For the most part, we've written the content to match the order of the objectives. This way, you can follow along with the official CompTIA A+ objectives and mark them up as you wish while you progress through the book. After Chapter 65, you will find a practice exam that is designed to test your knowledge of the 220-1202 objectives.

Core 2 (220-1202) Domains

The CompTIA A+ Core 2 exam objectives are broken down into four domains:

- 1.0—Operating Systems
- 2.0—Security
- 3.0—Software Troubleshooting
- 4.0—Operational Procedures

After this introduction, we'll address these objectives in order, starting with Chapter 29, "Common Operating Systems." Be sure to study each of the domains! To do so effectively, we recommend studying in a hands-on

manner. If at all possible, get your hands on some operating systems such as Windows, Linux, macOS, Chrome OS, Android, iPadOS, and iOS. Work with as many of these systems as possible so that you can learn how the software really works. Then apply that knowledge to the objectives and the content in this book.

Core 2 (220-1202) Checklist

You must be fully prepared for the exam, so we created a checklist that you can use to make sure you are covering all the bases as you study. Take a look at the following table and make sure you check off each item before attempting the 220-1202 exam. Historically, our readers and students have benefited greatly from this type of checklist. Use the table as a guide for ordering your studies. We suggest you bookmark this page and refer to it as you complete each item.

Exam Preparation Checklist

Step	Item	Details	220-1202 Status
1.	Read the Core 2 (220-1202) content.	Thoroughly read through Chapters 29 through 65.	
2.	Review the Exam Alerts.	The little boxes with Exam Alerts are interspersed throughout the book. Review them and make sure you understand every one.	
3.	Review the Cram Quizzes.	Cram Quizzes are categorized by exam. You can review them in the text or on the companion website.*	

Step	Item	Details	220-1202 Status
4.	Complete the practice exam in the book.	Directly after Chapter 65 is a 220-1201 practice exam. Your goal should be to get at least 90 percent correct on the exam on the first try. (100 percent would be preferable!) If you score less than 90 percent, go back and study more!	
5.	Study the Core 2 Real-World Scenarios.	These can be found on the companion website. Complete them by reading and answering the scenarios and questions within the PDFs and accessing the corresponding videos and simulations.	
6.	Create your own cheat sheet.	Although there is a Cram Sheet in the beginning of this book, you should also create your own. The act of writing down important details helps commit them to memory. Keep in mind that you will not be allowed to take your own cheat sheet or the Cram Sheet into the actual testing room.	
7.	Register for the exam.	Do not register until you have completed the previous steps; you shouldn't register until you are fully prepared. When you are ready, schedule the exam to commence within a couple of days so that you won't forget what you have learned! Registration can be done online. Register at Pearson Vue (https://home.pearsonvue.com/). It accepts payment by major credit cards for the exam fee. You need to create an account to sign up for exams.	
8.	Read the test-taking tips.	You can find these tips in the last chapter of the book and on the companion website.	

Step	Item	Details	220-1202 Status
9.	Study the Cram Sheet and cheat sheet.	The Cram Sheet is a fold-out in the beginning of this book. It is also on the companion website. Study from the Core 2 portion of the Cram Sheet and your cheat sheet during the last 24 hours before the exam. (If your exam is delayed for any reason, go back to step 3 and retake the Cram Quizzes and practice exam 24 hours prior to your test date.)	
10.	Take the exam!	When you pass, place that final check mark in the box! Good luck!	

* Some electronic editions do not have access to the practice test software.

ExamAlert

Do not register for the exam until you are thoroughly prepared. Meticulously complete items 1 through 6 in the checklist before you register.

Core 2 (220-1202)

Domain 1.0: Operating Systems

CHAPTER 29 Common Operating Systems

CHAPTER 30 Operating System Installations and Upgrades

CHAPTER 31 Basic Features of Windows Editions

CHAPTER 32 Microsoft Operating System Features and Tools, Part I

CHAPTER 33 Microsoft Operating System Features and Tools, Part II

CHAPTER 34 Microsoft Command-Line Tools, Part I

CHAPTER 35 Microsoft Command-Line Tools, Part II

CHAPTER 36 Windows Control Panel Utilities

CHAPTER 37 Windows Settings

CHAPTER 38 Windows Networking

CHAPTER 39 macOS

CHAPTER 40 Linux

CHAPTER 41 Application Installation and Configuration Concepts

CHAPTER 42 Cloud-Based Productivity Tools

Chapter 29

Common Operating Systems

This chapter covers the following A+ 220-1202 exam objective:

- **1.1** – Explain common operating system (OS) types and their purposes.

Welcome to the first chapter of the 220-1202 section of this book. Until now, we have been talking about hardware for the most part. But without software, hardware is fairly useless. So now we'll dig into the software side of things.

What type of operating system do you run at home? What do you run at work? What do other people you know use? Think about these questions for a moment. The answers usually depend on the type of computer a person has: desktop, laptop, handheld, and so on. They also depend on a person's preference, or a company's preference. Often, the choice is based on *need*. Always consider what kind of work a user needs to perform. The answer will, in part, dictate what type of operating system—and ultimately the type of computer—a user requires. Let's discuss the most common operating systems now.

ExamAlert

Objective 1.1 focuses on workstation operating systems, mobile operating systems, various file system types, vendor life-cycle limitations, and compatibility concerns between operating systems.

Workstation Operating Systems

Workstation operating systems include Microsoft Windows, Apple macOS, Linux, and Chrome OS. In this case, *workstation* means a desktop or laptop computer that a user sits at to perform work—so we are not including servers in this section.

ExamAlert

Remember that Exam Objective 1.1 lists workstation systems (OSs) as Windows, Linux, macOS, and Chrome OS. So, you will likely need to know how they function.

By far the most common workstation OS in the workplace is Microsoft Windows, so Windows is the main focus of the rest of this book. For the exam, you need to be able to work with Windows 11, but be ready for other versions, both older and newer, in the field! The A+ exam objectives in 1202 1.3 (see Chapter 31, "Basic Features of Windows Editions") even cover Window 10 Pro for Workstations—designed for high-end hardware being used for intensive computing tasks, but otherwise not commonly seen in regular use. The good thing about different Windows versions is that they are quite similar architecturally and from a user standpoint. Most of the built-in programs work in the same manner, though the names and navigation might be slightly different. Also, the command line hasn't changed too much in the past 10 years; even with the migration to PowerShell, basic commands remain the same. Most of the exam questions you will come upon and most of the Windows problems you will face can be approached in the same manner, regardless of the *version* of Windows.

Next on the list is macOS, previously known as OS X. It is the proprietary operating system used by Apple for its Macintosh desktop computers and MacBook Pro and Air laptop computers. This operating system (and the Mac computer in general) has been a favorite of multimedia designers, developers, graphic artists, and musicians since the 1990s. macOS has used version numbers since its inception, such as macOS 10.14 (codenamed Mojave) and version 12 (Monterey). Apple used the name OS X through version 10.11 (El Capitan) but changed to the name macOS at version 10.12 (Sierra). The latest version of macOS as of this writing is macOS 15, code named Sequoia, released in September 2024.

Although some Macintosh computers may have Intel processors, they are not PCs. Likewise, macOS is not always compatible with PC add-on hardware. Conversely, PC-based operating systems, such as Windows and Linux, do not normally run on Macintosh computers—though it can be done in the case of Windows (for example, with Boot Camp, as described in Chapter 39, "macOS").

Note

macOS can be run in a Windows virtual machine such as VirtualBox or VMWare by downloading and installing a macOS image and installing it into the virtual machine. However, some compatibility issues can come into play, and they may require some additional technical knowledge. Plus, macOS may not run perfectly within the virtual environment.

Linux is an ever-expanding group of operating systems that are designed to run on PCs, servers, gaming consoles, DVRs, mobile phones, IoT devices, and many other devices. Originally, Linux was designed as an alternative operating system to Windows; however, it has been estimated that no more than 4.5 percent of the US market uses Linux on PCs (though it is likely higher, since much of the 4.5 percent "unknown" category in the survey is likely Linux as well). Compare that to Windows at approximately 73 percent, and macOS at 15 percent. Linux does, however, have a much larger market share when it comes to servers, penetration-testing laptops, embedded systems, IoT appliances, and other computer devices,

and in those markets, the percentage is growing rapidly. Linux was originally written by Linus Torvalds (thus the name) and can be freely downloaded by anyone. Several organizations and companies emerged and developed this free code (or a variant of the free code) into their own versions of Linux, which are referred to as *distributions* (often abbreviated as *distros*). Some examples of Linux distributions include Red Hat, Fedora, Debian, Ubuntu, and Kali, each of which uses its own version number scheme. Although Linux is free to download, it is licensed under a General Public License (GPL), which states that derived works can be distributed only under the same license terms as the software itself.

The Chrome operating system (Chrome OS) is designed by Google to act as a workstation that uses mostly web-based applications. Chrome OS can run on a variety of devices but is best known for being loaded on Chromebooks, which are a favorite among schools and some home users. While Chrome OS is based on Android, and ultimately based on Linux, and it can access many apps from the Google Play Store, it is still considered to be a separate operating system because it has been so heavily modified to work with Chromebook hardware. However, Chrome OS is designed in such a way that users could accomplish everything they need to do from within the Chrome browser.

Chrome OS is designed to be used online, with the web browser providing access not just to web browsing but also to online productivity applications such as Google Workspace (Docs, Drive, Gmail, and so on) and Microsoft 365, but also streaming media, online photo editing, video conferencing, and any other tasks that can be done in a lightweight, browser-based environment. Because Google controls the Chrome OS ecosystem and it is browser-based, it can be kept lightweight and relatively secure, and management is streamlined for individuals who have less-intensive computing needs.

Note

If you have access to Windows, macOS, Linux, and Chrome OS, we recommend that you attempt to locate the following for each: Settings, the command line, and the built-in Internet browser. This will get you started on your way to becoming familiar with each interface. Quick tip: The Chrome OS command line (called Crosh) is not important for the exam, but you can access it by pressing Ctrl+Alt+T, which launches the Terminal in a new browser tab.

ExamAlert

Chrome OS is browser-centric. Users are in the browser the majority of the time (most users are in the browser all of the time, in fact). They will use productivity applications such as Google Workspace (Gmail, Drive, Docs, and so on), streaming media, basic online photo editing, video conferencing, and other cloud-based tasks. It is ideal for users who rely primarily on online applications and require a lightweight, online-centric, secure operating system. Students, individuals with basic computing needs, and those with basic computing skills are the main targets of Chrome OS devices.

Mobile Operating Systems

The world of mobile device operating systems consists of four main players: Android, iOS/iPadOS, Chrome OS, and Windows. But when it comes to actual smartphones and tablets, Android and iOS/iPadOS are the primary players. So, we'll focus on them in this section.

Mobile device software comes in one of two forms: open source, which is effectively free to download and modify, and closed source, otherwise known as commercial or vendor-specific, which cannot be modified without express permission and licensing. There are benefits and drawbacks to each type of system. Because you will see both in the field, you should know each one equally. Let's consider examples of these types, using Android and iOS.

ExamAlert

Exam Objective 1.1 specifically lists mobile OSs as iPadOS, iOS, and Android. Know them well for the exam!

Android

Android is an example of open-source software. It is a Linux-based operating system used mostly on smartphones and tablet computers and is developed by the Open Handset Alliance, a group directed by Google. Google releases Android 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. You know you are dealing with the Android open-source OS and related applications when you see the little robot caricature, usually in green.

Android versions were referred to by such sweet names as Lollipop, Marshmallow, Nougat, Oreo, and Pie (versions 5 through 9, respectively), until version 10, when the delectables were discontinued. To find out what version you are currently running, start at the Home screen, which is the main screen that boots up by default. Access the Settings screen (often by swiping down from the top and clicking the Settings gear). Locate the About page (within General or a similar section) and tap it. The version should be listed there.

Suppose a company wants to create a custom version of Android for a handheld computer that it is developing. According to the license, the company would be allowed to do this and customize the OS to its specific hardware and applications. This is exactly what smartphone manufacturers do, and it's what differentiates those devices' software packages from each other. Such companies all design their own types of launcher software. The launcher is the part of the graphical user interface (GUI) in Android where a user can customize the Home screen.

Manufacturers of Android-based devices (as well as the general public) can create their own applications for Android as well. To do this, a developer needs to download the Android

application package (APK), which is a package file format used by Android for distribution and installation of application software and middleware.

iOS

Apple's iOS is an example of closed-source software. It is found on iPhones and older iPads. To learn what version of iOS you are running, go to the Home screen and then tap **Settings**. Tap **General** and then tap **About**. You'll see the version number. For example, if you saw Version 11.3.1 (15E302), then 11 is the version, .3.1 is the point release, and 15E302 is the build number.

Unlike Android, iOS is not open source and is not available for download to developers. Only Apple hardware uses this operating system. This is an example of vendor-specific software. However, if developers want to create an application for iOS, they can download the iOS software development kit (SDK). Apple license fees are required when a developer is ready to go live with an application.

iPadOS

iPadOS is a variant of iOS developed specifically for iPad tablet computers. iPads previously used the iOS operating system through version 12; however, at version 13, iPads starting using iPadOS.

iPadOS has a different design and orientation than iOS, taking advantage of the additional real estate of a tablet compared to a smartphone. A user can open more than one instance of an application and can take advantage of additional multitasking that might not be available on iOS. With iPadOS, you can also use an iPad as a secondary monitor/drawing tablet when connected to a macOS system.

Keep in mind that there are many similarities between iPadOS and iOS, including the fact that iPadOS is closed source (but with open-source components).

ExamAlert

Understand the difference between open source and closed source. Open-source software and code like Linux and Android are available to the public, whereas closed-source software and code like Windows, macOS, iOS, and iPadOS are restricted and proprietary.

Note

What about Chrome OS? Is Chrome OS open or closed source? The answer is "partially both." The Chrome OS includes added features that are not part of open-source Chromium OS, making it partially proprietary or closed source.

Note

Detailed use of Android, iOS, iPadOS, or Chrome OS is beyond the scope of this book. This knowledge is considered a prerequisite for the CompTIA A+ exams. We do cover mobile OS troubleshooting later in the book, but if you are new to Android, iOS, iPadOS, or Chrome OS, consider getting your hands on a device or two and practicing with the operating systems!

File System Types and Formatting

In Chapter 15, "Storage Drives," you learned about the types of storage drives. All of your data and the operating system itself will be stored on these drives, regardless of whether the drive is mechanical or solid state or what type of interface it uses to connect to your device.

Before you can use a drive, you must partition it, which we will discuss in Chapter 30, "Operating System Installations and Upgrades." Once the drive is partitioned, it must be formatted to accept your data, and there are some choices to be made about how to format each partition on the drive; each formatted partition is referred to as a *file system*. That is the focus of this section.

Windows File System Basics

Chapter 30 covers partitioning drives in more detail. You learned about RAID drives in Chapter 15, where we discussed the different RAID configurations. Once you have made the decision about the RAID configuration for your drive(s) and have decided on how to partition your drive(s), you will be ready to decide on how to format the drive(s).

When formatting a storage drive in a Windows environment, you have the option to format it as NTFS (recommended), FAT32, or FAT. NTFS is a more secure and stable platform and can support larger volume sizes. It also supports encryption with the Encrypting File System (EFS) and works better with backups. FAT32 and FAT should be used only to interact with older versions of Windows and to format devices such as USB flash drives. Depending on the cluster size used, NTFS can support partitions up to 16 TB (4 KB clusters) or 256 TB (64 KB clusters), but some systems are 2 TB due to the limitations of partition tables on older MBR-based drives. This hardware limitation applies to maximum FAT32 partition sizes of 2 TB as well (aside from the installation maximum of 32 GB). To go beyond this, you would have to use a set of striped or spanned dynamic drives, creating a multidrive volume.

Resilient File System (ReFS) is the newest file system from Microsoft, designed for scale and data integrity. It is designed to eventually replace NTFS and overcome problems that were not anticipated when NTFS was created, specifically surrounding the drive size, data integrity, and virtualization.

Key advantages of ReFS include integrity and data scrubbing checks being done automatically, eliminating the need for tools such as chkdsk (see Chapter 34, "Microsoft Command-Line Tools, Part I," for details about that tool, which will still be useful until ReFS

becomes standard). ReFS can easily handle very large files up to 35 petabytes (PB), with checksums stored independently to help ensure reliability of the stored data. Drives can be up to 35 petabytes in size (up from 256 terabytes [TB] in NTFS), with additional tools to support scalability for large data sets and virtualization. Because ReFS is still relatively new, you will likely only see it in enterprise deployments, specifically Azure servers using Storage Spaces; however, it will likely be deployed more widely as time goes on, so knowing the basics now will be helpful in your career.

Another file system introduced by Microsoft, called the Extended File Allocation Table (exFAT), is suited specifically for USB flash drives but addresses the needs of many other mobile storage solutions. The successor to FAT32, it can handle large file sizes and can format media that is larger than 32 GB with a single partition. In fact, exFAT (also colloquially known as FAT64) has a recommended maximum of 512 TB for partitions, with a theoretical maximum of 64 ZB (zettabytes). The file size limit when using exFAT is 16 EB (exabytes). This file system can be used in many versions of Windows, and is seamlessly interoperable with Linux, macOS, and Chrome OS devices as well. If NTFS and ReFS are not plausible solutions and the partition size needed is larger than 32 GB, exFAT might be the best option; for external solid-state drives such as USB flash drives, exFAT is your best option.

As of the writing of this book, exFAT is generally not used for internal storage drives; it is used for flash memory storage and other external storage devices. exFAT is considered to be a more efficient file system than NTFS when it comes to flash memory storage; it experiences less fragmentation, leading to more possible read/write cycles over the life of the flash memory device. Figure 29.1 shows how to configure formatting of a flash drive for exFAT.

ExamAlert

Know the differences between NTFS, ReFS, FAT32, and exFAT. Remember that NTFS is the default file system used by Windows and allows for file-level security assigned by a user or group. exFAT is suited specifically for USB flash drives but addresses the needs of many other mobile storage solutions. The successor to FAT32, it can handle large file sizes and can format media that is larger than 32 GB with a single partition.

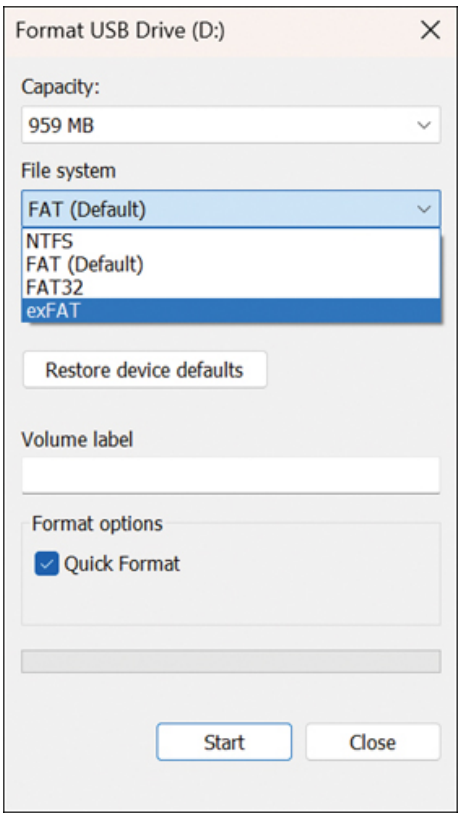


FIGURE 29.1 **Formatting a Flash Drive Using exFAT**

Regardless of the file system used, in Windows, you can opt for a quick format or a full format (which is also known as a *normal format*). In Windows, a quick format removes *access* to files on the partition or drive; a full format writes zeros to the entire partition and also scans the partition or drive for bad sectors, which can be quite time-consuming. Generally, technicians should avoid the full format. However, if a drive is brand new and has never been formatted, or if a drive has been acquired from another source and you are concerned with its integrity, you should consider running a full format. But be careful with full formats because they put a lot of stress on the drive, which can reduce its lifespan, especially in the case of magnetic-based hard drives. If you are concerned that a partition was "quick" formatted and possibly has bad sectors, you can run the **chkdsk /r** command to find out for sure.

Note

Quick and full formats are *not* considered secure solutions for drives that will be repurposed or that have been obtained from other parties. More secure solutions that do *multiple* passes (zeroing out the data) are required. We'll discuss this further in Chapter 50, "Data Destruction and Disposal."

Linux File System Basics

Linux supports many file systems, including the ext family, FAT32, and NTFS. It also supports the Network File System (NFS), a distributed file system that allows a client computer to access files over the network. It was designed especially for Linux and UNIX systems, but other systems such as Windows can use it as well.

Note

In the following two paragraphs, we'll discuss commands that you can type in Linux. This is done in the Terminal, which is the command-line tool used in Linux and macOS. It is similar to the PowerShell/Command Prompt used in Windows. You can open it by searching **terminal**.

However, the most common file systems used on the local system are ext3 and ext4. ext4 is the Fourth Extended file system, which can support volume sizes of up to 1 exabyte (EB). You can discern the type of file system used in Linux by typing the **df -T** command. On systems commonly used during the writing of this book (early 2025), /dev/sda1 (where the Linux OS is installed) is usually ext4.

ExamAlert

Remember that ext4 is the Fourth Extended file system in Linux. It is a journaling file system that supports file sizes up to 16 terabytes and volume sizes of up to 1 exabyte (EB).

In /dev/sda1, /dev refers to the file system representation of devices. There can be more than one storage drive within the /dev path. Originally, sd stood for SCSI devices, but now it also includes SATA drives. Instead of calling each disk "disk 0," "disk 1," and so on (as Windows does), Linux refers to them as "a," "b," "c," and so on, and the number at the end of the path is the number of the partition. Linux is normally installed to partition 1, the full path being /dev/sda1; this is known as the *boot partition*. The second partition listed is an extended partition, similar to the Windows extended partition in that it can be used to create additional partitions for data, such as /dev/sda2 or /dev/sda3 and beyond. You might find that a particular partition (for example, /dev/sda5) is used by the OS as a swap file (that is, a paging file) between the memory and the storage drive. You can find a list of the partitions available on most Linux systems by opening the command line (Terminal) and typing **lsblk**, which is short for *list block devices*.

The following is an example of a Debian Linux system with two storage drives:

```
sda           8:0    0 465.8G  0 disk
├─sda1        8:1    0 433.9G  0 part /
├─sda2        8:2    0     1K  0 part
```

```
└─sda5        8:5    0  31.9G  0 part [SWAP]
sdb           8:16   0 111.8G  0 disk
```

In this example, there are two solid-state drives: sda (465 GB) and sdb (111 GB). sda is divided into three visible partitions: sda1, where the OS is installed; sda2, which is a startup partition; and sda5, the swap partition. Is **lsblk** the only command you could use? No. In Linux, there are always more commands, but **lsblk** is a good one.

> **Note**
>
> Linux uses a variety of other file systems, so be prepared for lots of different acronyms.

As you can see in the example, Linux makes use of a *swap partition*, also known as *swap space*. The swap partition acts as an overflow for RAM. If the RAM fills up, any subsequently opened applications will run inside the swap partition on the storage drive until some RAM space is cleared up. This is somewhat similar to the Windows pagefile concept, but the Linux swap space exists on a separate partition, whereas the Windows page file exists on C:\ by default.

We'll discuss Linux further in Chapter 40, "Linux."

macOS File System Basics

As of the writing of this book, and since macOS version 10.13, Apple has used the Apple File System (APFS). It is the successor to Hierarchical File System Plus (HFS+). These file systems work in a similar fashion to Linux-based file systems (it's all UNIX-based by the way) and can be analyzed in a similar way in the Terminal. For example, to see a list of the partitions, type **df -t** (lowercase *t* here) or use the macOS command **diskutil list**. macOS also uses a set of swap files in a similar manner to Linux. They are stored in /private/var/vm. They can be displayed with the Disk Utility program, or in the Terminal using the **ls -lh /private/var/vm/swapfile*** command.

We'll discuss macOS further in Chapter 39.

> **ExamAlert**
>
> Apple uses the Apple File System (APFS) on macOS and some other Apple-based devices. It works in a similar fashion to Linux-based file systems.

Hard Drive Formatting Comparison

When formatting a hard drive (especially a magnetic drive with spinning disks), you will have several options regarding how to format it. Most of the time the default that your operating system suggests will be the correct choice, but it is important to know the different format types and why one format is better than another. Table 29.1 lists many of the most common formatting types as well as their feature sets.

TABLE 29.1 **Hard Drive Formatting Comparison**

	NTFS	ReFS	FAT32	exFAT	Ext4	XFS	APFS
Compatibility	All Windows versions, macOS, Linux, many other OSs	Windows with Storage Spaces	Windows, macOS, Linux, most other devices	Windows, Mac, Linux	Any system that can mount ext3 and ext2, including Linux and some Windows	Linux, Windows, and macOS with third-party tools	Native to macOS, Windows, and Linux with third-party tools
Max volume size	8 PB	35 PB	2 TB	128 PB	1 EB	8 EB (may be limited by operating system)	Limit of the storage device (practical limit 8 EB)
Max file size	256 TB	35 PB	4 GB	16 EB (practical limit 128 PB)	1 TB	8 EB	8 EB
Fault tolerance	Yes	Yes	Not supported	Not supported	Yes	Yes	Yes. Copy-on-write
Compression	Yes	Yes, including block cloning and deduplication	Not supported	Not supported	Not supported	Not supported	Yes

Vendor Life-Cycle Limitations

Today, most computing devices and their operating systems have limited lifespans. Some manufacturers of hardware and software decide on an end-of-life (EOL) date as part of the

original design of a system. This can mean a couple of things, including the discontinuation of updates (especially security updates) and the ending of support for software/hardware. It's all part of the life-cycle policy.

Typically, a device's software support can be expected to last between three and five years before EOL—and that's it. Think that over for a moment. It means that your organization needs to continually plan what will happen to the multitude of devices and operating systems that it supports. The more types of devices and operating systems, the more complex the work. It can be daunting. That is why most organizations implement complete life-cycle planning—from initial installation to decommissioning.

While EOL dates are not set in stone, manufacturers usually adhere to them once they have published them. Pay attention to the Windows "end of *extended* support" dates, which are the important dates to know.

Because the end of life of your particular operating system is important to know but difficult to predict due to the variety of operating system versions available, it is easy to look up the information. One of the easiest is the endoflife.date tool.

> For Windows, that is https://endoflife.date/windows.
>
> For macOS, that is https://endoflife.date/macos.

Unfortunately, that site does not keep track of Chrome OS, but Google lets you track it on the devices themselves. For where and how to look for the information, see https://support.google.com/chromebook/answer/9367166?hl=en.

What does all this mean? You need to be cognizant of the fact that all hardware and software has a limited lifespan. When the end-of-support date comes, no more updates—most importantly, security updates—will be available. Being without security updates is a risk that most companies are not willing to take. So, in many cases, a company needs to upgrade software (and potentially hardware) every couple of years—and more often if the company uses several different platforms.

Beginning with Windows 10, Microsoft took a bit of a different approach compared to previous Windows versions. Instead of the point release numbering convention, beginning with Windows 10, there are different "versions" of Windows, such as Windows 10 version 20H2 and Windows 10 21H1. It is similar conceptually. As a version comes close to the end of its support date, it will automatically attempt to auto-update to the next version. If you run Windows 10 Home or Pro, and if not configured properly, the update could happen at an inopportune time (in newer versions of Windows, you will be prompted and can cancel the update if it is not a convenient time). Companies that run Windows Enterprise (and other select editions) often disable auto-update and/or defer updates until they can be tested. To find out the version of Windows you are running, go to the **Run** prompt and type **winver**.

Note

For more about the Windows life cycle and extended support end dates, see https://docs.microsoft.com/en-us/lifecycle/faq/windows.

ExamAlert

Remember that a software version has an end-of-support date, also known as an end-of-life (EOL) date. Be ready to have an upgrade plan well before that date!

Some companies don't publish end-of-support dates until they stop supporting a version. But you can take a good guess as to when this will happen, based on historical data. For example, Android 6.0, released in late 2015, was discontinued in late 2018, and Google stopped updating security patches for it at that point—a three-year span. This is typical. Another example: Typically, Apple only supports MacBooks that were built in the past five years or so. What it boils down to is this: You can expect a device to be supported for *x* amount of time before security patches stop. Plan for it!

Compatibility Concerns Between Operating Systems

In a computer network that has multiple platforms, there is definite concern about how the different operating systems will work with each other. That's why some organizations opt to become single-shop houses—meaning they use only one manufacturer, such as Microsoft. But that isn't always possible (or preferable), so operating systems often have to interoperate. That means cross-platform compatibility for apps, file-sharing compatibility, and the process of different systems logging in to each other—for example, a Linux computer connecting to a Microsoft domain or an Apple macOS system interacting with Chrome OS. As we progress through the book, we'll discuss different ways to approach compatibility between different systems.

Many companies are moving to cloud-based services to help alleviate these compatibility issues and leverage the strength of the network platforms.

For instance, Amazon Web Services (AWS) is frequently used to provide virtual machines, servers, and storage to organizations, providing scalability and serviceability while also providing anywhere, anytime access.

Microsoft Azure provides similar services, allowing for business-critical applications to run from the Microsoft cloud and extending the existing Azure Active Directory into the cloud space, allowing anywhere, anytime access to virtual services within the Microsoft cloud.

Google has developed its own object platform for virtual machines and containers to run within its cloud space. Like the examples from Amazon and Microsoft, these include virtual servers and storage but also include sophisticated search and analytics solutions.

Collectively, organizations are making these moves to cloud-based environments for several reasons:

- **Cost efficiency:** Organizations no longer need to host their own on-site servers and other equipment.
- **Scalability:** Organizations can expand or reduce computing power as needed to meet fluctuating business requirements. When needs are greater, virtual servers can be spun up to meet the needs. When needs are reduced, the servers can be moved offline. This is not possible with physical servers.
- **Improved agility:** As the market changes, adjustments can be made to the applications and services provided to customers and employees.
- **Accessibility:** Data and applications can be made available from anywhere at anytime, so long as someone has an Internet connection.
- **Enhanced security:** Each of the highlighted tools has an enhanced security suite available, providing robust security for the virtual assets. This augments any security team that an organization may have on-site.

Cloud computing is discussed more in depth in Chapter 42, "Cloud-Based Productivity Tools."

Even if two systems *are* compatible, it doesn't mean that every *version* of each of those systems is compatible. An older version of Android might have no chance of connecting to a newer Windows domain controller. Or an older version of Windows (such as Windows 7) won't be able to interact properly with a newer version of a Linux server—not to mention that Windows 7 is not supported anymore and is a major security risk. As we've said, we'll get into compatibility issues more as we progress through the book.

The bottom line is this: The more platforms and systems you introduce to your infrastructure, the more complex things get, and the more you need to think about how these systems will all interact from networking, security, and usability standpoints.

Cram Quiz

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

1. Which of the following operating systems is a free download with no evaluation period limitations?

   - ○ **A.** Windows
   - ○ **B.** Ubuntu
   - ○ **C.** macOS
   - ○ **D.** iOS

2. According to the CompTIA A+ objectives, which of these are not mobile operating systems (OSs)? (Select three.)

- **A.** Windows
- **B.** Chrome OS
- **C.** Android
- **D.** iPadOS
- **E.** Linux

3. As of summer 2026, which of these operating systems will *not* be a major security concern?
   - **A.** Window 8.1
   - **B.** Windows 10 (21H2)
   - **C.** Ubuntu 22.04 LTS
   - **D.** macOS 13.0
4. Which of the following statements is true?
   - **A.** All operating systems have an end-of-life date.
   - **B.** Linux distros cost money to distribute.
   - **C.** Android is an example of closed-source software.
   - **D.** Chrome OS is designed by Apple to use mostly desktop applications.
5. Which of the following does macOS use that works in a similar fashion to Linux-based file systems?
   - **A.** APFS
   - **B.** EOL
   - **C.** ext4
   - **D.** exFAT
6. Which of the following are considered closed-source proprietary operating systems? (Select three.)
   - **A.** Android
   - **B.** Windows
   - **C.** macOS
   - **D.** iOS

Cram Quiz Answers

1. **B.** Ubuntu Linux (regardless of the version) is a free download. While you can download some versions of Windows, they are only for evaluation periods of time.

Apple-based operating systems, such as macOS and iOS, are not free downloads.

2. **A, B, and E.** Windows, Chrome OS, and Linux are not mobile operating systems. Android and iPadOS are used in tablets. You will see iOS in Apple phones as well. Windows, Chrome OS, and Linux are commonly found in laptops and listed in the CompTIA objectives as workstation operating systems (OSs), but for the purposes of the exam, mobile includes tablets and phones.

3. **A.** Windows 8 expired years ago and is a huge security concern. If your organization must run a Windows 8 instance, be sure to run it on a separate network segment (or, preferably, completely independent of any network at all!). Windows 10 (21H2) entered Long Term Support (LTS) in 2021 and will completely exit support in January 2027. Update if possible. Ubuntu 22.04 entered LTS in September 2024, and will be in Maintenance and Security Support until 2027. After that, it will receive security updates only until 2032. MacOS 13 was released in October 2022. Apple usually maintains them for about three years, which should last until 2025.

   But really now, this is a bit of a trick question. All of them are security concerns! Every OS and device on a network should be a security concern, regardless of age. Consider that.

4. **A.** Every operating system has an end-of-life date. Linux is free to distribute, so this statement is not true. Some distributors may charge for service and support. Android is technically open source, so this statement is not true. Chrome OS is written by Google, not Apple, and relies on the user using the Chrome browser for mostly web-based applications, so this statement is not true.

5. **A.** Apple uses the Apple File System (APFS) on macOS and some other Apple-based devices. It works in a similar fashion to Linux-based file systems. End-of-life (EOL) is the discontinuation of updates and the ending of support for software/hardware. ext4 is the Fourth Extended file system in Linux. exFAT is the successor to FAT32 in Windows, it can handle large file sizes and can format media larger than 32 GB.

6. **B, C, and D.** Closed-source software like Windows, macOS, and iOS are restricted and proprietary. Open-source software and code like Linux and Android are available to the public.

Wow! We just ran the gamut of operating systems, so to speak. If you can build a knowledge base for each of the operating systems in this chapter, then you can be a powerhouse technician! Continue the good work!

Chapter 30

Operating System Installations and Upgrades

This chapter covers the following A+ 220-1202 exam objective:

- **1.2** – Given a scenario, perform OS installations and upgrades in a diverse OS environment.

A technician might be called upon to install or reinstall an operating system on a new computer, an older computer, or a virtual machine. A smart technician knows the various ways to boot from an installation source, which may be removable media, a source that is internal to the computer, or a source that is stored on the network. Professional technicians will ask questions like these: What type of installation is it? How will we partition and format the drive? Are there any special considerations during setup? Always consider these questions as part of your planning for an operating system installation or upgrade.

When you're working in a small environment, clean installations are typical; when you're working in a larger environment, network installs, unattended installations, imaging, and repairs are much more common. This chapter covers the basics when it comes to operating system considerations. When you are done here, you should understand how to install any OS (Windows, Linux, macOS, and so on) from any source and to any destination drive. Let's begin.

ExamAlert

Objective 1.2 focuses on boot methods, types of installations, partitioning, drive format, upgrade considerations, and feature updates.

Boot Methods

To install an operating system to a computer, you first have to boot the system to the installation media. There are several types of boot methods you should know for the exam:

- **Local installation from an external drive/flash drive:** The most common type of local installation is via USB flash drive. To do this, download the operating system .ISO file (or similar file type) from the OS developer's website. Make the USB flash drive bootable and extract the contents of the .ISO file to the drive. There are free programs available that can speed up the process by making the drive bootable, formatting it, and extracting the .ISO all at once (for instance, Rufus, Yumi, and the Windows USB/DVD Download Tool). Once the flash drive is set up, insert the flash drive to the target system, boot the computer, change the BIOS/UEFI boot order to USB flash drive first, and get installing! Often this process will be quick and painless. Less commonly, you might install from a hot-swappable drive within a USB drive enclosure or perhaps from an eSATA drive.

Note

Try downloading an .ISO image of Linux or Windows (evaluation) and extract the contents to a USB flash drive. Then, install the OS on a physical computer so that you can see the installation process. You can also run through the installation process with virtual machines by accessing the .ISO file directly.

> **Note**
>
> When you sit at a computer and answer all the questions it asks you, step-by-step, it is known as an *attended* installation; you are attending to the computer as the installation progresses.

- **Network boot (PXE) installation:** You can install an OS to a client by booting to the network and using a Windows server and the Microsoft Endpoint Configuration Manager (MECM), Microsoft Deployment Toolkit (MDT), or by accessing any Windows or Linux server acting as a repository for the Windows installation files. (Those servers may also operate as DHCP and TFTP servers.) If you do need to perform an over-the-network installation, be sure that the target computer has a Preboot Execution Environment (PXE)–compliant network adapter. This allows the computer to boot to the network and locate the DHCP server and, ultimately, perform the installation (as long as the server is configured properly). We'll discuss a couple of those options in an upcoming section.
- **Internal drive installation:** You can install from fixed media inside a computer; however, usually the source of the media needs to be a different location from the target area for the OS. There are two options here: Install from a separate partition of a storage drive or install from a separate drive altogether. As usual, we are using the term *storage drive* loosely. It could be a magnetic-based disk, an SSD, an NVMe-based drive, or even a USB flash drive if the motherboard has an internal USB port (with a USB drive inserted). Some power workstations and server motherboards come with these, for installation purposes, or even to run the OS! In any case, the installation media will have to have the .ISO or another image of the operating system installed.
- **Internet-based installation:** Operating systems can also come directly from the Internet, either in part or completely. For example, Ubuntu Server has options for automated server provisioning in bare-metal cloud environments and instant operating systems that are ready for virtualization platforms such as VirtualBox, Hyper-V, and KVM. Just go to the website, click, and start installing. Going further, you might also

do installations of software, or even install entire operating systems, by using Microsoft's task sequencer. An example might be a Windows in-place upgrade using MECM—most likely within the Azure cloud. For more information, see https://docs.microsoft.com/en-us/mem/configmgr/osd/deploy-use/deploy-task-sequence-over-internet.

Note

As of this writing, MECM and related products were being migrated into the Intune family of products for branding purposes; it is unclear how that will impact functionality, if at all.

ExamAlert

Know these boot methods for OS installation and upgrades: external/flash drive, network boot (PXE), internal drive, and Internet based.

Whatever method you choose, be sure to select that method as the first boot option in the BIOS/UEFI of the computer. Other configurations might also be necessary. When you are finished, reset the BIOS/UEFI boot priority to storage drive first and, if necessary, disable any removable media options in the BIOS/UEFI settings.

Types of Installations

While most currently shipping hardware can handle the latest version of Windows, it is not uncommon to be asked to upgrade older equipment to newer versions of Windows. In this case, it is important to know the system requirements of each version.

Table 30.1 shows the minimum system requirements for Windows 10.

TABLE 30.1 **Windows 10 Minimum System Requirements**

Operating System	Windows 10	Windows 10
Architecture	32-bit	64-bit
Processor	1 GHz or faster processor or System on a Chip (SoC)	1 GHz or faster processor or SoC
Memory	1 GB	2 GB
Free hard disk space	16 GB	20 GB
Graphics card	Microsoft DirectX 9 or later graphics device with WDDM 1.0 driver	Microsoft DirectX 9 or later graphics device with WDDM 1.0 driver
Display	800 × 600	800 × 600
Internet Connection	Internet connection necessary to perform updates and to download and take advantage of some features, and during initial device setup.	
Microsoft Account	Microsoft account (MSA) or Azure Active Directory (AAD) account required.	

Table 30.2 shows the minimum system requirements for Windows 11.

TABLE 30.2 **Windows 11 Minimum System Requirements**

Operating System	Windows 11
Architecture	64-bit
Processor	1 GHz or faster processor with two or more cores or SoCs
Memory	4 GB
Free hard disk space	64 GB
Graphics card	Microsoft DirectX 12 or later graphics device with WDDM 2.0 driver

Operating System	Windows 11
Display	High definition 720p
Additional hardware	UEFI and TPM 2.0 required
Internet Connectivity	Internet connection necessary to perform updates and to download and take advantage of some features, and during initial device setup.
Microsoft Account	Required during initial setup and for some features.
Feature-Specific Requirements	Some features such as Co-pilot+ require specific hardware. See https://www.microsoft.com/en-us/windows/windows-11-specifications?r=1 for details.

ExamAlert

Know the minimum system requirements for installing Windows 10 and 11.

Along with the boot method, you should be prepared for the type of installation you require. There are several types of OS installation:

- **Clean install:** With a clean installation, the OS is installed to a blank partition. It could be a new storage drive or a drive/partition that was wiped clean of data. Generally, a clean install is attended to by the technician, who interacts step-by-step with the OS as it is installing. Newer hardware might not be seen correctly by some operating systems, so be ready to supply third-party drivers for hardware (such as storage drives or video). These drivers can usually be found at the manufacturer's website if they are not available from Windows Update. Note that Microsoft is phasing in its own Internet Printing Protocol (IPP) drivers for most printers, eliminating the need to install separate drivers for most printers and thus simplifying printer installation.

- **Upgrade:** With an upgrade installation, the target storage drive (or partition) already has an operating system installed and is upgraded to a newer version of that operating system—for example, from Windows 8.1 to Windows 10 or from Windows 10 to Windows 11. Another example is an in-place upgrade (often used for repairs), in which the OS is effectively reinstalled but without losing files or applications. The repair in-place upgrade and other similar repair-based installations are usually last-resort options for fixing individual systems. Remember that upgrades may or *may not* retain a user's data. Regardless of the upgrade type, you should always back up the data and the user preferences/profile before initiating the upgrade. Also, be sure that current applications will function on the new OS and that any older hardware will have an applicable driver for the newer OS before upgrading.
- **Unattended installation:** This type of installation requires an answer file that has been created in advance. Also, it normally requires a specific service. For instance, to automate the process of installing Windows, you can use Microsoft Endpoint Configuration Manager (MECM) or the Microsoft Deployment Toolkit (MDT). This server-based program works with the Windows System Image Manager program in Windows. It can be used to create the answer file that is used during an unattended installation. The answer file provides the responses needed for the installation, eliminating the need for user intervention. In Windows, there is a single XML-based answer file called autounattend.xml; this file can be placed on a USB flash drive or on a remote server.

> **Note**
>
> The Windows System Image Manager (SIM) is part of the Windows Assessment and Deployment Kit (ADK) for Windows, which can be downloaded from Microsoft's website.
>
> For more information about Windows deployment with the ADK, visit https://docs.microsoft.com/en-us/windows/deployment/windows-deployment-scenarios-and-tools.

- **Image deployment:** Images can be made and deployed in a variety of ways, such as by cloning the entire drive image of another installation. This can be done by using programs such as Acronis True Image or Ghost. When you're cloning a drive image, both computers must be identical, or as close to identical as possible. The drive of the target for a cloned installation must be at least as large as the original system. To avoid security identifier (SID) conflicts, use the Sysprep utility. The Sysprep utility for Windows is installed with the operating system and can be found in C:\Windows\System32\Sysprep\. Sysprep uses an answer file created with the SIM. It creates a unique SID and makes other changes as needed to the network configuration of the system. You can also "image" the computer with a *premade* OS image. Do this with the Microsoft Deployment Toolkit (see https://docs.microsoft.com/en-us/windows/deployment/windows-deployment-scenarios-and-tools) or with third-party tools such as Ghost. In addition, you can install from a recovery disc/drive that you created or that was supplied by the vendor of the computer.
- **Remote network installation:** A remote network installation can be initiated while the target computer is booted to a preexisting OS or by booting a PXE-compliant computer to the network and specifying the server (where the OS installation files are located) to access from the BIOS/UEFI.
- **Zero-touch deployment (also called zero-touch provisioning):** In this special type of remote installation, devices are automatically configured at the device suppliers, with the serial numbers and other configuration information registered automatically at the third-party reseller. When purchased, the device is automatically enrolled in the organization's Azure Active Directory domain, and the requisite software is automatically downloaded and installed on the device. The device can then be shipped to the end user directly without having to be provisioned first by an organization's IT department; it comes to the end user already configured. The end user needs only to log in, and the device will get final configuration information downloaded for that user's specific needs and the user is ready to go.

- **Reset/restore:** These are options for troubleshooting problems with a Windows system. In Windows 10/11, for example, **Reset your PC** enables the user to clear everything or keep personal files. Restoring the PC means undoing recent changes. Windows can also be installed from a previously made System Restore image.

  In Windows 11, you can reset your PC by doing the following:

  1. Go to **Start > Setting > System > Recovery**.
  2. Select **Reset PC**.
  3. Choose **Remove everything** to fully reset your device. Choose **Keep my files** to reset the operating system only (which is a repair installation).

  Figure 30.1 shows the options available to reset the operating system from the Reset PC dialog box.

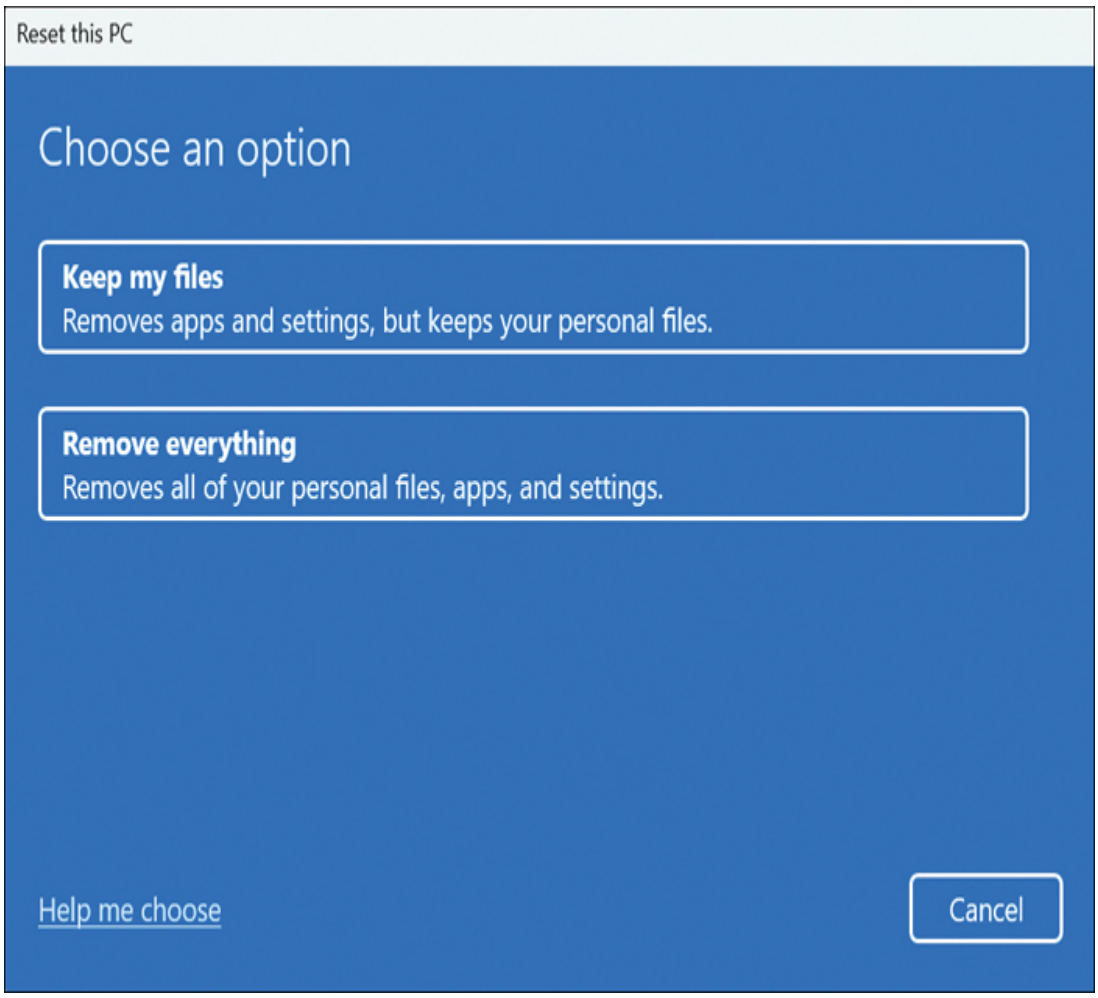


FIGURE 30.1 **The Reset PC Dialog Box Enables You to Choose to Keep Your Files (a Repair Installation) or Remove Everything (Reset Your PC)**

- For more information on System Restore and troubleshooting Microsoft Windows in general, see Chapter 53, "Troubleshooting Microsoft Windows."
- **Installing from a recovery partition or disc:** Computers with Windows preinstalled use a recovery disc, a hidden partition, or both. This disc and/or partition contains a factory image of Windows. The purpose is to enable users to return their computers back to their state when they were first received. This means that the system partition (usually the C: drive) will be properly formatted and reimaged with Windows. This works well in a two-partition system, in which the operating system is on C:

and data is stored on D: or another drive letter. In this scenario, when the operating system fails and cannot be repaired, the computer can be returned to its original "factory" state, but the data won't be compromised (and neither will applications if they were installed to the other partition!). When you buy a computer from a company such as HP, Dell, and so on, make sure it offers some kind of factory recovery partition, recovery disc (or flash drive), or other recovery option.

ExamAlert

Know the difference between clean install, upgrade, local/remote network, drive image, recovery partition, and repair installations.

Multiboot

Since the 1990s, technicians have been setting up two or more operating systems on the same drive; this is known as *dual-booting*, *tri-booting*, and so on, or more generically, *multibooting*. The process is easier today than it used to be back in the 1990s; now you can usually get away with using built-in tools in Windows or Linux. For example, if you have Windows installed, you can modify the partition structure with Disk Management, create an additional partition, and install another OS to that new partition. This approach requires a bit of planning, but if successful, both operating systems display in a menu when the computer is booted. The information pertaining to these operating systems is stored in the Boot Configuration Data (BCD) store in Windows and in GRand Unified Bootloader (GRUB) in Linux.

Partitioning

Partitioning is the act of dividing a storage drive into sections. It's kind of like a floor plan for your drive, with "walls" that separate your formatted areas for data. You don't have to have any walls, so to speak; you can have a single partition, or you can have more than one. The design is up to you. Let's talk about the basic partitioning terms you should know for the exam.

Primary and Extended Partitions and Logical Drives

The first partition that the OS is installed to is called a *primary partition*. Many systems have a single primary partition, which is inhabited by the operating system; it is set to boot from this drive by default. This partition also stores the data. In Windows, it is usually known as the C: drive. However, it is a good practice when first partitioning a drive to create two partitions: one for the OS and one for the data (perhaps C: and D: or C: and F:). Having two partitions keeps the data *safer* in the event of an OS crash and subsequent repair or reinstall of the OS. In a typical Windows system, the storage drive is limited to four partitions. Those can be four primary partitions or three primary partitions and one extended partition. The extended partition can be further broken up into logical drives, allowing a person to have as many sections as there are letters in the alphabet—which is usually enough! Letter assignments (C:, F:, G:, and so on) are also referred to as *volumes*. A volume can be a single partition or logical drive, or it can span different drives or even different systems. We discuss this topic further in Chapter 33, "Microsoft Operating System Features and Tools, Part II."

Basic and Dynamic Drives

A typical installation of an OS such as Windows normally results in a basic drive. This is a storage drive that has finite-sized partitions and volumes. Those partitions cannot be resized unless you convert the drive to a dynamic drive. This is a process done in Windows with the Disk Management program or at the command line with the **diskpart** utility. Once converted, partitions and volumes can be resized as the user sees fit—as long as there is space available on the drive. There is risk involved with using this process, and data should be backed up prior to initiating the conversion. It's a fairly easy process that we detail in Chapter 34, "Microsoft Command-Line Tools, Part I."

ExamAlert

Know the differences between basic and dynamic drives. Remember that a *basic drive* refers to a hard disk that uses a simple partitioning scheme with primary partitions and logical drives. *Dynamic drives* offer the capability to create volumes that span multiple disks (both

spanned and striped volumes). They also allow the ability to create fault-tolerant volumes (mirrored and RAID-5 volumes).

GPT vs. MBR

There are two partitioning schemes that you should know for the exam: GPT and MBR. These schemes define the maximum number of partitions that a drive can have as well as the maximum size of each partition. Which partitioning scheme will you use? You will usually make use of the globally unique identifier (GUID) Partition Table (GPT) instead of the older Master Boot Record (MBR). GPT is a newer standard and has, for the most part, replaced MBR; it is not limited in the way that MBR is. With GPT, you can have up to 128 partitions and no extended partition is necessary. Also, you are not limited to the MBR's maximum partition size of 2 TB. In addition, the index to the GPT (called a Partition Entry Array) is stored in multiple locations, so it is harder to corrupt the partition table data.

Note

Use of the term *master* is ONLY in association with the official terminology used in industry specifications and standards, and in no way diminishes Pearson's commitment to promoting diversity, equity, and inclusion, and challenging, countering, and/or combating bias and stereotyping in the global population of the learners we serve.

GPT is used heavily in Linux systems, and Windows has supported it since 2005. It forms a part of the UEFI standard, and your system needs to have a UEFI-compliant motherboard. It uses globally unique identifiers (secure 128-bit numbers) to reference partitions, making it virtually impossible for any two computers to have two partitions with the same ID.

In essence, GPT was designed to replace MBR, and it is strongly linked to how the UEFI is designed to replace (or augment) the BIOS. It's important to remember that you might need to select either GPT or MBR when you

first add a new drive or start an installation. You can convert a drive from MBR to GPT, but the drive will be wiped when you do this. For more information on how to do this conversion, visit https://docs.microsoft.com/en-us/windows-server/storage/disk-management/change-an-mbr-disk-into-a-gpt-disk.

Most systems today are UEFI compliant, so if you perform a fresh installation of Windows, it should automatically seek to use GPT, as long as UEFI is enabled.

ExamAlert

Know the differences between GPT and MBR! GPT is newer and better, has 128 partitions, and can go far beyond the 2 TB MBR maximum partition size.

More OS Installation and Upgrade Considerations

There are plenty of other considerations to make before and during an OS installation, including the following:

- **Load alternate third-party drivers when necessary:** For example, if you are installing Windows to a newer and less common storage drive (perhaps a brand-new-model NVMe), you might have to supply the manufacturer's drivers if Windows doesn't recognize the drive. Check the manufacturer's website for these drivers if they are not available on Windows Update.
- **Workgroup vs. domain setup:** If a Windows computer will be standalone or used in a small office, chances are it will be set up to connect in workgroup mode. In a larger environment that is controlled by a Windows server, you might have to select **Domain**. Regardless of whether you are on a workgroup or domain network, you will need to ensure that the network adapter is properly configured with the IP

address of the DNS server on the network or has obtained that information properly from a DHCP server.

- **Time/date/region/language settings:** During the installation, you will be prompted to enter basic information such as the time, date, time zone (and/or region of the world), and language you will be using. For the rest of this book, we will focus on English as the main language (out of personal preference as well as a necessity)!
- **Driver installation, software, and Windows updates:** You might be prompted to load additional drivers for storage, video, and network devices—especially network interface cards so that the system can access the Internet. Have these ready for beforehand. Check the manufacturer's website for these drivers if they are not available on Windows Update.
- **Properly formatted boot drive with the correct partitions/format:** If you install Windows and decide to customize the partitions, you have to be sure to use the right formatting and build out at least one recovery partition. The unwritten rule is to use the NTFS file system for the main primary partition where the OS will be housed, and the written rule is to make it 32 GB or more for Windows 10, 64 GB for Windows 11. The minimum size of the recovery partition will depend on the version of Windows, but, for example, Windows 10 will often use 450 MB, whereas Windows 11 defaults to 768 MB but prefers at least 1 GB. A recovery partition is created automatically if you do a default installation of Windows and if you select the default partition layout. After the installation is complete, you can view the partitions in Disk Management or with the **diskpart** utility in the Command Prompt. For example, type **diskpart** to enter the utility, type **select disk 0** (where 0 is the first drive), and then type **list partition**. Figure 30.2 shows an example of this. In this example, Partition 4 is 145 GB. That is the C: drive, and it is where we installed Windows 10. We've stored the data separately on Partition 7, which is 86 GB. Also, there are three recovery partitions in this case, ranging between 300 and 450 MB. The Disk Management equivalent is shown in Figure 30.3, though this does not display Partition 3 "Reserved." Keep in mind that your default installation of Windows will probably have fewer partitions; for

example, you might see a recovery partition, an EFI system partition, and the OS partition.

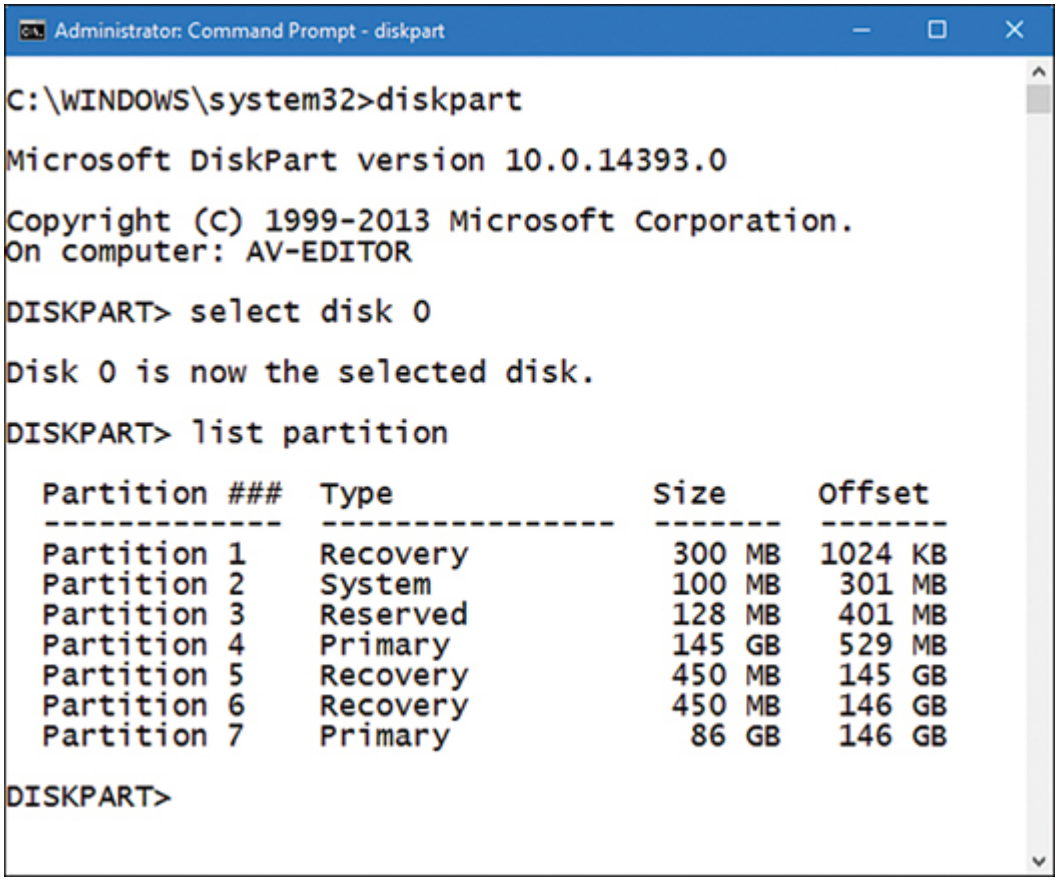


FIGURE 30.2 **The diskpart Utility, Showing the Partitions of a Windows Boot Drive**

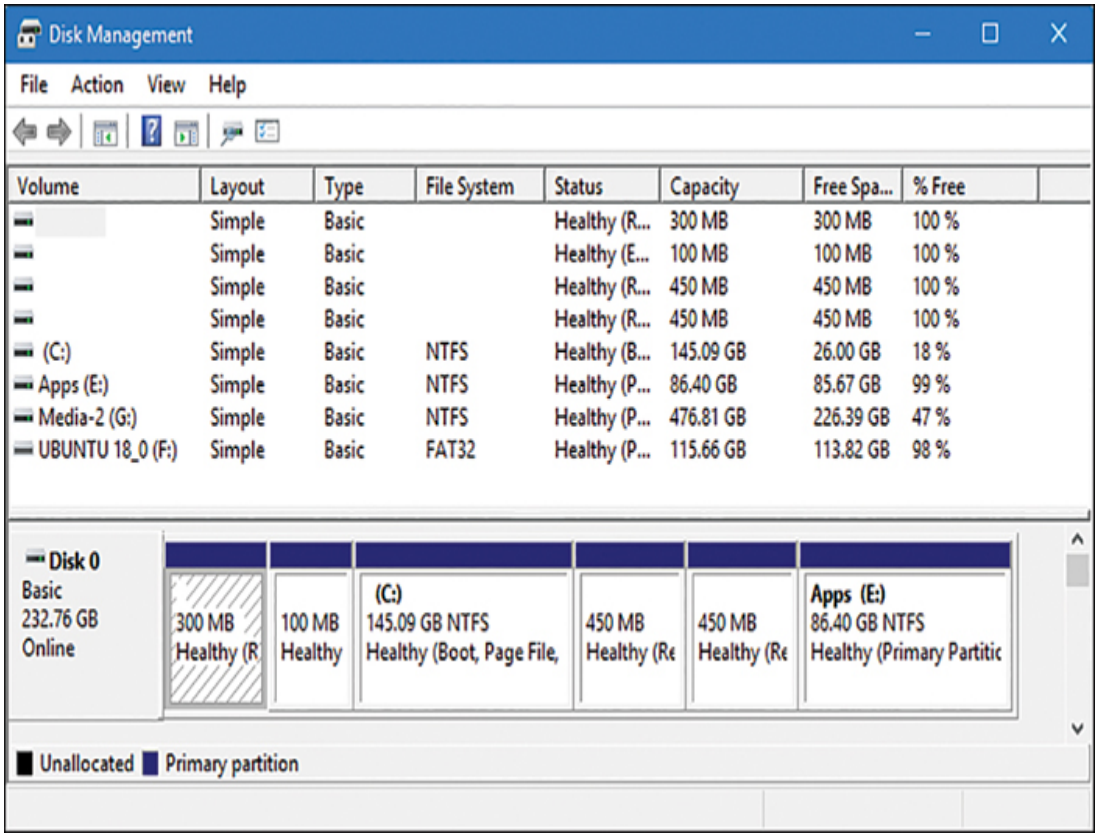


FIGURE 30.3 **Disk Management, Showing the Partitions of the Same Windows Boot Drive as in Figure 30.2**

ExamAlert

Know how to use the Disk Management and **diskpart** utilities!

- **Factory recovery partition:** If you buy a computer from a manufacturer, the software may be preloaded. In that case, there will usually be one or more recovery partitions on the storage drive that are separate from the system partition. These are generally less than 1 GB each and can be used to repair the system and recover from any errors that occur.
- **Prerequisites/hardware compatibility:** As mentioned earlier, you have to make sure that your physical computer (or virtual machine) will meet the minimum requirements as set by Microsoft or another OS developer.

Before installing, you should also check the hardware compatibility list for the particular OS and make sure that the motherboard, CPU, video card, audio card, network adapter, and storage drives will work with that OS.

- **Application compatibility:** This all stems from the original question: What are you going to use the computer for? If it's going to be used to run Logic (audio software), then you need a macOS system. If you are running Pro Tools, then you need to decide whether you will use Windows or macOS. Or maybe you want to build a Hyper-V virtualization system using Windows. If so, it will run on any edition except Home. Know what you are doing with the computer before installing the OS and know whether the applications will run on the computer's hardware and within the version and edition of the OS you wish to install.
- **OS compatibility/upgrade path:** If you are upgrading from one OS to another and wish to save the data/settings, you have to make sure that the upgrade path is valid. We discuss upgrade paths further in Chapter 31, "Basic Features of Windows Editions."
- **Product life cycle:** Remember to keep in mind any operating system or application life cycle. For example, once an OS is released, it typically is supported for three to five years (depending on the OS). After that, it won't receive security updates (and other important feature updates) unless it is upgraded to a new version of the OS. For instance, support for all versions of Windows 10 Home and Pro ends on October 14, 2025 (see https://docs.microsoft.com/en-us/lifecycle/products/windows-10-home-and-pro). Well before the end of the product life cycle, you and your team will need to decide what will become of the device and its software. This is part of Microsoft's Modern Lifecycle Policy, which covers those products that are updated continuously. So long as the user is licensed to use the product and stays current with the updates, Microsoft will continue with system and security updates. Information on specific products can be found at https://learn.microsoft.com/en-us/lifecycle/products/.

Planning Is Crucial!

There is a lot to consider in this chapter. We always say that *planning is key*. Clean and sharp planning helps you avoid problems and saves time in the long run. Planning is extremely important when dealing with all things technology.

Cram Quiz

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

1. Which of the following installation types would require PXE compliance?

   - **A.** Local
   - **B.** Network
   - **C.** Internal
   - **D.** USB flash drive

2. To avoid SID conflicts when drive imaging, which program should you use in Windows?

   - **A.** Sysprep
   - **B. diskpart**
   - **C.** SIM
   - **D.** Microsoft Endpoint Configuration Manager (MECM)

3. You are tasked with installing Windows with the standard configuration. It needs to support a storage drive with a single 8 TB partition. Which of the following should you configure the system to use?

   - **A.** GPT
   - **B.** FAT32
   - **C.** MBR

- ○ **D.** ext4

4. Which of the following uses an answer file to provide responses and eliminates the need for user intervention?

   - ○ **A.** Factory recovery partition
   - ○ **B.** Clean installation
   - ○ **C.** Unattended installation
   - ○ **D.** Reset your PC

5. What should a technician consider first when planning to install Windows to a newer, less common storage drive? (Select the best answer.)

   - ○ **A.** Alternate third-party drivers
   - ○ **B.** A repair installation
   - ○ **C.** Recovery partition
   - ○ **D.** The product life cycle

6. Which of the following are the minimum system requirements for installing 64-bit Windows 11? (Select two.)

   - ○ **A.** 1 GHz or faster CPU with two or more cores or Systems on a Chip (SoC)
   - ○ **B.** 2 GB RAM
   - ○ **C.** 64 GB free hard disk space
   - ○ **D.** UEFI and TPM 1.0 required

Cram Quiz Answers

1. **B.** A network-based installation requires that the network card be PXE compliant so that it can boot to the network and locate a DHCP server and deployment server. Local installations, such as those using a USB flash drive or optical disc, do not need the network adapter. Internal installations, such as those that are done

from a secondary internal drive, also do not need a PXE-compliant network card.

2. **A.** Sysprep can modify unattended installations so that every computer gets a unique SID (and other unique information). Windows SIM creates the answer files for unattended installations. **diskpart** is used to view and configure partitions from the Command Prompt in Windows. Microsoft Endpoint Configuration Manager (MECM) is run on Windows Server and is used to deploy operating systems across the network.

3. **A.** Use GUID (globally unique identifier) Partition Table (GPT) as your partitioning scheme (instead of MBR) and follow that up by using NTFS as your file system for the partition. That is the typical setup when installing Windows. In this scenario, GPT and NTFS can support 16 TB partitions. FAT32 is an older file system that you could use, but it would not support the 8 TB partition that is required. ext4 is a Linux-based file system not used in Windows. Know your file systems for the exam!

4. **C.** An unattended installation uses an answer file that provides the responses needed for the installation. A factory recovery partition is preloaded by the computer manufacturer. A clean installation means that the OS is installed to a blank partition or new drive. Reset your PC is an option in Windows that allows a user to repair a computer by reinstalling the OS with one of two options: wiping all data or keeping user files.

5. **A.** If you are installing Windows to a newer and less common storage drive, you might have to supply the manufacturer's drivers (or third-party drivers) if Windows doesn't recognize the drive. A repair in-place upgrade and other similar repair-based installations are usually last-resort attempts to fix individual systems. The purpose of a recovery partition is to enable users to return their computers back to their state when they were first received. A product's life cycle is everything that happens from purchase to installation to end-of-life (EOL) and recycling/disposal. Support is the important thing here when it comes to software. For example,

once an OS is released, it is typically supported for three to five years (depending on the OS).

6. **A and C.** The minimum system requirements for installing 64-bit Windows 11 are 1 GHz or faster processor with two or more cores or Systems on a Chip (SoCs), 4 GB RAM, 64 GB free hard disk space, and UEFI and TPM 2.0. Know the Windows installation system requirements for the exam and the real world!

As your tech coaches, we have to say, “You are doing great! Keep going!”

Chapter 31

Basic Features of Windows Editions

This chapter covers the following A+ 220-1202 exam objective:

- **1.3** – Compare and contrast basic features of Microsoft Windows editions.

In this chapter, we'll discuss Windows 10 and 11 editions (such as Windows 10 Home, Windows 11 Home, and Windows 11 Pro), Windows features that are available in each edition, and ways to upgrade to the various editions of Windows. We'll also cover the basic components of a Windows operating system. Let's go!

ExamAlert

Objective 1.3 concentrates on Windows 10 and 11 editions, feature differences, upgrade paths, and hardware requirements.

Note

Don't forget that a complete list of the Core 2 (220-1202) objectives can be found on the companion website of this book (see the

Introduction for details) and on CompTIA's website: https://www.comptia.org/certifications/a.

Windows 10 Editions and Feature Differences

Windows 10 is a group of operating system (OS) editions including Home, Pro, Pro for Workstations, and Enterprise. There have been more derivatives of Windows 10, but to align ourselves with the CompTIA A+ objectives, we'll focus on these four. As a technician, you should be less interested in cosmetic differences than in technical differences between editions. Take a look at Table 31.1 for a basic comparison of the technical differences between these editions.

TABLE 31.1 **Comparison of Windows 10 Editions**

Component	Windows 10 Home	Windows 10 Pro	Windows 10 Pro for Workstations	Windows 10 Enterprise
RAM limitation	128 GB	2 TB	6 TB	6 TB
Physical CPU support	2, up to 32 cores	2, up to 32 cores	2, up to 32 cores	4, up to 256 cores
Remote Desktop Protocol (RDP)	✓ but client only	✓ client and server	✓ client and server	✓ client and server
Domain access	—	✓	✓	✓
EFS and BitLocker	—	✓	✓	✓
Hyper-V	—	✓	✓	✓
Group Policy Editor (gpedit.msc)	—	✓	✓	✓

✓ = Full upgrade is supported, including personal data, settings, and applications.
— = Cannot upgrade to that edition.

ExamAlert

Windows 10 editions RAM limits: Home = 128 GB, Pro = 2 TB, Pro for Workstations/Enterprise = 6 TB.

Windows 11 Editions and Feature Differences

Windows 11 is the most current Windows operating system. It is a group of OS editions including Home, Pro, Pro for Workstations, and Enterprise, also referred to as Windows 11 Business. There have been more derivatives of Windows 11, but to align ourselves with the CompTIA A+ objectives, we'll focus on these four. As a technician, you should be less interested in cosmetic differences than in technical differences between editions. Table 31.2 lists minimum system requirements for any version of Windows 11.

TABLE 31.2 **Windows 11 Minimum System Requirements**

	Windows 11
Architecture	64-bit
Processor	1 GHz or faster processor with two or more cores or System on a Chip (SoC)
Memory	4 GB
Free hard disk space	64 GB
Graphics card	Microsoft DirectX 12 or later graphics device with WDDM 2.0 driver
Display	High-definition 720p
Additional hardware	UEFI and TPM 2.0 required

ExamAlert

Know the minimum system requirements for installing Windows 11.

All versions of Windows 11 share the same user interface and most features. Indeed, most consumers will have all the features they need with Windows 11 Home, which comes preinstalled with most home-grade devices. Some of the most important differences come when connecting to the workplace and are important for the technician to note. For instance, Windows 11 Home cannot connect to domain networks common in most mid-size to large networks. Home cannot use RDP and therefore cannot support remote management without third-party tools. And Home has a significantly more limited RAM maximum. All of these differences limit the capabilities of Windows 11 Home. For most home users, this will not be an issue, but for enterprise users, these are dealbreakers; those users will need the Pro or Enterprise versions of Windows 11. Table 31.3 lists some of the common differences that you might find on your exam. More detailed information is available at https://www.microsoft.com/en-us/windows/business/compare-windows-11.

TABLE 31.3 **Comparison of Windows 11 Editions**

Component	Windows 11 Home	Windows 11 Pro	Windows 11 Enterprise (Windows 11 Business)
RAM limitation	128 GB	2 TB	6 TB
Physical CPU support	2, up to 32 cores	2, up to 256 cores	4, up to 256 cores
Remote Desktop Protocol (RDP)	No RDP available. Must update to Windows 11 Pro or use third-party tool	✓ client and server	✓ client and server
Domain access	—	✓	✓

Component	Windows 11 Home	Windows 11 Pro	Windows 11 Enterprise (Windows 11 Business)
EFS and BitLocker	—	✓	✓
Hyper-V	—	✓	✓
Group Policy Editor (gpedit.msc)	—	✓	✓

✓ = Full upgrade is supported, including personal data, settings, and applications.
— = Cannot upgrade to that edition.

ExamAlert

Windows 11 editions RAM limits: Home = 128 GB, Pro = 2 TB, Pro for Workstations/Enterprise (Business) = 6 TB.

ExamAlert

Be familiar with the Windows 10 and Windows 11 editions feature differences, including domain versus workgroup, desktop styles/user interface, availability of Remote Desktop Protocol (RDP), RAM support limits, BitLocker, and gpedit.msc. Keep these features in mind as you progress through the book.

Note

See the following site for more information about Windows features, including a comparison between Windows 10 and Windows 11: https://www.microsoft.com/en-us/WindowsForBusiness/Compare.

You might wonder, “What would I do with 6 TB of RAM?” Well, you might not need that much, but it’s the ability to go beyond the limitation of 128 GB that is important. There are plenty of software packages that can only run with more RAM, and those software packages might require the Pro or Enterprise version of Windows. In addition, for CAD professionals, data scientists, and graphic designers who use software that is *incredibly* resource-intensive, the Pro versions provide the “server-grade” experience that might be required. Always check the minimum requirements of the software you plan to install. We’ll discuss this concept further in Chapter 41, “Application Installation and Configuration Concepts.”

You have probably noticed that the Home edition is missing most of the features in the table, but this makes sense. A typical home user doesn’t need them. For example, a home user usually doesn’t need to connect to and log on to a domain or use virtual machines, so those features are omitted from that edition. But business users will be more sophisticated when it comes to features. Their needs might include domain access, virtualization, encryption, remote access, and so on. We’ll discuss each of these features in more depth as we continue through the book.

Note

Regardless of what edition you run, it’s important to make sure that your system has the resources required to run Windows. For example, on a 64-bit system, the Windows 11 minimum requirements include 1 GHz CPU with two or more cores, 4 GB of RAM, and 64 GB of free storage space (less for virtual machines).

Windows Desktop/User Interface and Components

The essence of Windows is the graphical user interface (GUI), which allows users to interact with Windows. Normally, a keyboard, a mouse, a touchpad, or a touchscreen is used to input information to the operating system’s GUI, and that input is shown on the screen. Basically, everything you see on the

display (including windows, icons, menus, and other visual indicators) is part of the GUI, but remember that the GUI also governs how the user interacts with the OS.

The Windows GUI has many parts, including the desktop with all its pieces; applications such as File Explorer, Settings, and the Control Panel; and Windows Tools such as Computer Management and the Device Manager. To grasp Windows, you need to learn how to navigate quickly through the GUI to the application or tool that you need. But the system is pretty deep and can be a bit confusing at times. Quick tip: Know how to navigate the system, but especially know how to use the Search and Run components of Windows. More on those in a little bit.

In Windows 11, many administrative tools are still accessible within the Windows Tools folder in the Control Panel, essentially just continuing the functionality of the Administrative Tools folder from previous Windows versions like Windows 10. They have a slightly different name and location depending on the specific tool you need to access; the core functionality remains largely the same, however. Remember: Some functionality may not be present, or may be limited, depending on the Windows version, even if the control is still present (this is especially true of RDP).

What do you see when you start Windows? Some of the components that make up Windows include the following:

- **Desktop:** In Windows, the desktop environment is basically what you see on the screen—essentially, it *is* Windows, from a cosmetic standpoint. An example of the Windows desktop is shown in Figure 31.1, which shows the Start menu in the open position. The desktop is a key component of the GUI; it includes icons, wallpapers, windows, toolbars, and so on. It is meant to take the place of a person's physical desktop, at least to a certain extent, replacing calculators, calendars, notepads, and so on. Spend a minute looking at Figure 31.1, and then we'll talk about the various elements of the desktop. Note that Windows 10 and Windows 11 use similar desktop environments.

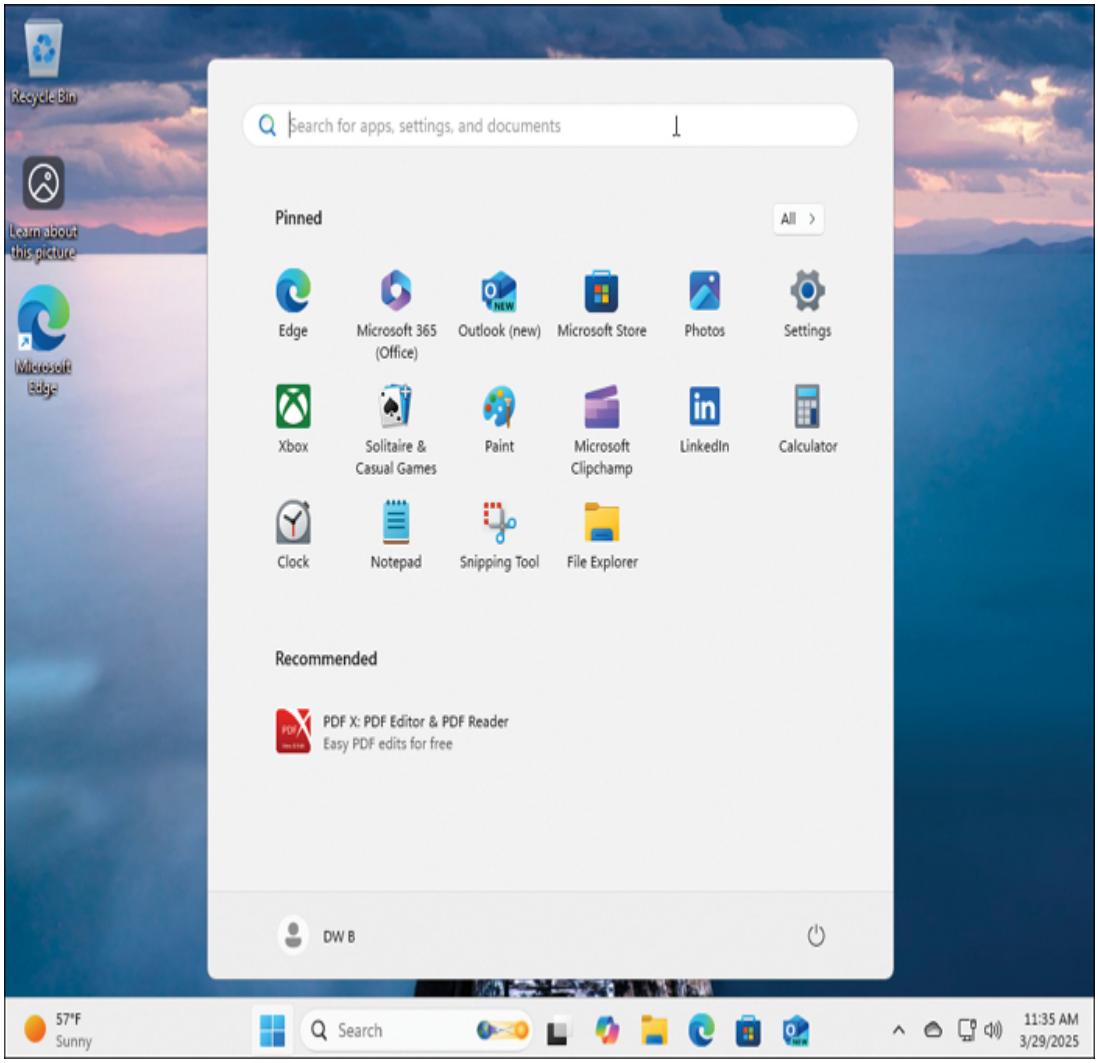


FIGURE 31.1 **Windows Desktop**

- **Icons:** Icons are the little clickable pictures you see on the desktop. They can be entire programs that run directly from the desktop, files that are stored directly on the desktop, or *shortcuts* that redirect to a program or file that is stored elsewhere in Windows. You can often tell that something is a shortcut because it has a little arrow in the lower-left corner of the icon. Shortcuts are small, usually around 1 KB to 4 KB in size, and store well on the desktop. However, storing actual files and programs on the desktop is not recommended because it can adversely affect the performance of the computer—and can quickly get really disorganized!

- **Start menu:** This is the main menu that is launched from the Start button. It contains a listing of all the tools within Windows and any Microsoft or third-party applications. From here, you can search for files and access the Control Panel. You can get anywhere in Windows from the Start menu. This menu shows who is currently logged on to the system and also enables you to log off, restart, shut down, or place the computer in sleep mode.
- **Taskbar:** This bar spans the bottom of the desktop. It houses the Start button, Quick Launch, any open applications, and the notification area (where applicable). It can be moved to the top or to any side of the desktop and can be resized. The taskbar and Start menu can be customized to just about any user's liking. To make modifications to these, right-click the taskbar and select **Taskbar settings**. From here, you can unlock/lock the taskbar, auto-hide it, and so on.
- **Search tool:** The Search tool is where you can search for files and applications. Use it! To open it, click in the search field area, click the magnifying glass, or press the Windows key and Q on the keyboard at the same time. (We'll refer to this shortcut simply as Windows+Q.) Then type whatever search you desire. Some versions of Windows will have artificial intelligence (AI), which can assist you in completing your work as well. We'll cover the implications of AI in Chapter 65, "Appropriate Use of Artificial Intelligence."
- **Pinned applications:** Windows enables you to "pin" applications or files to various locations in the GUI. You then have shortcuts to the applications and files. In the figure, the pinned applications exist on the taskbar. The beauty of pinned applications is that, by default, they are always visible, whereas shortcuts on the desktop background are covered up by open applications—if you have not hidden the Start menu, that is!
- **Notification area:** To the far right of the taskbar is the notification area, which houses the clock, volume control, network icon, battery power indicator, and so on. Also, if you click the show hidden icons symbol (^), you'll see the icons of applications that are running in the background. The more icons you see in the notification area, the more resources are used (in the form of memory and CPU power), possibly

making the computer less responsive. You can modify the notification area in the taskbar settings or by right-clicking the clock.

ExamAlert

Be able to identify the Windows icons, Start button, Start menu, taskbar, search tool, pinned applications, and notification area.

Today's versions of Windows can run side-by-side apps with the use of Snap technology. This means you can drag an application to an edge of the screen, and it will snap into place to inhabit that half of the display. A second application can be dragged in the same manner to the other side of the screen. This is an easy way to run two apps on the same screen without having to resize them manually. This feature becomes a bit more complex when you have multiple monitors, but, essentially, only the outer edges of the collective group of monitors can be used with Snap.

To actually do anything in Windows, you have to open a program (such as Calculator or WordPad) or a configuration window. Technicians are most concerned with the configuration windows. Be ready to work in Windows Settings, the Control Panel, and a variety of dialog boxes. For example, Figure 31.2 shows the Computer Name/Domain Changes dialog box, which was opened from System Properties. System Properties (not shown) runs as a process, and the Computer Name dialog box is just part of that overall process. A dialog box prompts a user for information—in this case, the name of the computer and the name of the network of which the computer is a member. You'll note that the network can be a workgroup (in a small office/home office) or a domain (in an enterprise business). This is just one example of many in Windows where you will configure the system.

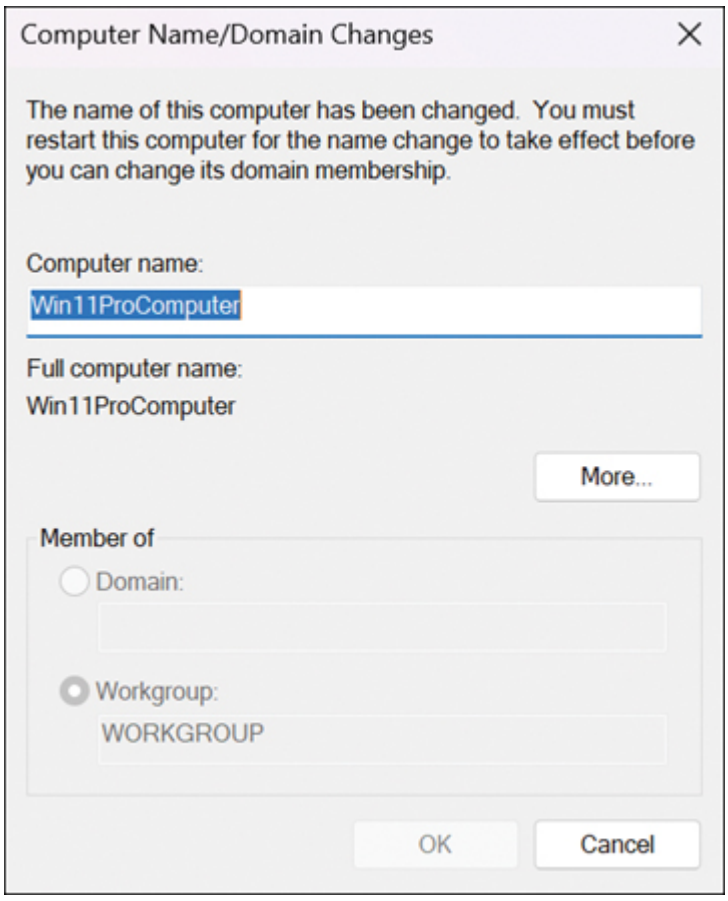


FIGURE 31.2 **The Computer Name/Domain Changes Dialog Box**

We have covered a lot of stuff in just a few pages. If you are not already familiar with Windows, we highly recommend that you practice navigating through the operating system and become accustomed to the desktop and all of its components.

Settings vs. the Control Panel

There are two main places in Windows that you can go to configure the system: Settings and the Control Panel. Over the past several years, Microsoft has been leaning toward using Settings by default over the venerable Control Panel. However, you will need to use each of them. Which one you use depends on the scenario, but you should be ready to work in both. To open Settings, simply click the **Start** button and then click the **Settings** gear, or use the Windows+I shortcut on the keyboard. There are several ways to open the Control Panel. One great way is to open the **Run** prompt and type **control**. By the way, to open the Run prompt, right-click the **Start** button and select **Run**, or use the Windows+R shortcut.

With both Settings and the Control Panel, finding what you want can at times be challenging. A potentially faster solution is to use the Search tool or the Run prompt to go directly where you want without all the navigation. For example, if you want to add the Hyper-V feature to Windows 10 Pro, open the Search tool and type **Turn on Windows features** (or just **turn**), and you will see that it searches for and finds **Turn Windows features on or off**, which you can just click to open. Alternatively, you could open the **Run** prompt and type **optionalfeatures**, which will take you directly to the same place.

We'll be working in both Settings and the Control Panel and will discuss them further as we progress through the book.

Windows Upgrade Paths

It's important for you to know which Windows operating systems can be upgraded to Windows 11, just in case you encounter an older system. Let's look at two scenarios and then summarize the various upgrade paths in a table (see Table 31.4).

TABLE 31.4 **Upgrade Paths to Windows 11**

From	To Windows 11 Home	To Windows 11 Pro	To Windows 11 Enterprise
Windows 10 Home	✓	✓	✓
Windows 10 Pro	—	✓	✓
Windows 10 Enterprise	—	—	✓
Windows 10 Pro Education	—	✓ (Education)	✓ (Education)

✓ = Full upgrade is supported, including personal data, settings, and applications.
— = Cannot upgrade to that edition.

In the first scenario, say that you work for an organization with a lot of older laptops running Windows 10 Pro. To be in alignment with organizational policy, all client systems should use Windows 11 Enterprise. As luck would have it, Windows 10 Pro can indeed be upgraded to Windows 11 Enterprise. However, whenever doing upgrades, you need to

make sure to back up all data (and applications) and be ready to supply a license/key for the software.

In the second scenario, say that you have a home user with a PC that has Windows 7 Home Basic installed; it's due for an upgrade. The user heard that the Enterprise edition of Windows 11 has lots of great features and asks you to upgrade to that edition. There's no "luck" here. Windows 7 Home Basic cannot be upgraded to Windows 11 Enterprise. That would require a *fresh* or clean installation, but as a reputable tech, you should discourage this path; chances are that the user does not need any of the features of Enterprise. The good news is that Windows 7 Home Basic can be upgraded to Windows 11 Pro, which is almost as good, especially for a home user—provided that the computer meets the minimum requirements. Or, you could convince the user to simply use Windows 11 Home. Always try to select an OS (and edition) with the consumer's best interests and needs in mind. And again, back up everything before you do any type of upgrade!

ExamAlert

Remember that a *clean install* of Windows completely wipes your hard drive and installs a fresh copy of the operating system; it erases all data and settings. An *in-place upgrade* updates your current operating system to a new version and preserves your existing programs, files, and settings; it doesn't format the hard drive.

Note

To save space in this book, we've listed some common upgrade paths, but the table is not complete. For more information about upgrade paths and *all* the possibilities, see https://docs.microsoft.com/en-us/windows/deployment/upgrade/windows-10-upgrade-paths.

You are probably wondering if you can upgrade the version of Windows from Home to Pro or Enterprise. The answer is “Yes!” Be sure to back up your files first! You can find details on how to do this at https://support.microsoft.com/en-us/windows/upgrade-windows-home-to-windows-pro-ef34d520-e73f-3198-c525-d1a218cc2818.

Windows 11

Most organizations have migrated to Windows 11. While you will see Windows 10 and earlier installations still, migrating to Windows 11 is an important step, and most organizations either have already migrated or will be doing so in the near future. There are several differences between Windows 10 and Windows 11, but they are fundamentally the same from a user standpoint.

Cosmetically, Windows 11 looks slightly different from Windows 10, as shown in Figure 31.3. The basic user interface functions the same.

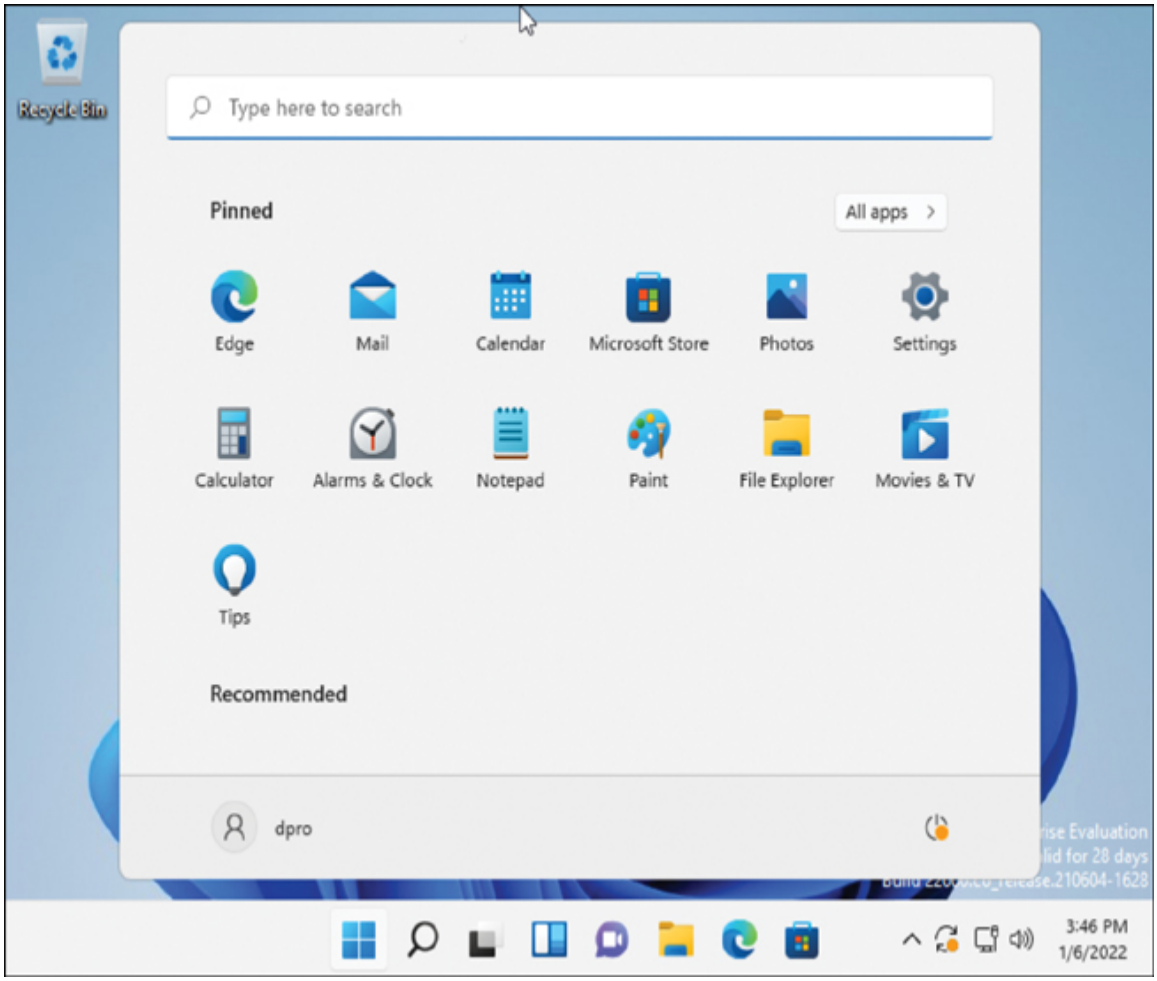


FIGURE 31.3 **Windows 11 Desktop**

In the figure, the Start button was clicked, displaying the centered Start menu (as opposed to the left-hand Windows 10 Start menu). By default, this shows the "pinned" applications, which are meant to be the most commonly used apps. For example, you can click on the Settings gear to open the Settings app, where you can make the necessary changes to Windows 11. (You'll note that Settings has been redesigned in Windows 11.) If you look at the taskbar, you'll see that the pinned apps are centered. These are the kinds of cosmetic differences that you will find in Windows 11.

However, for the most part, Windows 11 behaves in the same manner as Windows 10 when it comes to applications, Settings, the Control Panel, the Search tool, the Run prompt, PowerShell, and so on. And these are the things that are important for the exam.

Windows 11 editions are similar to Windows 10 editions (Home, Pro, Enterprise, etc.), and Windows 10 can be upgraded to Windows 11 easily.

Windows N

Windows 10 and 11 both come in N versions. N stands for Not with Media Player, and that's most of the difference: N operating systems ship without Windows Media Player and related applications. You can install those applications separately by installing the Media Feature Pack or a media player of your choice. Because many users are unaware of the difference, it can catch them unaware, so be ready for support calls from uninformed users who purchase a machine with a version of Windows N and are caught off guard. Luckily, it is a relatively simple fix to install the Media Feature Pack and get them on their way.

Windows 10 End of Support

Microsoft will end Windows 10 support in October 2025, so Windows 11 is Microsoft's focus. Be ready to support the cosmetically slightly different but architecturally similar Windows 11 in the field!

Cram Quiz

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

1. Which editions of Windows 11 offer Hyper-V? (Select three.)

   - ○ **A.** Windows 11 Home
   - ○ **B.** Windows 11 Pro
   - ○ **C.** Windows 10 Pro for Workstations
   - ○ **D.** Windows 11 Enterprise

2. Where should you go to find out what applications are running in the background in Windows?

- **A.** Taskbar
- **B.** Start menu
- **C.** Quick Launch
- **D.** Notification area
- **E.** Cortana

3. A customer requires a current operating system that can utilize 512 GB of RAM that is installed to a PC. Which of the following should you suggest? (Select two.)

- **A.** Windows 11 Home
- **B.** Windows 11 Pro
- **C.** Windows 8 Pro
- **D.** Windows 11 Enterprise

4. After a malware attack, a technician needs to completely wipe a customer's hard drive and install a fresh copy of the Windows 11 Pro. What should the technician do?

- **A.** Do an in-place upgrade
- **B.** Perform a malware scan
- **C.** Join the computer to a domain
- **D.** Do a clean install of Windows 11 Pro

5. Which of the following includes the same functionality as other editions of Windows, except for media-related technologies?

- **A.** Windows N
- **B.** Hyper-V
- **C.** Programs and Features
- **D.** BitLocker

6 A client wants to know if you can upgrade a Windows 10 Pro computer to Windows 11 Pro. The client's system has the following specifications:

Architecture: 64-bit

Processor: 1 GHz

Memory: 4 GB

Free hard disk space: 64 GB

Graphics card: Microsoft DirectX graphics device with WDDM 2.0 driver

Display: High-definition 720p

Additional hardware: UEFI and TPM 1.0

Does the client's system meet the minimum systems requirements for Windows 11 Pro?

- ○ **A.** Yes, all system requirements are met to upgrade to Windows 11 Pro.
- ○ **B.** No, upgrading to Windows 11 Pro requires 164 GB of free hard disk space.
- ○ **C.** Yes, with 64-bit architecture, anything is possible.
- ○ **D.** No, to upgrade to Windows 11 Pro, UEFI and TPM 2.0 are required.

Cram Quiz Answers

1. **B, C, and D.** Of the listed answers, Windows 11 Pro, Pro for Workstations, and Enterprise offer Hyper-V virtualization functionality. Windows 10 Home does not. Remember that just because Hyper-V is included as a feature doesn't mean it will work. The motherboard of the computer has to support virtualization; in addition, virtualization must be enabled in the BIOS/UEFI, and Hyper-V has to be enabled (turned on) within Programs and Features.

2. **D.** Go to the notification area to find out what applications are running in the background. (Another way is to use the Task Manager.) In Windows 11, click the arrow that points up to show hidden icons. In other versions of Windows, the applications might actually appear in the notification area itself.

3. **B and D.** You should suggest Windows 11 Pro or Enterprise to take advantage of the PC's 512 GB of RAM. Windows 11 Pro can access up to 2 TB of RAM, and Enterprise can access up to 6 TB (so you could say there is plenty of headroom here). However, Windows 11 Home can only access 128 GB of RAM—and that is not enough! And Windows 8 Pro can only access 192 GB of RAM. That wasn't mentioned in the chapter, but it doesn't matter because Windows 8 is *not current*. Support for Windows 8 ended in January 2023.

4. **D.** A clean install of Windows 11 Pro completely wipes your hard drive and installs a fresh copy of the operating system; it erases all data and settings. An in-place upgrade updates your current operating system to a new version and preserves your existing programs, files, and settings, meaning it doesn't format the hard drive. Performing a malware scan or joining a domain will not help in this scenario. A clean install of Windows 11 Pro is required here.

5. **A.** The N editions of Windows include the same functionality as other editions of Windows, except for media-related technologies, Windows Media Player, and certain preinstalled media apps. Hyper-V is a Microsoft virtualization program used to create and run virtual machines (VMs) on Windows systems. Programs and Features is a Windows tool used to manage updates and Windows programs. BitLocker is a Windows security feature used to encrypt an entire storage drive (or volume) to protect from unauthorized access.

6. **D.** The client's system does not meet the minimum system requirements to upgrade the Windows 10 Pro computer to Windows 11 Pro. The additional hardware requirement to upgrade

to Windows 11 Pro is UEFI and TPM 2.0. Microsoft states that "TPM 2.0 is a 'non-negotiable' requirement for Windows 11. TPM stands for Trusted Platform Module, and it's a secure cryptoprocessor that stores encryption keys and performs other cryptographic functions. Windows uses TPM 2.0 for security-related features like: Windows Hello for identity protection, BitLocker for data protection, and Secure Boot."

Great job! We suggest you review the chapter and make sure you have a Windows system of some sort to practice on.

Chapter 32

Microsoft Operating System Features and Tools, Part I

This chapter covers a portion of the following A+ 220-1202 exam objective:

- **1.4** – Given a scenario, use Microsoft Windows operating system features and tools.

Now let's move into the graphical side of things. The Windows GUI is popular because users are familiar with it, and for many people, its usage is intuitive—meaning it comes naturally. However, there are a lot of utilities, tools, and features for an administrator to know. In fact, there are so many utilities that we have split coverage of this objective into two chapters. In this chapter, we'll cover the Task Manager and a bunch of administrative Windows tools that you can incorporate into the Microsoft Management Console (MMC). This is super important stuff for the exam, so let's not waste any time.

ExamAlert

This portion of **Objective 1.4** concentrates on the Task Manager and the Microsoft Management Console (MMC) snap-in. Chapter 33, "Microsoft Operating System Features and Tools, Part II," will concentrate on Disk Management and additional tools (such as Resource Monitor, System Configuration, and Regedit).

Task Manager

One simple and effective tool to use when analyzing a computer is the Task Manager. Besides using the Search tool, there are several other ways to open the Task Manager, including

- Right-click the taskbar (or **Start**) and select **Task Manager**.
- Press Ctrl+Alt+Del and select **Task Manager**.
- Open the **Run** prompt and type **taskmgr**.
- Press Ctrl+Shift+Esc. (For keyboard shortcut hounds, this is often a favorite way to open the Task Manager.)

The Task Manager enables you to analyze a computer's processor and memory performance in real time; this can be done from the Performance tab, as shown in Figure 32.1, and the Processes tab, shown in Figure 32.2. You can see on the Performance tab that the CPU usage fluctuates and is currently at 10 percent. More importantly, the Processes tab shows that the Firefox and Chrome browsers are using the bulk of the memory on that system.

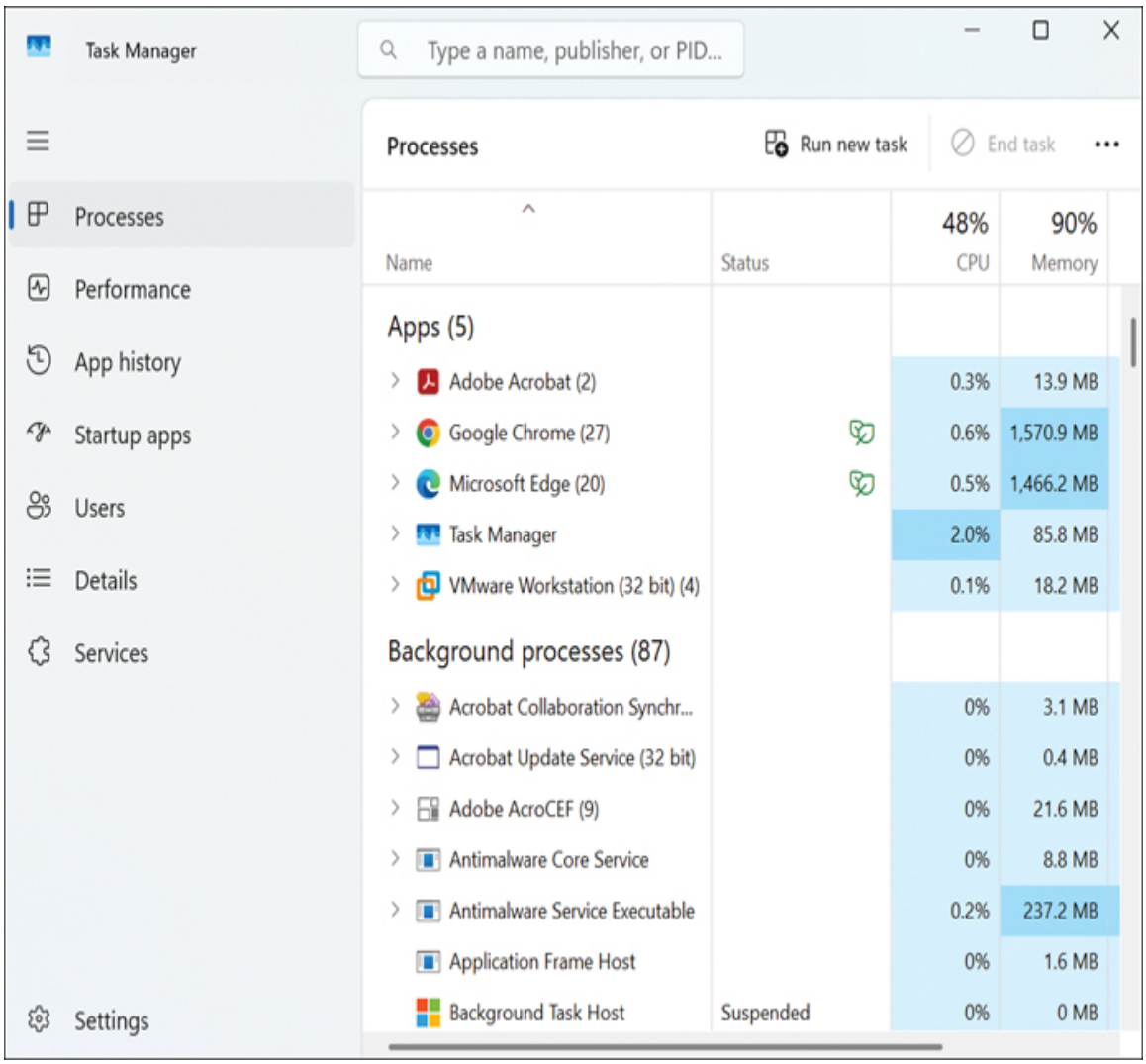


FIGURE 32.1 **Windows Task Manager, Showing the Processes Tab**

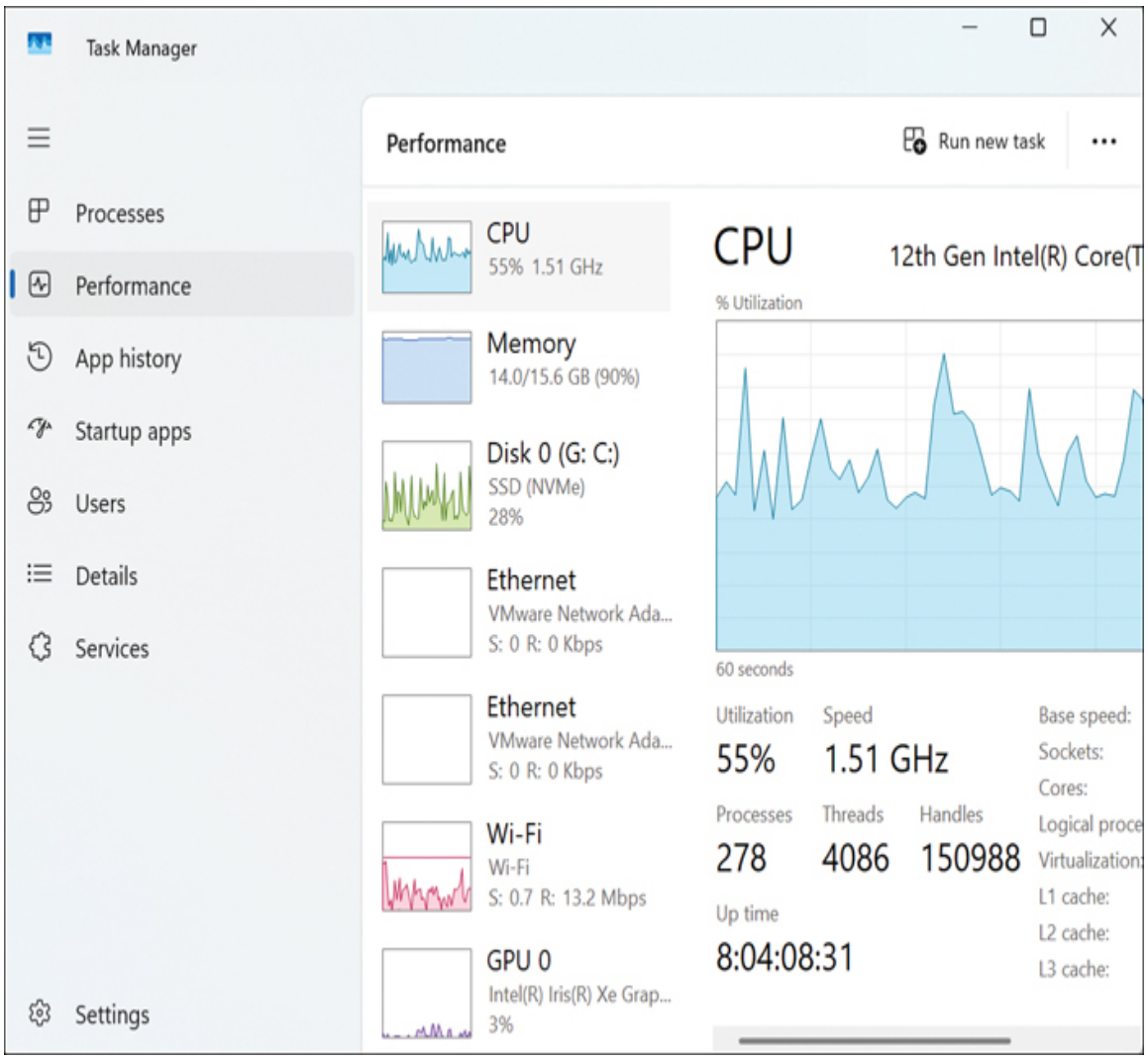


FIGURE 32.2 **Windows Task Manager, Showing the Performance Tab**

Optimizing a system can be as simple as shutting down programs. You can do this in the Processes tab. But sometimes you need to shut down underlying processes. For example, the Processes tab in Figure 32.1 shows all the processes that are running and the amount of CPU and RAM resources they are using individually. You can stop a process that is hoarding resources by right-clicking it and then selecting **End Task**. (You can also stop processes on the Details tab.) Keep in mind that this method shuts down the process or application only temporarily. If the process or application is designed to do so, it will turn back on when the computer is rebooted.

ExamAlert

Understand how to open the Task Manager; how to access and read its Processes, Performance, App history, Startup Apps, Processes, Users, Details, and Services tabs; and know how to end processes and applications.

The Task Manager has several other tabs, including Users, Startup apps, Services, and App History. Let's briefly discuss each of them.

The Users tab shows the resources being used by each user. Normally, on a Windows client computer, this tab shows only the user who is currently logged in. However, if another user is listed, and that account is using resources, then that user can be signed off from here (by right-clicking the username and selecting **Sign off**). This way, the resources are freed up. For example, if a remote user was connected previously and chose to disconnect instead of logging off, this tab shows that user as "Disconnected," but the user might still be using memory resources if some programs were opened before the user disconnected. This is common with Remote Desktop sessions. There is a difference between *disconnecting* and *logging off*. When you disconnect, the programs and resources are left open, allowing you to reconnect later and continue where you left off; when you log off, the programs are closed, and the resources are freed up.

The Startup apps tab shows applications in Windows, their status, and their startup impact. *Status* means whether the application is enabled or disabled. If it is enabled, then it will start every time the computer starts. If it is disabled, it won't. You can enable or disable the applications by right-clicking on them. *Startup impact* means how much of the system's resources are being used during the startup process. For example, you might see that an application has a low impact, which means it won't use too many resources on that system.

The Services tab displays any services that are available in Windows. Services are underlying programs used by applications and by Windows. There are a great many of them, but you don't need to know them all for the exam. You do need to know how to start and stop them, though. Some run

automatically, and others do not. Consider the Spooler service (Print Spooler), for instance. This service runs when Windows starts, but in some cases, you might need to stop it. Simply right-click the service to stop it. From there, you can also start it (run it), or you can do both successively by clicking **Restart**. This tab shows the process IDs (PIDs), which are numbers associated with the services that are running. (You'll learn more about PIDs later, in Chapters 53 through 56.) Although you can start and stop services here, you cannot enable or disable them. To start or stop a service, you need to right-click the service and select **Open Services**. That takes you to the Services console window, where you can start, stop, enable, disable, and more. You can get to the Services console window directly by going to **Run** and typing **services.msc**. (You'll learn more about this later in this chapter.)

The App History tab shows the applications that have run and the CPU and network resources used by each application. This tab differs from the Processes tab in that it shows cumulatively used resources, not real-time resources.

> **Note**
>
> Work with the Task Manager on your system and get to know the program. You will be using it often when troubleshooting systems.

The MMC and Administrative Windows Tools

Most of the tools used to make changes to settings on your system have been moved to the Settings app. However, some functions are still found only in the Windows administrative tools, and some older tools might be more familiar to technicians and other computer administrators (that's you!). Access to these tools has moved to the Windows Tools applet in Windows 11 (it is still called Administrative Tools up to Windows 10). The core functionality of most tools remains the same.

Figure 32.3 shows Windows Tools in Windows 11.

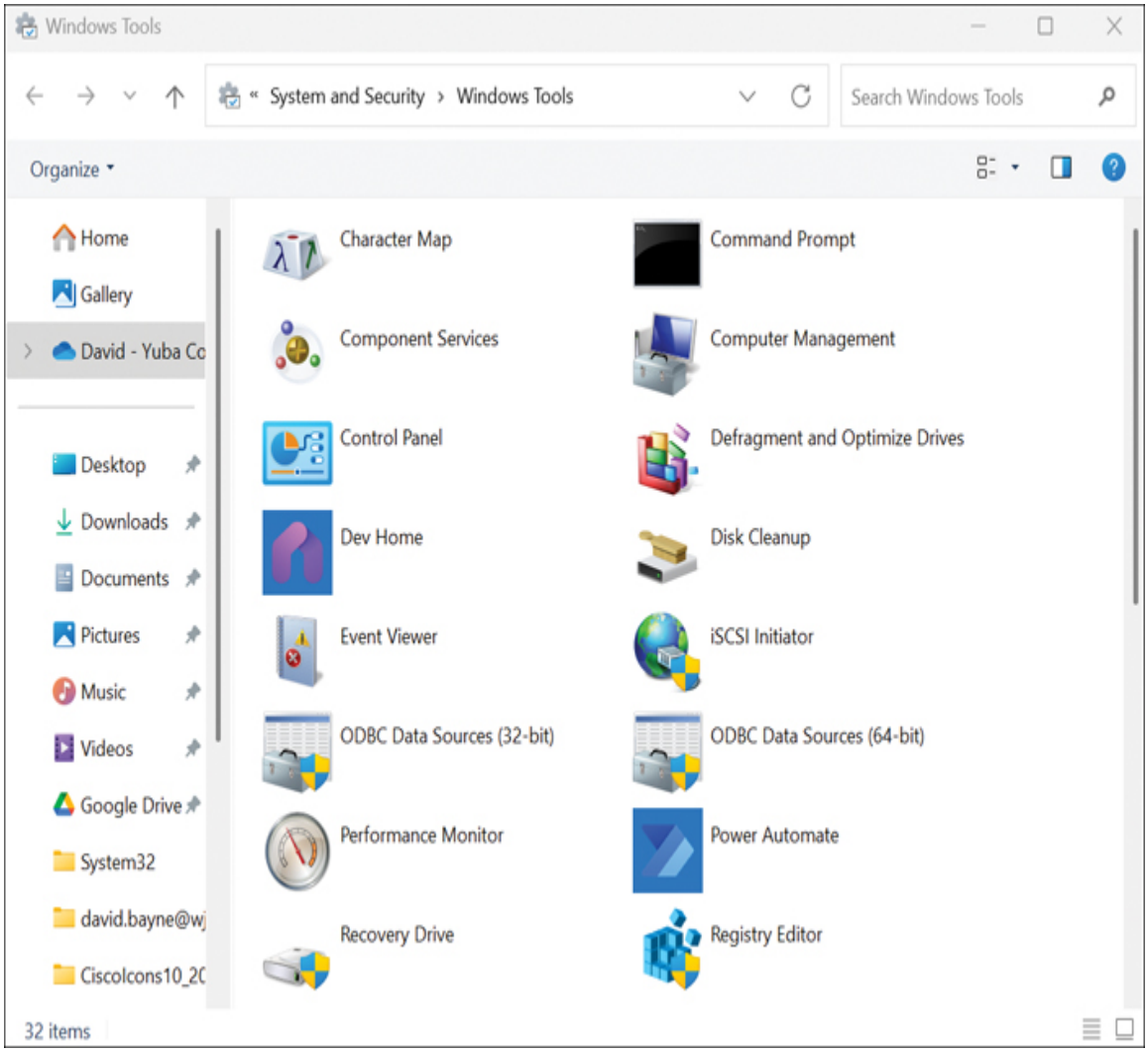


FIGURE 32.3 **Windows Tools in Windows 11**

You can access Windows Tools in several ways:

- Use the Microsoft Management Console (MMC), which is the console that houses all the other console windows. It's super-customizable. You'll learn more about the MMC in just a bit.
- Select **Start > Search > Enter Windows Tools**.
- Select **Control Panel > All Control Panel Items > Windows Tools**.
- Go to **Run** and type **control admintools**. This opens Windows Tools.

Note

For a table of the Run window commands covered in this book (and more), see https://greencurtaintraining.com.

The MMC

Console windows such as the Device Manager, Event Viewer, and Performance Monitor can be grouped into one super console window known as the Microsoft Management Console (MMC). The MMC acts as a shell for these other console windows. You can also use it to control remote computers in addition to the local computer. And you can control what particular users see by changing the Console Mode. Finally, part of the beauty of the MMC is that it saves everything you add and remembers the last place you worked. To create an MMC window, open the Run prompt or Search tool, type **MMC**, and press Enter. By default, the MMC window is empty.

Note

You will learn quickly that administrative functions should be carried out only by users who have administrative privileges. Even if you have administrative privileges, a pop-up User Account Control (UAC) window appears every time you try to access tools such as the MMC. Simply click **Yes** or **Continue** to open the program. Users who don't have administrative capabilities will either be blocked altogether or will have view-only access to the tools.

To add consoles (known as snap-ins), do the following:

1. On the menu bar, click **File** and then click **Add/Remove Snap-in**. The Add or Remove Snap-ins window appears.

   Select the components you want from the left by highlighting them one at a time and clicking the **Add** button. In some cases, you will

need to select the local computer or a remote computer. Click **OK** when finished. These snap-ins should now be shown inside the Console Root. Figure 32.4 shows an example of the MMC.

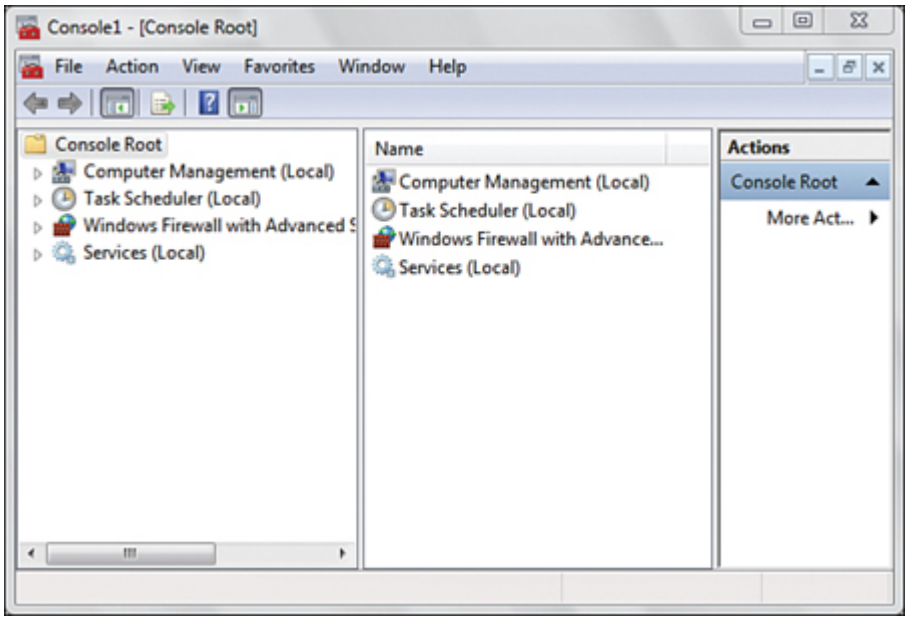


FIGURE 32.4 **The MMC**

2. Save the MMC. By default, this window prompts you to save to the Windows Administrative Tools folder of the user who is currently logged on. For easier retrieval of the MMC, consider saving it to a more accessible folder.

You can now access the console you created by navigating to the folder where you saved it. We suggest adding a shortcut to it within the Quick Launch for easy access. Or, once again, go to Run, Search, or the command line and type **MMC**. Click **File**, and you should see your console in the history list. Or you can open the specific MMC file directly from Run. For example, if you saved the file as console1.msc in the root of the C: drive, then you type

```
mmc C:\console1.msc
```

The Windows Tools (formerly Administrative Tools) discussed in this chapter can be added to the MMC. You should practice using the MMC. It will help your workflow and can be a real time-saver.

ExamAlert

Exam Objective 1.4 specifically calls out the Event Viewer (eventvwr.msc), Disk Management (diskmgmt.msc), Task Scheduler (taskschd.msc), Device Manager (devmgmt.msc), Certificate Manager (certmgr.msc), Local User and Groups (lusrmgr.msc), Performance Monitor (perfmon.msc), and Group Policy Editor (gpedit.msc) MMC snap-ins. Be sure you know how to add and use each of them!

Event Viewer

Applications are both a boon and a bane. They serve a purpose, but sometimes they are prone to failure. The operating system itself also can cause you grief by underperforming, locking up, or causing other intermittent issues. One good tool for analyzing applications and the operating system is the Event Viewer.

The Event Viewer (eventvwr.msc) tells a technician a lot about the status of the operating system and programs. It notifies you of any informational events or audits, warns about possible issues, and displays errors as they occur. Aside from accessing it from the Windows Tools folder, you can access it by typing **eventvwr.msc** in the Run or Search prompts or by right-clicking the **Start** button. Try opening it on your system!

Note

The extension .msc is used for a Microsoft Management Console snap-in control file, also known as a Microsoft console window. As mentioned, this and many of the other tools we'll discuss in this chapter can be added to the MMC as snap-ins. We recommend that you add them to your MMC so that you can get to them easily while you are studying.

Figure 32.5 shows an example of the Event Viewer. You can see that this console is a three-pane window. The left pane shows all of the places you might navigate to in the Event Viewer, including Custom Views and Windows Logs. The middle pane shows the details of whatever you click in the left pane. The right pane provides additional actions, which are also available on the menu bar. Many of the console windows use this three-pane design.

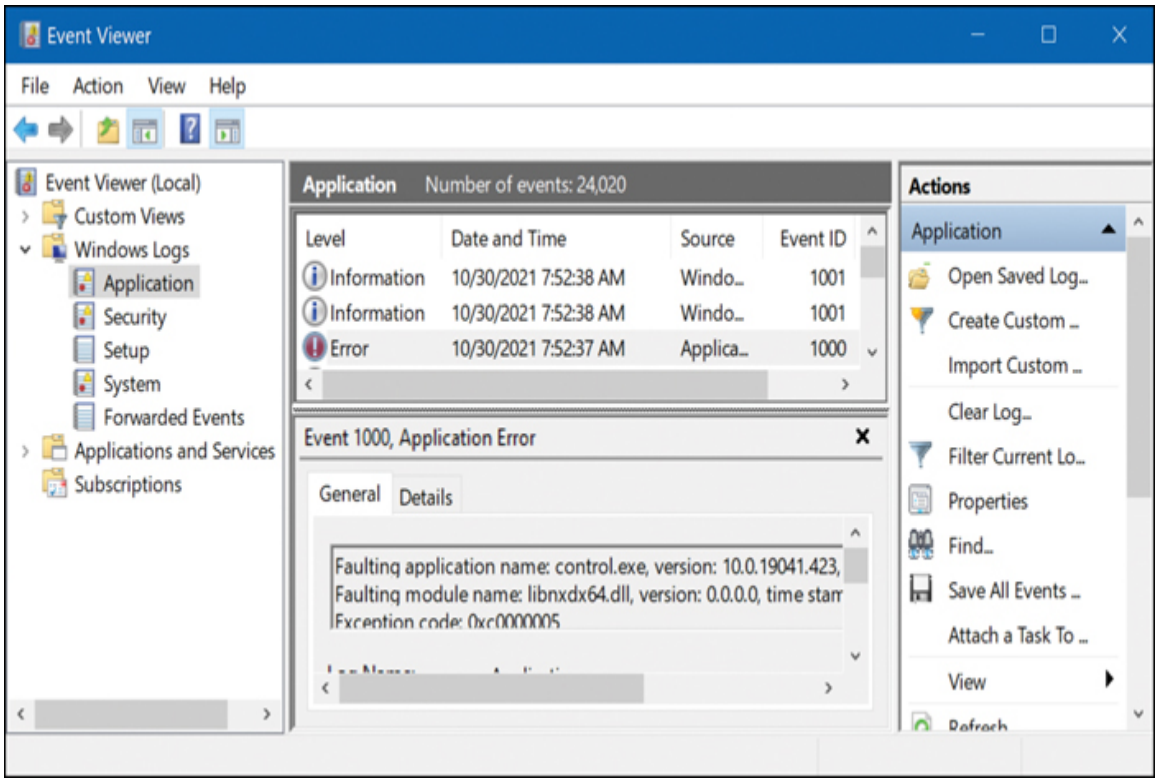


FIGURE 32.5 **The Event Viewer**

In the Event Viewer, information entries, auditing entries, warnings, and errors are stored in several log files within the Windows Logs folder. There are three main log files that you should know for the exam:

- **System:** The System log contains information, warnings, and errors about hardware, device drivers, system files, and so on. This log deals primarily with the operating system.
- **Application:** The Application log contains events about programs that are built into Windows, such as the Command Prompt and File

Explorer, and might contain information about applications that have been loaded since the operating system was installed.

- **Security:** The Security log holds information gathered for auditing and security purposes; for example, it might log who logged on to the computer or who tried to gain access to a particular file.

You can view an event listed in a log file by double-clicking it. Events are organized into four categories:

- **Information:** These entries, indicated by a letter *i* in a circle, give you basic information about a service starting or an application that ran successfully. The log files are usually chock-full of these entries as part of the normal operation of the system.
- **Warning:** These entries, indicated by an exclamation point (!) within a yellow triangle, might be messages telling you an installation did not complete or a service timed out. You should check for these entries now and again and investigate them if nothing else is pressing.
- **Error:** These entries, indicated by an exclamation point (!) in a red circle, mean that something failed or has been corrupted, a service failed to start, and so on. Errors should be investigated right away.
- **Audit success:** These entries, indicated by a gold-colored key, are located within the Security log file. They track what a user attempts to accomplish within the operating system. For example, if auditing was turned on for a specific folder and a person attempted to access that folder, a security event would be written to the log, especially if the person was denied access. Auditing entries are maintained by organizations so that they can trace what happened to deleted or modified data.

In Figure 32.5, you can see that the Application log is open. In the middle pane, you can see a highlighted application error. It tells you that that there was a faulting application named control.exe. It gives the event ID 1000. Essentially, this means the Windows Control Panel crashed. If this happens once in a while, it might not be a big deal, but if it happens often, you need to troubleshoot the problem further. (You'll see this type of troubleshooting in Chapter 53, "Troubleshooting Microsoft Windows.")

You can find more information about a specific error code by either typing the code number for the event or typing the description into Microsoft Help and Support: https://support.microsoft.com. You never know when an error might occur, so you should review the Event Viewer logs regularly. You can erase an entire log by right-clicking the log file (for example, System) and selecting **Clear Log**. The program asks if you want to save the log for future viewing. By right-clicking a log and selecting **Properties**, you can modify the maximum size of the log and disable logging altogether.

ExamAlert

Be able to describe the Event Viewer's System, Application, and Security log files as well as the information, warning, error, and audit success events.

Task Scheduler

The Task Scheduler (taskschd.msc) can run particular programs, send emails, or display messages at scheduled times designated by the user. You can open it from the Windows Tools (formerly Administrative Tools) folder or the Search tool, and you can also open it by going to **Run** and typing **taskschd.msc**.

Note

In Windows 11, administration tools are still accessible within the Windows Tools folder in the Control Panel, essentially just continuing the functionality of the Administrative Tools folder from previous Windows versions like Windows 10, with a slightly different name and location depending on the specific tool you need to access. The core functionality remains largely the same.

Once in the Task Scheduler, you can set up basic scheduling, specify certain conditions and triggers that cause tasks to run, and tell the Task Scheduler

which actions to take when a task starts. Plus, there are a bunch of built-in preprogrammed tasks in the Task Scheduler Library—from memory diagnostics to Disk Cleanup. Instead of reinventing the wheel, consider using one of these tasks to automate processes. Some of these built-in tasks are enabled by default. Try scheduling some tasks yourself, such as memory diagnostics, Chkdsk (disk repair), and time synchronization.

Device Manager

A computer probably has a dozen or more devices that all need love and attention. Taking care of a computer means managing these devices. The primary tool a technician uses to manage devices is the Device Manager.

There are a few ways to open the Device Manager:

- Use the Search tool, type **Device Manager**, and press Enter.
- Select **Settings > System > About** (and other locations in Settings).
- Use the Control Panel (in icons mode).
- Right-click **Start** and select **Device Manager**.
- Open the **Run** prompt and type **devmgmt.msc**.

When the Device Manager opens, as shown in Figure 32.6, notice the categories for each type of device. By expanding any one of these categories, you can see the specific devices that reside in your computer.

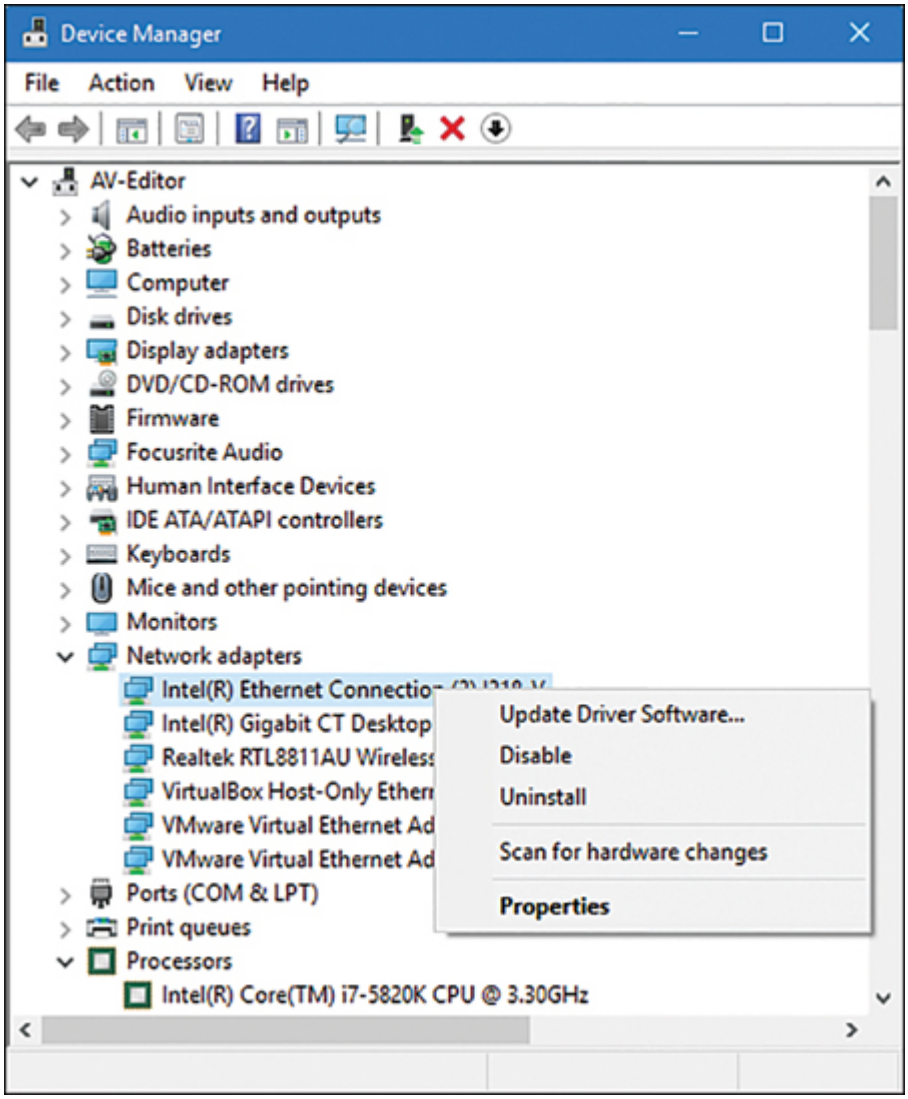


FIGURE 32.6 **Device Manager**

By right-clicking a specific device, you can update its driver; enable or disable it; uninstall it altogether; check for any hardware changes; or access additional properties, such as the driver details and resources used by the device. Figure 32.6 shows the menu that appears when you right-click a network adapter. These are the standard options, but you might have more or fewer options, depending on the device you right-click.

ExamAlert

Know how to access the properties of a device, install drivers, and enable/disable devices in the Device Manager.

Windows attempts to install drivers automatically when it recognizes that a device has been added to the system. If this doesn't work, you can go to the website of the device's manufacturer to download the latest version of the driver. This is especially true when dealing with video, audio, and storage controller drivers, because these drivers are frequently updated and you need the latest version for your device to work properly.

If you're still having trouble with a device even after updating the driver, you can roll back the driver to a previously installed version on the Driver tab of the Device Manager, as shown in Figure 32.7. In Figure 32.7, we cannot roll back our driver so that selection is greyed out; there is either not a prior version or it has been too long since we installed the updated driver. In that case, you can try uninstalling the driver entirely and then downloading a fresh driver from the manufacturer's website.

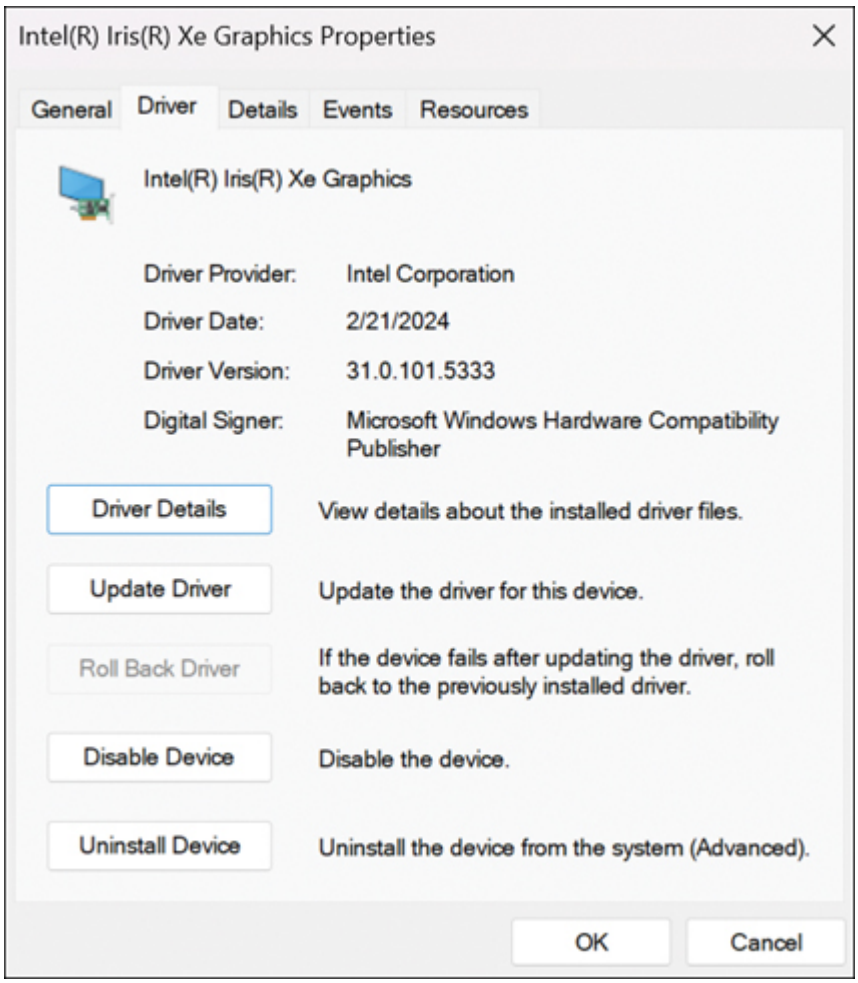


FIGURE 32.7 **The Driver Tab in Device Manager**

ExamAlert

Device Manager uses certain symbols that appear next to a device's name to offer informational details about a particular error condition with a device. A white circle with a black downward-pointing arrow means that a device is disabled. A yellow triangle with a black exclamation point means a device is in a problem state, usually related to a missing or outdated driver. A white circle with a blue question mark means that Windows cannot identify a device, most often because of a missing driver or incompatible device driver.

> **Note**
>
> Device Manager troubleshooting is covered in Chapter 53.

Certificate Manager

The Certificate Manager displays all security certificates that are installed in Windows. Certificates help secure your applications and connections to websites. You can open the Certificate Manager by going to **Run** and typing **certmgr.msc**. Digital certificates are part of a public key infrastructure (PKI) in which digital certificates, certificate authorities, and other registration authorities verify and authenticate the validity of each party involved in an electronic transaction through the use of public key cryptography. The certification authority issues certificates, and each certificate has a set of fields that are validated with a public key. The certificate authenticates the identity of the owner of the certificate to others, and these certificates are managed in Windows by the Certificate Manager. If you look at the certificates stored in the Certificate Manager, you will see that each has an expiration date as well as information about the issuer and how they can be used. Some certificates have many keys; others might have only one or a few.

Local Users and Groups

You can access the Local Users and Groups utility by going to **Run** and typing **lusrmgr.msc**.

Although you can add users within Settings or the Control Panel, Local Users and Groups is the place where you go if you want to take more control of user account management. From here, you can add users, change passwords, group users together, or take advantage of built-in Windows groups such as Backup Operators and Performance Monitor Users. We'll look at Local Users and Groups in Chapter 45, "Windows Security Settings."

Performance Monitor

There are several tools you can use to track the performance of a Windows-based computer. Performance Monitor is an extensive program that can track how much your devices are utilized, such as the percentage of the processor that is used or how much RAM is currently being accessed. Performance Monitor uses real-time graphs to track usage and can log the information for later viewing. You can access it from the Windows Tools folder or by going to **Run** and typing **perfmon.msc**. Figure 32.8 shows an example.

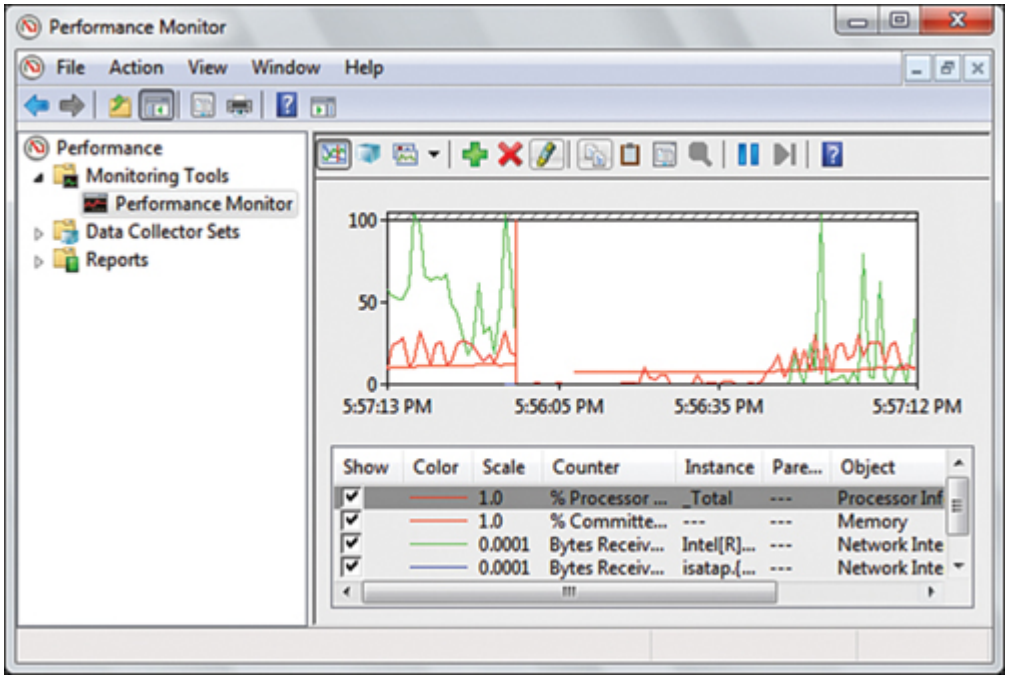


FIGURE 32.8 **Performance Monitor in Windows**

By working with Performance Monitor, you can track the usage of any device in a computer (known as an *object*) using a variety of measurements (known as *counters*). By default, this screen tracks only the CPU. By clicking the green + sign toward the center top of the toolbar at the top of the chart, you can add devices to track. Figure 32.8 shows that we added the default counters for memory and the network adapter card. The highest spikes are from the network adapter, which is sending and receiving a lot of data over the Internet. The second-highest levels are from the processor, which is running seven real-time applications simultaneously.

Information can be viewed in different formats, such as line charts and histograms, and can also be viewed and saved in Report view. Information can be exported as well. Any objects that are added in this program are not saved when you close the window, but you can configure the program so that it saves your additions. To do so, just add the Performance Monitor snap-in to your MMC. The MMC saves its contents and remembers the last place you were working. This feature works great if you will be analyzing the same things day in and day out.

Performance Monitor (and similar Windows applications) can tell you a lot about the functionality of your computer. When you're troubleshooting why a certain piece of hardware isn't living up to its promise, Performance Monitor can be invaluable.

Note

Other tools that you can use to track resource usage include the Resource Monitor (**Run > resmon.exe)** and the Performance tab of the Task Manager, although they are not as thorough as Performance Monitor, nor do they have the ability to save the tracked resource usage. Some tools, like resmon.exe, require administrative permissions to even view the data.

Group Policy Editor and Local Security Policy

The Group Policy Editor is the tool where you make the rules—or configure the rules put forth by your organization. The Group Policy Editor is used to configure rules for a computer system and its users. You can access it by going to **Run** and typing **gpedit.msc**. When it opens, the title bar of the console should read Local Group Policy Editor.

Note

If you want to add the Group Policy Editor to your MMC, go to **File > Add/Remove Snap-in**, click **Group Policy Object Editor**, and

then click **Add**. For the Group Policy Object, you will see Local Computer. Leave that as is and click **Finish**.

When you open the Group Policy Editor, you see Local Computer Policy, which has two main sections—Computer Configuration and User Configuration—each with Software Settings, Windows Settings, and Administrative Templates. As you can imagine, hundreds of settings are available here.

One section that you will probably use often is Local Security Policy. You can access this section in three ways:

- In the Group Policy Editor, navigate to **Computer Configuration > Windows Settings > Security Settings**.
- Open it from the Windows Tools folder.
- Access **Run** and type **secpol.msc**.

In Local Security Policy, you can configure policies for passwords, account lockout, encryption keys, software restriction, and much, much more. If you use Local Security Policy frequently, you can add it as a snap-in to the MMC. But remember, the content within the Local Security Policy is only a subset of the entire Local Group Policy Editor content. We'll be revisiting both of these issues in the security section of this book.

Services

The Services console window is another place where you can go to start, stop, and restart services such as the Print Spooler or Microsoft Defender Firewall. You can access it directly from the Windows Tools folder and from **Run > services.msc**. For example, if the Microsoft Defender Firewall service is interfering with another application, you can stop the service from the Services console window and see if that fixes the problem (at least temporarily). In the Services console, it's known as Microsoft Defender Firewall. You can also stop the service in the Task Manager, as mentioned earlier. In that case, you can search for Microsoft Defender Firewall (shown

in the Name column) or mpssvc (shown in the Service name field of the Microsoft Defender Firewall Properties dialog box). See Figure 32.9 for an example of Microsoft Defender Firewall Properties in the Services.msc console.

Note

As of Spring 2025, Microsoft was in the process of renaming Windows Defender Firewall to Microsoft Defender Firewall, and both names appear in Windows. They are the same product. When we reference them in this book, either in text or in images, know that it's because the versions of Windows we're using are, like yours, updated frequently and sometimes the names change daily. Eventually we believe that the new name will become Microsoft Defender Firewall, so have attempted to standardize on that name throughout the book, but you might see the other name sometimes, as in Figure 32.9.

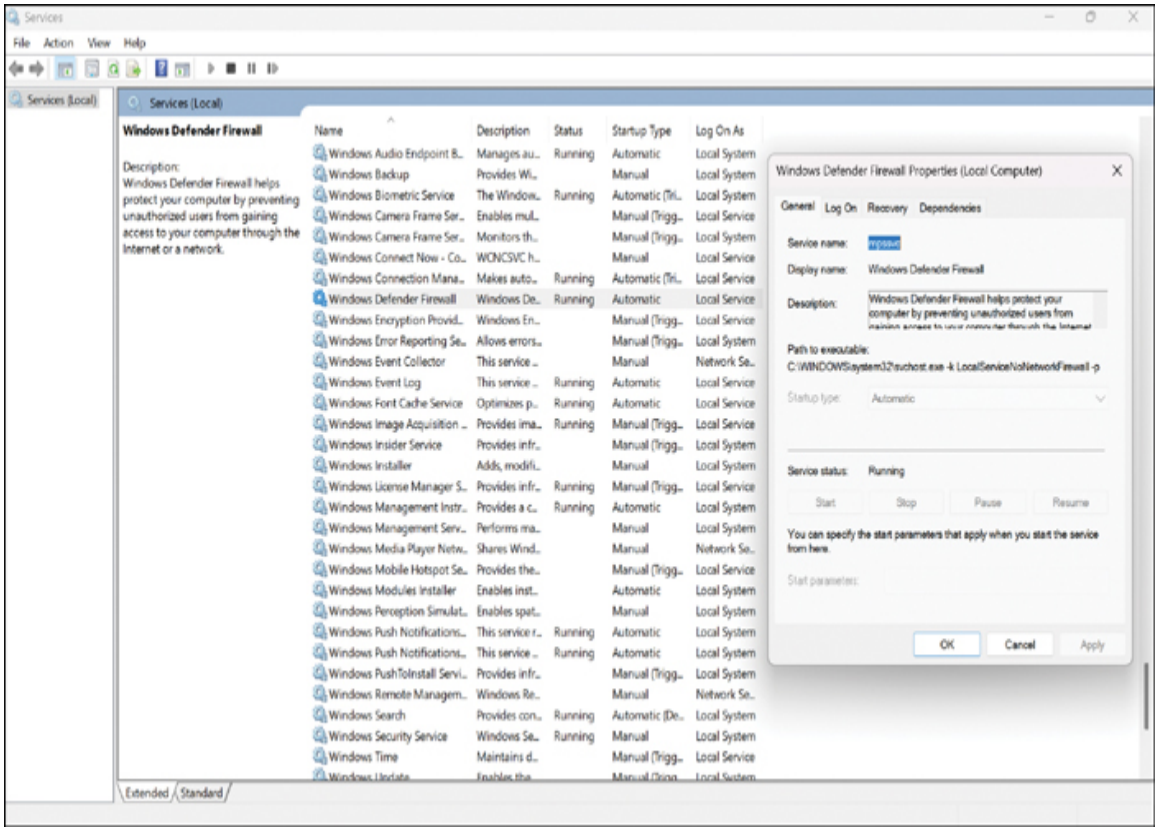


FIGURE 32.9 **Microsoft Defender Firewall Properties in the Services.msc Console**

You can also configure a service's startup type to be automatic, manual, or disabled. This configuration is persistent—meaning the startup type will remain every time the system reboots. It's important to understand the difference between *starting/stopping* services and *enabling/disabling* services. Essentially, starting/stopping is not persistent, whereas enabling/disabling is persistent (for the most part). You'll work with the Services console window more in the software troubleshooting section of the book.

Bonus Tool: Computer Management

We've already discussed a lot of tools. One tool that groups many of them together is Computer Management. It has many utilities loaded into one nice little console window, including the Task Scheduler, Event Viewer, Local Users and Groups, Device Manager, Services, and Disk Management. If you plan on using more than one of these tools on a consistent basis, consider using the Computer Management console window.

There are a few ways to open this window:

- Use the Windows Tools folder.
- Open the **Run** prompt and type **compmgmt.msc**.
- Right-click **Start** and then click **Computer Management**.

You can also add Computer Management to your MMC. It's one of the first things we do with a new Windows system. By using Computer Management and the MMC, you can increase your productivity when working in Windows.

Note

This chapter does not cover all of the Windows Tools (formerly Administrative Tools) yet, but you will learn about more of them as

you progress through the book.

Cram Quiz

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

1. Which of the following do you type in the Run prompt to open the Device Manager?

   - **A. mmc**
   - **B. secpol.msc**
   - **C. cmd**
   - **D. devmgmt.msc**

2. Which of the following would you use to track the percentage of resources being used?

   - **A. devmgmt.msc**
   - **B. eventvwr.msc**
   - **C. compmgmt.msc**
   - **D. perfmon.msc**

3. Where can a user go to start and stop services in Windows? (Select all that apply.)

   - **A. gpedit.msc**
   - **B.** Task Manager
   - **C. services.msc**
   - **D.** Command Prompt

4. Which log file in the Event Viewer contains information concerning auditing?

- ○ **A.** System
- ○ **B.** Application
- ○ **C.** Local Users and Groups
- ○ **D.** Security

5. Which tool can run particular programs at times designated by the user?

- ○ **A.** Services
- ○ **B.** Task Scheduler
- ○ **C.** Event Viewer
- ○ **D.** Task Manager

6. A technician sees a device with a white circle and a black downward-pointing arrow next to its name in Device Manager. What does this mean?

- ○ **A.** The device has a missing or outdated driver.
- ○ **B.** Windows cannot identify the device.
- ○ **C.** The device is working properly.
- ○ **D.** The device is disabled.

7. A client calls you in a panic after installing a new graphics card driver that isn't working properly. What do you suggest the client do to restore to the previous driver that worked?

- ○ **A.** Select **Device Manager > Update Driver**.
- ○ **B.** Select **Device Manager > Roll Back Driver**.
- ○ **C.** Select **File > Add/Remove Snap-in**, click **Group Policy Object Editor**, and then click **Add**.
- ○ **D.** Open the Run prompt and type **perfmon.msc**.

Cram Quiz Answers

1. **D. devmgmt.msc** is the Microsoft console window known as Device Manager. **mmc** opens a new blank Microsoft Management Console. **secpol.msc** opens the Local Security Policy window. **cmd** opens the Command Prompt.

2. **D. perfmon.msc** (or **perfmon.exe**) opens the Performance Monitor utility, which is used to graphically track the resources that are being used on a computer, such as CPU and RAM. You could also use **Task Manager > Performance** to track resource usage (but without the ability to save the data), as well as the Resource Monitor. **devmgmt.msc** opens the Device Manager. **eventvwr.msc** opens the Event Viewer. **compmgmt.msc** opens the Computer Management console window.

3. **B, C, and D.** You can start/stop services in **Task Manager > Services**, in the Services console window (services.msc), and in the PowerShell/Command Prompt by using the **net start**, **net stop**, **sc start**, and **sc stop** commands. **gpedit.msc** brings up the Group Policy Editor in Windows.

4. **D.** The Security log contains information about auditing and other security events. The System log contains information about the OS and system files. The Application log contains information about built-in Windows programs and some third-party programs. Local Users and Groups is an administrative tool you can use to add people and systems to the local computer.

5. **B.** The Task Scheduler can run particular programs at scheduled times designated by the user. The Services console window enables you to start, stop, and restart services. The Event Viewer is used to find messages about the system, applications, and security developments. The Task Manager is used to analyze the performance of a system and view the applications and services that are running.

6. **D.** Device Manager uses certain symbols that appear next to a device's name to offer informational details about a particular error condition with a device. A white circle with a black downward-pointing arrow means that a device is disabled. A yellow triangle with a black exclamation point means a device is in a problem state, usually related to a missing or outdated driver. A white circle with a blue question mark means that Windows cannot identify the device, most often because of a missing driver or incompatible device driver.

7. **B.** If a device fails after updating its driver, you can roll back to the previously installed driver that worked using the Device Manager Roll Back Driver feature. If you want to add the Group Policy Editor to your MMC, go to **File > Add/Remove Snap-in**, click **Group Policy Object Editor**, and then click **Add**. Going to Run and typing **perfmon.msc** opens the Performance Monitor.

Marvelous! This is a pretty power-packed chapter. You are doing very well. Be sure to review your notes, take a break, and then continue!

Chapter 33

Microsoft Operating System Features and Tools, Part II

This chapter covers a portion of the following A+ 220-1202 exam objective:

- **1.4** – Given a scenario, use Microsoft Windows operating system features and tools.

There is much to discuss when it comes to Windows features and tools. That's why we split coverage of this objective into two chapters. In this chapter, we'll complete the objective by covering disk management and a whole bunch of system utilities. Onward!

ExamAlert

This portion of **Objective 1.4** concentrates on disk management tools including System Information (msinfo32.exe), Resource Monitor (resmon.exe), System Configuration (msconfig.exe), Disk Cleanup (cleanmgr.exe), Disk Defragmenter (dfrgui.exe), and Regedit (regedit.exe).

Disk Management

The information in this section applies to working with new drives that are designated for operating system installation, as well as drives that have already been installed. Either way, the concepts of partitioning and formatting remain the same. Regardless of what you are doing with a drive, the proper order for drive preparation is to partition the drive, format it, and then copy files to your heart's delight. However, sometimes you might also

need to initialize additional drives within Windows; this would be done before partitioning. All of these things can be done within the Disk Management utility.

The Disk Management Utility

The Disk Management utility is a GUI-based application for analyzing and configuring storage drives. You access it from **Run** > **diskmgmt.msc** or from within Computer Management or by right-clicking **Start** and selecting **Disk Management**. You can do a lot with this tool, including the following:

- **Initialize a new drive:** File Explorer might not see a secondary drive installed in a computer immediately. To make it accessible, locate the drive (for example, it might be referred to as Disk 1), right-click the name of the disk, and then select **Initialize Disk**. When you install an OS to the only drive in the system, it is initialized automatically.
- **Create a volume:** Windows generally uses the term *volume*, but you will also see the terms *partition* and *logical drive*. To create a volume, right-click the area with the black header (which identifies it as unallocated), as shown in Figure 33.1.

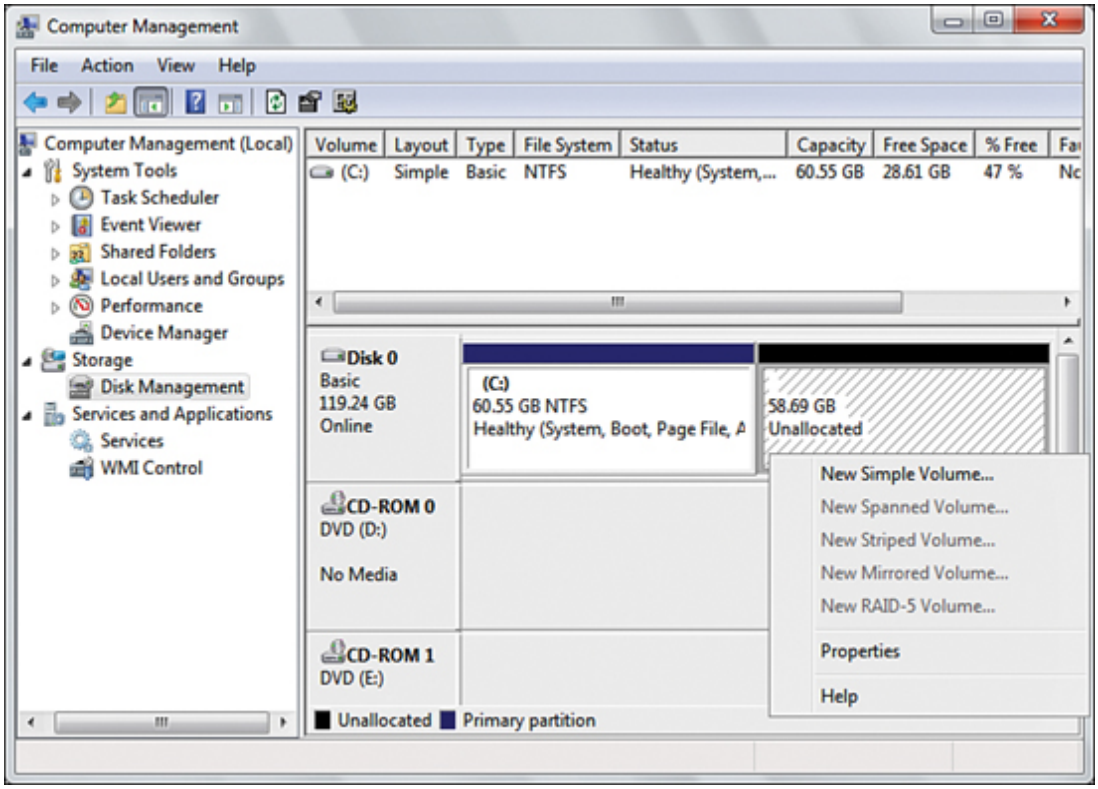


FIGURE 33.1 **Creating a Volume Within Unallocated Disk Space**

- **Format a volume:** When formatting a volume, select the file system (usually NTFS) and whether to do a quick format. Remember that quick format is usually the way to go. If you leave this option unchecked (for a full format), it will take much longer and could reduce the lifespan of the drive. When you format a partition, you must select a drive letter, such as C: or E: or F:. You can change drive letters in the future, but it's a good idea to plan them early on. You can use up to Z:, but you probably won't need to; regardless, keep a few drive letters open in case you need to map a network drive in the future.

Note

WARNING: ALL DATA WILL BE ERASED during the format procedure.

- **Make a partition active:** A partition needs to be set to active if you want to install an operating system to it. A system must have one active partition. The active partition contains the operating system (Windows) that starts when you turn on the system.
- **Convert a basic disk to dynamic:** Basic disks can have only simple volumes or regular partitions/logical drives. If you want to create a spanned, striped, mirrored, or RAID 5 volume, you need to convert the disk to dynamic. You do so by right-clicking the drive where it says Disk 0 or Disk 1, for example, and selecting **Convert to Dynamic Disk**. It's highly recommended that you back up your data before attempting this configuration.
- **Extend, shrink, or split a volume:** You can extend, shrink, or split a volume if you have converted it to a dynamic disk. Just about any volume can be shrunk or split, but to extend a volume, you need available unallocated space on the drive. By shrinking a volume that takes up the entire drive, you can also ultimately split that partition into two (or more) pieces, which gives you a way to better organize where the OS is stored and where the data files are stored.

ExamAlert

There is, technically, a difference between a partition and a volume. A partition is a logical division of a drive. A volume is any space among one *or more* drives that receives a drive letter. Remember that basic disks use partitions to manage data while dynamic disks use volumes. Dynamic disks are more flexible than basic disks and have the ability to create volumes that span across multiple disks.

You can also see the drive at the top of the window shown in Figure 33.1, along with its status. For example, the C: partition is healthy. You also see that it is a System partition, which tells you that the OS is housed there. It also shows the capacity of the drive, the free space, and the percentage of the drive used. What's more, this section tells you if the drive is basic or dynamic or if it has failed. In some cases, you might see "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 access the drive, add the drive to your computer's system configuration. You do this by right-clicking the drive and then clicking **Import Foreign Disks**. Any existing volumes on the foreign drive become visible and accessible when you import the drive.

Mount Points and Mounting a Drive

You can "mount" drives in Disk Management. A *mounted drive* is a drive that is mapped to an empty folder within a volume that has been formatted as NTFS. Instead of using drive letters, mounted drives use drive paths. This is a good solution when you need to work with disc or OS images. It's also helpful in the uncommon case that you need more than 26 drives in your computer (because you are not limited to the letters in the alphabet). Mounted drives can also provide more space for temporary files and can allow you to move folders to different drives if space runs low on the current drive. To mount a drive:

1. Right-click the partition or volume you want to mount and select **Change Drive Letters and Paths**.
2. In the displayed window, click **Add**.
3. Browse to the *empty* folder you want to mount the volume to and click **OK** for both windows.

To remove the mount point, just go back to Disk Management, right-click the mounted volume, select **Change Drive Letters and Paths**, and then select **Remove**.

Remember that the folder you want to use as a mount point must be empty, and it must be within an NTFS volume.

Disk Cleanup

The Disk Cleanup program is used to remove temporary Internet files, downloaded program files, the Recycle Bin, and more. It is located within the Windows Tools folder or can be opened from the **Run** prompt by typing

cleanmgr.exe. Simply select the drive you want to clean up and then select the items you want to remove (permanently) from the computer by checking them. You can also clean up system files—by clicking the button of the same name—including Windows Update cleanup (which can be substantial), Windows Defender Antivirus files, and Windows upgrade log files. A disk cleanup should be performed according to your organization's policies, which could specify once per week or once per month, for example. Note that the newer Storage Sense is intended as the replacement for Disk Cleanup; you'll learn more about it in Chapter 36, "Windows Control Panel Utilities."

> **Note**
>
> As of Spring 2025, Microsoft was in the process of renaming Windows Defender Antivirus to Microsoft Defender Antivirus, and both names appear in Windows. They are the same product. When we reference them in this book, either in text or in images, know that it's because the versions of Windows we're using are, like yours, updated frequently and sometimes the names change daily. Eventually we believe that the new name will become Microsoft Defender Antivirus, so have attempted to standardize on that name throughout the book, but you might see the other name sometimes.

Optimize Drives/Disk Defragmenter

When it comes to mechanical hard disk drives (HDDs), data can easily get jumbled. Over time, data is written to a drive and subsequently erased, over and over again, and gaps are left in the drive space. New data will sometimes be written to multiple areas of a drive in a broken or fragmented fashion by filling in any blank areas. When this happens, the drive must work much harder to find the data it needs—spinning more and starting and stopping more (in general, more mechanical movement). The more a drive has to access this fragmented data, the shorter its lifespan becomes due to mechanical wear and tear. Also, the computer will run more slowly and will continue to get worse until the problem is fixed. A common indicator of this

is a drive LED constantly showing activity. When this happens, you need to rearrange the file sectors so that they are contiguous—that is, you need to defragment!

You can defragment a drive by using Microsoft's Optimize Drives utility. This utility is actually listed within the Windows Tools folder in Windows as Defragment and Optimize Drives, but when it opens, the title simply says Optimize Drives. You can also search for it by typing **defragment** in the Search field or open it directly via **Run > dfrgui.exe**.

This program can be used to analyze your drives for fragmentation, remove fragmentation, and schedule periodic examinations. You can also access this utility by right-clicking a volume in File Explorer, selecting **Properties**, clicking the **Tools** tab, and finally clicking **Optimize**. The ultimate goal with this tool is to make the data contiguous—to move and reorganize it so that it is not fragmented—or at least not *as* fragmented. Although you don't need to physically defragment solid-state drives, the Optimize Drives application (dfrgui.exe) can perform useful maintenance on these drives as well. Overuse, however, can cause excessive wear and tear on solid-state drives, so unless there are problems, you don't need to run the utility if your device has a solid-state drive.

ExamAlert

Know how to access the Optimize Drives/Disk Defragmenter utility in Windows and know the **dfrgui.exe** command in the Command Prompt.

When you initiate a defrag, the process can take awhile, so it's best to do this off-hours. After it completes, a system restart is recommended.

Additional Windows Tools

There are more tools and programs in Windows than you can shake a stick at. In this section, we'll cover some of the important ones for the exam. But

remember, don't be a sheep! Use the right tool for the job, even if it might be a different one than everyone else is using.

Many of these tools are located in the Windows Tools folder (see Figure 33.2).

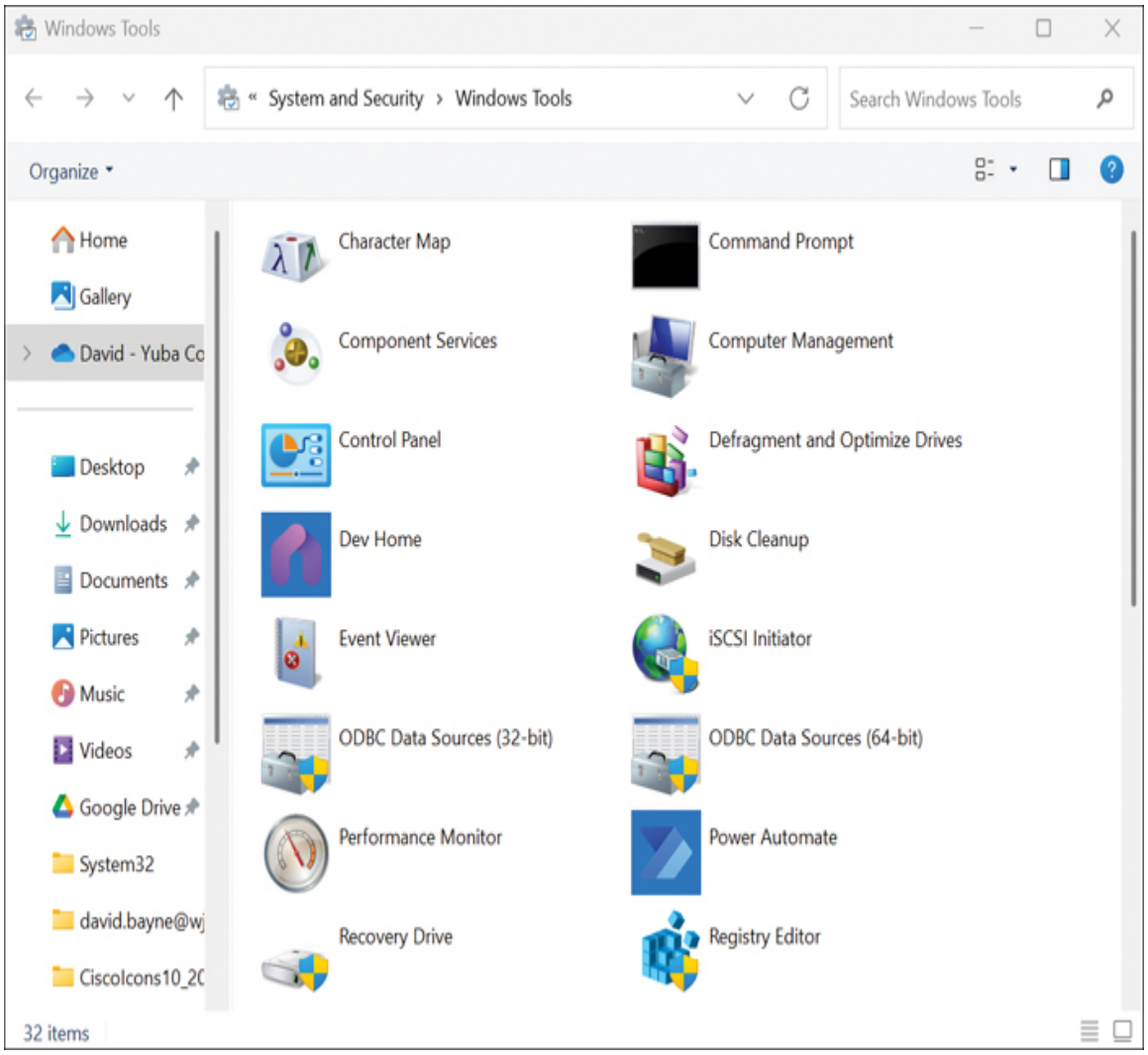


FIGURE 33.2 **Windows Tools**

System Information/msinfo32

The System Information tool is used for system and device analysis. You can access it by opening the **Run** prompt and typing **msinfo32.exe**. (Typing **.exe** actually isn't necessary by default.) Using this tool, you can view and analyze information about the hardware components, the software

environment, and the hardware resources used, but you cannot make any changes. You can view this information for the local computer and for remote computers as well by typing the name or IP address of the system you want to analyze. Figure 33.3 shows the System Information (msinfo32) screen.

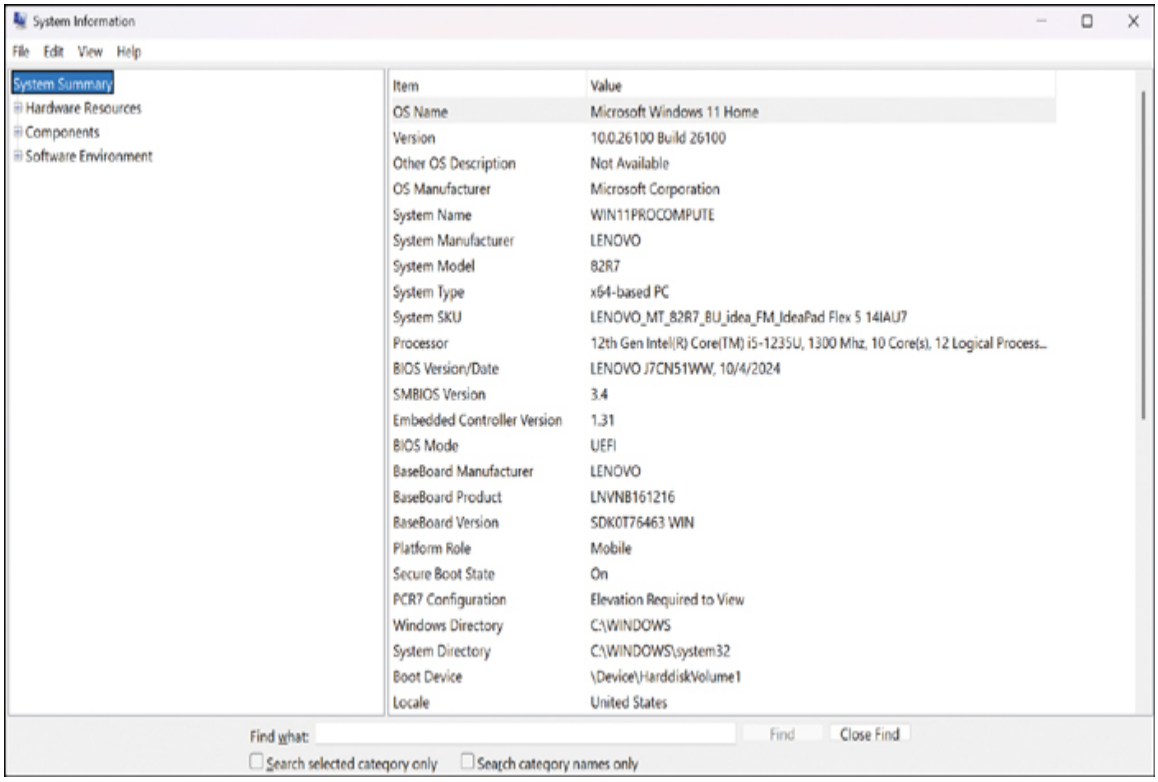


FIGURE 33.3 **The System Information msinfo32 Screen**

ExamAlert

System Information (msinfo32) gives you the Windows system summary for hardware resources, components, and the software environment.

Resource Monitor

The Resource Monitor tool is a handy tool that displays information about the hardware on a system and how the OS and software are using that

hardware. It gives more information than the Task Manager but is not as complicated as the Performance Monitor. Everything you commonly want to see is summarized nicely in the Overview tab, as shown in Figure 33.4. You can access the Resource Monitor from the Administrative Tools folder or by selecting **Run > resmon.exe**. You can also open it from the Performance tab of the Task Manager.

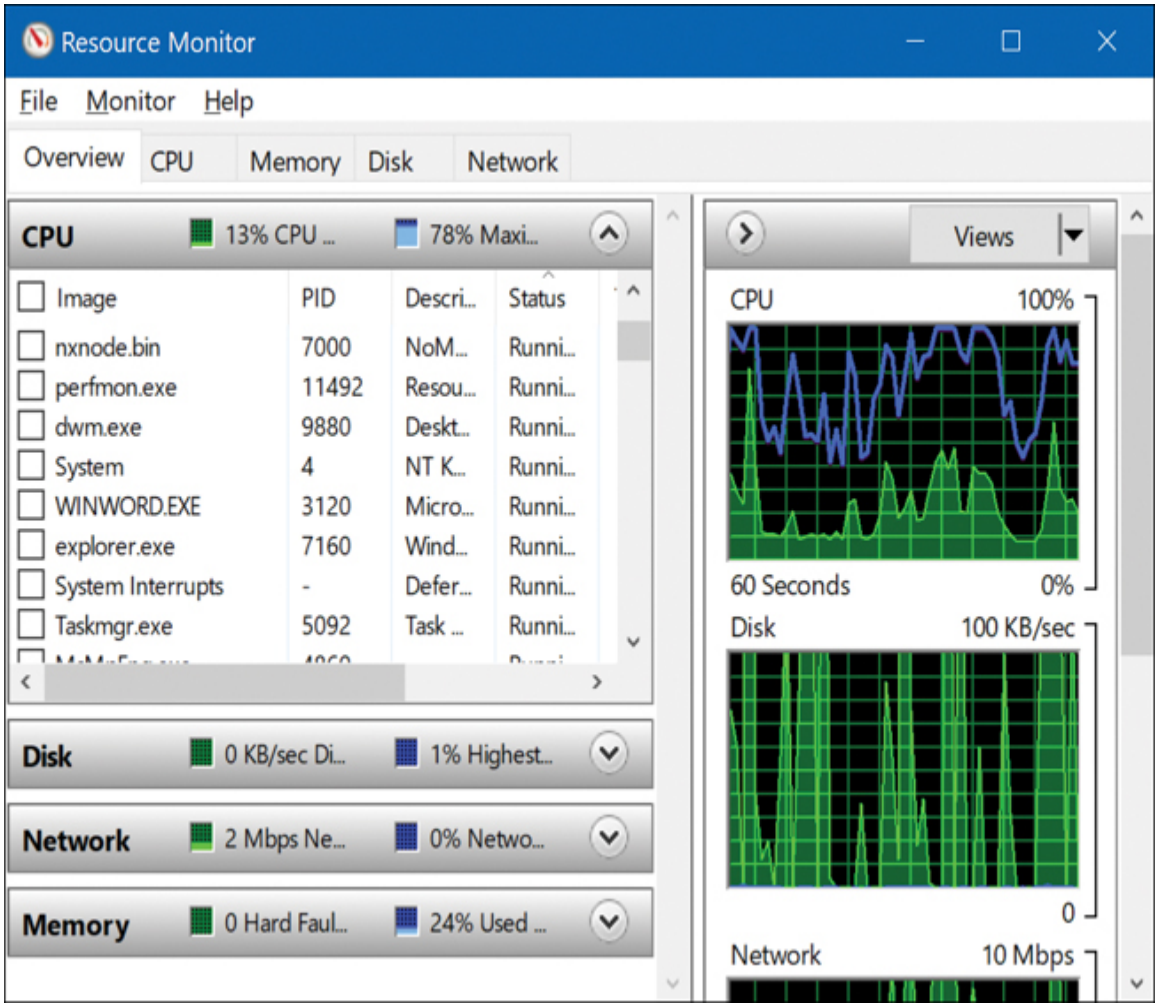


FIGURE 33.4 **The Resource Monitor Tool**

In the figure, you can see that the Overview tab displays the CPU information by default. This includes processes that are running such as WINWORD.EXE (Microsoft Word, which was used to write this chapter), perfmon.exe (the Performance Monitor utility, which is also open), and explorer.exe (the Windows GUI itself). It also shows the process ID (PID) and the status of each process. Similar displays are listed under Disk,

Network, and Memory. On the right in the figure are graphical charts for CPU, Disk, Network, and Memory. So, you can see that the Resource Monitor gives you a lot of information in a nice, condensed space. Try it out.

System Configuration/MSConfig

MSConfig (msconfig.exe) is the commonly used name for the System Configuration tool. It can help you analyze and troubleshoot various things, from operating system startup issues to application and service problems. Open MSConfig from the Windows Tools folder or by selecting **Run > msconfig**.

System Configuration is an excellent troubleshooting tool that has multiple tabs, as shown in Figure 33.5.

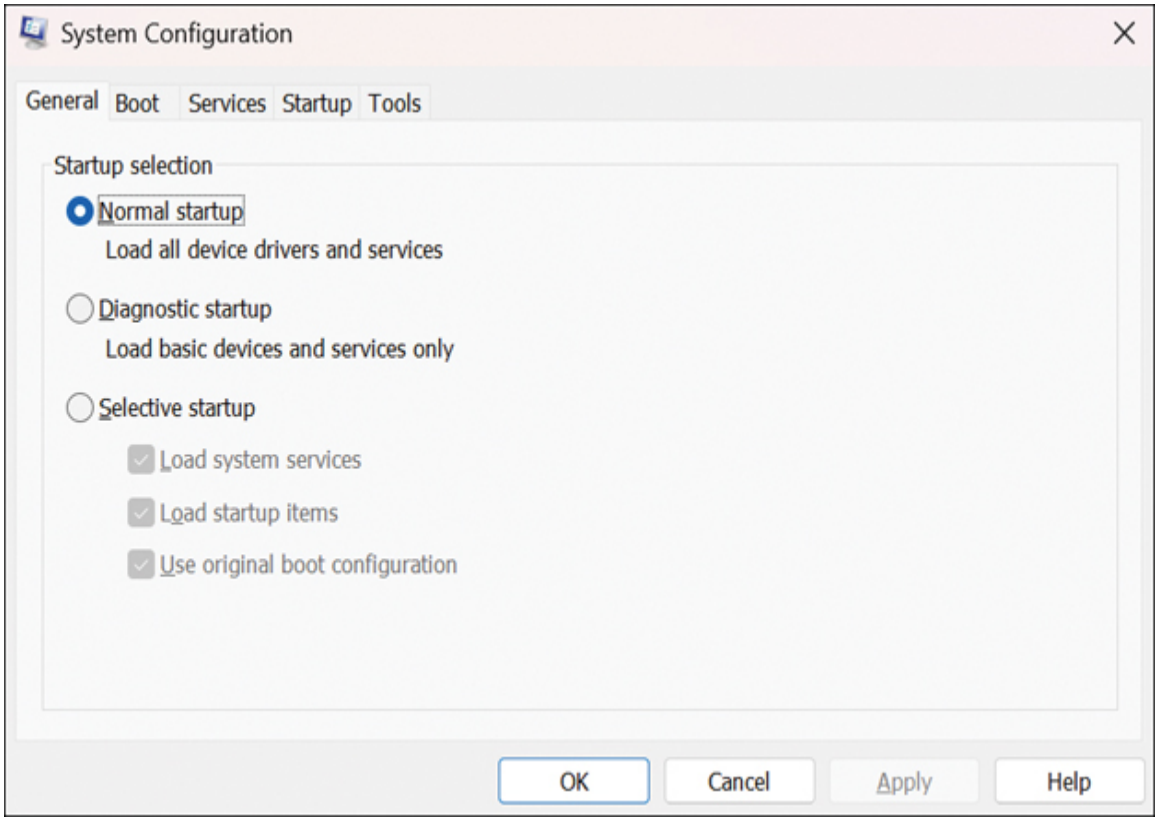


FIGURE 33.5 **The System Configuration (msconfig) Window**

- **General:** You can use this tab to configure the system for diagnostic or selective startup. This helps you troubleshoot devices or services that are failing.
- **Boot:** You can use this tab to modify OS bootup settings (such as using Safe boot), log the boot process, and boot without video. If you have multiple operating systems, you can change the order and choose which one to set as the default. Also, clicking the **Advanced options** button lets you choose things such as how much memory you want to use and what port to use if you need to output debugging information.
- **Services:** This tab lists the services and the current status of each one. You can enable or disable them from this tab (it requires a computer restart). However, you can't start or stop them. To do that, you need to go to the Task Manager or the Services console window, or you can do it from within the PowerShell/Command Prompt. The beauty of this tab is that it allows you to much more quickly enable/disable services than you can by using other options in Windows.
- **Startup:** In Windows 11, the Startup tab still exists but displays "To manage Startup items, use the Startup section of Task Manager" and provides a link to open the Task Manager.
- **Tools:** This tab lists a lot of the common utilities you might use in Windows and allows you to launch them. As a launching point for programs you use a lot (Task Manager, PowerShell, System Properties, Command Prompt, and so on), this tab can be a real time-saver.

MSConfig is a time-saver when you're changing boot settings, working with services, and troubleshooting the system. One caution: Be sure to reset MSConfig to the regular settings when you finish using it. For example, if a user complains about a system starting in Safe boot every time or other similar problems in which the user doesn't have full access to the system, MSConfig might need to be reconfigured to Normal startup on the General tab.

ExamAlert

Be able to open MSConfig (msconfig.exe) and identify what each of the tabs is used for.

The Windows Registry Editor

Left this one for last! The Windows Registry is a database that stores the settings for Windows. It contains hardware and software information and user settings. If you cannot make the modifications that you want in the Windows GUI and don't want to use the command line, the Registry is the place to go. To modify settings in the Registry, use the Registry Editor, which can be opened from the Windows Tools folder or by typing **regedit.exe** at the **Run** prompt. This displays a window like the one shown in Figure 33.6.

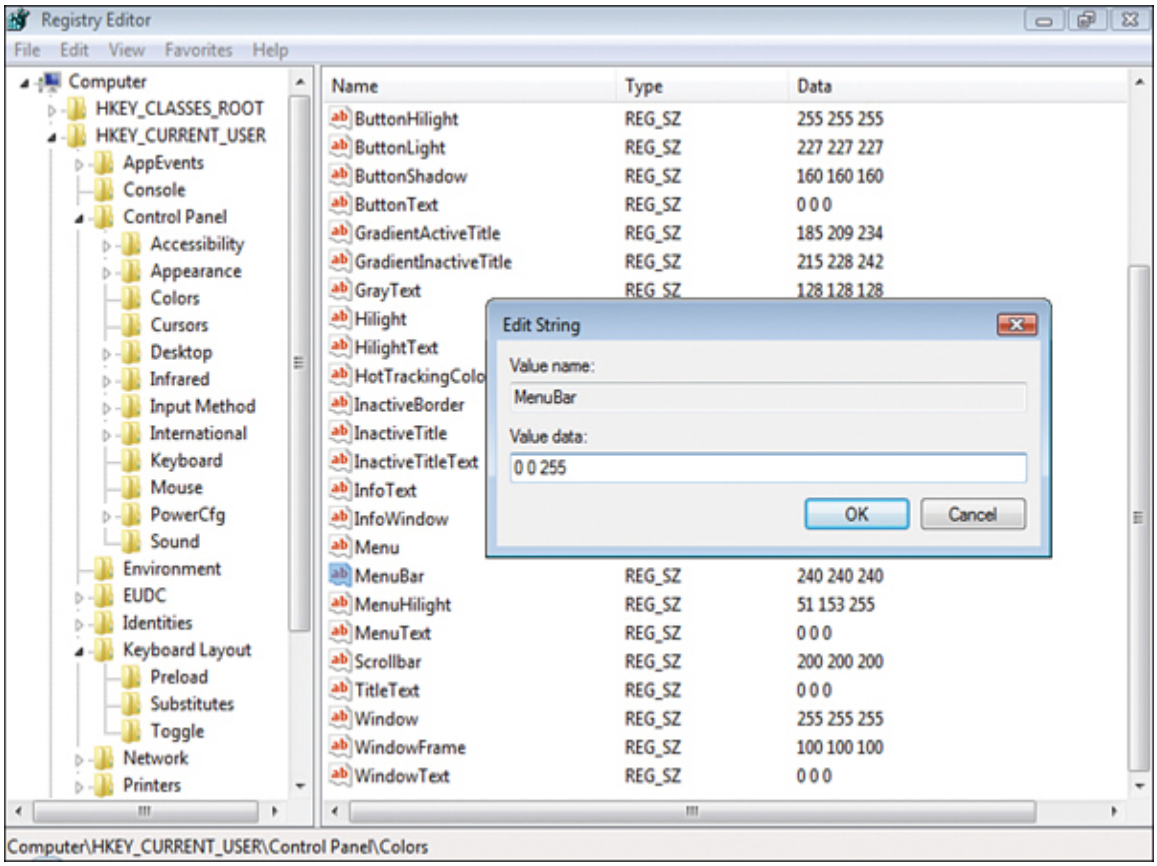


FIGURE 33.6 **The Registry Editor in Windows with an Open Entry**

The registry is divided into several sections, known as *hives*, each of which begins with the letters HKEY. Table 33.1 describes the five visible hives in the Registry Editor.

TABLE 33.1 **Description of Registry Hives in Windows**

Registry Hive	Description
HKEY_CLASSES_ROOT	Stores information about applications' file associations and Object Linking and Embedding (OLE).
HKEY_CURRENT_USER	Stores settings that concern the currently logged-on user. It is common to make changes in this hive.
HKEY_LOCAL_MACHINE	Stores hardware and software settings that are specific to the computer. This is where the bulk of a PC technician's Registry edits are made. One example of data stored here is the programs that run when the OS starts.
HKEY_USERS	Stores data corresponding to all users who have ever logged on to the computer.
HKEY_CURRENT_CONFIG	Contains information that is gathered every time the computer starts up.

Hives are also known as *keys*, and they contain other keys and subkeys. This forms the organizational system for the Registry. It is similar to folders and subfolders within File Explorer. However, the Registry does not store actual data files; it stores settings. Inside the keys and subkeys are registration entries that contain the actual settings. These can be edited, or new entries can be created. The types of entries include

- String values, which are used for decimal numbers
- Binary values, which are used for binary entries
- DWORD and QWORD entries, which are used for binary and hexadecimal entries

- Multistring values, which can contain a variety of information

Registry hive data is stored in \%systemroot%\System32\Config. For example, a complete copy of the HKEY_CURRENT_CONFIG hive data is stored as the SYSTEM file (with no extension).

Many users fear the Registry, but a technician need not. Just follow a couple of simple rules: Back up the Registry before making changes and don't make modifications or additions until you have a thorough understanding of the entry you are trying to modify or add.

Note

Don't forget: We made a table of Run commands for you, which you can find at https://greenmountaintraining.com. For example, **regedit.exe** opens the Registry Editor.

Table 33.2 provides a partial list of Run commands used to execute programs in Windows. Once you memorize them, it can be easier to type the executable than to navigate Windows. Note that you can run most of these commands at the Run prompt or the Command Prompt or PowerShell.

To open Run, press Windows+R or right-click **Start** and select **Run**. Don't forget that the Search option works pretty well too!

TABLE 33.2 **Run Commands**

Program	Command
About Windows	**winver**
Administrative Tools	**control admintools**
Calculator	**calc**
Certificate Manager	**Certmgr.msc**
Character Map	**Charmap**
Command Prompt	**cmd**

Program	Command
Computer Management	**compmgmt.msc**
Credential Manager	**control /name Microsoft.CredentialManager**
Date and Time	**Timedate.cpl**
Device Manager	**devmgmt.msc**
DirectX Diagnostic Tool	**dxdiag**
Disk Cleanup	**cleanmgr**
Disk Management	**diskmgmt.msc**
Event Viewer	**eventvwr**
File Explorer	**Explorer** (Windows+E)
Folder Options (also known as File Explorer Options)	Control folders
Internet Properties	**Inetcpl.cpl**
Local Group Policy Editor	**gpedit.msc**
Local Security Policy	**secpol.msc**
Local Users and Groups	**lusrmgr.msc**
Magnifier	**Magnify**
Microsoft Management Console	**mmc**
Network Connections	**Ncpa.cpl**
Optimize Drives/Disk Defragmenter	**dfrgui**
Performance Monitor	**perfmon**
PowerShell	**Powershell**

Program	Command
PowerShell ISE 5.1	**Powershell_ise** Or type **ise** from the PowerShell!
PowerShell Core 6 and higher (if installed)	**pwsh**
Print Management	**printmanagement.msc**
Programs and Features	**Appwiz.cpl**
Registry Editor	**regedit**
Remote Desktop Connection	**mstsc**
Resource Monitor	**resmon**
Services console window	**services.msc**
Sound (dialog box)	**Mmsys.cpl**
System Configuration (msconfig)	**msconfig**
System Information	**msinfo32** (Ctrl+Alt+F1)
System Properties dialog box	**sysdm.cpl**
System Restore properties	**systempropertiesprotection**
System window	**control system** (Windows+Break)
Task Manager	**taskmgr** (Ctrl+Shift+Esc)
Task Scheduler	**taskschd.msc**
Microsoft Defender Firewall	**firewall.cpl**
Microsoft Defender Firewall with Advanced Security	**wf.msc**
Windows Features	**optionalFeatures**

Program	Command
Windows Memory Diagnostics	**Mdsched**

Cram Quiz

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

1. You are preparing to troubleshoot a system that is having some driver issues. Which of the following tools should you use to configure the system to boot safely?

   - ○ **A.** Event Viewer
   - ○ **B.** Resource Monitor
   - ○ **C.** msinfo32
   - ○ **D.** System Configuration

2. You have been tasked with repairing a magnetic-based hard drive that is running sluggishly. Which of the following tools should you use to fix the problem? (Select the best answer.)

   - ○ **A.** Disk Management
   - ○ **B.** Optimize Drives
   - ○ **C.** msinfo32.exe
   - ○ **D.** Mount point

3. What is HKEY_LOCAL_MACHINE considered to be?

   - ○ **A.** A Registry entry
   - ○ **B.** A subkey
   - ○ **C.** A string value
   - ○ **D.** A hive

4. What must you do first to a basic disk to create spanned, striped, mirrored, or RAID 5 volumes in Disk Management?

   - ○ **A.** Extend it
   - ○ **B.** Shrink it
   - ○ **C.** Split it
   - ○ **D.** Initialize it
   - ○ **E.** Convert it to dynamic

5. In Disk Manager, which partition contains the operating system?

   - ○ **A.** Spanned
   - ○ **B.** Active
   - ○ **C.** Striped
   - ○ **D.** Mirrored

Cram Quiz Answers

1. **D.** Use the System Configuration utility (msconfig.exe) to configure the system to boot safely by going to the **Boot** tab and checking the **Safe boot** option, as shown in Figure 33.7. In the figure, it is configured as Minimal (the default), meaning that the system will boot with a minimal set of drivers and programs; however, several other options are listed there. Make sure you go through the Windows utilities and all the tabs. Know what everything does!

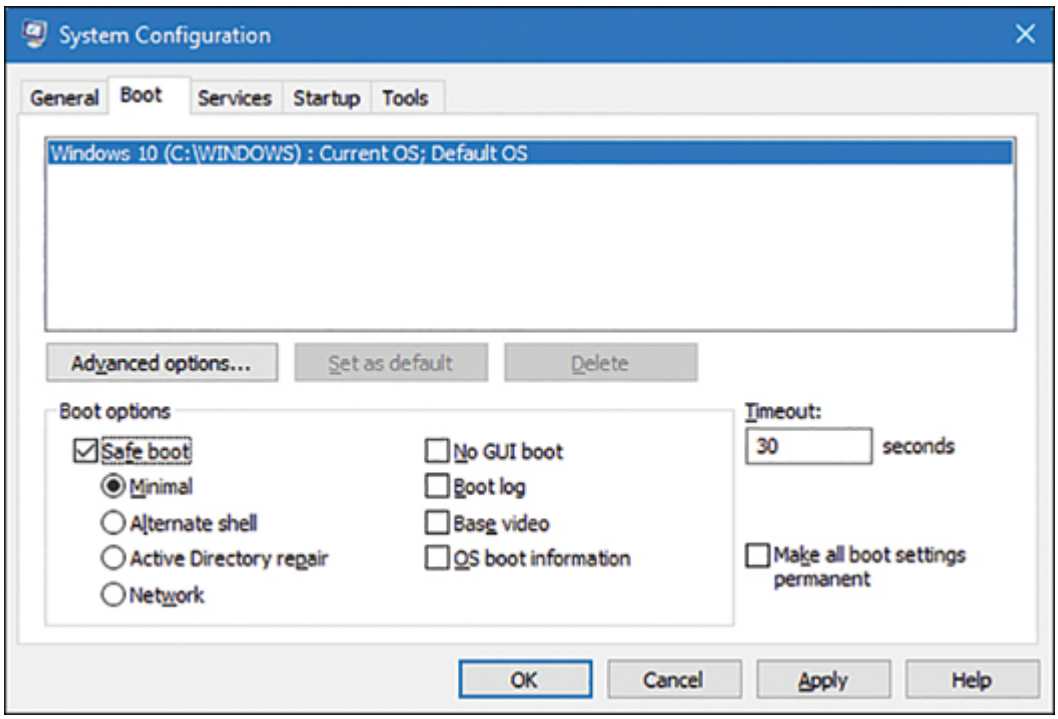


FIGURE 33.7 **System Configuration Utility Displaying the Boot Tab**

The Event Viewer is a tool you can use to review Windows logs, including informational entries, warnings, and errors. The Resource Monitor is an analysis tool for hardware on your system; it's more detailed than the Task Manager but less detailed (and easier to use) than Performance Monitor. The System Information tool (msinfo32) provides nonconfigurable information about hardware components and the software environment.

2. **B.** Use the Optimize Drives (Disk Defragmenter) utility. This utility attempts to defragment the drive and place the files in a contiguous order so that the hard disk drive (HDD) doesn't behave so sluggishly. Of course, there could be other causes for the poor hard drive performance, such as too many applications at startup, malware, capacity issues, and so on. Disk Management is the place where you go to configure the storage drive but not to repair it—at least not directly. The System Information tool is used for system and device analysis. You can access it by opening the **Run** prompt and typing **msinfo32.exe**. Using this tool, you can view and

analyze information about the hardware components. A mount point is a drive that is mapped to an empty folder; it is not a utility.

3. **D.** HKEY_LOCAL_MACHINE is one of the five visible hives that can be modified from within the Registry Editor. This hive stores hardware and software settings that are specific to the computer (for example TCP/IP settings).

4. **E.** Convert the disk to dynamic. Once this is done, the volume can be extended, shrunk, or split. You initialize a drive if it is not recognized by Windows immediately—for example, if it is a new or foreign drive that has been installed to a computer that already had Windows functioning.

5. **B.** A partition needs to be set to active if you want to install an operating system to it. A system must have one active partition. The active partition contains the operating system (Windows) that starts when you turn on the system. Basic disks can have only simple volumes or regular partitions/logical drives. If you want to create a spanned, striped, mirrored, or RAID 5 volume, you need to convert the disk to dynamic.

Absolutely fantastic. It's important to take your time so that the concepts can sink in properly. In essence, go slowly…but efficiently. Review and take a break before you move on to the next chapter. Great work so far!

Chapter 34

Microsoft Command-Line Tools, Part I

This chapter covers a portion of the following A+ 220-1202 exam objective:

- **1.5** – Given a scenario, use the appropriate Microsoft command-line tools.

The command line is where the real technicians live. Anything you can do in a GUI-based system, you can also do in the command line—and often you can do more at the command line. Get to know it. For Microsoft Windows, you should become fluent in PowerShell, the Command Prompt, and the Windows Terminal, and you should know as many commands as you can.

The command line is so important that we spread out this objective over two chapters. There are a lot of commands in this chapter, and we suggest you take a break after each group of commands. We'll begin with the types of command-line tools available in Windows. Then we'll cover how to navigate folders and files within the Command Prompt. (By the way, when we work in the command-line interface, the original name for folders was *directories*, so we will be using that term often.) Next, we'll discuss some of the commands that can be used to analyze and configure the storage drive and file system. Finally, we'll cover a couple of advanced tools.

If you are totally new to the command line and/or are already confused with the differences between Command Prompt, Shell, and Terminal, check out the following resources: https://learn.microsoft.com/en-us/shows/one-dev-minute/what-is-a-command-line-shell--one-dev-question is a video from Microsoft that explains the difference between a shell, a console, and a terminal. The article at https://www.hanselman.com/blog/whats-the-difference-between-a-

console-a-terminal-and-a-shell does the same but includes pictures as well to help explain the origins of the terms.

Once you get the hang of the command line, you'll see that it's a blast. The great thing about the command line is that it hasn't changed much over time. It has certainly not changed nearly as much as the GUI in Windows. Plus, many companies desire technicians who have good command-line skills, which can ultimately translate to job security. Enough said.

ExamAlert

Objective 1.5 focuses on command-line tools designed for directory navigation, network connectivity, disk management, file management, information gathering, and OS management. This chapter covers the basics of the command line and tools for managing files, directories, and disk management. Tools for managing the network will be covered in the next chapter, Chapter 35, "Microsoft Command-Line Tools, Part II."

Microsoft Command-Line Basics

Microsoft has three command-line options: the Command Prompt, PowerShell, and Windows Terminal. The first two are text-based interfaces where you can issue commands to the operating system. The last one acts as a launching point for the other two tools. Let's examine each of them now.

Command Prompt

The Command Prompt is the original Windows command-line interface (CLI). You can use this program to issue commands concerning files and directories (folders), networking, services, and so on. In Windows, you can open it in several ways, including the following:

- Open the Search tool and type **cmd** (or search for a variety of words/phrases associated with the Command Prompt).
- Press Windows+R to open the Run prompt and type **cmd** (my personal favorite).
- Click **Start** and then, on the programs list, scroll down to **Windows System > Command Prompt**.

In Windows, some commands need to be run as an administrator. To open the Command Prompt as an administrator, do one of the following options (and type the password for the administrator account if necessary):

- Go to **Start > Windows System**, right-click **Command Prompt**, click **More**, and select **Run as administrator**.
- Open the Search tool and type **cmd** in the Search field; then right-click **Command Prompt** and select **Run as administrator** (or press Ctrl+Shift+Enter).

Note

In Windows 11, right-clicking the Start button shows Terminal instead of Command Prompt by default. This opens a PowerShell terminal window, which has more functionality than a standard Command Prompt.

If you want to change the behavior back—opening the Command Prompt instead of a PowerShell terminal—you can do that by following these steps:

1. Right-click the Start button and select **Terminal (Admin)**.
2. Click the arrow next to the Administrator tab.
3. Select **Settings**.
4. Under Default profile, click the drop-down menu and select **Command Prompt**.
5. Click **Save**.

PowerShell

You will likely want to use PowerShell more often than the Command Prompt. PowerShell is a combination of the Command Prompt and a scripting language. It enables administrators to use typical commands and also to perform administrative tasks that integrate scripts and executables. You can open PowerShell in the following ways:

- Open the **Search** tool and type **powershell**.
- Go to the **Run** prompt and type **powershell.exe**.
- Navigate to **Start > Windows PowerShell > Windows PowerShell**.
- Right-click **Start** and click **Windows PowerShell** (in Windows 11, this is called Terminal or Terminal (Admin), but opens the PowerShell terminal window).
- By the way, another great keyboard shortcut is Windows+X. This is the same as right-clicking the **Start** button.

Note

The option in the last bullet might not be set up by default in Windows 10. To change the option from Command Prompt to PowerShell, you have to go to **Settings > Personalization > Taskbar** and toggle the **Replace Command Prompt with PowerShell** option. In Windows 11, this option is not necessary because the system defaults to Windows Terminal, which is a PowerShell terminal.

ExamAlert

Know how to open PowerShell from the Search tool, from the Start menu, and from the Run prompt.

You need to open PowerShell as an administrator to run advanced procedures. You can do this in the following ways:

- Open the Search tool and type **powershell** in the Search field; then right-click **PowerShell** and select **Run as administrator** (or press Ctrl+Shift+Enter).
- Go to **Start > Windows PowerShell**, right-click **Windows PowerShell**, and select **Run as administrator**.
- Right-click any pinned shortcut to PowerShell and select **Run as administrator**. Pinned shortcuts might be placed on the taskbar, the Desktop, or elsewhere. Very handy!
- Right-click **Start** and click **Terminal (Admin)** (if configured).

Running PowerShell (or any other program) as an administrator is also known as running it in *elevated mode*. You will be using PowerShell in elevated mode often. We'll discuss PowerShell further in Chapter 62, "Basic Scripting, Part I," and Chapter 63, "Basic Scripting, Part II."

Note

Administrators who write scripts often are likely to use Visual Studio Code (known as VSC or VSCode). This is an integrated development environment (IDE) that can be used to build PowerShell scripts and scripts in other programming languages (such as Python). It has a built-in command line as well—often defaulting to PowerShell—that you can use to test your scripts. It's free and open source as of the writing of this book. Also, it's cross-platform—meaning you can run it on other systems as well, such as Linux. We highly suggest checking it out: https://code.visualstudio.com.

Windows Terminal

Windows Terminal is another place to run commands. It is multitabbed, meaning you can run multiple sessions within the same program. You can

run any Windows command-line tool or shell within the tabs—PowerShell, the Command Prompt, and so on.

The term *terminal* can be confusing because it is used in Linux, Mac, and Azure environments also. What you need to know here is that in Windows, the Terminal environment is PowerShell. Other operating systems also use a terminal.

Taking it further, you can also run an Azure Cloud Shell in Windows Terminal. Or, if you have the Windows Subsystem for Linux (WSL) installed, you can run various distributions of Linux in different terminal tabs, usually with a Bash shell (don't worry, it isn't as confusing as it sounds).

Ask for Help!

If you are ever stumped about a particular command, read the help file associated with it. The naming convention for this is

```
[command name] /?
```

This means to use whatever command you want to learn more about followed by the **/?** characters. For example, for more information about the **ping** command, you can type **ping /?**. In some cases, you can also type **help** and then the command (for instance, **help dir**), but **/?** is the best all-around way to do it because this option encompasses all the commands available. You can also find out more about Microsoft commands at https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/windows-commands.

Challenge: Access Each of the Microsoft Command-Line Tools

Go forth and use the command line! Try to access the Command Prompt, PowerShell, and the Windows Terminal (which you might need to install). Then try to run each of them as an administrator. Type the command **help** in both the Command Prompt and PowerShell and browse through the help files for each. Think about some of the scenarios where you might use the

command line. For example, you might want to build a script, or run multiple tabs, or just navigate through the directories. Which tool would fit best in each of those scenarios?

Navigating in the Command Line

Have we mentioned yet that just about anything you can do in the Windows GUI you can also do by using the command line? It's true. And sometimes using the command line is faster than using the GUI—if you can type quickly!

Note

As a reminder, *directory* is the original name for *folder*. The more accurate names are *directory* when working in any command line and *folder* when working in the GUI, but the two terms are often used interchangeably.

There are three main commands used to work with directories in the command line: **cd**, **md**, and **rd**. Feel free to use PowerShell or the Command Prompt for these three commands:

- **cd:** Change directory. This command enables you to move from one directory to another. Actually, you can go from any one directory to any other by using just one **cd** command. Two simple commands that you can issue are **cd ..** and **cd **. The **cd ..** command moves you up one directory; it takes you from the current directory to the parent directory. The **cd ** command takes you directly to the top (root) of the volume that you are working in.
- **md:** Make directory. This command creates directories.
- **rd:** Remove directory. This command enables you to remove directories. You can also remove directories that contain files by using the **/S** switch.

Note

The older versions of the **md** and **rd** commands are **mkdir** and **rmdir**, respectively. They still work, so practice with them!

All of these commands can be used such that their functions affect any directory you choose within the directory structure (which used to be known as the *DOS tree*, and is also referred to as the *directory tree*). Figure 34.1 provides a sample directory structure.

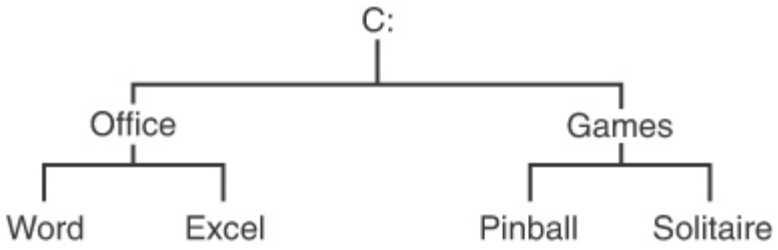


FIGURE 34.1 **A Sample Directory Structure**

For example, let's say that your current position is C:\Office. From here or any other location, you can do anything to any directory in the entire directory tree. Let's consider a couple of examples:

- To change the current position to the Pinball directory, the command would be either **cd c:\games\pinball** or just **cd \games\pinball**.
- To make a directory called **documents** within the Word directory, the command would be **md c:\office\word\documents**.
- To delete the directory **excel**, the command would be **rd c:\office\excel**.

ExamAlert

Know how to use the **cd**, **cd ..**, and **cd ** commands in PowerShell or the Command Prompt.

So far, we've been working in the C: drive. In Windows land, we use the terms *volumes* or *drives* when referring to storage drive areas that are

assigned letters. Chances are that you will have multiple volumes, and you will sometimes want to change from one volume to another. For example, maybe your operating system is installed in the C: drive, and you have data stored in the F: drive. To change from one to the other, you use drive navigation inputs. To do so, simply type the name of the drive, such as **F:**.

A quick way to find out what volumes you have on your system is to issue the **wmic logicaldisk get name** command, as in this example:

```
PS C:\Data> wmic logicaldisk get name
Name
C:
F:
PS C:\Data> F:
PS F:\> C:
PS C:\Data>
```

In this example, we issued the **wmic logicaldisk get name** command, and Windows told us that we have a C: drive and an F: drive. We then switched to the F: drive and back to the C: drive.

You'll note that the system remembers the last directory you were working in for each drive that you access. The PS means that you are working in PowerShell. (Another good option for learning what volumes are available is **get-volume**, but it works only in PowerShell.)

As you can guess, you can apply the **cd**, **md**, and **rd** commands mentioned previously to any drive letter. For example, if you were working in the C: drive and needed to get into the test1 directory in the F: drive, you would issue the command **cd F:\test1**, like this:

```
PS C:\Data> cd F:\test1
PS F:\test1>
```

Finally, you might see the *x*:\ drive letter in documentation. When you see this, *x* is a variable, and it can take the place of whatever drive letter is required. For example, you might install a program from a USB flash drive, but the program's creator will not know what drive letter your USB drive

will be assigned by the operating system. Yours might be D:, and another user's might be F:, and so on. So, we use *x* as a catch-all. Fun!

Working with Folders/Directories and Files

Some other commands you might use when working with folders/directories and files include **dir** and **robocopy**:

- **dir:** This is the directory command. When used alone, it displays the contents of the current directory. But it can be configured to show information in any other directory. For example, **dir \office\excel** shows the contents of the excel directory, regardless of what directory you are currently in. You can also use the **dir** command to customize how content is listed. For example, **/p** shows information by the page, **/w** is wide list format, and so on. To find out more about the **dir** command (or any other command, for that matter), type **dir /?**. Here, **/?** is the switch that tells the Command Prompt to display the help file for that command. It can be placed on the end of any valid command in the Command Prompt.
- **robocopy:** Robust File Copy is a directory replication tool. It is meant to copy directories that contain lots of data, and it can even mirror complete directory trees from one computer to another. **robocopy** is the successor to **xcopy**. Some of the advantages of this tool are that it can tolerate network interruptions, skip past junctions (such as the \Documents and Settings to \Users junction), take advantage of multithreading, and preserve data attributes and timestamps. **robocopy** is not intended for the copying of individual files; it copies directories and their contents. For example, **robocopy c:\office c:\games** copies all the information within the \office directory to the \games directory, including any subdirectories. This command also gives in-depth results of its actions. You can also use **robocopy** to copy information to other computers by using *computername**share*, which is Microsoft's Universal (or Uniform) Naming Convention (UNC).

Note

You can create a file such as test.txt within Notepad, which is available via the Search tool or by going to **Run** and typing **notepad**. Notepad is the default graphical text editor in Windows, and you can use it for editing text files and scripts. However, you might opt to use another editor, especially if you plan on doing any scripting or coding. (Some alternatives include Notepad++, Sublime Text, Atom, and one of our favorites—though it is not graphical—Vim in Linux.)

Note

Vim is a free, open-source text editor that's pre-installed on most Linux distributions.

Note

There are other file management commands that can be used to copy files quickly and easily from the command line. Among them are **tree**, **copy**, **xcopy**, and **del**. While not on the exam, these commands (and plenty of others) can be useful for file management, especially for large groups of files. While the GUI makes things easy, the CLI can almost always be faster when you're copying large numbers of files (multiple megabytes) that you might see in a business or enterprise situation.

ExamAlert

Understand how to use **cd**, **dir**, **md**, **rmdir**, and **robocopy** for the exam.

Partitioning and File System–Based Commands

There are a slew of commands that you can use to make changes to your storage drive's partitions and file systems and to check the integrity of your storage drive and file system. These are a few of the commands that you should know for the exam:

- **diskpart:** This utility is the command-line counterpart of the Windows Disk Management program. To start diskpart, open a command prompt and type **diskpart** or select **Start > Run > diskpart**. A new window will launch with the DISKPART> prompt. From here, you can create, delete, and extend volumes; assign drive letters; make a partition active; and so on. Essentially, everything that you can do in the Disk Management graphical utility can be done with **diskpart**. When you are in the DISKPART> prompt, you can enter a question mark (**?**) to learn about the various options within the Diskpart program. When you finish using **diskpart**, type **exit** to return to the standard Command Prompt.
- **format:** You use this command to format storage media to a particular file system, such as NTFS, FAT, or FAT32. An example of formatting a USB flash drive at the command line would be **format F:**. You can specify the type of file system that the media will be formatted to with the switch **/FS:***filesystem*, where *filesystem* equals NTFS, FAT, and so on.

chkdsk and sfc

A good technician uses commands to analyze and possibly repair a storage drive and its system files. Two commands that can aid you in this endeavor are **chkdsk** and **sfc**.

chkdsk

chkdsk checks a drive, fixes basic issues like lost files, and displays a status report; it can also fix some errors on the drive with the addition of the **/F** switch.

One issue that plagues users is the infamous "Missing Operating System" message. This message usually means that the drive has a few small errors. But even though the system won't boot, you can still run **chkdsk** to find

and fix problems on the drive. Boot to the repair environment (if possible) or boot to the Windows media, access Windows RE, and then open the Command Prompt. From there, run **chkdsk** with either the **/F** switch (which fixes errors on the drive) or the **/R** switch (which locates bad sectors and recovers data)—or run both. This procedure can also help with "Invalid Boot Disk" errors. (Of course, first check that the BIOS/UEFI is booting to the correct drive in the boot priority menu.) If you can fix the drive, it is recommended to back up files right away because there could be subsequent drive failure.

sfc

System File Checker (sfc) is a Windows utility that checks protected system files. It replaces incorrect versions or missing files with the correct files. SFC can be used to fix problems with Edge/Internet Explorer and other Windows applications. To run SFC, open the Command Prompt and type **sfc** with the appropriate switch. A typical option is **sfc /scannow**, which scans all protected files immediately and repairs files. During this procedure, SFC writes the details of each repair to a file called CBS.log, located in %systemroot%\Logs\CBS, which can be used to further analyze the system and the integrity of files. Another option is **sfc /verifyonly**, which scans the integrity of files but does not perform a repair. If SFC finds that some files are missing, you might be prompted to reinsert the original operating system .iso file so the files can be copied to the DLL cache (if you have a recovery partition, those files will usually be accessed automatically).

Note

%systemroot% is the folder where Windows was installed; by default, it is C:\Windows.

ExamAlert

Know the basic switches for **chkdsk** and **sfc**, such as **chkdsk /F** and **sfc /scannow**.

winver

The **winver** command brings up a window that tells you what operating system you are running, the edition, and the build number. It also displays trademark and licensing information. This is one of those commands that you can run from anywhere: at the command line, in the Run prompt, in the Search tool, and so on. An example of using the **winver** command is shown in Figure 34.2.



FIGURE 34.2 **An Example of Using the winver Command**

The figure shows that this system is running Windows 11 Home version 24H2, which began to be rolled out in October 2024 (and has updates since then that aren't shown). However, the availability of a new version doesn't mean that all devices get it at the same time; the updates are delayed for a variety of reasons. If you so desire, you can attempt to force an update by going to **Windows Settings > Update & Security > Windows Update** and clicking the **Check for updates** button.

In Figure 34.2, you can also see the build number (26100.3194), which is what developers sometimes go by when working deep in Windows. In this case, this version of Windows 11 is also referred to as version 10.0.26100.3194, which is what you would see if you typed the **ver** command in the Command Prompt or the **$psversiontable** command in PowerShell. Try all three! Note that your build number will most likely be different from the one shown here. In fact, you may notice that Windows 11 will show up as Version 10.x.xxxxx.xxxx; that is not usual either. Build version numbers are not always related directly to the public version of Windows that you are running, and this is not a problem at all. As long as you stay updated, you're fine.

Note

Here's an example of a Windows 11 version and build number displayed by using the **winver** command:

Version 24H2 (OS Build 26100.3194)

Advanced Commands: gpupdate and gpresult

Let's now look at two advanced commands: **gpupdate** and **gpresult**.

Windows uses a set of policies to define rules that users and computers are effectively forced to follow. These policies can be viewed within the Local Group Policy Editor (**Run > gpedit.msc**) and a subset of that, the Local Security Policy (**Run > secpol.msc**). To properly work with these policies and tools, you should be running Windows Pro edition or higher.

You can also use commands to view and analyze that information. For example, the **gpresult** command displays the Resultant Set of Policy (RSoP) information for a user and computer. (It is designed for remote users/computers.) You can use **gpresult /R** to get some basic information about the local computer, the user, and what policies are running. You can view this information for remote computers and users by using the **/S** switch and the name of the remote system. For example:

```
gpresult /S computername /R
```

In this command, *computername* is whatever the target system's name is. To save the reported information, use the **/x** (for XML) or **/h** (for HTML) parameters.

In many cases, policy changes that were made in the Local Group Policy Editor or Local Security Policy won't take effect until the admin logs off and logs back on. Enter the **gpupdate** command, which can be used by itself or by specifying a remote system. When run, it updates all policies that have been modified on the target computer, without requiring the administrator to log off and log back on.

These commands can be run on Windows workstations or servers. But be very careful when using them. You have to be sure your policy changes are allowed, and you should consider scheduling them to run after work hours.

Note

For more information on **gpresult** and **gpupdate**, see the following sites:

https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpresult

https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate

Note

Although we just hit you with a lot of commands, you should try to memorize as many of them as you can! Try them on your computer and write them down to force those little gray cells into action.

Cram Quiz

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

1. Which command can copy multiple files and entire directory trees?

   - ○ **A. copy**
   - ○ **B. cut**
   - ○ **C. paste**
   - ○ **D. robocopy**

2. Which command determines whether protected system files have been overwritten and replaces those files with the original version?

   - ○ **A. chkdsk**
   - ○ **B. md**
   - ○ **C. sfc**
   - ○ **D. xcopy**

3. You need to assign drive letters and make a partition active from the Command Prompt. Which of the following will allow you to perform these activities?

   - ○ **A.** Disk Management
   - ○ **B. format**
   - ○ **C. defrag**
   - ○ **D. diskpart**

4. You have been tasked with bringing the policies of a Windows 11 computer up to date. You won't be able to log off and back on, and you must use the Command Prompt. Which of the following tools should you use?

   - ○ **A. shutdown**
   - ○ **B. rd**
   - ○ **C. gpupdate**
   - ○ **D.** Local Security Policy
   - ○ **E. winver**

5. Which command is the best option for a technician to learn more about the **ping** command from a Command Prompt?

   - ○ **A. ping help**
   - ○ **B.** [*command name*] **/?**
   - ○ **C. ping /?**
   - ○ **D.** Hey Siri, what is ping?

Cram Quiz Answers

1. **D. robocopy** can copy an entire drive of information with just one command (including switches). **xcopy** could also do the job, but **robocopy** takes its place.

2. **C. sfc** determines whether system files have been overwritten and replaces those files with the original versions. **chkdsk** can check for errors and fix some errors, but it cannot work with system files. **md** is the command used to make a directory. **xcopy** is used to copy large amounts of data to a new location.

3. **D. diskpart** is the command-line counterpart of Disk Management. From the DISKPART> prompt, you can create, delete, and extend volumes; assign drive letters; make a partition active; and so on. The **format** command is used to format storage

media to a particular file system, such as NTFS, FAT, or FAT32. **defrag** is the command-line version of the Disk Defragmenter; these tools help make the files on a drive contiguous instead of fragmented.

4. **C.** You should use **gpupdate** to bring the Windows policies up to date without requiring the admin to log off and on again. The **shutdown** command is used to turn off or restart a computer. **rd** is used to remove directories. The Local Security Policy is the place where you can go to modify many policy settings (such as the password policy), but it is a graphical tool. To enforce the changes made in the Local Security Policy, use the **gpupdate** command. **winver** is used to find out what operating system version you are running.

5. **C.** For more information about the **ping** command, you can enter **ping /?** at a Command Prompt. If you are ever stumped about a particular command, read the help file associated with it. The naming convention for this is **[***command name***] /?. ping help** is not a valid command. **[***command name***] /?** won't work unless you enter a valid command followed by a /?. Although Siri will tell you that **ping** is a computer administration software utility used to test network connectivity, Siri won't work from a Command Prompt!

Oh yeah! Now we're really starting to cook. The command line is what it's all about here. If you are new to the command line, we strongly urge you to review this chapter very carefully before you continue, and get in some practice as well; it's important that you become comfortable with the command line in order to be a success!

Chapter 35

Microsoft Command-Line Tools, Part II

This chapter covers a portion of the following A+ 220-1202 exam objective:

- **1.5** – Given a scenario, use the appropriate Microsoft command-line tools.

The command-line interface (also known as the CLI) is just so much fun we had to write another chapter about it. So, let's get into the networking side of commands. Now.

Networking Commands

There are many command-line tools that you can use in Windows to help analyze and troubleshoot a computer's network connection; in this section, we'll delve into several of them. We recommend that you try all the variations of these commands on your computer. Some commands require that you open the PowerShell or Command Prompt as an administrator (elevated mode).

The most commonly used command for analyzing a computer's networking configuration is **ipconfig**. Let's start with that.

ipconfig

The Internet Protocol configuration command, **ipconfig**, displays current TCP/IP network configuration values. This is one of the first tools you should use when troubleshooting network connectivity. When you type **ipconfig**, you get results similar to the following:

```
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
Link-Local IPv6 Address. . . . . :
fe80::404b:e781:b150:b91a%11
IPv4 Address. . . . . . . . . . . : 192.168.0.100
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.0.1
```

ipconfig combined with the **/all** option shows more information, including whether or not DHCP is being used, the DNS server's IP address, and the MAC address. The MAC address is the hexadecimal address that is burned into the ROM of the network adapter. It is a set of six hexadecimal numbers (for example, 00-03-FF-A0-55-16).

ExamAlert

To view additional IP configuration information, such as DNS servers and MAC addresses, use the **ipconfig /all** command.

Note

In Linux systems, the **ip** command is the equivalent of the Windows **ipconfig** command for configuring network interfaces.

The **ipconfig /all** command can offer a lot of information that can help you troubleshoot a problem. For example, if a user cannot connect to any Internet resources, the reason could be that the gateway address is improperly configured. Remember that the gateway address must be on the same network number as the IP address of the client computer. If a user can't connect to any websites but can connect to other computers on the LAN, the reason could be that the DNS server address is incorrectly configured. **ipconfig** also tells you whether the client computer's IP address

is obtained from a DHCP server or assigned via APIPA and whether it is a private or public address.

ipconfig can also be used to release and renew IP addresses. Sometimes this needs to be done if a computer's IP address is not working properly and you want to obtain a new address from a DHCP server. To release the current IP address, type **ipconfig /release**; to renew, type **ipconfig /renew**.

Finally, if you are having DNS issues (for example, problems connecting to websites), you can erase the DNS cache by typing **ipconfig /flushdns**. Check out the various **ipconfig** options by opening the Command Prompt and typing the **ipconfig /?** command. You should try this with every command in this section.

> **Note**
>
> Another way to flush the DNS cache is to issue the command **netsh int ip** in PowerShell. But beware: This command completely resets the TCP/IP connection for the network adapter.

ping

ping tests whether another host is available over the network. Using this command is an easy way to see if another host is "alive." Let's say your gateway's IP address is 192.168.0.1. To ping that device, you would type **ping 192.168.0.1** (as an example) and hopefully get the following output:

```
Pinging 192.168.0.1: with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

The replies in this case indicate that the host is alive, available, and can be communicated with on the network. Any other message would indicate a problem (for example, a "Request Timed Out" or "Destination Host Unreachable" message would require further troubleshooting). Keep in mind that if the local computer is configured incorrectly, you might not be able to ping anything! Also watch for the amount of time the ping takes to reply. A longer latency time could indicate network congestion.

Note

Latency is the time it takes for a remote computer to receive sent data packets. Latency increases with distance, type of network connection used, and network congestion. For example, a ping to a computer on the LAN should have very low latency—perhaps less than 1 millisecond (ms). But a ping initiated from a computer in New York City to a computer in Los Angeles over a cable Internet connection might have a latency of 25 ms. This can be a very enlightening piece of the ping results.

You can also use **ping** to test whether a computer has TCP/IP installed properly, even if it isn't wired to the network! To do this, use the **ping 127.0.0.1** command for IPv4 and **ping ::1** for IPv6. As you learned previously in the book, these IP addresses, known as *loopback addresses*, are used for testing and are available on every host that has TCP/IP installed. They differ from the IP addresses we talked about previously (for example, 192.168.0.100) in that they work internally. Loopback **ping** commands enable you to ping yourself, meaning you can test the local computer's network connection without a valid IP configuration and without a physical connection to the network. Replies are simulated within the local computer; they prove whether the network adapter and TCP/IP have been installed properly. However, they do not prove whether TCP/IP has been *configured* properly for a particular network.

Note

You can also use the **ping loopback** and **ping localhost** commands, adding **-4** for IPv4 and **-6** for IPv6. However, for testing, pinging the IP address is usually recommended.

ExamAlert

Know how to ping the local loopback IPv4 and IPv6 addresses.

You can also modify the way that **ping** works with options (also known as switches). Six that you should know for the exam are **-t**, **-n**, **-l**, **-a**, **-4**, and **-6**:

- **ping -t:** This pings the host until the command is stopped. Remember that a host is any device or computer that has an IP address. An example of this would be **ping -t 192.168.0.1**. The option can go before or after the IP address. You will keep getting replies (or timeouts) until you stop the command by pressing Ctrl+C or by closing the Command Prompt. This is a great way to test cable connections. After running the command, you can plug and unplug cables and watch the screen to see which cables or ports are live. You can also use this option to monitor a connection over a period of time to discern whether there are many packet drops or whether the connection slows down at certain times.
- **ping -n:** This pings a host a specific number of times. For example, the command **ping -n 20 192.168.0.1** would ping that host 20 times and then display the results. This can be a good baselining tool that you can run every day against a router or server and compare the results. (You would probably want to use a higher number than 20.)
- **ping -l:** This pings the host, but you can specify the number of bytes per packet to be sent. If you look at the previous ping results, you can see that the default number of bytes is 32, but this can be increased to simulate real data. For example, **ping -l 1500 192.168.0.1** would send

four 1500-byte packets to the other host. This can also be beneficial when testing how a server, a router, or another device reacts to larger packet sizes.

- **ping -a:** This resolves addresses to hostnames. When pinging an IP address with **-a**, you also see the hostname associated with the IP address.
- **ping -4:** This forces the use of IPv4 and results in IPv4-based data. For example, in Windows, if you are running both IPv4 and IPv6 and type a command such as **ping loopback**, your results will, by default, be IPv6 based and might result in a reply from ::1 (that is, if your system is working properly and IPv6 is configured). But by adding the **-4** option, you force the use of IPv4, so the command **ping -4 loopback** can result in a reply from 127.0.0.1. Try it!
- **ping -6:** This forces the use of IPv6 and results in IPv6-based data. For example, a **ping -6 loopback** will result in a reply from ::1.

ExamAlert

Know how to use the **-t**, **-n**, **-l**, **-a**, **-4**, and **-6** options with **ping**.

These options can be combined as well; for example, **ping -n 450 -l 1500 192.168.0.1** would send 450 pings, each 1500 bytes in size. To create a baseline, you could use this command at a specific time every month, store the results, and then compare them to find possible deficiencies in the performance of a server, router, and so on.

tracert and pathping

tracert, short for *traceroute*, builds on **ping** in that it sends packets to destinations beyond the local computer's network. It pings each router along the way between you and the final destination. If you run the command **tracert example.com**, you get output like this:

```
PS C:\Windows\System32> tracert example.com

Tracing route to example.com [93.7.128.175] over a maximum of 30 h
```

```
  1    <1 ms    <1 ms    <1 ms  gateway.localdomain [192.168.0.1]
  2     7 ms    17 ms     8 ms  10.42.13.1
  3     8 ms     8 ms     6 ms  router1.greencurtaintraining.
com[208.58.XXX.XXX]
  4    11 ms    12 ms    12 ms  router2.greencurtaintraining.
com [207.17.XXX.XXX]
  5    10 ms     9 ms    11 ms  router3.greencurtaintraining.
com [207.17.XXX.XXX]
  6    20 ms    11 ms    11 ms  207.17.XXX.XXX
  7    10 ms    10 ms    11 ms  96.7.128.175
Trace complete.
```

Note

The results of a **tracert** change based on origination and destination points. When you run this **tracert** yourself, you will have different results because your network is different than ours (try it from home and from work; you will find at least slight differences there). Sometimes you will even get slightly different results when running the same **tracert** at different times, depending on the load on the servers responding. That is completely normal. What you are looking for is the connection itself.

ExamAlert

Be able to recognize the output of a **tracert** command!

Some of the names and IP addresses have been changed to remain anonymous. In this example, note the three ping results per line item, each measured in milliseconds (ms). Every line item (hop) is a new entry, and may contain a router name and IP address, which will not always be true in

the real world (and that's okay; not all routers are registered with DNS). **tracert** starts by sailing through the various routers in the fictitious ISP, greencurtaintraining.com. It ends at a server simply named 96.7.128.175 (which is example.com). Try your own trace using **tracert example.com** (or another domain of your choice) from your own device to see results based on your location and ISP. Keep in mind that some traces will take longer and will go through additional hops.

If you see any asterisks in place of the millisecond amounts, you might question whether the router is functioning properly. If **tracert** stops altogether before giving the message Trace Complete, you should check your network documentation to find out which router it stopped at and/or have the appropriate personnel troubleshoot the router. As with **ping**, the **-4** and the **-6** options force IPv4 and IPv6, respectively.

The **tracert /d** command does not resolve IP addresses to hostnames. All names along the way (such as greencurtaintraining.com and gateway.localdomain) are shown as their corresponding IP addresses only. Running numeric versions of commands can be faster because there is no name resolution to get in the way. Connecting directly by IP address will always be faster than connecting by name.

Another command similar to **tracert** is **pathping**. One of the differences is that it does not show the three individual pings per hop initially; it instead computes the statistics of the pathping at the end. (You can specify the number of individual pings with the **-q** option, though.) Sometimes, this command might freeze (or *hang*), requiring you to press the Ctrl+C shortcut to break out of the process. **tracert** displays a list of all routers between the source and the destination and the time between the individual hops. **pathping** displays all the details that you get with **tracert** and also includes details like latency and packet loss between all the routers and the source computer.

hostname

The **hostname** command simply displays the name of the local computer. Try typing the command **hostname** at the command line, and you will see the name of the system displayed. This is the same hostname that is shown

in the Computer Name/Domain Changes dialog box (refer to Figure 31.2 in Chapter 31, "Basic Features of Windows Editions"). However, you can't *change* the hostname at the command line with the **hostname** command; you have to do it in the GUI either in the Computer Name/Domain Changes dialog box or by going to **Windows Settings > System > About** and clicking **Rename this PC**. Now, you might say, "Hey! This is a chapter about doing things at the command line! How do I do it?" Okay, since you asked, open PowerShell and type this:

```
rename-computer -newname "name here"
```

Then you need to restart the computer for the changes to take effect. (Or simply add **-restart** to the end of the command to do a restart automatically.)

> **Note**
>
> Programmatically, the hostname is referred to as the %COMPUTERNAME% variable in any Windows system. Developers can use this variable to specify the system's name without knowing the actual hostname! Try the following command in the Command Prompt:
>
> **echo %COMPUTERNAME%**
>
> You will then see the hostname displayed once again—only this time it's all uppercase characters. We will cover variables further in Chapter 62, "Basic Scripting, Part I," and Chapter 63, "Basic Scripting, Part II."

As you read the next section, see if you can locate the hostname of the local computer.

netstat

netstat shows the network statistics for the local computer. The default command displays sessions to remote computers. In the following example, we connected to google.com and ran the **netstat** command:

```
Active Connections

TCP Music-Box:1395 8.15.228.165:https ESTABLISHED

TCP Music-Box:1396 he-in-f101.google.com:https ESTABLISHED
```

ExamAlert

Be able to recognize the output of a **netstat** command!

The above output shows two established TCP sessions to the same website, google.com. In the local address column, you see the computer's name (Music-Box) and the outbound ports it uses to access the website (1395 and 1396). In the foreign address column, you see an IP address and the protocol used (https); in the second session, you see a hostname followed by the protocol (again https). The protocol used by google.com corresponds to port 443.

This command can tell you a lot about your sessions (for example, whether a session times out or whether it closes completely). To see this information numerically, try using the **-n** option. To see TCP and UDP sessions, use the **-a** option. To see TCP *and* UDP in numeric format, use the **-an** option. To include the executable name for each session shown, use the **-nab** option.

Note that if you said *Music-Box* is the hostname of the local computer in the preceding example, you are correct!

Note

There are plenty of other **netstat** options. For example, **netstat -e** shows Ethernet statistics. For more information on **netstat**, see https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/netstat.

nslookup

nslookup queries DNS servers to discover DNS details, including the IP addresses of hosts. For example, to find the IP address of example.com, you would type **nslookup example.com**. The resulting output should look something like this:

```
Non-authoritative answer:
Name: example.com
Addresses: 93.184.215.14
2606:2800:21f:cb07:6820:80da:af6b:8b2c
```

From this output, you now know the IP addresses that correspond to the domain name example.com. The results show an IPv4 address (93.184.215.14) and an IPv6 address (2606:2800, etc.).

nslookup means *name server lookup* and can aid in finding DNS servers and DNS records in a domain as well. If you type the command by itself, it brings you into the **nslookup** shell. From here, you can use several commands. To find out more about these commands, type **?** and press Enter. To exit the **nslookup** shell, type **exit**, press Ctrl+C, or press Ctrl+Break. The Linux equivalent of this is **dig**, which can also be installed in Windows as part of the BIND DNS tools (see https://www.isc.org/downloads/). We strongly suggest that you use **dig** whenever possible. You will learn more about **dig** in Chapter 40, "Linux."

net

The **net** command is actually a collection of commands. You can use the **net stop** command to stop a service and the **net start** command to start a service from the command line. In networking, you might use the **net view** command to see which computers are currently available on the network or the **net share** command to share folders for other users to view.

For the exam, you should know the types of **net** commands that enable you to view or create mapped network drives. To view any currently mapped

network drives, simply type **net use**. To create a mapped network drive, use the following syntax:

```
net use x: \\computername\sharename
```

where *x*: is the drive letter. (In this case, *x* is a variable; you can use whatever drive letter you want, if it's available, including x!) *computername* is the name of the remote host you want to connect to, and *sharename* is the share that was created on that remote host. You can connect to whatever share you want, as long as you have permissions to do so.

You can even connect to hidden shares—denoted with a $ at the end of the share name. For example, say there is a network share called c$ on another computer on the network. The following example shows the command to connect to it and the resulting output:

```
net use f: \\Music-Box\c$
The command completed successfully.
```

This example uses f: as the drive letter; the computer connected to is called Music-Box, and the share is c$ (the default hidden share).

For more information on the **net** command, type **net /?**. For more information on the **net use** command, type **net use /?**.

ExamAlert

Know how to use the **net use** command, and why!

Note

See the following link for a video demonstrating how to use **net share** and **net use** between two systems: https://youtu.be/3r3GeejOqY8. Although this video is older, the content is still relevant and valid for small network sharing.

Another **net** command listed in the A+ objectives is **net user**. When typed by itself, this command lists the user accounts on the local computer. You can also create accounts from here with the **net user /add %username%** command, where **%username%** is a variable. For example, to create the user account *user*, you would type **net user /add user**. This creates a standard user account. In addition, you can activate or deactivate user accounts with the **/active** option or delete accounts with the **/delete** option. There is lots more; check out the command with **/?** for more information.

whoami

The **whoami** command displays user, group, and privileges information for the currently logged-in user. Without parameters, it also displays the current domain and username.

Especially when you're working with remote devices, it is important to know which device and user you are dealing with to ensure that you have the correct device and permissions. **whoami** gives you that information.

If you want all of the information about a specific device, you can use the **/all** parameter; this will tell you not just the domain and user but also the Active Directory groups (as applicable), any privileges, and any additional permissions information that is applicable for this user and system. Using this command, you can learn a significant amount of information about a system quickly to diagnose and resolve problems.

Cram Quiz

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

1. Which command shows the path of routers between your computer and a web server?

   - **A. ping**
   - **B. ipconfig**

- ○ **C. tracert**
- ○ **D. nbtstat**

2. You need to map a network drive to a share named data1 on a computer named Jupiter-Server. You want to use the J: drive letter. Which syntax should you use to do this in the Command Prompt?
   - ○ **A. net use J: \\Jupiter-Server\data1**
   - ○ **B. net use J \Jupiter-Server\data1**
   - ○ **C. net use Jupiter-Server\J\data1**
   - ○ **D. net use J: \Jupiter-Server\data1**
3. A user's computer is powered on and appears to work properly. However, the user cannot access any wired network resources, printers, or shared drives. In addition, the user cannot access the Internet. Which of the following commands should you use to troubleshoot the problem?
   - ○ **A. netstat**
   - ○ **B. net use**
   - ○ **C. ping**
   - ○ **D. nslookup**
4. A customer is unable to access a network share. However, the customer can access email. You analyze the system and confirm that the customer has the correct permissions to access the share. Which command should you use first to troubleshoot the problem?
   - ○ **A. nslookup**
   - ○ **B. net use**
   - ○ **C. ipconfig**
   - ○ **D. ping**
5. A customer's computer running Windows cannot connect to any Internet resources. Which command should you use to ensure that

the gateway address of the customer's computer is on the same network number as the IP address of the client computer? (Select the best answer.)

- **A. ip**
- **B. whoami**
- **C. ipconfig /all**
- **D. pathping**

Cram Quiz Answers

1. **C. tracert** is used to run a trace between the local system and a remote destination. It shows all routers along the way. **ping** is used to test connectivity to another system directly. **ipconfig** displays the Internet Protocol configuration of the local computer. **nbtstat** shows the name table cache and services running on the system.

2. **A.** You should use the command **net use J: \\Jupiter-Server\data1**. All the other answers are incorrect. The Universal Naming Convention (UNC) is *computername**sharename*.

3. **C.** Of the listed answers, the best one is the **ping** command. It will help you to decipher what the problem is. However, consider using **ipconfig /all** before running **ping**. The **netstat** command shows a list of current connections (among other things). Chances are that there are none currently in the scenario. The **net use** command displays and makes connections to remote shares. The **nslookup** command does name resolution between domain names and IP addresses.

4. **B.** Implement the **net use** command so that you can make the connection to the network share. (Of course, you could also do this in File Explorer, but this chapter is about the command line!) Use **nslookup** to resolve domain names to IP addresses or to modify DNS servers. Use **ipconfig** to analyze the system. Use **ping** to test whether another system is "alive" on the network.

5. **C.** The **ipconfig** command displays current TCP/IP network configuration values such as IP address, subnet mask and default gateway. The **ipconfig /all** command can offer a lot of information that can help you troubleshoot problems. If a user cannot connect to any Internet resources, the reason could be that the gateway address is improperly configured. Remember that the gateway address must be on the same network number as the IP address of the client computer. In Linux systems, the **ip** command is the equivalent of the Windows **ipconfig** command for configuring network interfaces. The **whoami** command displays user, group, and privileges information for the currently logged in user. Without parameters, it also displays the current domain and user name. **pathping** displays all the details that you get with **tracert** and also includes details like latency and packet loss between all the routers and the source computer.

That's it for the Windows command line—for now. But keep practicing! Chances are you'll be called on to use it.

Chapter 36

Windows Control Panel Utilities

This chapter covers the following A+ 220-1202 exam objective:

- **1.6** – Given a scenario, configure Microsoft Windows settings.

In Windows there are two main configuration areas: the Control Panel and the newer Settings (covered in Chapter 37, "Windows Settings"). Over time, Microsoft has been moving away from the Control Panel and more toward Settings; however, the Control Panel is still a useful place for administrators to configure some things in Windows.

In this chapter, we'll discuss some of the utilities that are stored in the Windows Control Panel, and we'll dig through a bunch of dialog boxes and other utility windows. Take some time to look at your Windows system's Control Panel and familiarize yourself with the various icons that are displayed—in Category mode and in icons mode. Let's begin.

Note

Some of the items listed in this CompTIA A+ objective are covered elsewhere in the book.

As always, we highly recommend opening and working on programs and utilities within a virtual machine or on a system that is located on an isolated test network (or both!).

ExamAlert

Objective 1.6 concentrates on the following Control Panel utilities: Internet Options, Devices and Printers, Programs and Features, Network and Sharing Center, System, Microsoft Defender Firewall, Mail, Sound, User Accounts, Device Manager, Indexing Options, Administrative Tools, File Explorer Options, Power Options, Ease of Access, Time and Language, Update and Security, Personalization, Apps, Privacy, System, Devices, Network and Internet, Gaming, and Accounts.

Opening and Viewing the Control Panel Utilities

An administrator can use the Control Panel to make system configuration changes, such as making connections to networks, installing or modifying new hardware, and so on. You can open the Control Panel in a variety of ways, including

- Click **Start**, enter **Control Panel** in the search bar, and select it.
- Type **control** in the Search field or Run prompt.

By default, the Control Panel shows up in Category view. For example, in Windows 10, System and Security is a category. To see all the individual Control Panel icons, click the drop-down arrow next to **View by: Category**, and then select either **Large icons** or **Small icons**. By doing so, you change the path to **Control Panel > All Control Panel Items**, which you will be using for the rest of this chapter.

Get used to working in the Control Panel but keep in mind that as of Windows 10, some of the icons and configurations have been moved to the Settings area, and this continues with each version of Windows 11. Be ready to operate these tools—for the exam and for the real world.

ExamAlert

The CompTIA A+ exams expect you to know the individual icons in the Control Panel. In Windows, this is also referred to as All Control Panel Items. Study them!

You will see a few dozen items within the Control Panel when you open it as All Control Panel Items, otherwise known as icons mode. Let's examine some of them now.

Internet Options

If you want to make configuration changes for Internet Explorer (IE), you go to Internet Options; however, Internet Explorer has been replaced by Edge (which, for the most part, has its own settings), and many organizations use other browsers. It's on the CompTIA objectives though, so let's look at it at least briefly.

If you open the Internet Options applet in the Windows Control Panel, it brings up the Internet Properties dialog box. You can also open it by going to **Run** and typing **inetcpl.cpl**. If you need to configure Internet Explorer to open a certain home page or use a specific certificate, these tabs are where you need to go. Another example is special network connections, such as proxy-based connections, which you can configure in the Connections tab. But remember that these settings are specific to the Internet Explorer browser, which was end of life (EOL) in June 2022. Since EOL, it now is used to configure the "IE Mode" within Edge only.

Note

To configure settings in the newer Edge browser, open the browser and type **edge://settings** in the address bar, or go to the three dots in the upper-right corner of the Edge page and select the gear (Settings).

These are the tabs in Internet Options:

- **General:** In this tab, you can set the home page (or pages), configure how pages are displayed, delete the browsing history, and change the appearance of the browser.
- **Security:** Here, you can create and modify security zones—including the Internet—and change the security levels for each zone.
- **Privacy:** In this tab, you can block or allow specific websites (domains) and enable/configure the pop-up blocker.
- **Content:** Use this tab to find out what security certificates have been installed that the browser can use and to import new certificates. You can get more in-depth information about certificates in the Certificate Manager (certmgr.msc). In this tab, you can also change the setting for AutoComplete, which suggests full words and phrases based on the first several letters that you type into the URL bar and text fields.
- **Connections:** Here, you can set up different connections to the Internet, including broadband and dial-up, and manage LAN settings, including the ability to connect to websites via a proxy server.
- **Programs:** Use this tab to select how links will be opened, manage add-ons, use an HTML editor, and set programs and associations with Internet Explorer/Edge.
- **Advanced:** This tab is the catch-all for the rest of the settings that don't fit in the other tabs, as well as advanced settings such as international, multimedia, and security settings. You may have to access this tab from time to time. Take a minute to scroll through the different options that are listed here.

Devices and Printers

In Devices and Printers, you can add, configure, troubleshoot, and remove printers and other devices, such as monitors, UPSs, wireless devices, mice, and audio/multimedia devices. Most technicians use Devices and Printers for printers, and if you do, you'll find that it can be a good launching point for the configuration of other devices on the system. If you open Devices and Printers within the Windows 11 Control Panel, the Bluetooth & devices

Settings app opens. We discuss this Control Panel utility further in Chapter 19, "Multifunction Devices/Printers," and elsewhere in the book.

Note

We'll discuss the Network and Sharing Center, another Control Panel utility listed under Objective 1.7, in Chapter 38, "Windows Networking."

Programs and Features

You use Programs and Features to modify Windows applications and features, as well as third-party applications and features, and to repair them or uninstall them.

You can get to the list of options under Programs and Features from the Control Panel by selecting **Programs** (this time in Category view). You can then see options to uninstall programs, turn Windows features on or off, view the installed updates for Windows and other programs, and run programs made for previous versions of Windows. Except for that last one, these options are also available if you go to **Control Panel > All Control Panel Items > Programs and Features**. (Or you can go directly there by accessing **Run** and typing **appwiz.cpl**.)

If you need to uninstall or repair a program, or if you need to add features (such as Hyper-V or the .NET Framework), use Programs and Features.

ExamAlert

Know how to access Programs and Features to repair, uninstall programs, or turn Windows features on or off.

Microsoft Defender Firewall

The Microsoft Defender Firewall is Microsoft's built-in software that can protect a system from unwanted inbound connections. To make sure it is on, simply click the Control Panel icon and view the status of the private and public networks. Remember that green is good, and red is bad. To enable or disable the firewall, click **Turn Microsoft Defender Firewall on or off** and then modify the firewall as necessary. You can also access it by going to **Run > firewall.cpl**. We'll discuss this tool further in Chapter 37 and in the security portion of this book.

> **Note**
>
> As of Spring 2025, Microsoft was in the process of renaming Windows Defender Firewall to Microsoft Defender Firewall, and both names appear in Windows. They are the same product. When we reference them in this book, either in text or in images, know that it's because the versions of Windows we're using are, like yours, updated frequently and sometimes the names change daily. Eventually we believe that the new name will become Microsoft Defender Firewall, so have attempted to standardize on that name throughout the book, but you might see the other name sometimes.

Mail

The Mail icon opens a control panel that allows you to create one or more email profiles that work with Microsoft Outlook. To create a new profile, you need to know your email address, password, and server types. For more information on email client configuration, see Chapter 3, "Mobile Device Network Connectivity and Application Support."

Sound

Audio takes a back seat in the A+ certification somewhat, but in some environments it is crucial. To troubleshoot audio problems, click the Sound icon to open the Sound dialog box, as shown in Figure 36.1. You can also

get to this dialog box by right-clicking the sound icon in the notification area and selecting **Sounds** or by going to **Run** and typing **mmsys.cpl**.

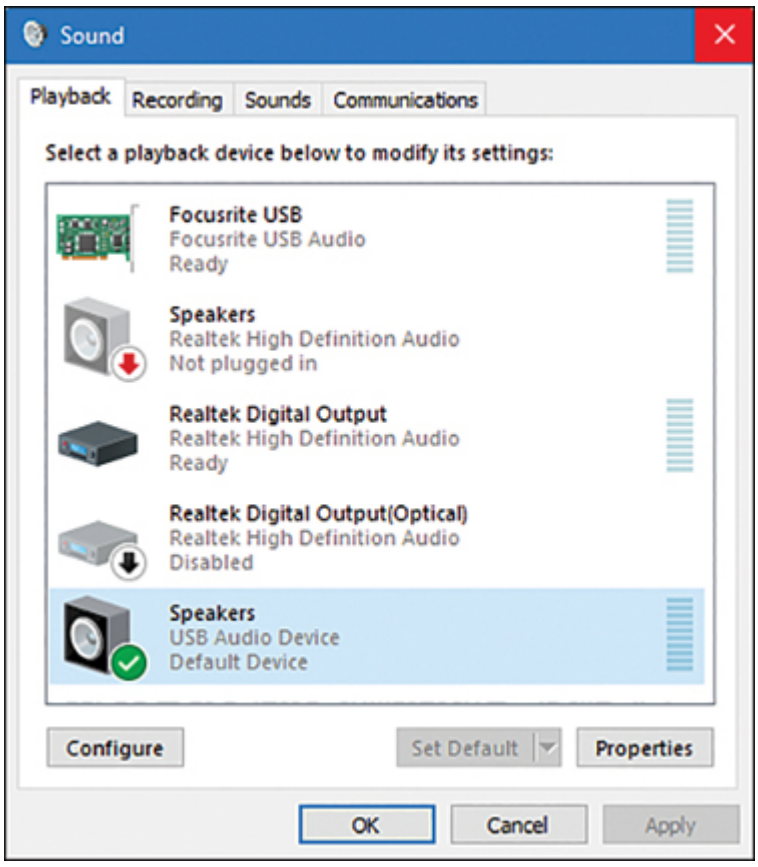


FIGURE 36.1 **Sound Dialog Box in Windows**

You can use this dialog box to modify which audio devices are used for playback and recording and to select specific sound themes for Windows. You can also modify what happens with the volume of Windows and programs when communications are detected (for example, video chatting or webinars).

In Figure 36.1, notice that the device simply called Speakers is checked; this means it is the default device that will be used for the playback of audio. On your system, perhaps that is a USB headset. In addition, there is a Focusrite USB device whose status is Ready. To output audio from that device, you could right-click its icon and select **Set as default device**. The same process is necessary in the Recording tab if you are using multiple microphones and recording devices. For technicians, educators, presenters,

and video bloggers who want to incorporate better microphones than the ones that are included with a system, the Recording tab of the Sound Control Panel is critical. However, if you have a custom audio processor with its own software, you might have to access that instead of the Sound dialog box to get full functionality—or, possibly, to have any functionality at all.

ExamAlert

Know how to enable and disable audio devices in the Playback and Recording tabs of the Sound dialog box.

User Accounts

When you open User Accounts, you can change your account name and account type (for example, administrator or standard user), and you can manage other accounts. You can also manage credentials and file encryption certificates, modify User Account Control (UAC) settings, and configure advanced user profile settings. However, to create new accounts, you either need to be redirected to the Settings area or use Local Users and Groups (which is the preferred method for administrators) by accessing **Run** and typing **lusrmgr.msc**. We'll discuss user accounts further (especially user security) as we move through the book.

Note

We cover the Device Manager in Chapter 32, "Microsoft Operating System Features and Tools, Part I."

Indexing Options

Indexing is the cataloging of file information. It helps you find results faster when you search your files for names or keywords. Indexing runs automatically on Windows and constantly tracks any changes to indexed

areas. The index can take up as much as 10 percent of the size of the indexed files, so this is something to keep in mind when you're working with Windows systems.

When you open the Indexing Options control panel, you see a list of indexed locations such as Users and Microsoft OneNote. If you click the Modify button, you can change what locations are indexed. But be careful! If you select an entire drive (for example, C:), you could really slow down the performance of the system. If you click the Advanced button, you will see options to rebuild the index, change the index storage location, and change the file types that will be indexed.

> **Note**
>
> Most of the tools have been moved to the Windows Tools as of Windows 11 (Administrative Tools in Windows 10 and earlier). We cover the bulk of these tools in Chapters 32, "Microsoft Operating System Features and Tools, Part I," and 33, "Microsoft Operating System Features and Tools, Part II."

File Explorer Options

You can use the File Explorer Options icon to modify how folders display information, whether or not certain data is visible, and how indexes are searched. Once the File Explorer Options control panel is open, you see a few tabs. Let's look at them now.

> **Note**
>
> You can also open this control panel within File Explorer. To do this, make sure you have This PC or a folder clicked. Then, on the menu bar, click **View**, locate and click the **Options** drop-down menu, and then click **Change folder and search options**. (In Windows 11, click the three dots to the right of View.)

The General tab gives you the option to change how folders are browsed. By default, folders are opened in the same window, but you could modify this setting so that each clicked folder opens in a separate window. Just be careful because clicking folders could result in a lot of open windows and confusion. You can also choose whether to single-click or double-click to open items as a preference. You can also increase privacy by deselecting the two options for showing recently used files and folders in the Quick access areas.

The View tab allows you to apply a *view*, which is a way of organizing all folders. So, for example, if you were viewing a current folder in File Explorer in Details view, you could set that view to all folders in the system by clicking **Apply to Folders**. Note that this option works only if you are currently in File Explorer and have a folder open. It doesn't work if you open File Explorer Options from the Control Panel.

Importantly, the View tab offers some more specific options (see Figure 36.2).

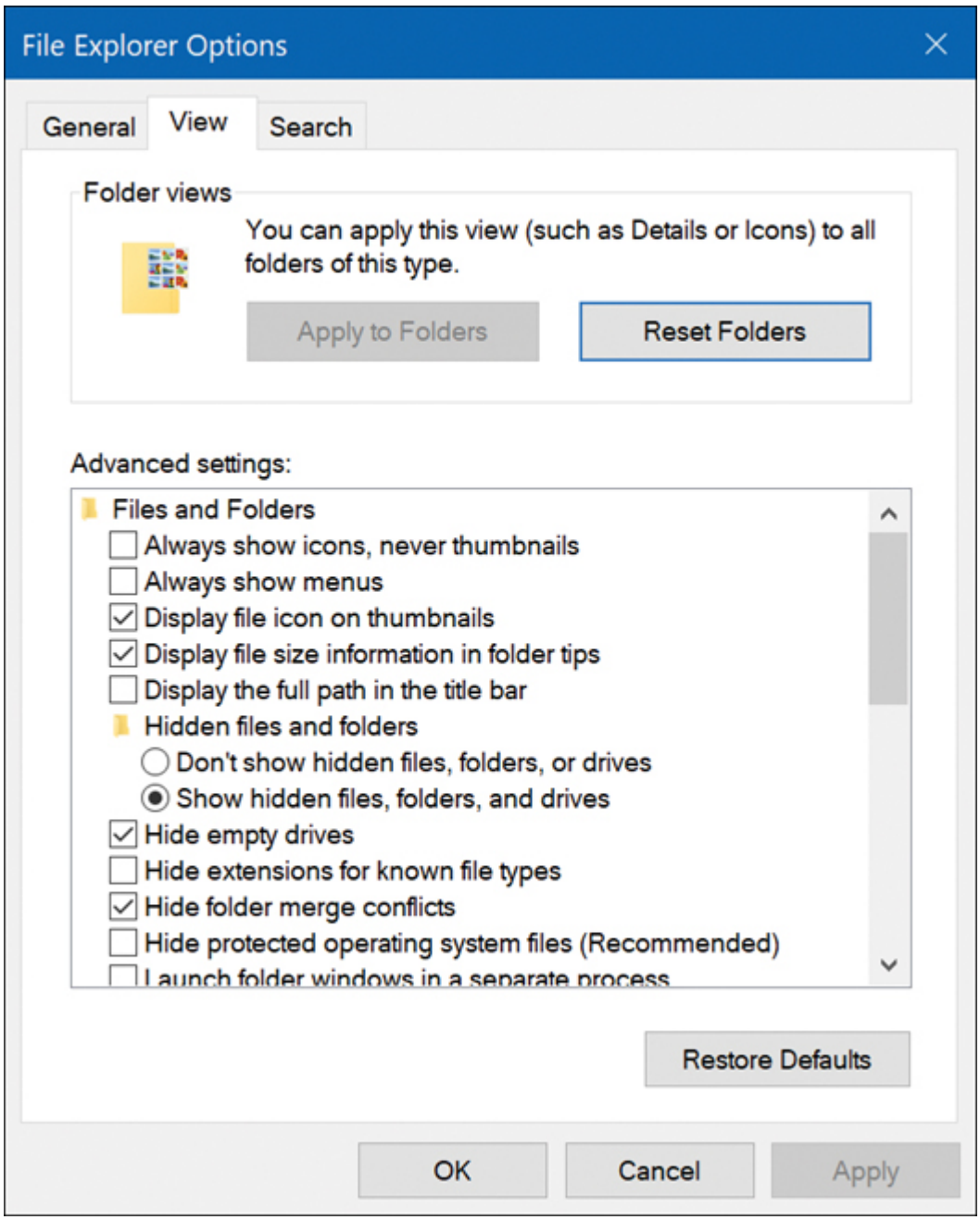


FIGURE 36.2 **The File Explorer Options Dialog Box, Opened to the View Tab**

For example, hidden files are not displayed by default. But if you select the **Show hidden files, folders, and drives** radio button, hidden files will be displayed in File Explorer. Another option a couple of lines below that is **Hide protected operating system files (Recommended)**. This option is

checked by default, but if you were to deselect it, system files would become visible to you. If you were to do both of these things, then files such as bootmgr and pagefile.sys would become visible in the root of C:. You can also deselect the **Hide extensions for known file types** checkbox so that you can see all the extensions associated with files. All these are great options for an administrator, but they are not set up by default so that typical users don't get any more information than they need. Spend a little time configuring the various File Explorer options in the View tab and consider what would be best for the typical user and what would be best for the admin.

ExamAlert

Exam Objective 1.6 calls out certain File Explorer options. You must be able to view hidden files, show and hide file extensions, and know how to deal with other general and view options when viewing files. These will be on your test, so be sure to pay close attention to them.

The Search tab enables you to turn off indexing. Doing this might result in slower searches, but you might need to turn off this option when troubleshooting a system if you suspect an issue with the indexing system, and especially if you suspect the indexing system is causing system-wide slowdowns.

Power Management

Optimizing an operating system involves managing power wisely. You can manage power for storage drives, the display, and other devices; you can even manage power for the entire operating system.

Some configurations can be done from the Power Options icon (which you can access directly from **Run > powercfg.cpl**). You can select what the Power button does and what closing the lid of a laptop does. For both of these, you can select from Do nothing, Sleep, Hibernate (if enabled), Shut down, and Turn off the display. You can also display the Sleep and

Hibernate options in the Power menu, and you can turn on fast startup, which helps restart the computer faster after a full shutdown.

You might also want to turn off devices in Windows after a specified amount of time. From the Power Options initial screen, you can create or select a power plan such as Balanced, Eco, Power Saver, or High Performance, depending on the computer. Proprietary computers (such as Dell, HP, and so on), especially laptops, have their own preferred plans that balance power and performance according to the laptop's hardware.

There are a lot of settings within these power plans. For example, you can select **Balanced** and click **Change plan settings**, and you see that the display is set to turn off after a certain amount of time; you can set it to anywhere from 1 minute to 5 hours, or you can set it to never.

Going a little further, if you click the **Change advanced power settings** link, the Power Options dialog box appears, as shown in Figure 36.3. Using this dialog box, you can specify how long before the storage drive turns off and set power savings for devices such as the processor, display, PCI Express, and so on.

Another option is USB Selective Suspend. It is enabled by default, and it effectively reduces the power to USB devices that have been inactive for a period of time. It is a great power saver for laptops. Take a few minutes to look through the options in the Power Options dialog box.

Now, let's go a bit beyond the Control Panel. Some users confuse the terms *standby* and *hibernate*, but the two terms have different meanings:

- **Standby:** This means that the computer goes into a low-power mode, shutting off the display and storage drives. Information that you were working on and the state of the computer are stored in RAM. The processor still functions but has been throttled down and uses less power. Taking the computer out of standby mode is a quick process; it usually requires the user to press the Power button or a key on the keyboard. It takes only a few seconds for the CPU to process the standby information in RAM and return the computer to the previous working state. Storage drives and other peripherals might take a few more seconds to get up to speed. Keep in mind that when there is a loss

of power, the computer will turn off, and the contents of RAM will be erased unless there is a built-in battery (as in a laptop) or the computer is connected to a UPS; but either way, uptime will be limited. Note that some laptops still use a fair amount of power when in standby mode.

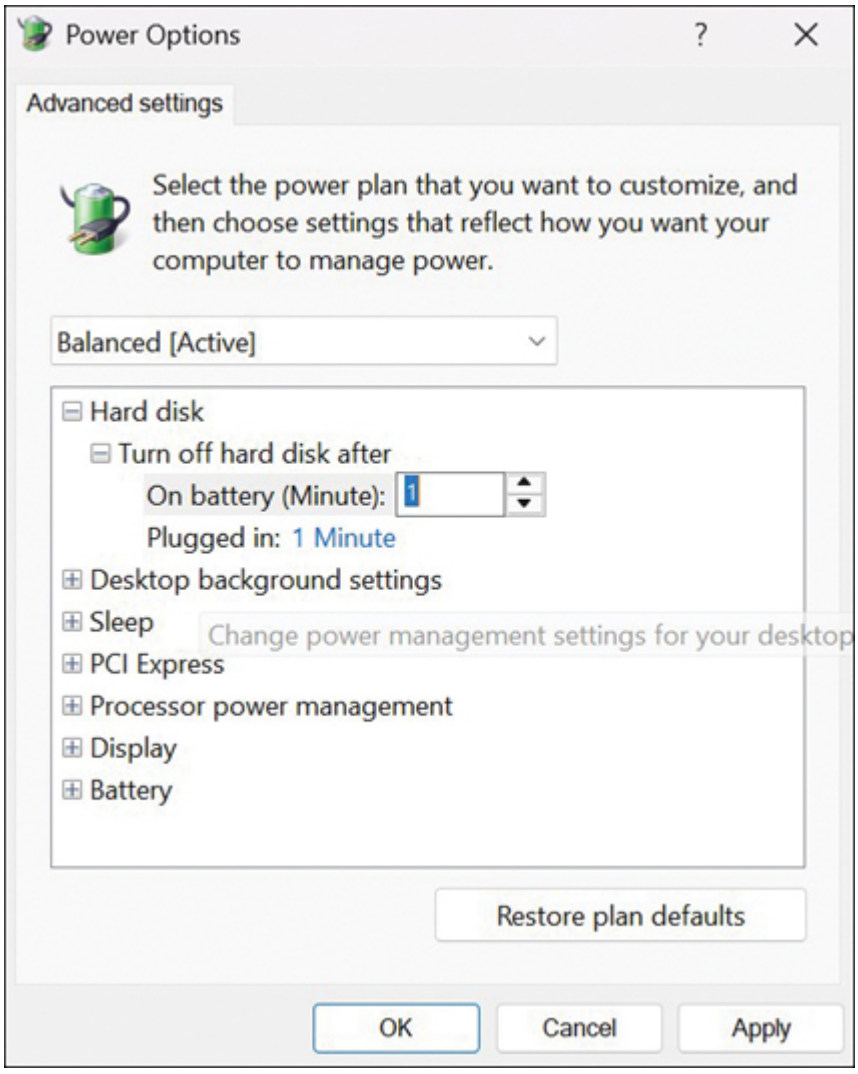


FIGURE 36.3 **Windows Power Options Advanced Settings Dialog Box**

- **Hibernate:** This is different from standby in that it effectively shuts down the computer. Hibernation consumes the least amount of power of any power state except for when the computer is turned off. All data that was worked on is stored to the C: drive, in a file called hiberfil.sys. This is usually a large file. Because RAM is volatile and the storage drive is

not, hibernate is a safer option when it comes to protecting the data and the session that you were working on, especially if you plan to leave the computer on for an extended period of time. However, because the drive is so much slower than RAM, coming out of hibernation takes longer than coming out of standby mode. Hibernation has also been known to fail in some cases and cause various issues in Windows.

Standby is known as Sleep in Windows and is accessible in the same location as the Shutdown or sign out options. Either use the **Start** button (click or right-click) or press Alt+F4 (after all other programs have been closed).

Before you can use hibernation, you might need to turn on hibernation. This requires some doing, so hold on to your hats! To enable hibernation in Windows, do the following:

1. If you have the Power Options dialog box open, close it.
2. Open the PowerShell/Command Prompt as an administrator. Then type **powercfg.exe /hibernate on**.
3. Open the Power Options dialog box. Hibernate should now appear as an option in the dialog box.
4. Expand **Sleep** and expand the **Hibernate after** option and set it to the number of minutes you desire. The system is now set to automatically go into hibernation mode after the number of minutes of inactivity that you selected.
5. Finally, you can display the Hibernate option in the power menu. Go to **All Control Panel Items > Power Options** and click either **Choose what the power buttons do** or **Choose what closing the lid does**. From there, you can click the **Hibernate** checkbox so that it will show in the power menu. (If the checkbox is grayed out, click the **Change settings that are currently available** link above so that you can modify the setting.) Save your settings.
6. Check the Start menu again, and you should see the Hibernate option there, just below Sleep.

To disable hibernation, deselect the settings you chose in steps 4 and 5 and run the command **powercfg.exe /hibernate off**.

ExamAlert

Know the differences between standby, sleep/suspend, and hibernate and understand how to set up hibernation in Windows. Understand the various Power Options power plans and settings for Choose what closing the lid does, Turn on fast startup, and USB selective suspend.

Note

For a detailed review of managing power settings in Windows, visit https://www.windowscentral.com/how-manage-power-settings-windows-11.

Ease of Access Center

The Ease of Access Center allows a user to turn on a variety of tools: the magnifier to view small objects more easily, the narrator for voice prompts while working in Windows, the onscreen keyboard, and high contrast.

Several other options are available to make Windows easier to use, including making the display easier to see, using the computer without a keyboard or mouse, making the keyboard and mouse easier to use, and so on. There is also an Ease of Access Center available in Settings (which is accessible via the keyboard shortcut Windows+U).

Bonus: Storage Sense

A new feature has been implemented in Windows called Storage Sense. This feature allows Windows to clean up your temporary files and empty

the trash can automatically. If you set it to do so, it can also delete files in your Downloads folder.

The old method for doing this was with Disk Cleanup, which worked great but had to be run manually. Storage Sense automatically detects low disk space and runs to free up space on your drives. You can also select when you want it to run. To configure Storage Sense, navigate to **Start > Settings > System > Storage**.

Cram Quiz

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

1. Which power management mode stores data on a storage drive?

   - ○ **A.** Sleep
   - ○ **B.** Hibernate
   - ○ **C.** Standby
   - ○ **D. Pillow.exe**

2. What tool can assist a user who needs to find results faster when searching for files on a storage drive?

   - ○ **A.** firewall.cpl
   - ○ **B.** Internet Options
   - ○ **C. appwiz.cpl**
   - ○ **D.** Indexing

3. You are about to start troubleshooting a Windows system. You need to be able to view the bootmgr file in the C: root of the storage drive. Which of the following should you configure to make this file visible? (Select the two best answers.)

   - ○ **A.** Hidden files and folders

- ○ **B.** Extensions for known file types
- ○ **C.** Encrypted or compressed NTFS files in color
- ○ **D.** Protected operating system files

4. A customer wants you to set up the system to scale images at 200 percent. Which Control Panel icon should you access to configure this?
   - ○ **A.** Programs and Features
   - ○ **B.** Mail
   - ○ **C.** Sound
   - ○ **D.** Ease of Access Center
   - ○ **E.** Devices and Printers
5. Which of the following would you use to repair or uninstall a program or turn Windows features on or off?
   - ○ **A. firewall.cpl**
   - ○ **B. mmsys.cpl**
   - ○ **C. lusrmgr.msc**
   - ○ **D. appwiz.cpl**

Cram Quiz Answers

1. **B.** When a computer hibernates, all the information in RAM is written to a file called hiberfil.sys in the root of C: within the storage drive.
2. **D.** Indexing helps you find results faster when you search your files for names or keywords. Indexing runs automatically on Windows and constantly tracks any changes to indexed areas. **firewall.cpl**, when issued in the Run prompt or at the command line, opens Microsoft Defender Firewall. The Internet Options dialog box (**inetcpl.cpl**) is primarily associated with the Internet

Explorer web browser. But some settings within Internet Options, which are part of the Windows system, can still influence Microsoft Edge's behavior, particularly regarding security and privacy settings. **appwiz.cpl** opens the Programs and Features window, where you can uninstall or change programs and turn Windows features on and off.

3. **A and D.** In **File Explorer Options > View**, you can configure hidden files and folders and set it to **Show hidden files, folders, and drives**, and configure protected operating system files by deselecting the check mark for the setting **Hide protected operating system files**. Files such as bootmgr are hidden and protected by default; you need to unhide them in both ways to see them.

4. **D.** You can use the Ease of Access Center to turn on the magnifier and increase the view of the display to 200 percent. You can also operate the magnifier with keyboard shortcuts: Windows+Plus (+) to turn it on or to increase scaling; Windows+Minus (-) to reduce scaling; and Windows+Esc to turn off the program. Programs and Features is used to add and remove programs and add specific features to Windows. Mail and Sound are self-explanatory: They allow you to configure email and sound profiles, respectively. Devices and Printers is where you go to configure printers, keyboards, and multimedia devices.

5. **D.** Accessing **Run** and typing **appwiz.cpl** opens Programs and Features in Windows, where you can repair, uninstall programs, or turn Windows features on or off. You can access the Microsoft Defender Firewall by going to **Run** and entering **firewall.cpl**. Entering **mmsys.cpl** from **Run** opens the Sound dialog box. Entering **lusrmgr.msc** from **Run** opens Local Users and Groups.

Tremendous! Review your notes, take a short break, and then continue!

Chapter 37

Windows Settings

This chapter covers the following A+ 220-1202 exam objective:

- **1.6** – Given a scenario, configure Microsoft Windows settings.

The Windows Settings utility is designed to be the replacement for the Control Panel. Keep this in mind as you work in both configuration systems. Windows Settings is set up to be easy for typical users to navigate and to search for the options they require.

This chapter starts easily enough, but it gets a little deep as it progresses. Be sure to take notes and practice the configurations on a test installation of Windows. Since Windows 10 is end of life in late 2025, we will concentrate on Windows 11. Where there are major differences in Windows 10, we will mention them. Let's get into Settings now.

ExamAlert

Objective 1.6 concentrates on the following Windows settings: File Explorer Options, Power Options, Time & Language, Update & Security, Personalization, Apps, Privacy, System, Devices, Network & Internet, Gaming, and Accounts.

Note

Administrative Tools in prior versions of Windows is now called Windows Tools starting in Windows 11. Realize that it's pretty much the same content. Where the content you expected to see is no longer in Windows Tools, you should look for that content in Settings.

How to Access Windows Settings

The typical way to get to Windows Settings is to click **Start** and click the **Settings** gear; however, there are many other options. Here are some alternatives for you:

- Right-click **Start** and select **Settings**.
- Open the **Search** tool and type **Settings**.
- Press the Windows+I keyboard shortcut.
- Open **Run** and enter the **ms-settings:** command.
- Open PowerShell or the Command Prompt and enter **start ms-settings:**.
- Open it from File Explorer or from the Action Center.
- Create a shortcut by right-clicking on the desktop and going to **New > Shortcut**. Then, in the Location field, type **ms-settings:** and complete the creation of the shortcut.

Note

To enhance the **ms-settings** command in the Run window, enter **ms-settings:display**, which opens the Settings program directly to the Display portion of Settings. You can run similar commands for Uniform Resource Identifiers (URIs) such as sound, printers, taskbar, and USB. For a list of the URIs for **ms-settings**, see https://docs.microsoft.com/en-us/windows/uwp/launch-resume/launch-settings-app for additional information.

Open Settings now and take a minute to look over the categories that are listed. You can see that each category is identified with a different icon. Let's get into the various Settings options now.

Internet Options

In prior versions of Windows, you would go to the Internet Options Control Panel to make changes to your Internet settings. Now any changes only impact Microsoft Internet Explorer (and some features in Edge) but are otherwise not used.

For example, the Internet Options Control Panel will impact the following features.

For Internet Explorer (IE) and IE engine applications:

- **General tab:** Settings here, like the home page, browsing history, and temporary files, mainly affect IE's behavior.
- **Security tab:** This tab enables you to configure security levels for different zones (Internet, Local Intranet, Trusted Sites, Restricted Sites), which can impact how IE interacts with websites in those zones.
- **Privacy tab:** This tab controls cookie settings, allowing you to block or allow cookies based on the website or type of cookie, and also controls website access to location data and pop-up blocking.
- **Connections tab:** Changes made here, like proxy settings or network connections, can affect how IE and other applications that use the IE engine connect to the Internet.
- **Advanced tab:** This tab contains various advanced settings, some of which might be specific to IE, while others might have broader implications.

For Microsoft Edge and other browsers:

- **Security and Privacy:** Some security and privacy settings in the Internet Options can affect other browsers, including Edge, particularly those related to cookies and security zones.

- **Connections:** Settings in the Connections tab, such as proxy settings, can affect all web browsers because they determine how applications connect to the Internet.
- **TLS Settings:** Certain TLS settings in the Advanced tab of Internet Options might be needed for accessing specific websites, which could affect Edge as well.

For other applications:

- **Outlook desktop app:** Internet Options settings can affect the Outlook desktop app because it uses the IE engine for displaying content.
- **Applications using IE DLLs:** Some applications, like PowerShell and third-party apps, might also be affected by Internet Options settings if they utilize IE DLLs.

If an app has its own settings for any of these items, those settings will not be impacted by what is listed in the Internet Options Control Panel item. Instead, what you configure there will be what the app looks for instead.

Network & Internet

If you want to configure network settings, you used to do that in the Network and Sharing Center control panel. While that control panel still exists, there is an easier and better way in later versions of Windows. Figure 37.1 shows the Network & internet window in Windows 11, including both Wi-Fi and Ethernet; your screen may vary slightly.

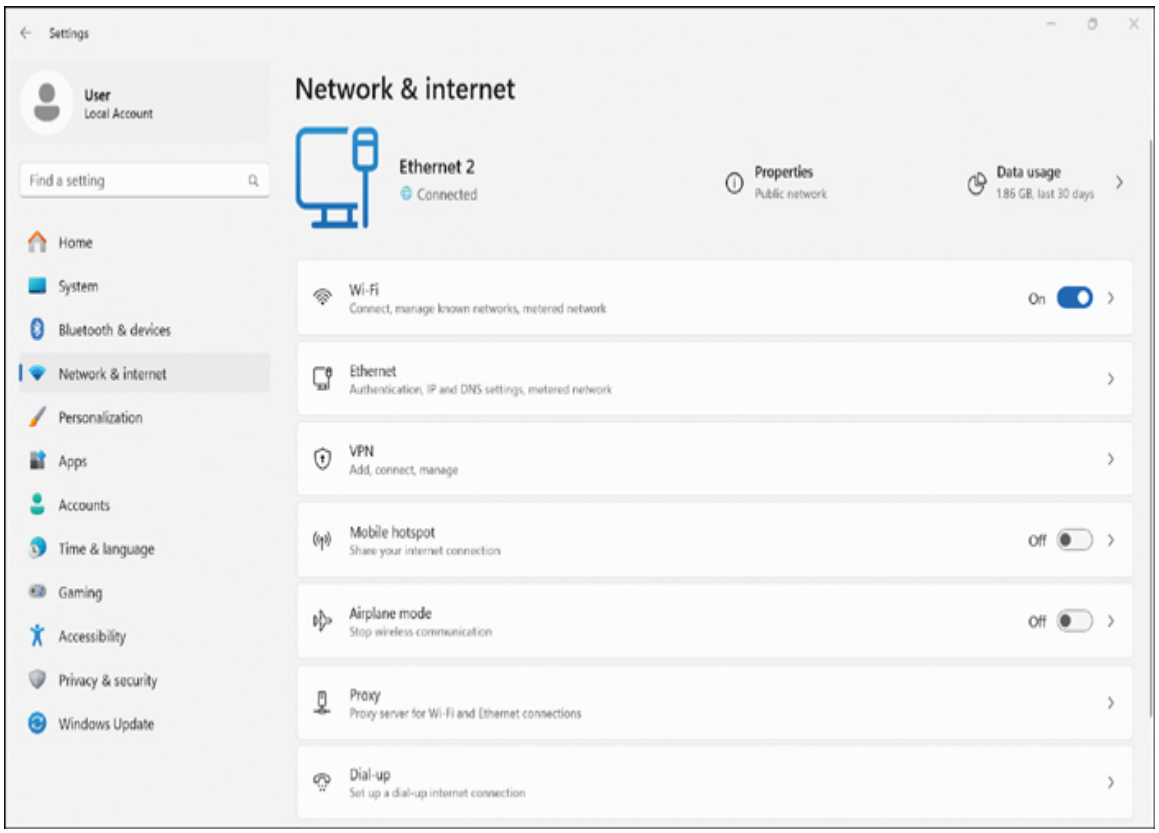


FIGURE 37.1 **Network & Internet Window in Windows 11**

In the Network & internet window, select **Wi-Fi**. You can see the configuration of your Wi-Fi card as well as the network password.

You can also define whether you are on a public or private network. Public networks (the default) allow you to access printers and other devices on the network but do not allow others to connect to your device. Private networks lower the barriers, so to speak; your device becomes discoverable on the network, and other devices can see and connect to your device automatically. Use this option only if you trust all devices on your network. Note that domain networks will have different options, but they work in similar ways.

You can set up how you want your device to get an IP address (via DHCP—the most common method—or manually). Most people and businesses use DHCP, but you should understand how IP addressing works (that topic was covered in Chapter 9, "SOHO Network Configuration"). You can also set up DNS servers in this window (that topic was also covered in Chapter 9).

The SSID is the Wi-Fi network you connect to. Information regarding that network and the Wi-Fi network card is on this screen as well. Clicking the **Edit** button next to Advanced Wi-Fi network properties will allow you to adjust additional Wi-Fi settings.

If you have a physical Ethernet adapter, you will have an option to make similar configuration changes for that. The major difference is that you can decide if your Ethernet connection is a metered connection; a metered connection is one for which you pay a fee per unit of data transmitted (usually after a cap). If you have such a connection, you can configure a data limit for the connection to help you control costs. You will see that VPN connections have a similar metered and cap option; otherwise, the Ethernet options mirror those of Wi-Fi, which makes sense because they are both network connections.

ExamAlert

Understand how to manage connections to networks. You will use this knowledge in your job as a technician, and several exam standards cover this material.

If you want to share your Internet connection to other devices, you can do that by turning your machine into a mobile hotspot. This possibility works really well for Ethernet connections and if sharing a connection that requires a login, but it opens you up to security concerns, so use with caution.

Airplane mode turns off all radios on your device. As with Wi-Fi, you can also turn this option on and off from the system tray.

We'll discuss this category and its concepts further in Chapter 38, "Windows Networking."

Note

If you click **Show** in the Network & internet > Wi-Fi area, Windows will show you the Wi-Fi password and also generate a QR code that can be used to connect to the Wi-Fi network automatically. This option is great for helping guests and new devices connect to your network quickly and easily. Securing your network is always a balance between security and convenience; you want people to be able to access your network easily while also keeping it secure, so be careful using this feature because the QR code contains your Wi-Fi network login information.

Finally, you can adjust Advanced sharing settings. Formerly housed in the Network and Sharing Center control panel (which is still available), these settings enable you to turn on Network discovery, which allows other devices to find your device on the network. You can also configure your device to share files and printers with others on your local network. By default, both of these options are disabled on public networks—a good thing since you don't want strangers browsing the files on your device! On a private network, file and printer sharing is enabled by default, so you can easily share files if other devices know that they are available. By default, anyone attempting access will need a password to access.

Bluetooth & Devices

In older versions of Windows, a user would go to the **Control Panel > Devices & Printers** when wanting to install and configure printers and other directly connected devices. That task has been moved to the Settings and is now in the Bluetooth & Devices category.

The Bluetooth & Devices category is the place where you turn Bluetooth on and off (you can also do this in the Windows system tray), plus configure your printers and scanners, mobile devices, cameras, mouse, touchpad, touch gestures, Pen & Windows Ink (useful if you use a stylus), and Bluetooth devices, and printers. You can also configure typing settings (such as auto correction), set handwriting/inking options, enable/disable AutoPlay, and you can use this category to have Windows notify you if there are any issues with USB devices (except keyboards; keyboard settings

are in the Time & language and Accessibility sections. Additional mouse controls are in the Accessibility section).

If you want to add a device, select **Add device** from the Devices area in Bluetooth & devices. If you need to add a printer (it likely was automatically detected) or see which printers are installed, that is in the Printers & scanners section on that same page. Figure 37.2 shows the Bluetooth & devices screen.

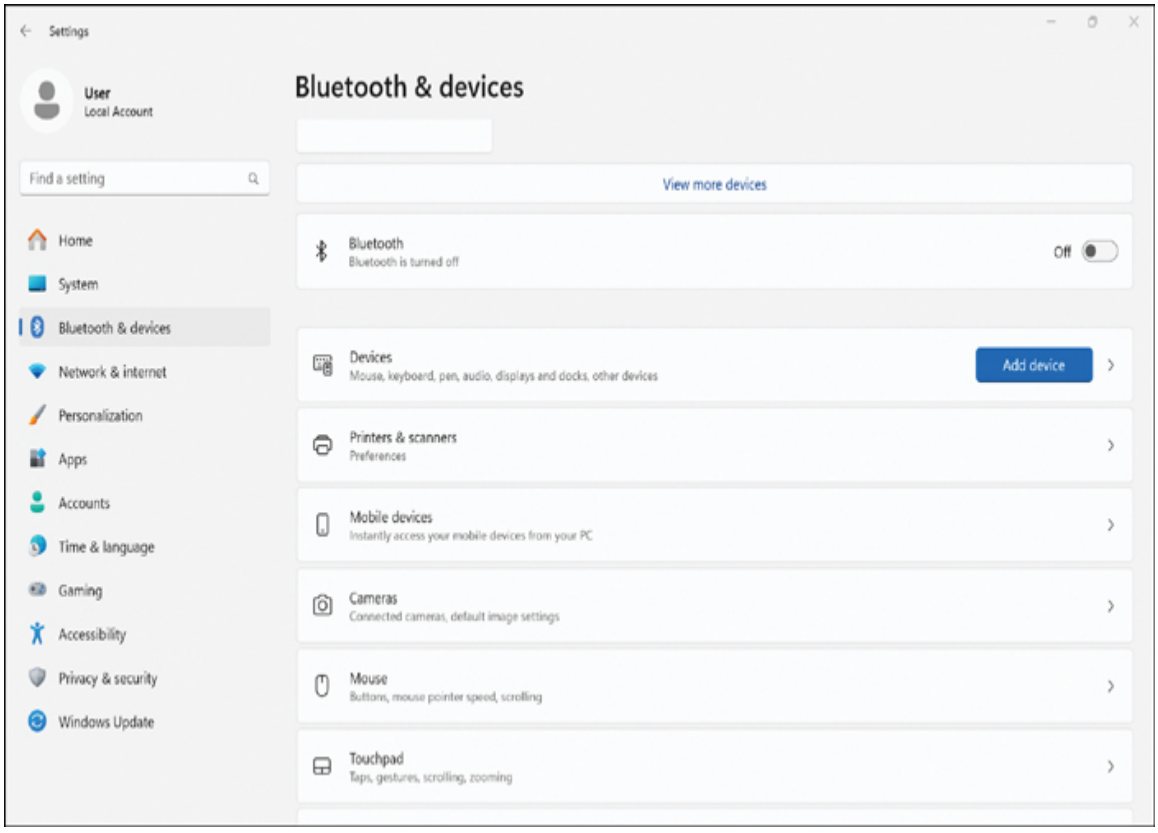


FIGURE 37.2 **Bluetooth & Devices Screen in Windows 11**

USB battery saver is an interesting option. It enables your device to shut off unused USB ports, and unused devices on those ports, without impacting other USB devices on your system. Shutting off these devices can substantially improve power economy and battery life on your device. In past versions of Windows, this option was called USB Selective Suspend, which is still available in the Control Panel (see the note that follows).

Note

One example of a configuration you might perform in Devices is modifying the scroll rate for the mouse wheel. Some people like to scroll through documents one or two lines at a time; others like to scroll entire pages at a time. You can change this setting from multiple lines at a time to pages at a time from the drop-down menu in the Mouse section. If it is set to lines, you can modify the exact number of lines per mouse wheel movement.

Note

Windows offers a lot of settings for USB drives that many users don't even think about. Check out the AutoPlay and USB sections of the Bluetooth & devices settings. Under AutoPlay, you can set the defaults to open a folder in File Explorer or even autoplay any content that is in the drive (not necessarily a great idea for security). You can use the USB settings to adjust the notifications and even see information about connected devices. See Chapter 48, "Workstation Best Practices," for more information on how to protect yourself.

Note

USB Selective Suspend, now called USB battery saver, can also be accessed via the Power Options Control Panel or the Device Manager.

Apps

Once upon a time, if you wanted to remove a program, you would select the **Programs and Features Control Panel** item, which has a selection named Uninstall a program. This option allows you to fully uninstall a program or change its installed settings. You also have the option to turn Windows

features on or off from this same location. Although this option still exists, it doesn't work with all programs, and newer versions of Windows have a better method.

> **Note**
>
> Programs are often called *applications* or *apps*. There was a time when there was a difference, but as technology has advanced, the terms have become synonymous. Microsoft changed its naming; older versions of Windows use the term *program*; newer versions use the term *app* or *application*.

In the Settings app, go to the Apps screen (**Settings > Apps**). Here, you have options to see all installed apps, as well as advanced app settings, your default app settings, locations for offline maps, apps for websites (for data that opens in programs other than a browser, like Outlook for email), video playback options, and startup for apps that start automatically when you sign in to your device.

Probably the most important of these options is Installed apps, where you can see all of the apps installed. If you click the three dots at the right side of the app itself, you can choose to modify or uninstall the individual application. This is the location you will use when you need to uninstall when upgrading or replacing a program as part of troubleshooting. Figure 37.3 shows the Installed apps screen where you can see all installed applications.

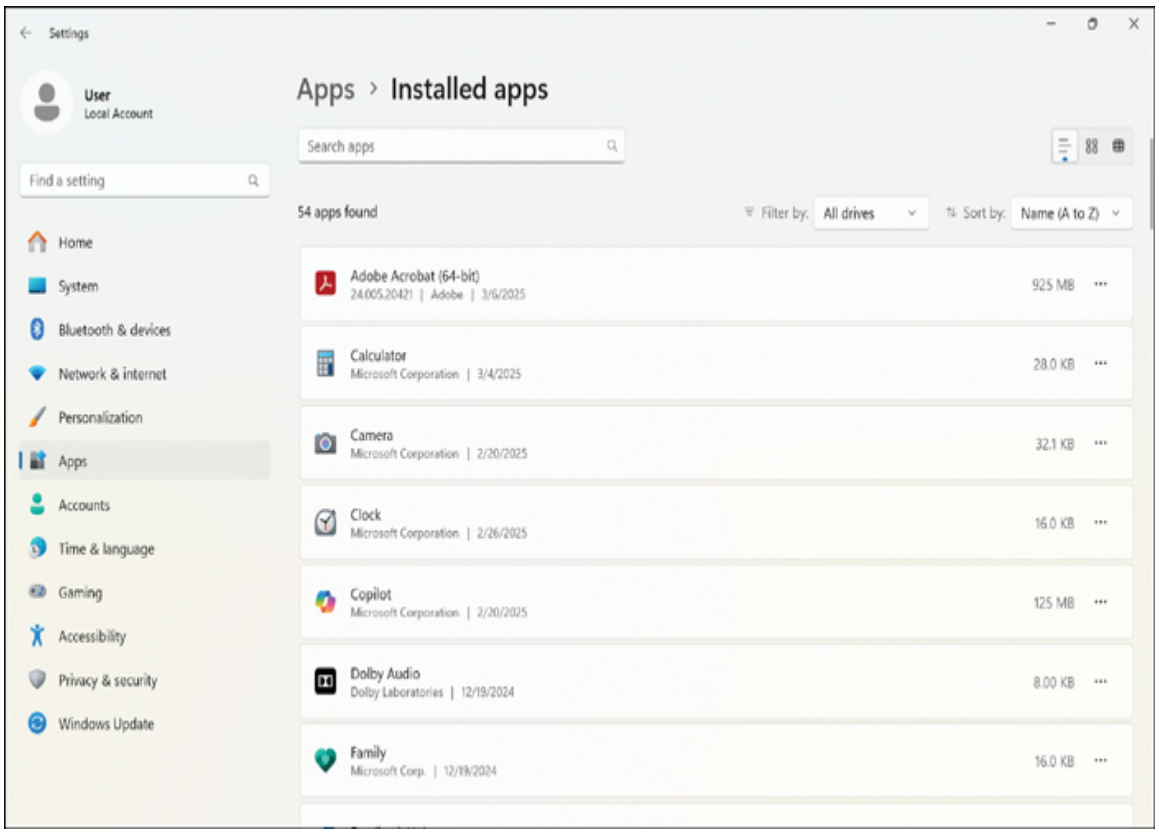


FIGURE 37.3 **Installed Apps Screen in Windows 11**

You can also control where you get applications from. Although Microsoft would prefer that you get them from the Microsoft Store, you can download from anywhere on the Internet. Be cautious when installing any programs; any program can contain viruses or other issues. Installing from a manufacturer's website or the Microsoft Store is usually safe. This topic is discussed more fully in Chapter 52, "Browser Security," in the section on trusted and untrusted sources.

You can set the default apps, which will automatically open a particular app for a particular file type. If you need to change this, **Apps > Default** apps is the place to look.

In the days before anywhere, anytime Internet access, offline maps were critical tools. Even now, being able to access maps while offline can be useful. The Offline maps screen allows you to control exactly what types of maps will be downloaded and where they will be stored.

Sometimes links should be opened in an app instead of the browser window. The Apps for websites window allows you to control this.

Video playback helps you control the videos that you play on your device. You can enhance (either better or lesser quality), conserve network bandwidth, and even save battery power by playing at a lower resolution while on battery power.

Finally, you can control which apps get to start when you log in to your device. While many apps will stay minimized, having them start at all takes system resources; if you rarely use an app, it is best to not have it start upon login. For instance, if you only rarely use Microsoft Teams, go ahead and turn it off in startup. Starting it will take a little longer when you do run the program, but it will not take resources until you need it.

Figure 37.4 shows the Apps window in Windows 11, with all of the options visible.

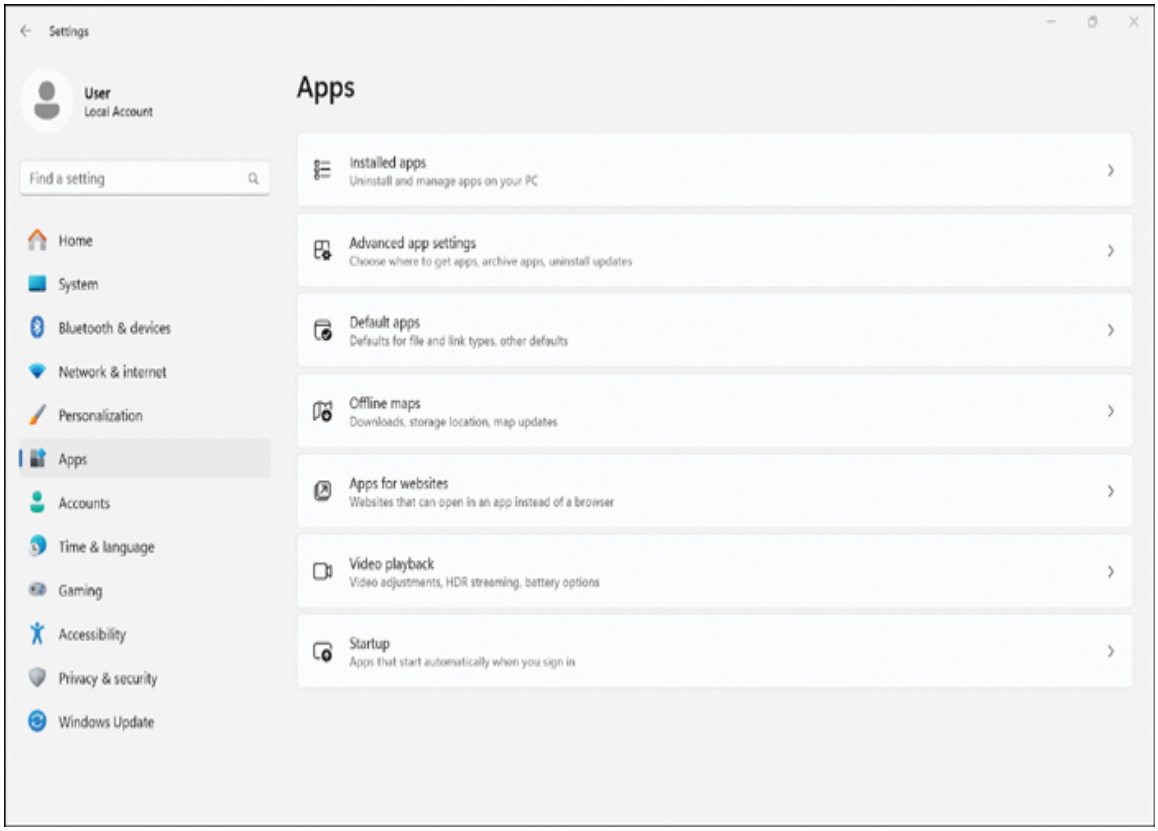


FIGURE 37.4 **The Settings > Apps Window in Windows 11**

System

The System window of Settings is the place where you, as a technician, will spend a lot of time. The settings here govern your display, sound, notifications, power, storage, and more. That's a ton of stuff. Let's spend some time examining some of the options. Although we won't go into all of them here (we will cover some in other chapters), you will eventually need all of them in your work as a technician.

About

At the bottom of the System section, you will find the About screen. Everything you used to find in the System control panel is here. We're starting here because it shows important information about your device that you might need quickly and which is otherwise important to be able to access. In the About screen, you can rename this PC (you learned about this option in Chapter 31, "Basic Features of Windows Editions"—see Figure 31.2 for that information). You can also see all of the device specifications, including the processor and installed RAM and which operating system is installed. You also have the option to upgrade your edition of Windows in the Product key and activation section. There are several other options to explore, each of which can help you troubleshoot a device that is acting up.

ExamAlert

Know the parts and pieces of the About screen and the options contained within the secondary screens there. They are important for your work as a technician and are fair game on the exam.

ExamAlert

Know the options in the System > About window.

There are many other options in the System window. Now let's look at a few more.

Sound

The Sound section of System settings allows you to view and adjust the audio input and output settings of your device.

You can choose which speaker or headset you will hear alerts and music through. You can also adjust the Spatial sound settings, which will allow for a more immersive audio experience through a concept called 3D Spatial Sound.

Finally, you can also choose which microphone to use. Since much of your work may involve audio (even office workers spend a good deal of their time in online meetings after all), a good microphone is a must, and you can use this setting to set which one you will use.

The Advanced area allows you to see and work with all sound devices and even has an audio mixer called Volume mixer, which allows you to determine which programs have access to the audio at all. In other words, this is the place where you control which programs can produce sound and which can listen to the sound that you are producing. It is a very powerful concept but simple to use. Figure 37.5 shows the System > Sound window, where you can see and configure your sound options.

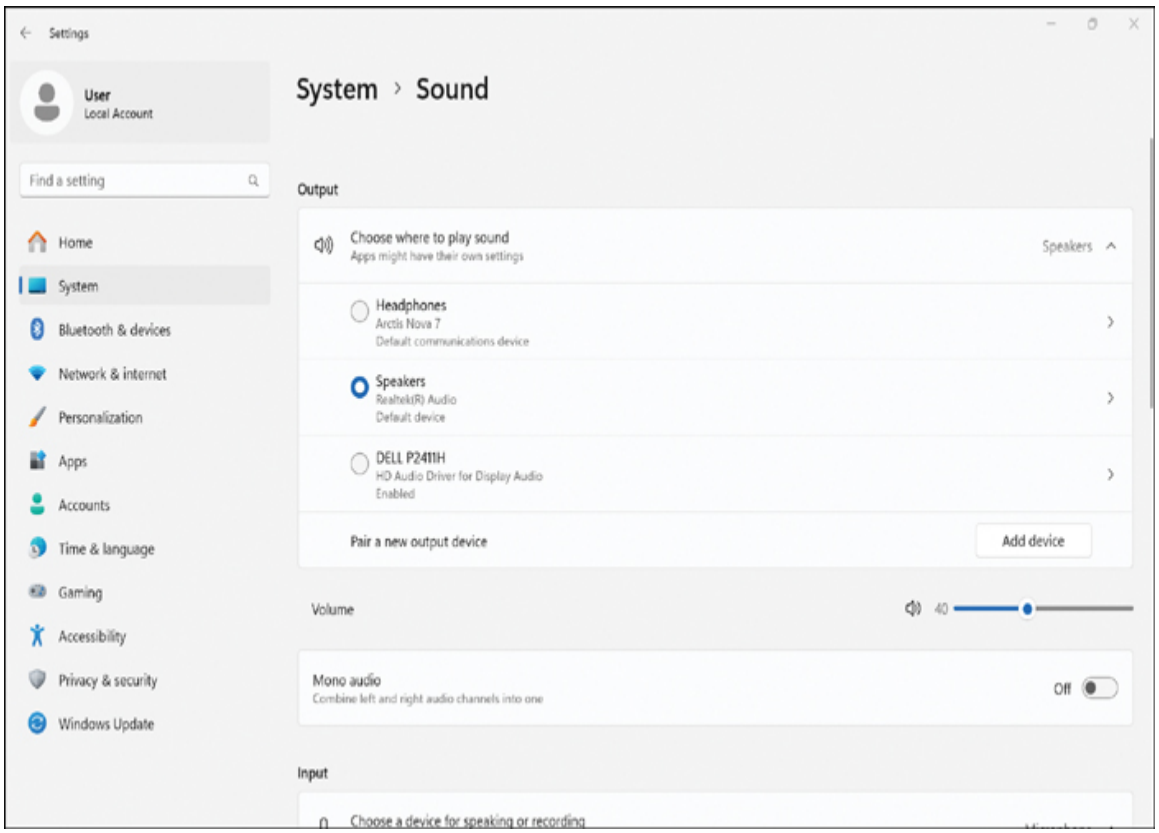


FIGURE 37.5 **The Sound Window**

For Developers

In the For developers section of the System window, you can edit a lot of very specific items. Let's look at the File Explorer options.

By default, file extensions are hidden. By toggling the switch, you can see all of the file extensions in File Explorer. Windows uses file extensions to associate files with the programs that open them; for instance, .exe files are executable (program) files, .pdf files are Acrobat files, .xlsx files are for Microsoft Excel, and so on (there is often metadata inside the files themselves to assist with this process as well, but the file extension is the first thing that Windows looks at). By showing file extensions, you can see what Windows is looking at as it makes the determination for file associations.

In addition, many files are hidden from the average user, but it can be useful during troubleshooting to see all of the files that exist in a folder. Show hidden and system files allows you to see all of the files and folders on your system. This option can also help you track down random files and other extraneous lost files that may make their way into a system. Figure 37.6 shows a portion of the System > For developers screen where you can choose the File Explorer options.

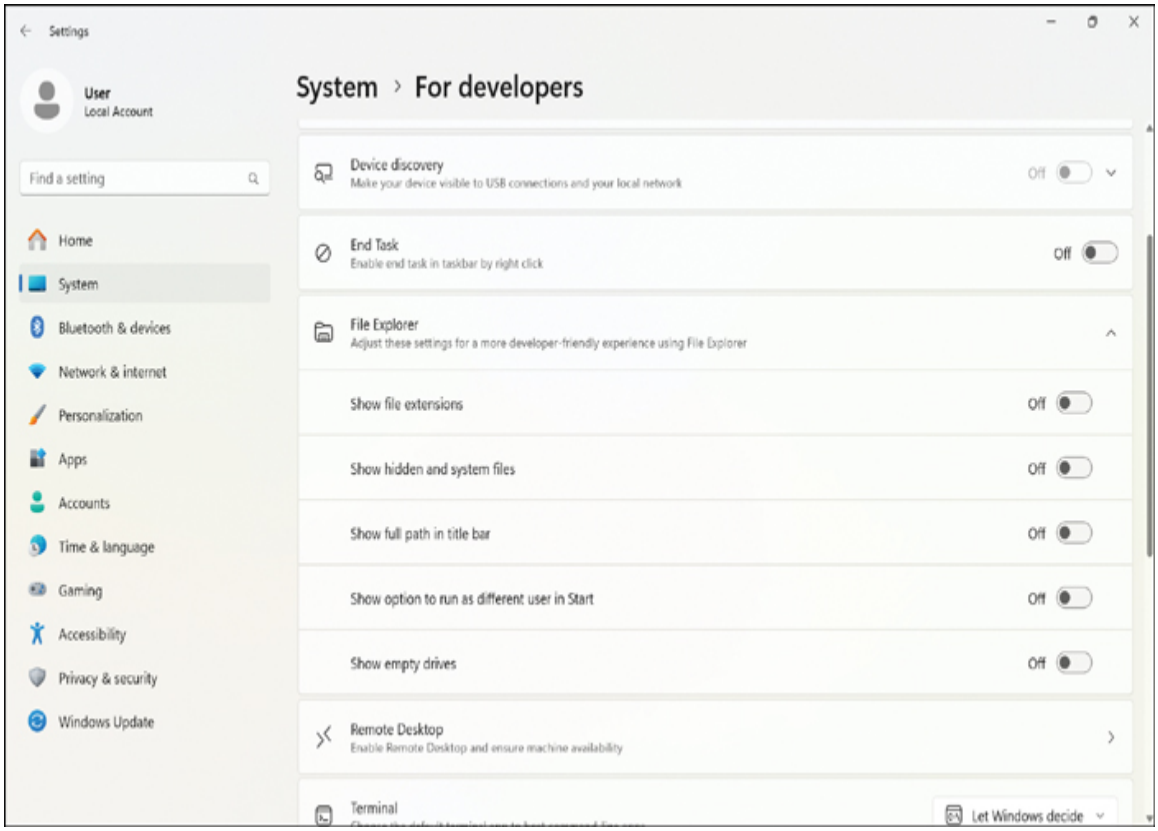


FIGURE 37.6 **The For Developers Screen, Scrolled to Display the File Explorer Options**

You can show the full path in the title bar. By default, Windows shows only a shortened, simplified path in the title bar. By selecting this option, you can see the entire path on your drive to a specific file or folder.

If multiple users share a device, you can show their separate logins at the startup screen or in the Start menu. This way, you can quickly switch back and forth between users.

By default, Windows will hide any drive with no media inserted. For instance, if you have an SD card reader but no SD card inserted, the drive will not appear in the File Explorer window at all. Selecting this option will show all possible options installed, including those where media is not inserted, so you would see the fact that you have an SD reader installed regardless of whether media were inserted.

There are several other useful tools in this section, but these are the ones that are most aligned with the A+ exam.

Power & Battery

Continuing our work in the System window, we get to the Power & battery section. This section replaces several of the older Control panel items regarding power management. The options here are straightforward, so let's get started. Figure 37.7 shows the window.

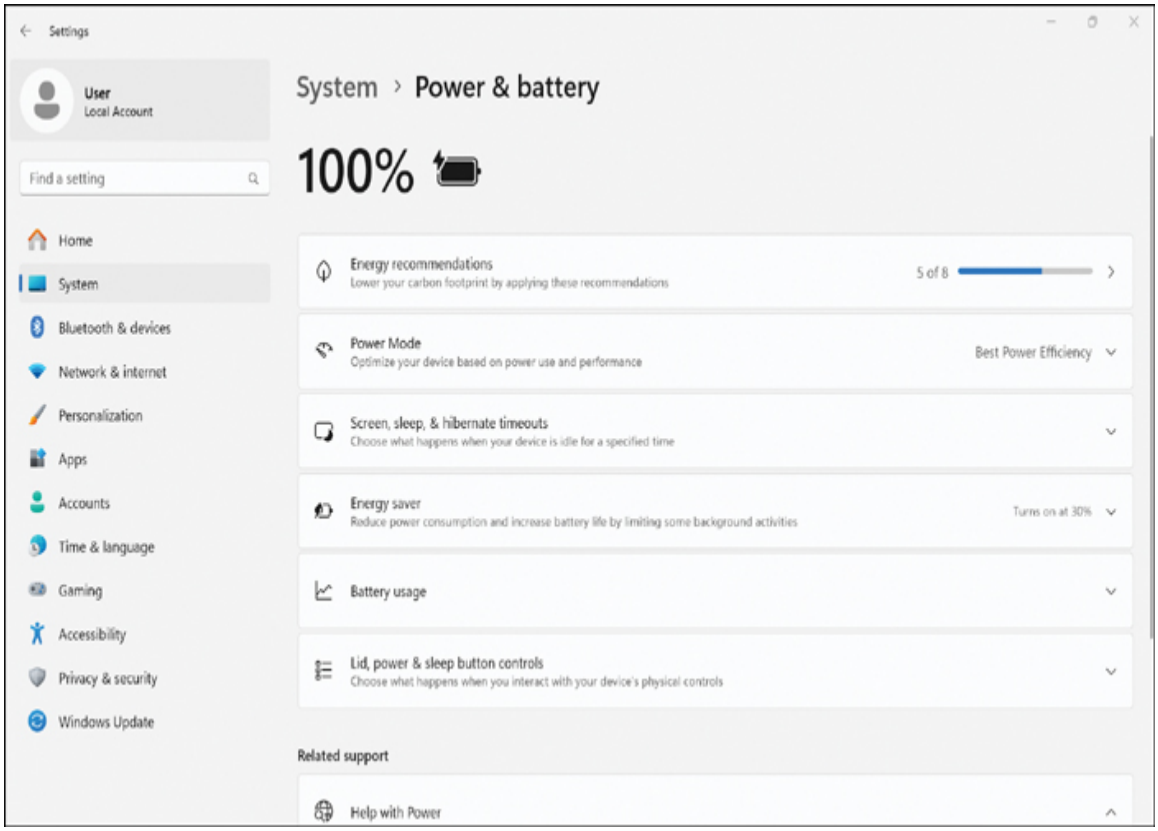


FIGURE 37.7 **The Power & Battery Window in Windows 11**

The first thing to notice is the Energy recommendations. You should review them to help you save the most energy.

Next is Power Mode, which allows you to automatically set certain power modes. Your options are Best Power Efficiency, Balanced, and Best Performance. Essentially, these will dim or shut off devices when not in use. For instance, after a period of nonuse, your monitor may dim and then shut off. Your hard drive may shut off. Any USB devices may power down or go into a standby/low-power state. For mobile devices (laptops and tablets), you can set this separately for when the device is plugged in or on battery.

You can also determine when your screen turns off or your device goes to sleep. By default, this is after 3 minutes of nonuse, but you can set this to be as quickly as 1 minute or to never if you don't want it to sleep or blank the screen at all. You are in charge here.

Devices with a battery will have a Battery usage area, allowing you to see the status of the battery over time (by default, this is 24 hours, but you can see up to 7 days of battery usage). This information can be helpful if you are concerned about battery health.

Finally, you can control what happens when you close the lid, press the sleep button (if your device has one), or press the power button of your PC. Options include Do Nothing, Sleep, Hibernate, and Shutdown. Sleep mode puts your computer into a low-power state, which enables you to quickly resume right where you left off. All documents are intact, right where you left them. It does take a small amount of power to keep Sleep mode active because RAM stays active. In prior versions of Windows, Sleep was called Standby mode (there is still a Standby S0 mode, which enables the network to continue operating, but that's beyond the A+ exam). Hibernate mode saves the current state of your device to the hard drive and then shuts down the computer. Unlike in a regular shutdown, when the device is turned back on, it will reload the saved state of the device instead of having to reload the entire operating system, so it is a bit faster. Hibernation mode does not take any more power than turning off the device entirely.

ExamAlert

Know the differences between the different low-power modes. See https://support.microsoft.com/en-us/windows/shut-down-sleep-or-hibernate-your-pc-2941d165-7d0a-a5e8-c5ad-8c972e8e6eff for additional information that can be useful if you get confused about the differences, especially between Sleep and Hibernate.

Note

Fast Startup is an interesting hybrid of shutdown and hibernate. Windows will initiate a logoff of the operating system, then save the kernel information—the operating system before it gets to the user information, including device drivers—to the hard drive in the same way that hibernate does (but without the user information that hibernate uses), and finally shut down the machine the rest of the way. When the device powers up again, instead of loading up the operating system from scratch, it instead loads the saved kernel and then proceeds to a login prompt. This feature can improve boot times for slower machines, especially those with mechanical hard drives, but modern machines need it less. The feature is enabled by default from the Power Options control panel, where you can also disable it. The video at https://www.youtube.com/watch?v=OBGxt8zhbRk explains it pretty well if you're interested in more details about how it works.

There is a lot more in the System window; you should take the time to familiarize yourself with all of it. This information will all be useful in the long run.

Accessibility

Information in the Accessibility window merges options from many different Windows control panels, most especially Ease of Access, with the goal of putting accessibility and ease of use in one place. Figure 37.8 shows the Accessibility window.

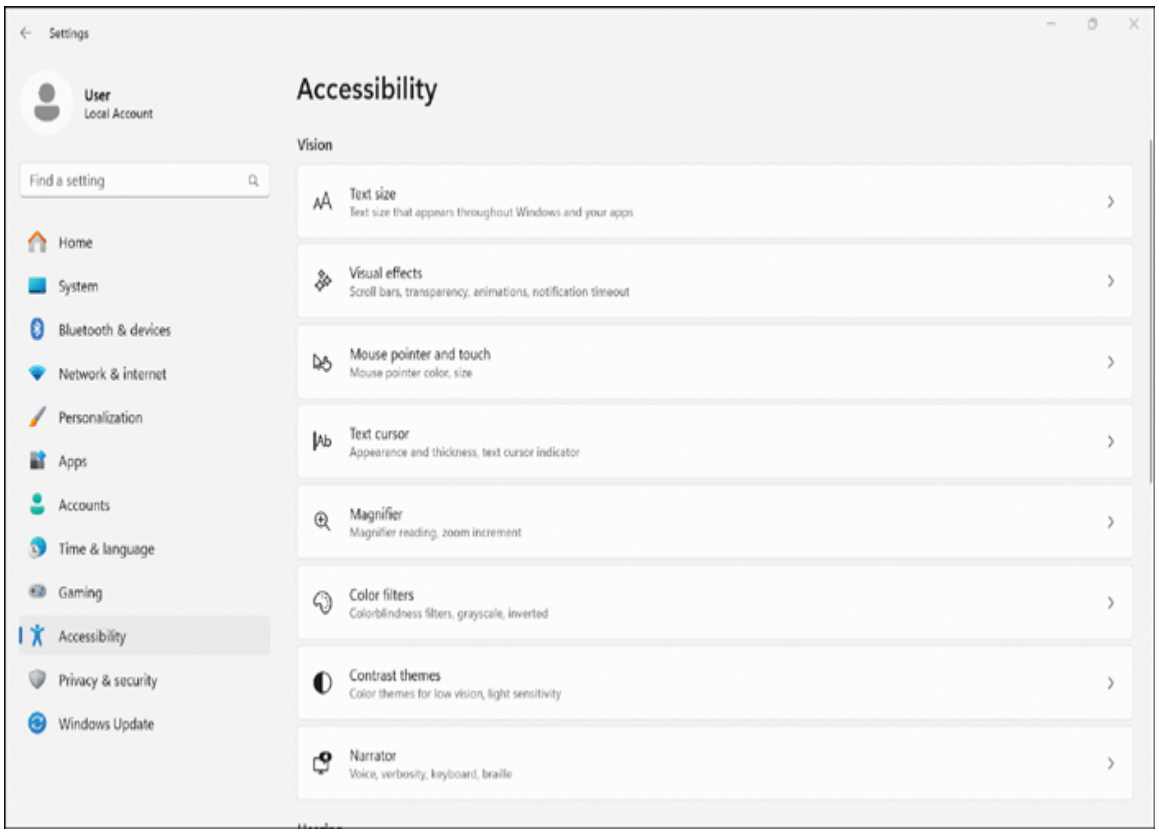


FIGURE 37.8 **The Accessibility Window in Windows 11**

Text size will enable you to adjust the size of the text in windows across all of the operating system. Think of it as one-stop shopping to adjust your device to meet your particular vision needs.

Visual effects adjusts the settings of scrollbars, transparency, and animation. Some people love these; others dislike them or find them distracting. You can also set how long a notification will show before automatically dismissing; the default is 5 seconds.

You can adjust the size and style of your mouse pointer and can enable a touch indicator if using a touch screen. A touch indicator puts a circle around where you touch the screen, making it easier to see where you have touched.

Your text cursor can be adjusted as well. You can place an indicator in a color of your choice, adjust the thickness of the text cursor, or both. Either or both of these can make it easier to see the text cursor on your screen.

The screen magnifier lets you see the screen elements more clearly. You can turn it on or off and adjust the magnification level. To enable the magnifier without having to come to the Settings, press the Windows key and the plus sign. Windows+Escape shuts off the magnifier.

Some people have trouble with color vision (by some accounts, it's just over 8 percent of the population). The Color filters window allows for adjustment of the Windows color palette to account for color deficit.

For those with vision impairments, high contrast is often useful (and some people just find it soothing). Contrast themes has four palettes available: Aquatic, Desert, Dusk, and Night Sky (think dark mode). Try each to see what they look like; you may find that one suits your fancy.

Narrator provides voice narration to screen options. The keyboard shortcut to turn it on or off is Windows+Ctrl+Enter. There are lots of settings, but the most important part to remember is that Windows has the capability to read the entire contents of the screen to someone with vision impairments, built right into the operating system.

Audio settings include mono audio, where all audio is combined into one audio channel, and flashing the screen during audio notifications.

If you have a Bluetooth Low Energy (BLE) Audio hearing device (a type of hearing aid), you can configure certain settings here, allowing computer audio to go directly to the hearing aid.

Note

Bluetooth Low Energy (BLE), also known as Bluetooth Smart, is a wireless technology designed for low-power applications, offering reduced energy consumption and cost compared to Classic Bluetooth while maintaining a similar communication range. It is often used in IoT and medical applications.

BLE Audio is a related technology specific to hearing aids and allows a wearer to receive computer audio via the BLE connection directly to the hearing aid itself.

Captions enable you to produce live captions of audio and video streams right on your device in near real time. Note that voice data is processed locally, not in the cloud, and does not require Internet access. There are options for how the captions are displayed as well.

The Speech window allows for voice access to your device. Windows+ Ctrl+S turns this on or off as well if you don't want to come to the Settings. You can then control your device with your voice and dictate text.

There is a set of keyboard settings. They include Sticky keys, which allow you to use multiple keystrokes, such as Control or Shift, while pressing the keys separately. This feature is good for people who don't have a lot of strength in their hands and thus move their hands slowly. You can also set Filter keys, which ignore repeated keystrokes, which is good for people who inadvertently hold down keys for an extended amount of time while keying information into their device. Toggle keys will play a sound as you press certain keys, which is good to ensure that you aren't pressing certain keys accidentally.

An onscreen keyboard also is available. Windows+Ctrl+O will turn it on or off. It works just like your regular keyboard. You can also select to turn on screen capture using the Print screen key.

If you are more comfortable with the keyboard than the mouse, you can turn on Mouse keys and use your numeric keyboard instead of the mouse. There are configuration settings in the Mouse window as well.

Finally, Eye control allows someone with an eye tracker to use Windows.

Lots of options for Accessibility are built right into Windows. These aren't just for those who have some sort of special need; many of them are useful for people who wouldn't think of themselves as needing anything special. They help everyone use the device better and be more productive. Because they're included in Windows, everyone benefits.

Time & Language

You can use the Time & Language category to modify date and time settings, language and region information, typing, and speech options for

microphone-based speech recognition.

Here's one scenario where you would use Time & Language. Say that you don't want to have Windows set the time automatically for you (which it does by default). If that's the case, you can navigate to the **Date & time** page under Time & Language, disable the **Set time automatically** slider, and then click the **Change** button to set the date and time manually. Most organizations (and most individuals, too) want their computers' time to be synchronized to a time server (such as time.windows.com). Think about the time change twice yearly; this is done automatically if you let it.

Remember that there is always more than one way to get to a particular setting in Windows. For instance, if you right-click the clock in the lower-right corner of your screen and click **Adjust date and time**, Windows will take you to the same Settings window.

> **Note**
>
> We use the term *right-click* quite often in this book. However, if you are using a touch screen (or another device), the right-click procedure might be different. For example, on a Microsoft Surface device, you would long press the screen to activate a context (or right-click) menu. On other devices, you could use a two-finger tap on the touchpad. Sometimes you will need to hold down the Alt key and click. The sequence will differ from one device to the next, but for ease of reading, we simply refer to the process as right-clicking.

Take a few minutes to look through the Time & Language settings—and do this for each of the Settings categories covered in this chapter. If you make any changes, be sure to put everything back as it was when you are finished. You don't want to accidentally mess up your computer! If you don't want to worry about accidentally messing up your main device, you could always install Windows in a virtual machine (VM), which would allow you to make any changes you want. Because any changes are in the virtual machine, they won't impact your main machine. Virtual machines are discussed in Chapter 21, "Virtualization Concepts."

Note

As you progress deeper through the Settings options, you might find that a link will actually open a Control Panel dialog box or even a Control Panel window. Be ready for it!

Windows Update & Security

The Update & Security Control Panels category has been split up in the Settings of Windows 11. It now encompasses Windows Update, which includes updating Windows itself as well as advanced options about update timing and other update settings. Most other Windows Security tools are found in the Privacy & Security category, including antimalware, firewall, and encryption settings. Activation is in the System settings area. Windows backup can be found in the Accounts area. Windows Security, including antimalware and firewall features, backup and recovery options, troubleshooting tools, Windows activation options, and advanced developer options will be discussed after that. We'll discuss the security side of Update & Security, as well as backup, recovery, and troubleshooting, later in the book. For now, let's briefly examine Windows Update and Microsoft Defender Firewall a little more.

Windows Update

Like any other operating system, Windows should be updated regularly. Microsoft recognizes faults in the OS—and possible exploits that could occur—and releases patches to increase OS performance and protect the system. These patches can be downloaded and installed automatically or manually, depending on the user's needs or the organization's needs, and they are controlled via the Windows Update program.

To access Windows Update, go to **Settings > Windows Update** (in Windows 10, you would go to **Settings > Update and Security > Windows Update**). Or you can search for "windows update" or go to **Run > ms-settings:windowsupdate**. You can also update the system from PowerShell, if necessary. After you open the Windows Update window, you

can see if your system is up to date, and you have the option to check for updates and install them.

From within Windows Update, you can decide how updates will be delivered and installed. Windows 11 makes it difficult to defer updates indefinitely without using Active Directory (which your company may use). The downsides of pausing updates far outweigh the upsides of delaying updates. After all, the updates keep your device safer from online threats. You can pause for up to 5 weeks, however, if necessary (for instance, if you are working on a big project—like writing a book—and don't want to worry about Windows updates interfering with the workflow).

Troubleshooting Windows Update Program Issues

If you are having trouble installing Windows updates, help is available on the Windows Update screen itself. Scroll down to Related Support and select one of the topics, depending on what you are having trouble accomplishing. You can get help on uninstalling problematic Windows updates, pausing updates for a convenient time, installing pending Windows updates, and manually updating your device drivers. To learn more about installing Windows Updates, visit https://support.microsoft.com/en-us/windows/install-windows-updates-3c5ae7fc-9fb6-9af1-1984-b5e0412c556a.

ExamAlert

Know how to run and troubleshoot Windows Update.

Privacy & Security

Settings for Microsoft Defender Firewall have been moved to the Privacy & Security window. Microsoft Defender Firewall is a built-in software-based firewall in Windows. We mentioned it in Chapter 36, "Windows Control Panel Utilities," when we discussed the Control Panel icon, but it has a different look in Settings. If you select the Windows Security option, you will open a new screen. If you click any of the icons, you will get a new

Windows Security dialog that enables you to configure the security of the firewall or any of the other built-in security items.

Figure 37.9 shows the Firewall & network protection window. From here, you can turn the firewalls on or off for the domain and for private and public networks. You can also allow individual programs through the firewall (known as exceptions). Finally, you can run Microsoft Defender Firewall with Advanced Security by clicking the **Advanced Settings** link (or directly with **Run > wf.msc**). The main difference between this and the basic Microsoft Defender Firewall is your ability to create rules for incoming and outgoing traffic. We'll discuss both in more depth in the security section of this book.

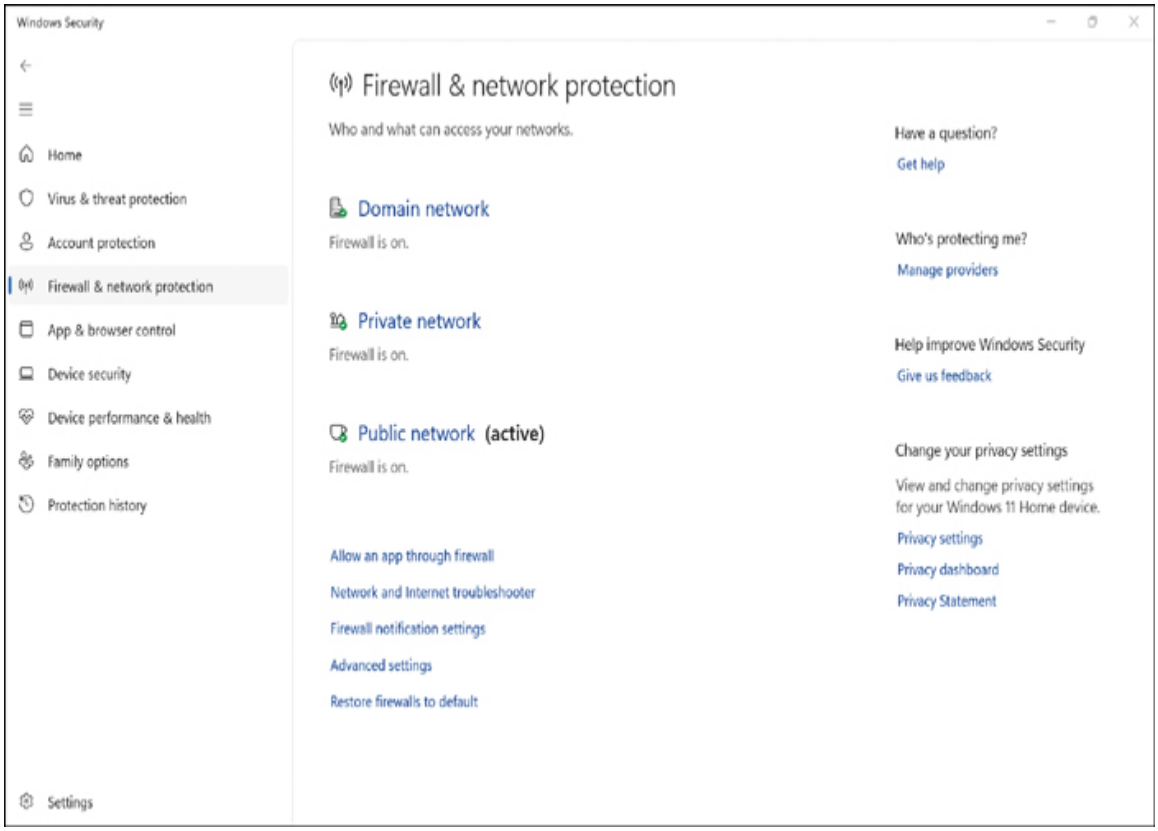


FIGURE 37.9 **Microsoft Firewall & Network Protection Window**

There are other items in the Privacy & Security area that are worth exploring. Find my device can track your device. The device must be connected to the Internet, and it uses Internet location information but can be helpful.

Device encryption, often referred to as BitLocker encryption, encrypts data on your device. It is on by default. When you encrypt data on your device, it becomes that much harder to have your data stolen, even if someone were able to gain access to your device.

The General window deals with personalization. We recommend shutting off the advertising ID because that feature allows you to be tracked across the Internet using a personal advertising ID. Some people like personalized ads, but the tracking can be intrusive and is a privacy concern.

Windows can improve Start and search results by tracking which apps you use most frequently if you let it. Read the other items for details.

Speech recognition in the Privacy & Security section will go online to process your speech. By default, it is off, and you will only use local resources.

Inking & typing personalization allows you to create and use a custom dictionary throughout all of Windows, not just your Microsoft applications. If you use specialized terminology for your job, this option can be invaluable.

Diagnostics & feedback data tells you about your device. If you allow it (it is on by default), the data will be sent to Microsoft to help with error reporting. Be cautious though; some of these options are related to ads as well. Luckily, this is also where you can see the data collected about you.

Activity history shows what you were doing when, which is useful when your device restarts and you need to get back to where you left off. You can clear the activity history for this account whenever you feel the need.

Your Search permissions are here. As you search in Microsoft Edge, it uses these settings to determine the type of results you will receive.

Windows will automatically index your drives. We used to use the Indexing Options Control Panel, but now you can control which parts of your drives it indexes and how often in the Searching Windows window. You can exclude certain folders from the search; by default, these are program and operating system folders. By adding additional folders to the index (or removing them from the index), you can save time and trouble when the

indexing is running. Note that indexing must be done before a document can be easily found. After the initial index is done, it is usually pretty quick to get future indexing done.

Finally, you can configure permissions for types of applications. Location, microphone, voice, and task information are included in the list. You should review the list to ensure you have a handle on all the options since there are too many to list.

Note

As you go through the options, keep in mind that you should not be giving out any more information about yourself and your customers than you absolutely have to. After all, privacy is important. By keeping that in mind, you'll be okay.

Personalization

Finally, a place to have some fun with the system! In the Personalization section, you can style your Windows computer the way you want. You can add custom backgrounds, modify colors, choose fonts, and modify how the Start menu and taskbar behave. We'll let you play around in the settings here without further discourse.

Gaming

The Gaming section focuses on using your PC for games: the game bar, keyboard shortcuts, screen, and video captures, and how to optimize the computer for gameplay with Game Mode. Absolute fun for sure, but it probably won't show up on the exam much. You should review the settings to know what is here so that you are familiar with them.

Accounts

The Accounts section is about user accounts. In it, you can manage an existing account or add new ones. By default, Microsoft attempts to have

you sign up for a Microsoft account, but other accounts are allowed as well, including work and school accounts. (This requirement becomes more stringent in the Enterprise version of Windows.) Work and school resources are available in this section as well. Additional email accounts can be created also.

To create an email account, click **Settings > Accounts > Email & accounts** and follow the prompts. (Later, you can go to **Privacy & security > Email** to decide which apps can access your email.) You can also shut off access to the email program from this same area if you don't want to allow anyone to use the installed version of Mail to access their email from this device.

Sign-in options enable you to modify the security factors used for logging in to Windows, including Windows Hello Facial recognition, fingerprint recognition, PIN, security key, password, and picture password. You'll also find a handful of other options regarding locking your device automatically when you're away.

The Other Users (Family & other users in Windows 10) section allows you to add additional accounts to the device and is generally used to set up family members and specify the access levels for those accounts. For example, kids are often given less access by an adult creating an account. In this section, you can add local accounts for people who only want to sign in to Windows without using a Microsoft account. By default, new users are given Standard User access. You can change this setting in Other Users (again, Family & other users in Windows 10). You can also use this area to remove the account and data of users who no longer need access to your device.

Note

Several older versions of Windows came with Windows Mail, a bare-bones email client, along with Calendar and People apps. As of December 2024, those apps have been discontinued. Microsoft recommends transitioning to Outlook for Windows or Outlook.com. You can also use another web-based email service, as discussed in Chapter 42, "Cloud-Based Productivity Tools." See https://support.microsoft.com/en-us/office/outlook-for-windows-the-

future-of-mail-calendar-and-people-on-windows-11-715fc27c-e0f4-4652-9174-47faa751b199 for more information.

ExamAlert

This chapter just touches the surface of the options in the Settings area. As a technician, you will find yourself doing lots of your troubleshooting and setup here, so knowing the Settings is critical to success, both on the exam and in your workplace.

Control Panel Operations

While Settings is the preferred method of accessing and configuring your device, other configuration options are available in the Control Panel. As a reminder, you get to the Control Panel by going to **Start > Control Panel**.

As discussed in Chapter 36, you can view the Control Panel by category or by large or small icons. When viewing by category, you can see that some settings actually open the appropriate Settings controls; others will open controls that are not available yet in the Settings. Eventually, everything will move over to Settings, and you won't have to guess which is where; for now, remember that you can always use Search in either window to find the correct tool, regardless of where it resides.

System and Security

While you do have access to the Microsoft Defender Firewall settings from the Settings security area, the location in the System and Security Control Panel category gives you more granular control over the settings.

You can adjust Power Options here, adjusting a power plan for your device. Although this approach is available, we recommend that you use Settings instead for this; it is more efficient for modern machines and you have more control of specific items such as hibernation, sleep states, what closing the lid does, and fast startup. However, older devices may not support all of

those items, so knowing that this is here in the Control Panel options is important. The one item that is available only here is Fast Startup; to use it, select **Power Options > Change plan settings > Change advanced power settings**. You might have to click the **Change settings that are currently unavailable** checkbox to see the option.

Device Manager

The Device Manager keeps track of all devices attached to your system. By reviewing the devices, you can determine if the devices are running properly. While most of the settings can (and should) be configured at the Settings window or (occasionally now) the Control Panel, sometimes you need to go to the Device Manager to reinstall drivers or to see if devices are running properly. Take a look at the Device Manager on your system and look at the options. You will be surprised at the amount of data that you can get about your system just by paying attention to the information in the Device Manager.

> **Note**
>
> Windows is constantly being improved. This means lots of updates and changes over time. Be sure to work on the latest versions of any software to keep *yourself* up to date.

Cram Quiz

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

1. Which of the following sections of Windows Settings allows a user to copy important information about a PC and possibly send it to a technician for troubleshooting purposes?

   - ○ **A. System > About**

- ○ **B. Network & Internet > Ethernet**
- ○ **C. Ease of Access > Narrator**
- ○ **D. Privacy > Diagnostics & Feedback**

2. Where would you go to see the current Wi-Fi settings?
   - ○ **A. System > About**
   - ○ **B. System > Hardware > Wi-Fi**
   - ○ **C. System > Network & Internet > Wi-Fi**
   - ○ **D. Control Panel > Network and Sharing Center > Wi-Fi**
3. Where can a technician create rules for inbound and outbound network traffic? (Select the two best answers.)
   - ○ **A.** Microsoft Defender Firewall with Advanced Security
   - ○ **B.** Microsoft Defender Firewall
   - ○ **C.** Apps & Features
   - ○ **D.** Wf.msc
4. Why should you continue to run Windows Update?
   - ○ **A.** Windows is unstable and updates make it more stable.
   - ○ **B.** Windows updates provide patches to fix vulnerabilities.
   - ○ **C.** Windows updates install programs.
   - ○ **D.** Windows does not need to be updated.

Cram Quiz Answers

1. **A.** Navigate to **Windows Settings > System > About**. Here, you can copy device and Windows specifications and paste them into an email or to another location.
2. **C.** Navigate to **System > Network & Internet > Wi-Fi** to see the settings for your Wi-Fi network. You can set up a connection in the

Control Panel > Network and Sharing Center, but the option is called Set up a new connection or network and works very differently from the Settings area (and is much more difficult to manage).

3. **A and D.** The main difference between Microsoft Defender Firewall with Advanced Security and the basic Microsoft Defender Firewall is the ability to create rules for incoming and outgoing traffic. You can run Microsoft Defender Firewall with Advanced Security directly with **Run > wf.msc**. While the standard Microsoft Defender Firewall can allow apps through, it can't make specific rules. The Apps category opens up the Apps & features section of Settings, where you can see a list of what applications are loaded on the system and how much space they take up and uninstall them if necessary.

4. **B.** Windows is a complex program (every operating system is really a type of program). As such, there are flaws. Windows Update patches the flaws that are found over time. Sometimes these flaws affect stability. Sometimes they affect security and other vulnerabilities. In addition, Windows Update sometimes distributes new features to your system. All are good reasons to keep your system up to date. Although Windows can be unstable (remember Windows Vista? It was a fine OS, just unstable), and some updates do improve stability, security is the main reason why you should run updates. Windows Update does not install applications (programs). And you already know that you SHOULD update Windows, so you know that isn't correct.

As mentioned, Windows is a morphing system; it is changing constantly. Be ready for this. Know the Control Panel and especially know Windows Settings for the exam, since that is the direction that Microsoft has moved. What's the best way to hedge your bets as you prepare to work in the IT field? Know the command line the most. It changes far less rapidly than does the GUI—and it rules. Continue.

Chapter 38

Windows Networking

This chapter covers the following A+ 220-1202 exam objective:

- **1.7** – Given a scenario, configure Microsoft Windows networking features on a client/desktop.

To a certain extent, Windows networking is automated. In a lot of scenarios, the technician doesn't have to configure very much. However, the larger and/or more complicated a network becomes, the more configuration is usually required.

This chapter goes over some of the basics of Windows networking, including reviewing the network types, sharing and connecting to data, establishing different networking connections, and modifying additional networking settings. It might seem like a lot, but the great thing about TCP/IP—and computer networking in general—is that it works in essentially the same manner across the board, regardless of the operating system that is installed on the computer. So, the more you learn about networking, the easier it becomes to network *any* operating systems together.

Let's continue on our quest toward the A+ certification.

ExamAlert

Objective 1.7 focuses on workgroup vs. domain joined setup, local OS firewall settings, client network configuration, network

connections, proxy settings, public networks vs. private networks, File Explorer navigation and network paths, and metered connections and limitations.

Domain Joined vs. Workgroup Setup

After you have configured a network adapter, you are ready to join a network. There are only a couple of choices: either workgroup or domain.

Workgroups and domains are logical groupings of computers. A *workgroup* (sometimes also referred to as peer-to-peer) is usually a small group of computers that share the same network name. No single computer controls the network, and all systems are considered equal. One of the disadvantages is that a computer storing data can be accessed only by a maximum of 20 other systems simultaneously. A *domain* (sometimes also referred to as a client/server network) builds on this by having one or more computers (servers) that are in control of the network. This arrangement enables more computers, more simultaneous access, and centralized administration. A domain also gets a name, such as greencurtaintraining.com.

In Windows 11, you can go to **System > About** and select **Rename this PC** to rename your device, and select the **Domain or workgroup** link to join your device to a domain. In older versions of Windows (and in Windows 11 also, if you're old-school), you can also go to **Run** and type either **sysdm.cpl ,1** or **systempropertiescomputername**. Then click the **Change** button. This displays the Computer Name/Domain Changes dialog box, as shown in Figure 38.1.

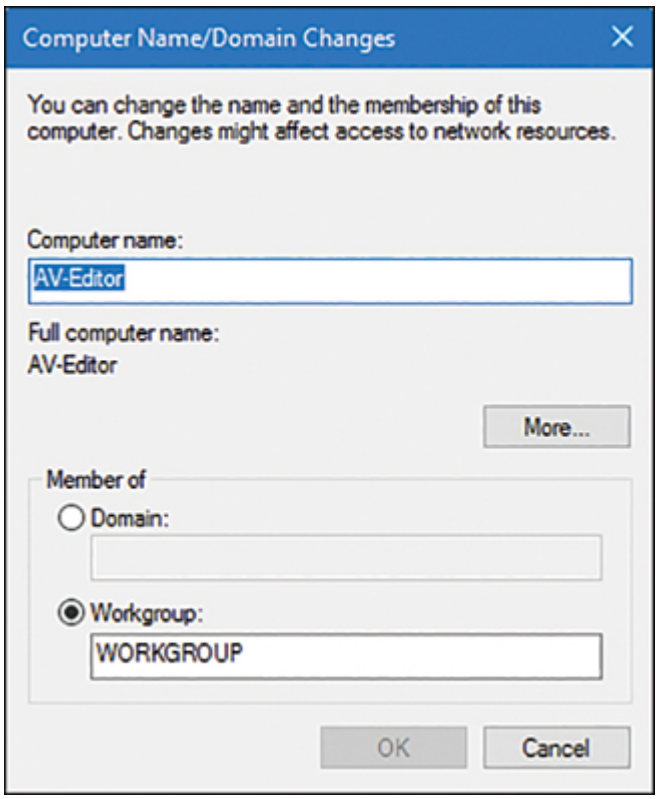


FIGURE 38.1 **Computer Name/Domain Changes Dialog Box**

If you are joining an Active Directory domain (businesses, schools, and other enterprise networks often run Active Directory), you will need to do the following. (Note that the Home version of Windows, of any era, cannot connect to Active Directory.)

1. Go to **Start > Settings**.
2. Select **Accounts**.
3. Select **Access work or school**.
4. Select **Connect**.
5. Select **Join this device to a local Active Directory domain**.
6. Enter the domain name.
7. Enter your credentials (you will need to get permission from your network administrator first).
8. Restart your computer.

You can use this dialog box to join a workgroup (which is the default) or attempt to join a domain. Your small office/home office (SOHO) network will probably not have a domain; domains are more commonly found in larger organizations.

Note that the default workgroup name is WORKGROUP, but you can change it to anything you want. Changing the name increases privacy in your network. Any devices on your network will need your workgroup name to share files and otherwise communicate with each other. Note that there is a 15-character maximum length for a workgroup name.

A domain is controlled by a Microsoft server known as a *domain controller*. To connect to the domain from a client computer, you need to know the domain name (for instance, greencurtaintraining.com) and the DNS server IP address for that domain. You also need an account on the domain and need to log on to that domain with a username and password assigned to you by the system administrator. It's also a good idea to make sure that the workstation's time and server's time are synchronized.

ExamAlert

Be able to define the differences between a workgroup and a domain and know where to change from one to the other (**System Properties** dialog box > **Computer Name** tab).

Sharing Resources and Making Network Connections

Before anyone can view the amazing things you have to offer on your computer, you need to *share* them. First, let's discuss the sharing of data, and then we'll discuss the sharing of printers.

To be able to share data, you first must turn on sharing. To do this, go to **Control Panel > All Control Panel Items > Network and Sharing Center**. Then click the **Change advanced sharing settings** link. The Advanced sharing settings window appears. In Windows 11, you can also

get to this point by going to **Settings > Network and Internet > Advanced network settings > Advanced sharing settings**.

> **Note**
>
> You also can quickly get to the Advanced sharing settings window by opening the Search tool and typing **sharing**.

In the Advanced sharing settings window, you can turn on file and printer sharing for private networks only, guest or public networks only, or all networks. You can also enable or disable password-protected sharing. What you select depends on your environment, the kind of network you have, and the security level you desire. You do not need to be overly concerned with these settings in a domain environment (other than turning off sharing for the client computers), but in a workgroup environment, you might opt to have sharing enabled on one or more network types. Some small offices turn off password-protected sharing to make it easier to share resources with other users on other computers, but there is a potential security risk in doing this.

> **Note**
>
> Some companies with small networks avoid Windows sharing altogether and instead install a network-attached storage (NAS) device that also has print server capabilities.

After sharing has been configured for the computer that will host the data, sharing can then be enabled for *individual* resources. For example, let's say you have a folder named data, and you want to share the contents of that folder to other users and computers. You would need to locate the folder, right-click it, and either select **Give Access To** or select **Properties** and then click the **Sharing** tab. Figure 38.2 shows the Sharing tab of a folder's Properties page. You can use this tab to share the folder; plus, you can use this tab to enable Advanced Sharing and set custom permissions for users.

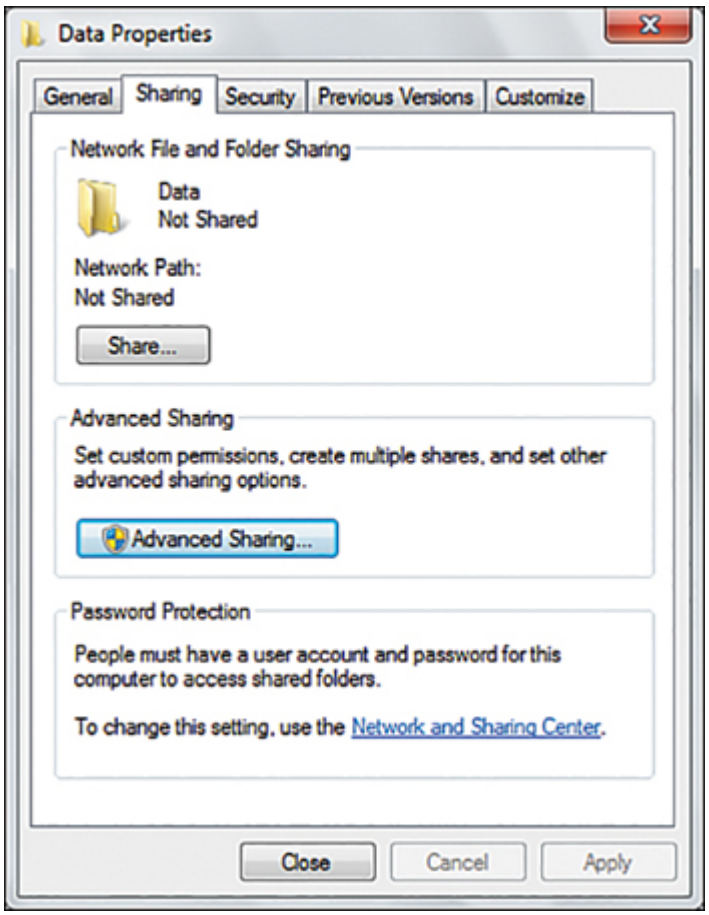


FIGURE 38.2 **The Sharing Tab of the Data Properties Window**

You can also create hidden shares, which can be seen by administrators but not by typical users. To do this, add a dollar sign (**$**) to the end of a share name. Drive letters are automatically shared as administrative shares (for example, C$). An example of a built-in Windows administrative share is admin$, which is the share name for C:\Windows. We'll discuss administrative shares further in Chapter 45, "Windows Security Settings."

Note

Use caution to only share a resource from the device where it physically lives or (in the case of printers) is directly connected. Otherwise, you run the risk of a resource being unavailable even if the device sharing it is available because the device where it actually resides is offline. This situation is especially common for shared

printers, where the printer gets shared multiple times on various devices and then connected and reshared. It can be difficult to troubleshoot as well as difficult to use, not to mention that the devices themselves run more slowly due to the unnecessary extra overhead.

Now, if you want to access shares on another computer, you can do it in a couple of ways. First is browsing the network, which is done in File Explorer. Simply click **Network** in the left pane. You might have to wait while the computer refreshes the information before other systems and devices show up. Click to open a remote computer, and its shares (if any) should show up there.

Another way to access shares is to map a network drive. This means making a permanent logical connection to a shared folder using File Explorer and assigning it a drive letter. These network drives are mapped according to Microsoft's Universal Naming Convention (UNC), which is \\computername\sharename (note that the backslash is the one above the Enter key, not the forward slash next to the period, on a standard US QWERTY keyboard).

To map a drive, follow these steps:

1. Locate the Map Network Drive window.
   - **In Windows 10:** Open **File Explorer**, select **This PC** in the left pane, click **Computer** on the menu bar, click the **Map network drive** drop-down, and again click **Map Network Drive**.
   - **In Windows 11:** Open **File Explorer**, select **This PC** in the left pane, click the three-dot button on the toolbar, and select **Map Network Drive**.
2. Select a drive letter (for example, F:).
3. Type the entire path to the share you want to map to. Use one of the following naming conventions:

```
\\servername\sharename
\\IPaddress\sharename
```

4. Click **Finish**.

Figure 38.3 shows an example. Note that the computer name in this example is nasbox1, and the share name is datashare. In this case, we mapped a drive to a NAS device instead of to a Windows computer, but the process works the same way. In the figure, we used Y: for the drive letter. Some organizations like to use F: or M: or Z:, but what you choose is really just a matter of a preference. The key is to be consistent. If 10 computers are going to map a drive to the same resource, consider using the same letter to do so; this makes it easier for the administrator to recognize where mapped drives are connecting.

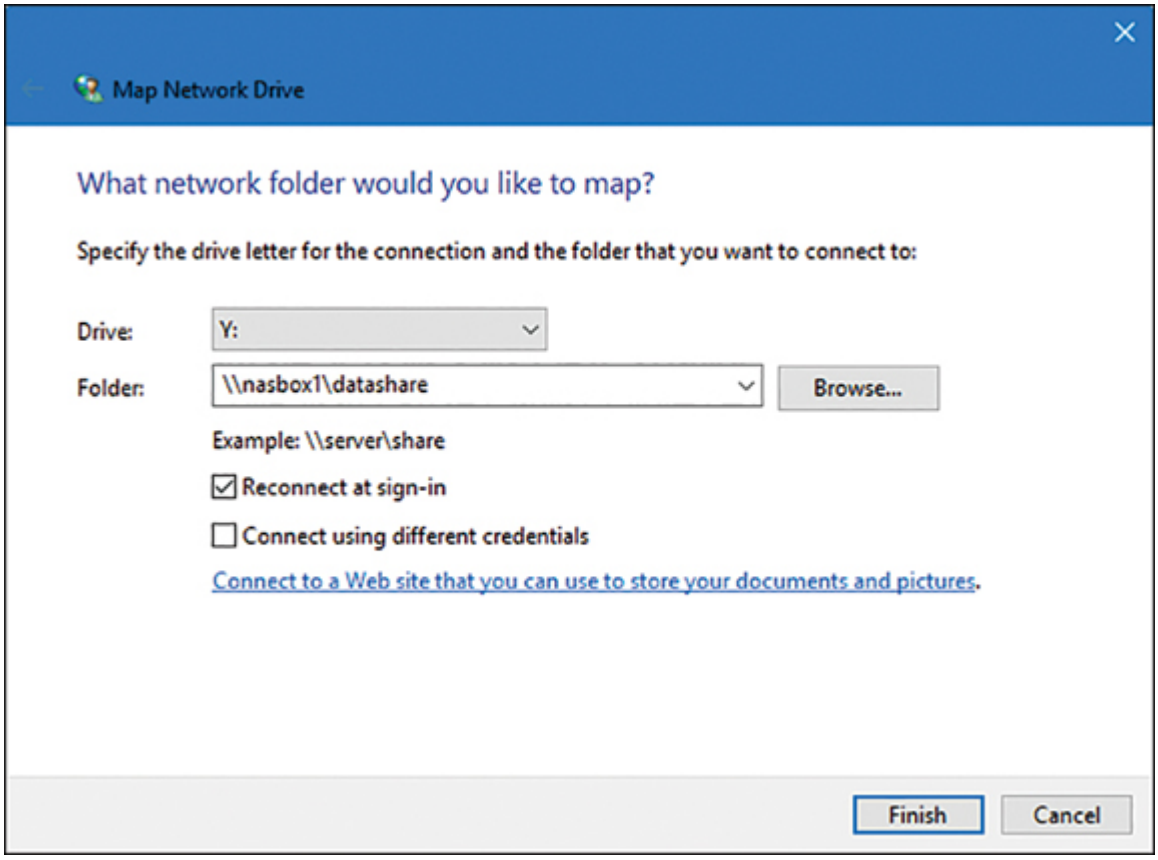


FIGURE 38.3 **The Map Network Drive Window**

Note that Reconnect at Sign-in is checked. When this option is selected, users won't have to reconnect and supply credentials every time they want the data. Always check this setting if you are troubleshooting a shared/mapped network drive that isn't working after a system is rebooted.

The option Connect Using Different Credentials might be necessary if the remote share, or network policy, requires it. If this option is selected, the system will prompt a user to enter a username and password.

You also can map network drives in PowerShell and the Command Prompt by using the **net use** command. For example, to map the same drive as shown in Figure 38.3, the command would be **net use y: \\nasbox1\datashare**. We discussed this command in Chapter 35, "Microsoft Command-Line Tools, Part II."

ExamAlert

Know how to map network drives in the GUI and at the command line.

Printer Sharing and Access

While most modern printers are network-ready, and thus can connect directly to a network, many older printers are not. Therefore, you will need to know how to share them manually. To share a printer, you need to first make sure that printer sharing has been enabled in the Network and Sharing Center (click the **Change advanced sharing settings** link and select either the Private, Guest, or Public profile drop-down). Then you can share the individual printer. Go to **Devices and Printers**, right-click the printer you want to share, select **Printer properties**, and access the **Sharing** tab. From there, check **Share this printer** and give it an easy-to-remember share name, preferably without spaces.

To connect to the printer from a remote computer, users can attempt to browse for it or add the printer by using its name (and network path). To do this, once again (but this time on the remote system) go to **Devices and Printers** (**Bluetooth & devices > Printers & scanners** for Windows 11)

and click **Add a printer** (**Add a printer or scanner** for Windows 11). If Windows doesn't find the printer on the network automatically, click **The printer that I want isn't listed**. You then have some options. First, you can select the shared printer by name—for example, \\av-editor\hp-printer1, where the printer share name is hp-printer1, and the computer it is connected to is AV-Editor. Figure 38.4 shows this configuration screen. HTTP and HTTPS connections can also be made if the computer that is controlling the printer supports this capability.

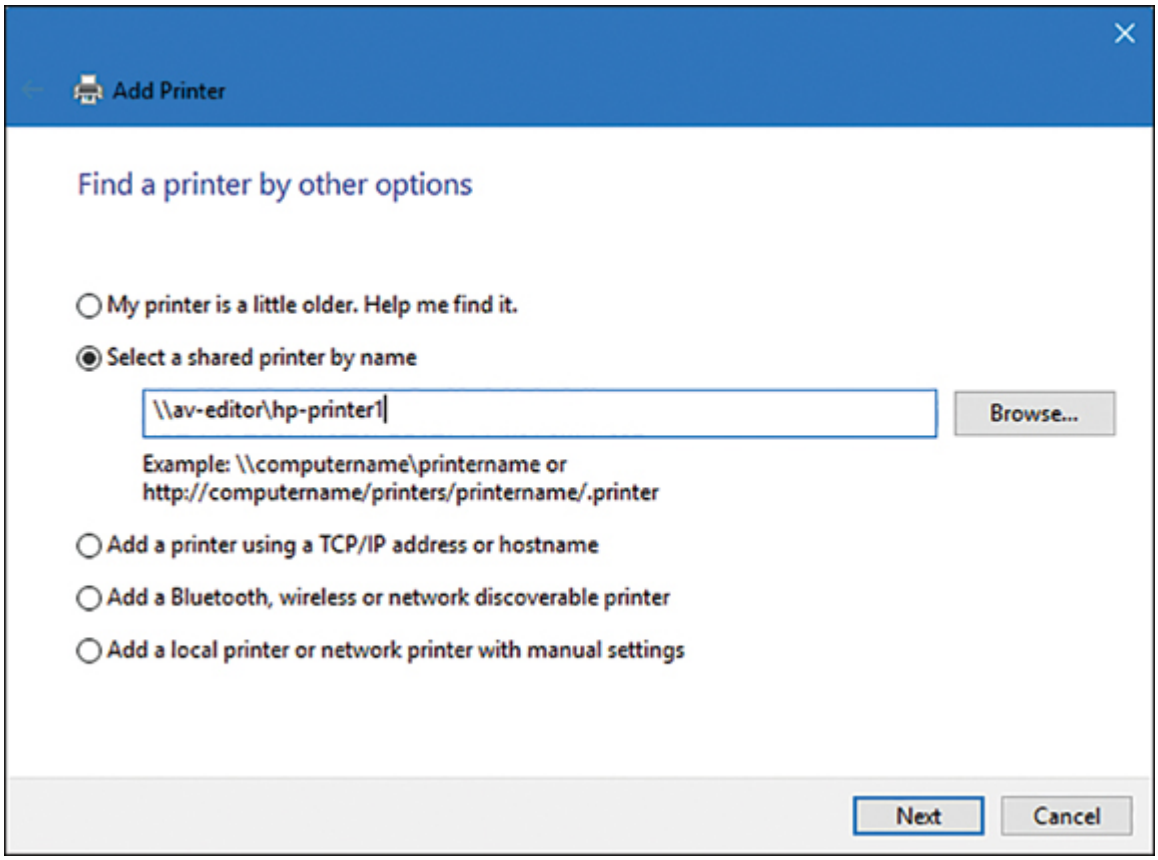


FIGURE 38.4 **The Add Printer Window**

You can also connect via TCP/IP by clicking the **Add a printer using a TCP/IP address or hostname** radio button. You can then connect to a standalone network printer by IP address directly or use Web Services for Devices (WSD) to connect to a printer. WSD is a Microsoft API that is used to enable programming connections to web service–enabled devices, such as printers, scanners, and file shares.

ExamAlert

Know how to connect (map) to a network printer by printer share name or IP address.

Note

The "Local OS firewall settings" portion of Objective 1.7 is covered in Chapter 45. The "Client network configuration" portion is covered in Chapter 9, "SOHO Network Configuration."

How to Establish Networking Connections

From within Windows, you can connect to a variety of networks. There are two main ways to do this:

- Navigate to **Settings > Network & Internet**.
- Navigate to the Network and Sharing Center and click the link **Set up a new connection or network** to display the window shown in Figure 38.5.

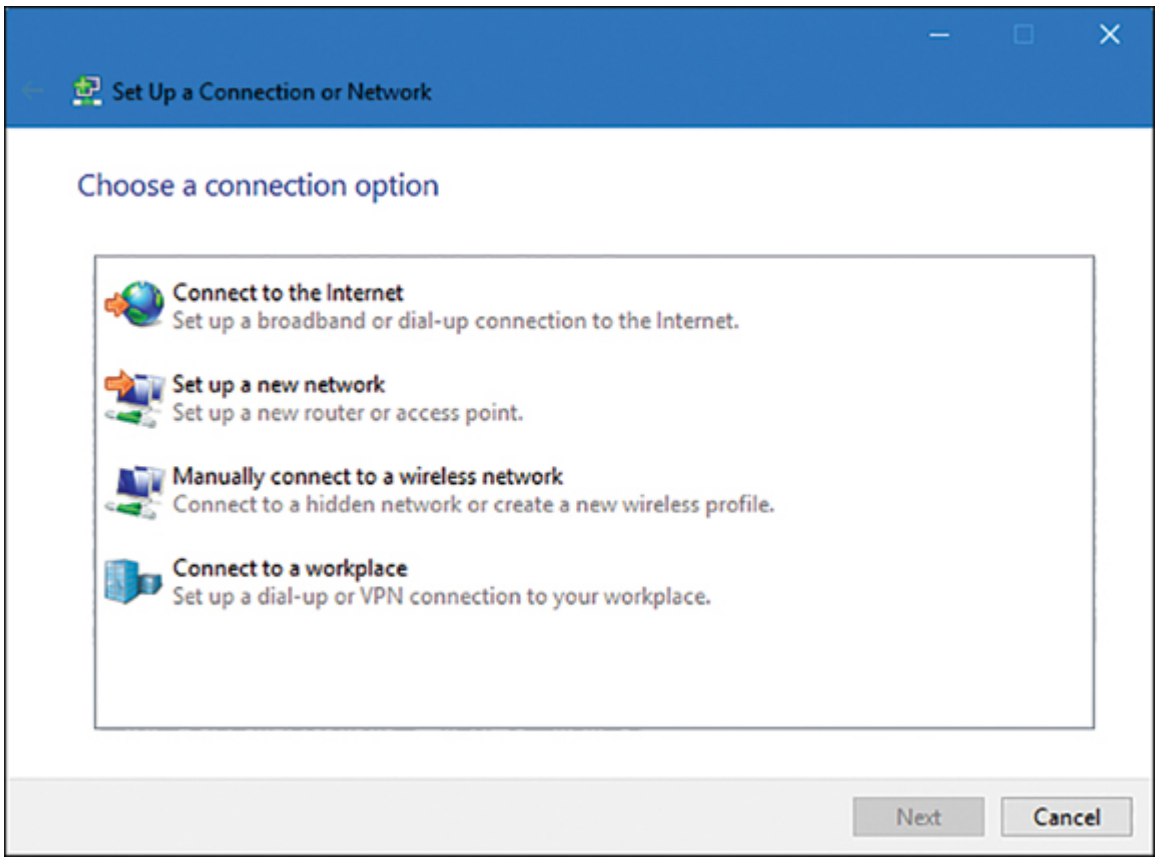


FIGURE 38.5 **The Set Up a Connection or Network Window**

From these locations, you can connect to wireless networks, wired Ethernet networks, virtual private networks (VPNs), dial-up networks, wireless wide area networks (WWANs), and, of course, the Internet.

From the window shown in Figure 38.5, you can do several things. First, you can make Internet connections via broadband or dial-up. You can also create a new network by configuring a SOHO router (if available). In addition, you can manually connect to a wireless network, which might be necessary if the AP is not broadcasting the SSID. You can also connect to the workplace via direct dial-up (which is uncommon) or VPN. To establish a WWAN/cellular connection, you usually rely on third-party software that comes with the WWAN adapter. You can also configure metered connections for VPNs and hotspots. This means you have control over your data cap (if you have one). Windows looks at a typical Ethernet or Wi-Fi connection as unlimited, but a user might have a service that is not

unlimited. By setting up a metered connection, you can watch over your data limitations and get notifications when you approach those limits.

Note

Metered connections in Windows will try to control and reduce data usage on the network automatically. In the case of a metered Internet plan, users pay for the data they use with a limit before additional charges are incurred. Oftentimes, mobile broadband is metered, so by default, Windows will treat those as metered accounts.

A *metered VPN* refers to a VPN service where users are charged based on the amount of data they use. This means they have a limited data allowance and will incur additional fees if they exceed it. This is similar to how a standard Internet data plan with a limited cap might work; essentially, it's a VPN where you pay for the data you consume, not just for access to the service itself.

Figure 38.6 displays the configuration screen for allowing a VPN connection, including allowing a VPN over a metered network configuration.

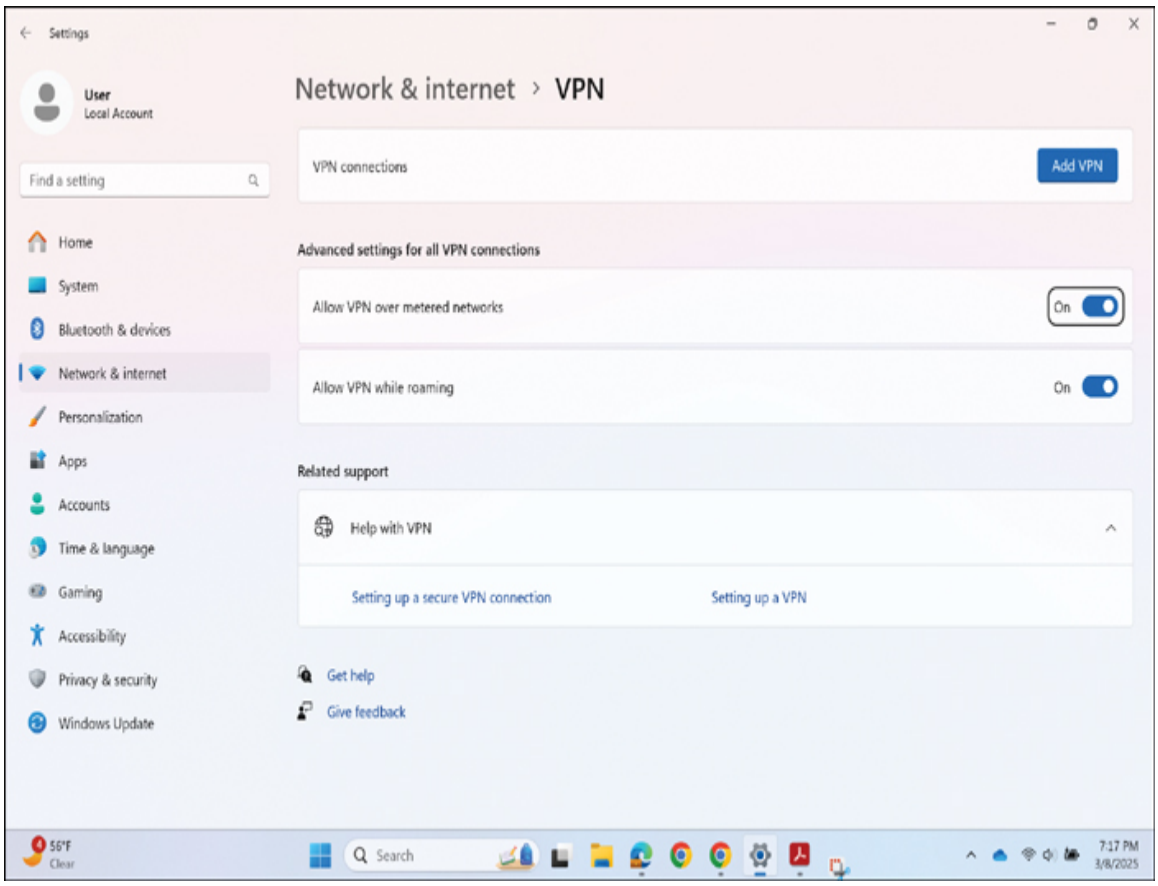


FIGURE 38.6 **VPN Configuration Screen, Including Metering Connection**

Note

Most VPN solutions have specific software that needs to be installed on the individual devices. Follow the publisher's recommendations if that is the case.

Usually, what you need to know is the IP address (or name) of the gateway or server that you need to connect to, as well as the appropriate passwords to get into the network and, possibly, to establish encrypted networking sessions.

In general, whenever you establish a new networking connection, you are asked to provide a *network location*. Windows asks you whether you want

it to be private or public. A private profile means that network discovery is turned on (and that the system is searchable on the network) and file and printer sharing is enabled. Private is good for home connections and when you're connecting to a workplace where you trust the systems that you are connecting to (and their surrounding systems). A public profile means that network discovery and file and print sharing are turned off; this connection is good for when you need to connect to public networks that you don't trust because you don't know what computers will be on those networks.

Proxy Settings

Some organizations use proxy servers to cache HTTPS, FTP, and other information. If you want to connect to the Internet in this scenario, the client workstations must have the Proxy server setting configured. This allows the client to access the proxy server, which then forwards requests out to the Internet and to the corresponding web servers or other types of servers.

The Proxy setting is located in different places, depending on the web browser you use:

- **Microsoft Edge:** Navigate to **Settings > Network & Internet > Proxy** or search for "proxy" in the Edge browser settings (**edge://settings**).
- **Internet Explorer:** Open the Internet Properties window, which can be opened from the browser, or go to **Control Panel > Internet Options**. From there, access the **Connections** tab, click the **LAN settings** button, and click the **Proxy server** checkbox.

You can have Windows attempt to set up a proxy connection automatically, and you can use a script to aid in the process. Otherwise, you have to manually set up the proxy connection. Essentially, that means you need to know the IP address and the port used for the proxy server. For example, 172.18.0.105:443 would mean that the IP address of the proxy server is 172.18.0.105, and the server's listening port is 443. You can also exclude particular addresses that you don't want to go through the proxy; for example, sometimes websites and services don't allow a user access if that user is using a proxy. In addition, you can disable the use of the proxy

server for local addresses (on the LAN or an intranet). We discuss proxy servers further in Chapter 8, "Network Devices."

ExamAlert

Know how to navigate to and configure the proxy settings in Windows!

Cram Quiz

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

1. Which of the following are administrative share names? (Select the two best answers.)

   - ○ **A.** C$
   - ○ **B.** C:\Windows
   - ○ **C.** ADMIN$
   - ○ **D.** System32
   - ○ **E.** $print

2. You need to design a local area network for 10 computers with very limited data sharing. Which of the following network types is the best option?

   - ○ **A.** Workgroup
   - ○ **B.** Client/server
   - ○ **C.** VPN
   - ○ **D.** Domain

3. You want to connect to a share on \\server1\data-share. Which of the following should be used to accomplish this?

   - **A.** Use a proxy server.
   - **B.** Right-click the folder and select **Share with**.
   - **C.** Use **ipconfig**.
   - **D.** Use **net use**.

4. You have been tasked with setting up a client Windows computer. It needs to gain access to the Internet, but all web traffic is cached and filtered by a go-between server on the LAN. What should you configure to enable Internet access for the Windows client?

   - **A.** VPN
   - **B.** Proxy server
   - **C.** Domain
   - **D.** Workgroup

5. In Windows, which network location profile setting should you choose if you are not sure what computers will be on the network or if you can trust them?

   - **A.** Private
   - **B.** VPN
   - **C.** Metered connection
   - **D.** Public

Cram Quiz Answers

1. **A and C.** Every volume gets an administrative share by default, including the C: drive, which is assigned C$. ADMIN$ is another administrative share; it is the share name for C:\Windows. System32 is simply a folder name within C:\Windows. $print is not an administrative share, but it could be used as a share name.

An actual administrative share is print$, with the $ at the end of the share name. By the way, the print$ share is used to deliver print drivers from the print server to the client computer.

2. **A.** The best listed option is the Workgroup. In Microsoft environments, it works well for 20 or fewer computers. Client/server networks such as Microsoft Active Directory Domains are designed for more computers, often in an enterprise setting. A VPN is usually implemented for users who need secure connections to other networks or the Internet.

3. **D.** The **net use** command can connect to shares such as \\server1\data-share or any other share on the network. Of course, you could also do this by mapping a network drive in File Explorer. A proxy server is used to filter and cache client connectivity to the Internet. Right-clicking the folder and selecting **Share with** allows you to share the folder but doesn't make a connection to the share. **ipconfig** is used in the command line to learn the IP configuration of the network adapter.

4. **B.** You can configure a proxy server by entering the IP address of the proxy server and the port to be used. A VPN allows secure connectivity to the Internet. A domain is a large network of computer systems that are centrally administered. A workgroup is a small group of networked systems.

5. **D.** A public network profile means that network discovery and file and print sharing are turned off; this connection is good when you need to connect to public networks that you don't trust (like at a coffee shop) because you don't know what computers will be on those networks. Private is reserved for networks where you trust the systems. While a VPN is private and secure (hopefully), it is not one of the "network location profiles" in Windows but rather a network connection type. A metered connection should be used for hotspots, VPNs, and other connection types that might have data caps.

We could go on and on about Windows networking. Be sure to explore Windows and the various configuration locations mentioned in this chapter. Review your notes, take a break, and then continue on. Great work!

Chapter 39

macOS

This chapter covers the following A+ 220-1202 exam objective:

- **1.8** – Explain common features and tools of the macOS/desktop operating system.

Although Windows has the largest market share of the desktop and laptop market, there are other operating systems you can choose from as well. macOS is a favorite with users who need to manipulate audio and video media. It's also commonly used by engineers and developers. Plus, some people just plain prefer macOS to Windows and favor the Apple MacBook Air and/or MacBook Pro over Windows-based PCs. This chapter discusses some basic features and tools of the macOS operating system.

ExamAlert

Objective 1.8 focuses on macOS: the installation and uninstallation of applications, system folders, Apple ID and corporate restrictions, best practices, system preferences, features, Disk Utility, FileVault, Terminal, and Force Quit.

macOS Basics

macOS is closed source. That means that the code is *not* released to the public; you cannot download it. The history of macOS is quite interesting but also quite involved. Without trying to be too reductionist, let's look at a brief overview of the history of macOS.

Classic Mac OS was the first operating system shipped with the original Apple Macintosh in 1984. It featured a graphical user interface (GUI), which allowed a mouse to navigate the operating system with graphical elements such as icons, buttons, and menus. Prior to this, most computer operating systems were just a command-line interface (CLI), where users had to type in commands to have the computer do anything. While we still use CLI interfaces today, like the Command Prompt in Windows or Terminal on the Mac, many users spend most of their time in the GUI of the operating system.

Classic Mac OS developed over the years, with the last version being Mac OS 9 in 1999; it was later renamed Classic Mac OS to differentiate it from the newer, completely different Mac OS that was coming. There are many great books written on Steve Jobs (the cofounder of Apple), the creation of Apple, his departure from Apple, and later his return to Apple. This information is beyond the scope of a certification book. However, it is important to know that when Jobs left Apple in 1985, he started another computer company called NeXT. NeXT computers ran an operating system called NeXTSTEP, which used a derivative of the BSD operating system. BSD, or Berkeley Software Distribution, is an open-source implementation of AT&T's UNIX operating system, which was proprietary and dates to the late 1960s. UNIX—and its open-source counterparts—is incredibly stable and built to be a modular operating system. This means that it can be very small and specific or large and full featured.

Apple bought NeXT in 1997, and with that, Steve Jobs returned to Apple. Apple was struggling with sales in the late 1990s, so Jobs decided to completely ditch the Classic Mac OS and make a brand-new operating system for Apple computers based on NeXTSTEP, which is based on BSD. It would be called Mac OS X. This new OS brought incredible stability and performance. After several versions, Mac OS X was renamed macOS with the release of macOS 10.12. This name change helped prevent consumer

confusion when Apple's mobile operating system, iOS, was going to hit its tenth release, iOS 10.

The original BSD was discontinued long ago, but it became the basis for a lot of software, including operating systems such as FreeBSD, OpenBSD, and NetBSD (which are open source), as well as macOS and iOS.

ExamAlert

macOS is closed source and is based on BSD (UNIX).

Note

People often say that macOS is based on UNIX. This is true and not true. It is actually based on BSD, which was an open-source, written mostly from scratch, copy of UNIX. UNIX was copyrighted by AT&T, so computer scientists at the University of California, Berkeley, wrote BSD to provide a free alternative while still maintaining the robustness of UNIX. The history is a little more complex than this, but this is the crux of it.

You will also hear about the incredibly popular Linux operating system. Linux runs the vast majority of Internet servers and most computer appliances today. The Linux kernel, the heart of the operating system, was written by Linus Torvalds in 1991. He also modeled his operating system on UNIX-like ideals. This is why you will hear people state macOS and Linux are related. They're not, but they're both made on UNIX-like operating systems.

Apple is credited with making the original graphical user interface that people manipulate with a mouse and keyboard—the mainstream way of working with a computer. macOS uses control panels (windows with icons) to configure, troubleshoot, and maintain the computer. Collectively, these are known as System Preferences. This is similar to the Microsoft Windows Control Panel, though different functions have varying names and locations.

Some applications are ported for macOS (for example, Microsoft Office for Mac); however, macOS uses its own web browser (Safari) as opposed to Microsoft Edge in Windows. Web browsers such as Chrome and Firefox can be run on macOS as well.

An example of the macOS GUI is shown in Figure 39.1. The macOS desktop has a user-friendly design that includes a basic menu bar at the top, which includes the Apple menu, the currently opened application (in this case, Terminal), and standard options (such as Edit, View, and so on). There are icons on the bottom (in the Dock) used for commonly used applications, such as Mission Control, Reminders, and Notes. The *Dock* is a major feature of the macOS GUI used to launch common applications and switch between running apps.

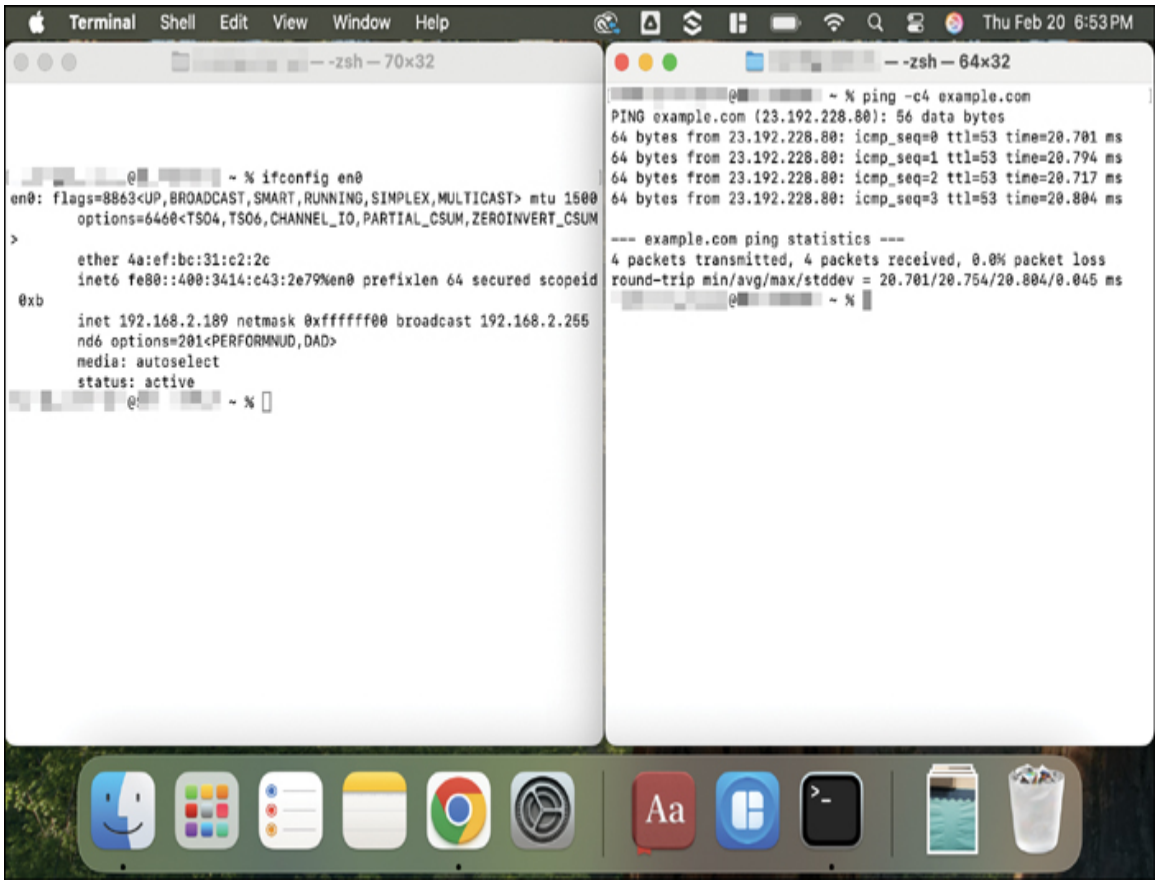


FIGURE 39.1 **Example of the macOS GUI**

ExamAlert

Use the Dock to open common applications and switch between running apps.

In Figure 39.1 you can see that the Terminal program is open. Two commands were run: the **ifconfig** command, which shows information about the network interface, including the IP address (192.168.2.189), and the **ping** command, showing 64-byte ping replies from example.com. The Terminal works in a similar fashion to the Linux Terminal but does not have many of the new Windows Terminal features like panes, GPU acceleration, and theming. Now, while the **ifconfig** command still works in macOS, as you can see in Figure 39.1, it has largely been replaced with the **ip** command. To see the same information from the **ifconfig** command, run **ip addr** instead.

Note

While Windows and macOS have a lot of similarities, there are also many differences. One difference that many Windows users aren't accustomed to is the placement of the close, minimize, and full screen buttons. On Windows, these buttons are on the upper right of the window. On macOS, they are on the upper left and color-coded instead of using the icon design of Windows.

In macOS, the left red button is close, yellow is minimize, and green is the window tiling control. In macOS, the new window tiling control, the green button, allows users to snap windows into different positions. Originally, the green button was full screen, but with the introduction of macOS Sequoia, the green button is similar to the Windows 11 Snap feature.

Another somewhat important differentiation between the two in this regard is the close button. In Windows, if you click the close (X) button, it exits the program. In macOS, when you click the red close button, it seemingly exits the program as well, but it actually suspends the program rather than fully exits it. This operation is similar to iPhones and Android phones that suspend the program

instead of exiting when closing the app. The idea is that suspending the app in RAM will allow it to come back faster. When you click the red close button, and the window disappears, look down at the Dock. You will see a small dot under the program icon. This shows the program is suspended rather than closed. To fully close the application, you can use the keyboard shortcut of Command (⌘) + Q or choose **App Name** and **Quit App** in the menu bar (your app window must be selected because the menu bar at the top is context sensitive).

System Preferences

To configure macOS, you go to System Preferences. It is similar to the Control Panel and Settings in Windows and Settings in Linux. There are many options here, including the following:

- **Displays:** Here you can modify the look of the display, change the resolution, and modify the brightness and color scheme.
- **Networks:** In this section you can modify wired networks, wireless connections, and USB Ethernet connections. You can also configure advanced TCP/IP settings.
- **Printers & Scanners:** Here you add or remove printers or scanning devices, work with the print queue, share printers, and modify printer options.
- **Security & Privacy:** In this section you can change your password, enable FileVault, configure the firewall, and enable/disable location services.
- **Accessibility:** This section enables you to make the system more accessible by incorporating keyboard shortcuts for zooming in and out of the display, setting up gestures via the keyboard, turning on dictation, enabling captions, and using additional keyboard, mouse, video, and audio options.

ExamAlert

Exam Objective 1.8 specifically calls out System Preferences, including Displays, Networks, Printers, Scanners, Privacy, Accessibility, and Time Machine (discussed later in this chapter). Be sure you are familiar with these common macOS features and can explain what they do!

System Preferences is the home to many other configurable options for the Dock, Mission Control, audio, energy savings, and much more. There are also programs that you can work with, including the Time Machine, which we'll discuss later in the chapter.

macOS Features

Many features in macOS make it a user-friendly environment. The CompTIA 220-1202 exam focuses on a small group of them, which we'll discuss now.

The best way to open applications or files is to use *Finder*, a program similar to File Explorer but designed to make finding applications easy. Finder is available on the menu bar as well as within the Dock. Applications and files can also be stored on the Dock and anywhere on the desktop, but if you don't see the application or file you want, you can use the Finder program.

If you still can't find what you are looking for or if you aren't even sure whether it is on your computer, use the *Spotlight* search tool. This tool is displayed as a spyglass in the menu bar on the top right of the desktop and can also be accessed by pressing and holding the Command (⌘) and spacebar keys simultaneously on the keyboard. (The Command key is similar to the Windows key on a PC keyboard.) This search tool searches through files, emails, apps, songs, printers, and so on. It can also search other computers on the network (which it discovers using Bonjour—a networking technology used by macOS to locate networked computers and devices). Plus, it looks through external sources such as Wikipedia and Google, to name a few. The goal is to receive a media-rich, definitive set of results to your query.

ExamAlert

Understand what the Finder and Spotlight programs are in macOS.

Let's get into what you see on a Mac and how it is displayed. First, you can modify how the desktop is displayed, or you can set up *multiple desktops*. This is done within *Mission Control*. Mission Control zooms away from the desktop, giving you a larger perspective of apps, "spaces," and virtual desktops. It acts as an application switcher and window manager. Mission Control can be launched in a variety of ways, including by swiping up on the trackpad with three fingers, double-tapping the Magic Mouse (which is an Apple mouse that allows for special clicking and gesturing, making it easier to navigate through macOS), clicking the Mission Control icon on the Dock, or pressing the Mission Control key on the keyboard. Now you can have multiple desktops by dragging windows to the upper-right corner, or you can add windows to already existing desktops by dragging them to the appropriate desktop at the top of the window.

The Dashboard is available here as well; it has some default functions, such as the clock, calendar, and calculator. You can also add special programs to the Dashboard by clicking the + sign. This technology has great implications for researchers, students, programmers, A/V editors, and so on. It allows a user to highly customize the user interface. But be careful because too many desktops and too many open applications will cause the system to run sluggishly. Also, users sometimes forget that they have applications open in other desktops; a quick, three-finger swipe up will reveal anything that is currently running.

Speaking of three-finger swipes, there are all kinds of *gestures* and multitouch gestures that can make you a more efficient macOS user. If you have the supporting hardware (such as a Magic Trackpad or Magic Mouse), you can make use of things such as tapping, scrolling, pinching, and swiping, similar to the same functions on a mobile device. For example, a two-finger swipe up or down will scroll content; a two-finger double-tap will perform a smart zoom, and you can do it again to return; and, of course, there is the pinch out to zoom. The list goes on and on. For a

complete list of available multitouch gestures, visit https://support.apple.com/en-us/HT204895.

You can also allow users on other Macs to view your screen and even take control of your computer with a tool called *Screen Sharing* (similar to Windows Remote Desktop). To enable this, go to the **Apple** menu > **System Preferences**, click **Sharing**, and then select **Screen Sharing**. For a step-by-step procedure on how to do this and how to connect from another system, visit https://support.apple.com/guide/mac-help/share-the-screen-of-another-mac-mh14066/mac.

Things get a little more complicated when you want a Windows computer to control (or just see) a Mac. Third-party Virtual Network Computing (VNC) software (such as RealVNC) can help with this. VNC works cross-platform between Windows, macOS, Linux, and mobile OS versions. VNC can also be used to view a Mac that has Screen Sharing enabled.

Note

Sometimes you might need to share the screen with a second display or to a projector. Many older Mac computers came with a secondary DisplayPort (DP) port to enable duplication of the screen. On newer Macs, this can still be done with a USB-C port replicator/docking station.

ExamAlert

Know how to configure multiple desktops, Screen Sharing, and the replication of the display to a secondary monitor.

What if you want to run Windows and macOS? With older, Intel-based Macs, you could run *Boot Camp*, which allowed you to dual-boot Windows alongside macOS. However, as Apple transitioned to ARM-based processors with the M1–M4 CPUs, *Boot Camp* was discontinued. If you

want to run both operating systems, you will need to run virtualization software on macOS and run Windows as a virtual machine.

For security, Apple provides the *Keychain Access* utility, a password management system that can contain not only passwords but private keys and certificates. Keys and certificates are cryptographic methods for storing (and transmitting) secrets; they are generally considered to be more secure than passwords. Keychain Access, which can be accessed from **Finder > Applications > Keychain Access**, enables a user to automatically populate passwords in applications and save passwords to the cloud (for example, to an iCloud account).

ExamAlert

Consider configuring the Keychain utility to save passwords to an iCloud account. This will enable password population even if a user switches to a replacement macOS device.

iCloud and Continuity

iCloud is Apple's cloud storage and synchronization service, deeply integrated into macOS and its core applications. It allows users to back up data, sync settings, and access files across multiple Apple devices. iCloud acts as a central hub, enabling seamless transitions between Macs, iPhones, iPads, and even the web. Key features include iCloud Drive for file storage, iCloud Backup for device backups, Keychain for password management, and synchronization services for apps like Contacts, Calendars, and Reminders. By leveraging iCloud, users can ensure their important data is always available and up to date, regardless of which device they are using.

iCloud plays a crucial role in the functionality of iMessage, FaceTime, and Drive in macOS. For iMessage and FaceTime, iCloud syncs messages, call history, and contacts across devices. This means you can start a conversation on your Mac and continue it seamlessly on your iPhone. iCloud Drive allows you to store files in the cloud and access them from any of your devices. You can save documents, photos, and other files

directly to iCloud Drive from within applications, making collaboration and sharing simple. Furthermore, app-specific data, such as preferences and settings, can be synced through iCloud, ensuring a consistent user experience across all Apple devices. This tight integration between iCloud and these core applications makes the Apple ecosystem cohesive and user-friendly.

In 2014, Apple introduced *Continuity* in macOS. It represents a collection of features that seamlessly integrate Apple devices, creating a unified and intuitive user experience. It bridges the gap between Mac, iPhone, iPad, and Apple Watch, enabling them to work together. Features like Handoff allow users to begin a task on one device and seamlessly transition to another, while Universal Clipboard facilitates effortless sharing of content between devices. AirPlay to Mac enables streaming from iOS/iPadOS devices or using the Mac as an AirPlay speaker, and Sidecar transforms an iPad into a secondary Mac display. Continuity Camera leverages iPhone as a webcam, unlocking unique features. Call and Message Relay, iPhone Mirroring, Instant Hotspot, and Unlock with Apple Watch further streamline workflows and enhance convenience.

These Continuity features rely on devices being signed into the same iCloud account, with Bluetooth and Wi-Fi enabled, and meeting specific system requirements. By leveraging Continuity, users experience a more fluid and productive workflow. This interconnectivity empowers users to seamlessly transition between devices, share information effortlessly, and ultimately, accomplish more with greater ease.

ExamAlert

Know what iCloud is and how it synchronizes all your data across your iPhone and macOS. Also, know how Continuity is a feature to maximize data synchronization across all of the Apple ecosystem.

macOS System Folders

In macOS, the following root-level folders serve distinct purposes in organizing the operating system and user data.

- */Applications* is the standard location for most user-installed applications. Think of it as the main "programs" folder.
- */Users* contains the individual home directories for each user account on the system. Each user's home directory (such as /Users/username) stores personal files, settings, and preferences.
- */Library* at the root level holds systemwide settings, resources, and support files used by applications and the operating system itself. It's crucial for the stability and functionality of macOS.
- */System* contains the core operating system files, including the kernel, frameworks, and essential system utilities. Modifying anything within */System* is generally discouraged because it can lead to system instability.

ExamAlert

Be sure you know the macOS System folders, including /Applications, /Users, /Library, /System, and /Users/Library. Be able to explain where they are and what they contain.

Within the */Users* directory, each user's home folder also contains a Library folder (/Users/username/Library). This user-specific Library folder is separate from the root-level /Library and stores settings, preferences, and support files that are specific to that user. This separation allows multiple users to have different settings and preferences without affecting each other. The user Library folder is often hidden by default but can be accessed through the Finder's Go menu by holding down the Option key. It's important to understand the distinction between the root-level */Library* (systemwide) and the user-level /Users/username/Library (user-specific) folders to effectively manage settings and troubleshoot issues. Figure 39.2 shows the root-level folders in the Finder window.

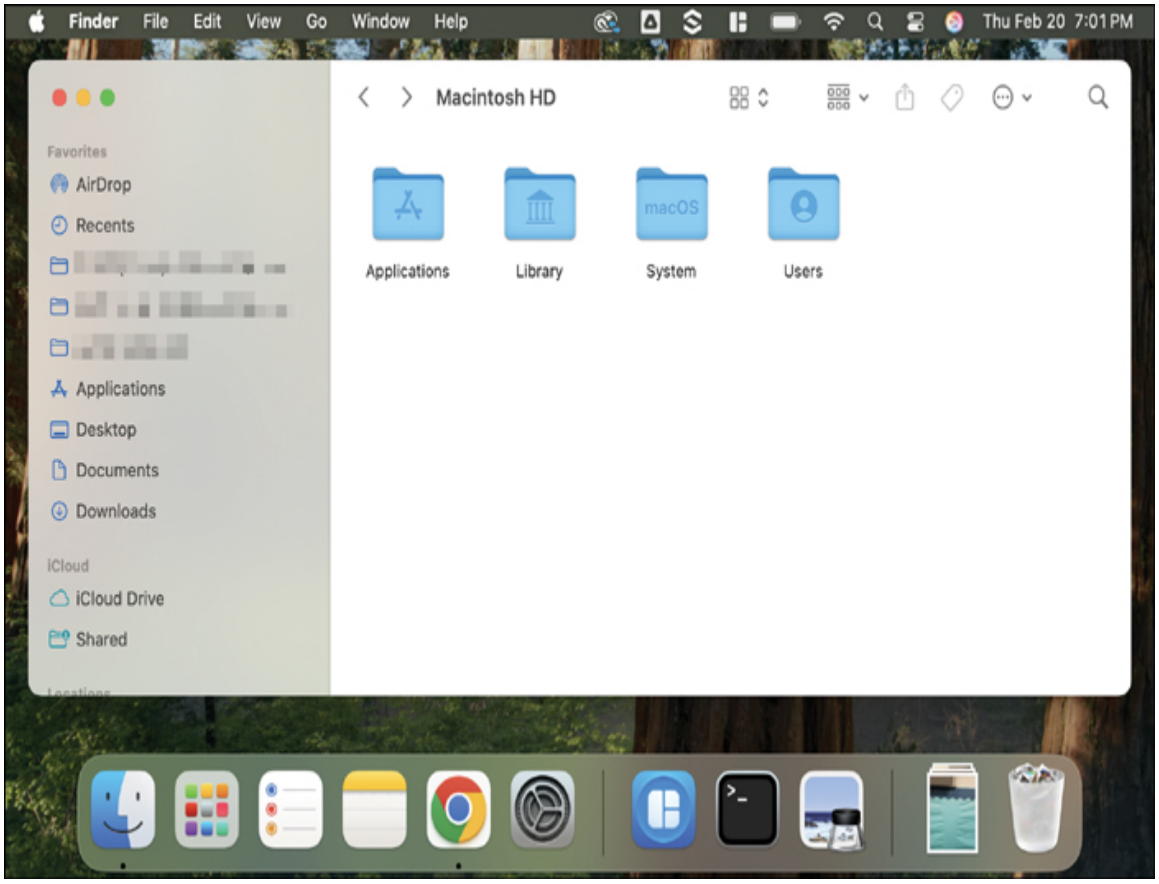


FIGURE 39.2 **macOS Root-Level Folders**

Managing and Maintaining macOS

Once again, for the location and management of files and running applications, macOS uses Finder. Finder will open automatically whenever you access a drive or file listing. From Finder, you can create files, copy and paste files, access favorites (such as Applications, Downloads, and so on), access removable drives, and tag files/applications with various colors. You can also manipulate files at the command line. As mentioned, macOS has a shell utility called *Terminal* that allows you to manipulate data and make configuration changes similar to the PowerShell or Command Prompt in Windows. However, the syntax is different and is similar to that of BSD and Linux. To open the Terminal, go to **Finder > Applications > Utilities > Terminal**. You can also open an application by using the Spotlight tool and simply typing the name of the application.

In addition to viewing locally stored data, you can view remote discs on other Mac computers by sharing them in the System Preferences, and you can view them from the local computer by selecting the **Remote Disc** option in **Finder > Devices**. Data can also be stored on the cloud; Apple's version is called *iCloud*. To back up data to iCloud, go to the **Apple** menu **> System Preferences**, click **Apple ID**, and click **iCloud**.

For backing up the state of the computer, macOS utilizes the *Time Machine* backup program. To enable it, go to the **Apple** menu and select **System Preferences**. Then select the **Time Machine** icon and turn it on to enable automatic backup of any drive. From here, you can back up drives locally or to iCloud.

You also can restore data from this program. Essentially, you can select the point to which you want to restore—be it a day ago or a year ago. To do this, simply select the desired snapshot from a timeline in the program. This is similar to Windows System Restore. Because the program saves multiple states of files over time, a separate backup method (such as a USB flash drive or other external media) is also recommended for important files.

Although Macs are known for their resilience, their drives should still be maintained. The built-in *Disk Utility* is used for verifying and repairing the storage drive, repairing drive permissions, and possibly booting from the recovery partition (which all Macs have). Disk Utility can also be used to create an image or to recover a system from that image. Note that macOS version 10.14 and higher require the GPT partitioning type. For more information about GPT, GUID, and MBR, please see Chapter 30, "Operating System Installations and Upgrades."

You can also encrypt the contents of the main storage drive on a Mac with *FileVault*. This program uses the Advanced Encryption Standard (AES) at 128-bit security (as of the writing of this book) to encrypt the entire contents of the drive and prevent unauthorized access to the data stored there. To enable it, go to the Apple menu and click **System Preferences > Security & Privacy**. Then click the **FileVault** tab, enter the administrator name and password, and click **Turn On FileVault**.

Sometimes you might encounter the *spinning pinwheel*, also known as the spinning pinwheel of death (SPOD). This multicolored spinning wheel is a

variation of the mouse pointer arrow; it appears when an application either becomes temporarily unresponsive or enters an infinite loop and cannot recover. If an application freezes or is otherwise not responding properly, you can force that app to close by using the *Force Quit* application. This is located on the Apple menu; after you open Force Quit, you can select the application you want to force to close. This is similar to using the Task Manager in Windows. You can also use the keyboard combination Command+Option+Esc, which is similar to Ctrl+Alt+Del on a Windows PC. However, be ready to troubleshoot further; launching the application again may result in another SPOD.

ExamAlert

If you experience the spinning pinwheel of death (SPOD) in macOS, it is very likely that a frozen app is the cause. It appears when an app exceeds the Mac's processing capability.

ExamAlert

Know how to use the Time Machine, Disk Utility, FileVault, and Force Quit tools in macOS.

General system maintenance includes system updates, antimalware updates, driver updates, and firmware updates. macOS can be updated by going to the **Apple** menu and selecting **Software Update**. It can also be updated from the App Store. Antimalware updates should, of course, be done within the third-party application you are using; we'll discuss malware in more depth in Chapter 46, "Wireless Security and Malware." The video driver is built into macOS, and it can only be updated by upgrading to a new version of the operating system. Keyboards, mice, and many other devices need to be approved for use with Mac computers; if you buy an Apple-approved device, it should work with macOS. Unfortunately, if a device requires a higher version of macOS, you'll have to upgrade. Most printers work with macOS also, and if a printer driver needs to be downloaded, macOS will

automatically run the AirPrint program to locate and download the driver. In general, macOS is designed to simplify the process of installing devices. Finally, firmware updates are usually done automatically when you upgrade to a newer version of macOS. Somewhat recently, Apple has rolled out what is called a *Rapid Security Response (RSR)* update. These updates are minor security updates that Apple releases to patch vulnerabilities between standard updates. These are similar to Microsoft's *hotfixes*. These updates are often small in size, install automatically, and often don't require a reboot of the computer.

ExamAlert

Know how to back up a Mac, how to update, and what an RSR is.

Installation and Uninstallation of Applications

Because Apple devices are designed to be extremely user-friendly, the installation and uninstallation of applications is usually very easy.

A typical way to get apps is to simply go to the App Store. From here, it's a breeze to search for, install, and update applications. However, while that process is very intuitive, sometimes you might need to go a little further. For example, you might need to download a program from the Internet that is not in the App Store. Usually, this is still a pretty straightforward installation: Once an application is downloaded to the Downloads folder, you double-click the package (or disk image) and follow the installer's onscreen instructions.

Here are the file types that you should know for the exam:

- **.dmg:** These are mountable disk image files that are intended for distribution of software to macOS systems. This format is commonly used by developers to build and distribute applications for macOS. These files can be validated during installation to make sure they have not been tampered with during transit. When a user double-clicks a package, it is opened by the Disk Image Mounter utility, which mounts

a virtual disk in Finder (and possibly on the desktop) that appears similar to a USB flash drive. The user may then find one or more program icons (APP files) that can be run from that location or dragged to another location such as the Applications folder.

- **.app:** Also known as APP files, these are application bundles that are designed to run under the macOS system. They run when they are double-clicked, in a similar fashion to .exe files in Windows. They are often found within .dmg software packages. While entire APP files can be moved to another location and run, individual files within an APP file should not be moved away from the rest of the files in the package.
- **.pkg:** These are packages of software and other files that can be installed to macOS and iOS devices. In some cases, a .pkg file is a file saved as plaintext; if that's the case, it can be opened with any text editor in macOS. The extension is also used by several other types of systems and may be developed by more insidious persons. macOS provides an automatic security safeguard related to these files, and a user might encounter a situation where the .pkg file can't be opened because it is from an unidentified developer. It's not recommended to install programs that give messages like this.

ExamAlert

Know the differences between .dmg, .app, and .pkg. For example, you can't install from a .dmg file on Windows because that file type is not compatible with Windows; it is designed for macOS.

You can uninstall applications within **Finder > Applications**. Generally, you want to use an uninstaller program. Open the application's folder and check for an uninstaller. If one exists, double-click it and follow the onscreen instructions to remove the application. If an uninstaller program does not exist, drag the application from the Applications folder to Trash (located at the end of the Dock by default). You can uninstall applications that came from the App Store by using the Launchpad program. In Launchpad, click and hold on the application that you wish to remove until

all the applications start to jiggle and then click the application's delete button.

In a corporate environment that uses Managed Apple IDs, users will not be able to install or uninstall applications. You'll learn more about Managed Apple IDs in the next section.

Apple ID

To sign in to Apple services and use iCloud for storage, Apple devices use the Apple ID, which identifies a user.

The Apple ID is designed to keep settings and services up to date across all Apple devices. If a person uses an iPad, an iPhone, and a MacBook, then things such as passwords, apps, documents, and configurations can all be synchronized among these devices.

By default, an Apple ID starts with an email address and a password. However, it can be augmented with two-factor authentication to allow connections only from trusted devices and only if the user knows the required multidigit verification code in addition to the password. This is designed to prevent unauthorized logins.

For example, if an iPad requires a user to sign in with an Apple ID, that user would have to type the password and then most likely access an iPhone (or other smartphone) to get the verification code requested on the iPad. As of the writing of this book, the secondary code is optional, but many technology companies are planning on making two-factor authentication mandatory for users. Typically, this is a more secure way of authenticating users, so be ready for it!

A company can also create Apple IDs to be assigned to users for business purposes. These are known as *Managed* Apple IDs. They are separate from a user's personal Apple ID and are assigned by the administrator at the company. However, a user can have the same email address and phone number for both a Managed Apple ID and a personal Apple ID. To protect the company, there are several restrictions for Managed Apple IDs. For example, these IDs cannot make purchases, and certain features are disabled. To get access to something, a typical user might have to contact

the administrator at the company. Effectively, the company owns the Managed Apple ID user accounts. Apple ID corporate restrictions include limitations on apps, services, and device settings. These restrictions are put in place to protect corporate data and ensure that employees can access only approved apps and content. Apple ID corporate restrictions also enable administrators to allow (whitelist) approved apps that can be downloaded and installed on company devices. This restriction prevents employees from installing potentially risky or irrelevant apps that could compromise device integrity or distract from work tasks. This can also include mobile device management, or MDM. See Chapter 49, "Mobile Device Security," for more information on MDM.

Note

Apple provides extremely concise instructions on how to do just about anything on an Apple device at https://support.apple.com.

Cram Quiz

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

1. Which of the following is the built-in web browser for macOS?

   - ○ **A.** Safari
   - ○ **B.** Chrome
   - ○ **C.** Firefox
   - ○ **D.** Edge

2. Which program should you use to access Utilities in macOS? (Select the two best answers.)

   - ○ **A.** Mission Control

- ○ **B.** Finder
- ○ **C.** Spotlight
- ○ **D.** Keychain

3. Which of the following should be enabled when you want a user at another Mac to take control of your computer?

- ○ **A.** Remote Desktop
- ○ **B.** Remote Assistance
- ○ **C.** Screen Sharing
- ○ **D.** Screen Mirroring

4. What root level folder contains core operating system files?

- ○ **A.** /Applications
- ○ **B.** /Users
- ○ **C.** /Library
- ○ **D.** /System

5. You want to save the state of a Mac running macOS. Which tool should be used?

- ○ **A.** System Restore
- ○ **B.** Time Machine
- ○ **C.** Force Quit
- ○ **D.** Disk Utility

6. Due to recent corporate espionage attempts, a technician needs to secure the contents of the main storage drive on the CEO's Mac. Which macOS utility will allow the tech to encrypt the drive? (Select the best answer.)

- ○ **A.** Terminal
- ○ **B.** FileVault

- ○ **C.** App Store
- ○ **D.** 128-bit encryption

7. Which program handles installing a printer's driver automatically in macOS? (Select the best answer.)
   - ○ **A.** Bonjour
   - ○ **B.** Magic Mouse
   - ○ **C.** AirPrint
   - ○ **D.** iCloud
8. You need to download an application that is not available on the App Store. It needs to be mounted as an image. Which of the following extensions should you use?
   - ○ **A.** .pkg
   - ○ **B.** .app
   - ○ **C.** .dmg
   - ○ **D.** Finder
9. A customer reports that a spinning wheel appears on the screen when trying to run a specific application. What does this spinning wheel represent? (Select the best answer.)
   - ○ **A.** A failing CPU
   - ○ **B.** An Apple macOS proprietary crash screen
   - ○ **C.** A Microsoft Windows proprietary crash screen
   - ○ **D.** A Linux proprietary crash screen

Cram Quiz Answers

1. **A.** Safari is Apple's web browser. It is used in macOS and iOS. Chrome is developed by Google and can be added to macOS.

Firefox (Mozilla) can also be added to macOS. Microsoft Edge is the built-in browser that Windows uses.

2. **B and C.** Finder is the application to use when looking for applications and files. Utilities is located in **Finder > Applications**. Spotlight can be used to locate just about anything on a Mac, including Utilities. Mission Control allows you to modify the desktop (and run multiple desktops). Apple provides the Keychain Access utility, a password management system that can contain not only passwords but private keys and certificates.

3. **C.** Use Screen Sharing in macOS to allow another user to view and take control of your Mac. (The remote user could also use VNC.) Remote Desktop and Remote Assistance are similar programs used in Windows. Screen mirroring is a technology (common in mobile devices) that allows the display to be mirrored to a TV or to another computer.

4. **D.** /System contains core operating system files. Usually, this is not an area to modify! /Applications stores user-installed applications. /Users contains the home directories for users, and /Library holds systemwide settings.

5. **B.** Use the Time Machine to save the state of the computer or to restore to that computer's earlier state. This is similar to the Windows System Restore utility. Force Quit is a utility in macOS that closes a nonresponsive application. Disk Utility is used to verify and repair macOS drives.

6. **B.** The tech can encrypt the contents of the main storage drive on a Mac with FileVault. Terminal allows you to enter commands, manipulate data, and make configuration changes and is similar to the PowerShell or Command Prompt in Windows. A typical way to get macOS apps (with a valid Apple ID) is to simply go to the App Store. Although FileVault implements AES 128-bit encryption to encrypt the entire contents of a drive, 128-bit encryption by itself is not a macOS utility.

7. **C.** AirPrint is the technology used to install a printer automatically in macOS (as long as the printer is compatible with macOS). Bonjour is a networking technology used by macOS to locate networked computers and devices. The Magic Mouse is an Apple mouse that allows for special clicking and gesturing, making it easier to navigate through macOS. iCloud is Apple's cloud infrastructure, where a Mac user can store and back up data. While AirPrint might locate the printer driver on iCloud, iCloud is not the best answer.

8. **C.** Download the .dmg file format. This provides a mountable image that is opened by the Disk Image Mounter utility when double-clicked. It then mounts a virtual disk in Finder, but Finder is a program, not an extension. The .pkg and .app file types do not mount an image the way that a .dmg does. However, an .app might exist inside a .dmg!

9. **B.** A pinwheel, also known as a spinning pinwheel of death (SPOD), is an Apple macOS proprietary crash screen. An example of a Microsoft Windows proprietary crash screen is the blue screen of death (BSOD). Linux is an open-source operating system. Although there are crash screens in Linux, they are not considered proprietary. A spinning wheel could possibly be *caused* by a failing CPU, but it is more likely caused by a stalled or frozen application.

---

macOS: Think different; click smarter. Review the chapter and your notes, take a sip of your favorite beverage, and then continue! See you in the next chapter!

Chapter 40

Linux

This chapter covers the following A+ 220-1202 exam objective:

- **1.9** – Identify common features and tools of the Linux client/desktop operating system.

On the desktop side, Linux is used mostly by enthusiasts and techies—such as system administrators, developers, engineers, gamers, and so forth. Linux on the desktop side has a smaller business market share than Windows (3.71 percent Linux vs. 71.91 percent Windows), but even its small share of the market still represents a substantial number of computers. Covering Linux is worthwhile for that reason alone.

On the server side, IT infrastructure is dominated by Linux. Couple this with the fact that any Linux system (desktop or not) can act as a server, and you see that it is important to cover some server-side content as well within this chapter.

Supporting Linux is a valued skill in today's job market. We won't go too deep, but you should come away from this chapter with a basic understanding of how to manipulate any Linux system, especially from the command line.

ExamAlert

Objective 1.9 focuses on Linux: file management, administrative commands, package management, network, informational

commands, text editors, common configuration files, OS components, and the root account.

Linux Basics

Linux is open source. The code for Linux can be downloaded and used/modified by anyone, which means anyone can build their own version of Linux. You might have heard of several (or more) different distributions of Linux. In no particular order, some common examples include Debian, Ubuntu, Fedora, Red Hat Enterprise Linux, Kali Linux, and Arch Linux. But the list goes on and on. These distributions are community supported, and some have client-side and server-side versions (for example, Ubuntu Desktop and Ubuntu Server). There are so many Linux distributions that we could fill a book describing them, and more are being released every week. This is the beauty of the General Public License (GPL) for Linux: It basically states that Linux is free to use and to develop. People at home can make their very own versions of Linux if they so desire.

On the client side, Linux users have the option of using one of several desktop environments (GUIs). One popular desktop environment is GNOME, which stands for GNU Network Object Model Environment. A GUI that runs on top of the Linux operating system, GNOME consists solely of free and open-source software. Its emphasis is on simplicity and accessibility and endeavoring to use a low amount of resources. Need more customization? Try the KDE GUI, or K Desktop Environment, which provides a plethora of customization options. Need a more lightweight GUI to run on older computers? Try Xfce, which provides an incredibly low RAM footprint. Basically, because of the open-source nature of Linux, a myriad of GUIs is available!

A number of programs available for Linux are fairly equivalent to Microsoft applications. For example, LibreOffice is a group of free software applications that can be used to create word processing documents, spreadsheets, slide shows, and so on. Files can be saved in LibreOffice with the same extensions used in Microsoft Office, and therefore they can be opened in either application.

The command-line functionality in most Linux distributions is in depth and well documented, allowing users to configure and troubleshoot just about anything from within the “shell,” or command line. To help you learn more about any commands, the operating system usually has built-in manual (or man) pages that are accessible online.

Linux Desktop Distributions

The most common types of Linux by far include Android (for mobile devices), Google Chrome OS, and various derivatives of Linux used by gaming consoles such as Valve’s Steam Deck that runs its own customized fork of Debian called SteamOS. However, this section concentrates on desktop computers and the types of Linux that can be loaded on them.

There are literally hundreds of Linux desktop distributions. As noted previously, most are used by PC enthusiasts and gamers, as well as by many programmers and engineers (and the number is growing). One popular distribution (or “distro”) is Ubuntu. Ubuntu is commonly used for a variety of purposes. Figure 40.1 shows Ubuntu Desktop (a client-side version of Linux).

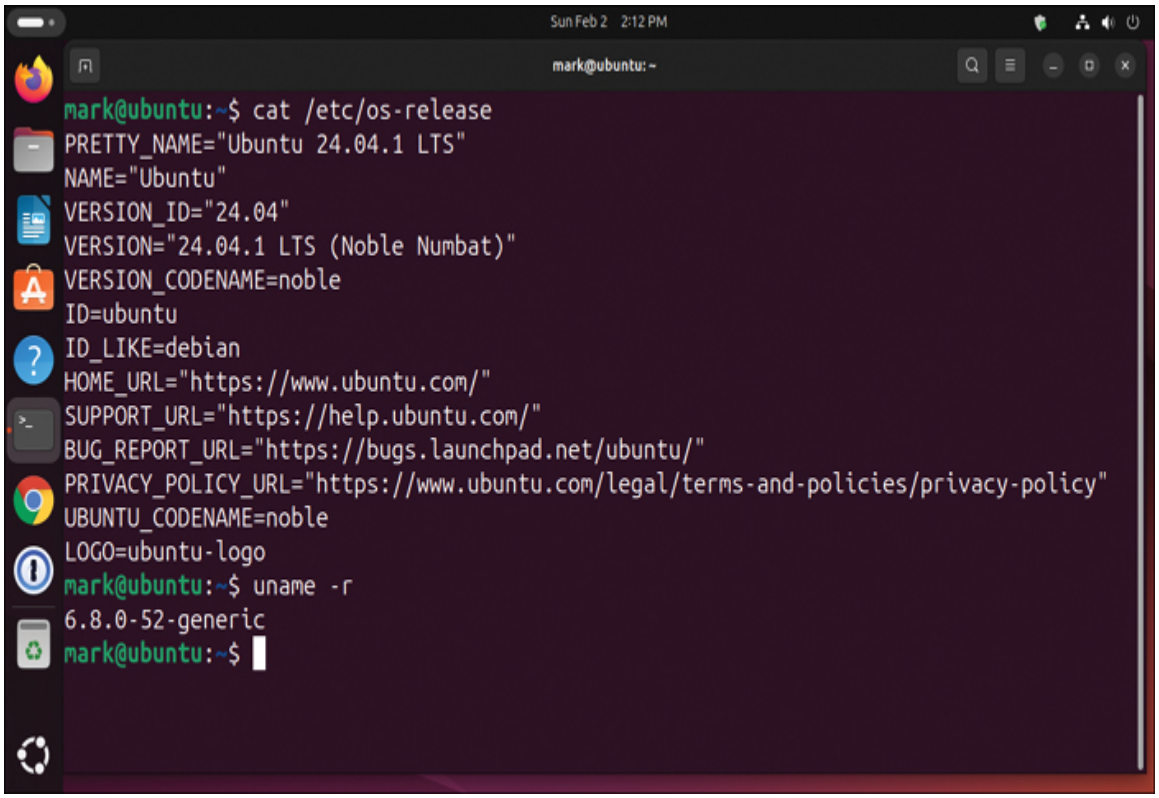


FIGURE 40.1 **Ubuntu Desktop**

In the figure, you can see a column of icons on the left; they allow a user to open programs such as the web browser (Firefox), mail, files, and more. The Terminal program is the command-line program included in most distributions of Linux.

In this Terminal window, you can see that we have run a couple of commands. The first one, **cat /etc/os-release**, results in the version number of Ubuntu that we are running (24.04.1 LTS). Notice that the first number, 24, indicates the year the OS was released, with the second number, 04, being the month it was released. LTS means long-term support. Ubuntu LTS releases are supported for 5 years with optional maintenance for Ubuntu Pro subscribers for 12 years! The second command, **uname -r**, indicates the Linux kernel version (6.8.0-52-generic). Commands such as these work on most distributions of Linux.

Note

For practice with Ubuntu, consider creating an Ubuntu bootable USB stick within Windows; see https://ubuntu.com/tutorials/create-a-usb-stick-on-windows#1-overview. An Ubuntu bootable USB stick enables you to boot Linux from the flash drive and practice Linux commands using the built-in Terminal application. You might also consider downloading the latest version of Ubuntu and installing it on a virtual machine. Or, if you are using Windows, consider using the Windows Subsystem for Linux (WSL); see https://learn.microsoft.com/en-us/windows/wsl/install. Ubuntu Desktop can be downloaded from https://www.ubuntu.com/download/desktop.

Linux Partition Scheme and File System

Linux uses the GUID Partition Table (GPT) to list and control the partitions on the systems. GPT supports UEFI, 128 partitions, and partition sizes

beyond 2 TB, and it is stored in multiple locations, making it superior to MBR technology. Linux most commonly uses the ext4 file system, which allows a user to resize partitions at will—if there is additional space available on the drive. However, some distributions, like Red Hat Enterprise Linux, now use the XFS file system by default. XFS offers improved performance for large files and is a great pick for servers.

Note

High-Performance Scalable File System (XFS) is a high-performance journaling Linux file system designed for storing and retrieving very large media files and databases.

ExamAlert

For the exam, remember that most Linux systems use the ext4 system and GPT by default.

Linux Command Line

For the typical Linux user, the command line is not a necessity. Today's Linux desktop interfaces (such as GNOME) offer most of the configuration settings that a standard user needs. However, for power users, sysadmins, and typical geeks, it's all about the command line. Use it.

The command line in Linux is normally referred to as *Terminal*, and you access it by using the search tool or by opening the list of applications. You can access the search tool by pressing the Superuser key (which is the Windows key on most keyboards). Then just type **terminal**. Or press Superuser+A (in the GNOME environment) to see the list of applications and select **Terminal** from there. In Ubuntu (and some other distributions), you can press Ctrl+Alt+T to open Terminal.

When you open Terminal, Linux places you in a *shell*, which is a command processor that runs within a command-line tool (usually Terminal). One of

the most commonly used shells is the Bash shell, or Bourne Again SHell, which offers improvements over the original Bourne shell. (Yes, open-source people have quite the sense of humor.) From a shell, you can enter commands and execute scripts. Everything we discuss in this chapter is based on the Bash shell.

> **Note**
>
> If you work on a proper Linux server, it is command line only, and there is no desktop. Be ready!

There are hundreds of Linux commands. The CompTIA A+ exam only requires you to know a couple dozen of them. Table 40.1 describes the commands you should know for the exam as well as some commands that are useful in real-world Linux administration.

TABLE 40.1 **List of Linux-Based Commands Based on Function**

File Management	
Command	**Description**
ls	Lists directory contents. Similar to **dir** in Windows.
pwd	Displays the full path/filename of the working directory. Don't confuse this command with **passwd**!
mv	Moves (or renames) files. Similar to the Windows **move** command.
cp	Copies files and directories. Similar to the Windows **copy** command.
rm	Removes files or directories. Similar to the Windows **del** and **rd** commands.
chmod	Modifies the read and write permissions for a file or directory.
chown	Changes ownership for files and directories.

File Management	
Command	**Description**
find	Searches for files (or directories) in a directory hierarchy.
grep	Searches for matching information in specified files and displays that information. The general syntax of this filtering command is **grep [*options*] *pattern* [*file…*]**. For example, to locate any lines that include the word *root* in the passwd file, you could type the **grep root /etc/passwd** command. That command normally displays one line item: `root:x:0:0:root:/root:/bin/bash` Various options can also be used, including **-i:** Makes the search case insensitive **-d:** Can specify how to handle directories **-w:** Finds exact matches of whole words **-c:** Counts the number of matches found in a particular pattern **-n:** Searches for line number matches Type **grep --help** or **man grep** for more information about **grep** options. You also can use **grep** to filter the results of another command. For example, **ip a | grep inet** shows all IP addresses associated with all network interfaces on the system.
Filesystem Management	
fsck	Scans and repairs inconsistencies within a file system. Note: You cannot run this filesystem check command on active disks and partitions. You will need to boot into recovery mode to do this. See the section "Recovery Mode" later in this chapter. See https://www.geeksforgeeks.org/how-to-fix-fsck-errors-in-ubuntu/ for information on how to use **fsck**.

File Management	
Command	**Description**
mount	Enables partitions, USB drives, network shares, and other storage devices to be “mounted” to a specific directory in your main file system tree. While most modern Linux distributions auto-mount USB drives, other storage devices won’t necessarily. For example, say you have a shared folder on another Linux machine in your office. You can mount that shared folder locally so that it acts as just another folder on your system. To do so, you would use **sudo mount -t nfs 192.168.1.50:home/user/documents /mnt/work_docs**. In the preceding example, **sudo** runs the command with administrator rights, **mount** indicates that you want to mount it to your system, the **-t nfs** argument states it is an NFS network share, **192.168.1.50** is the location of the other machine with **:/user/documents** being the remote location, and **/mnt/work_docs** is the local folder that you want to associate it to. An important note is that this will only mount the storage device temporarily; if you reboot, you’ll have to run the command again. You’ll need to make an entry in /etc/fstab. See https://www.geeksforgeeks.org/how-to-mount-and-unmount-drives-on-linux for more information on mounting and the /etc/fstab configuration.
Administrative	

File Management	
Command	**Description**
su	Switches to another user account. **su** stands for substitute user. For example, if you are logged in as the user Tyrell, and you want to switch to Maria's account, you would type **su Maria**. Note that you must know Maria's password in this example! If you don't specify a username after **su**, it will switch to the root user. Again, you need to know root's password. This generally is not advised. If you need to perform administrative tasks, rather than switching to root, it is advised to use the **sudo** command. You will see some documentation using **su** and **su -**. The hyphen option changes the behavior of **su**. One major difference is that **su** without the hyphen will switch the user but keep you in the same working directory, whereas **su -** will change the working directory to the target user's home directory. See https://www.geeksforgeeks.org/switch-users-on-linux-with-the-su-command/ for more information.

File Management	
Command	**Description**
sudo	Elevates privileges to administrator level for one command. **sudo** means Superuser do. By default, a user does not have administrator rights; however, the user could belong to the sudoers group, which allows the user to elevate their permissions to administrator for the entered command. For example, if you try to type the command **cat /etc/sudoers** to view that particular file, you get a permission denied error. You don't have permissions to view this system file. However, if you belong to the group associated to the **sudo** command, often the wheel group, you could type **sudo cat /etc/sudoers**, input your password, and see the output. Remember: With great power comes great responsibility! If you edit that file, you are editing as an administrator. This is the preferred way of carrying out administrative tasks rather than switching to the root user. See https://www.redhat.com/en/blog/sudo for even more information.
Package Management	
apt	Installs, updates, removes, and manages software packages on Debian and its derivatives like Ubuntu and Linux Mint. See the "Updates and Patches" section later in this chapter for more information.
dnf	Installs, updates, removes, and manages software packages on Red Hat–based operating systems such as Fedora, CentOS Stream, and RHEL. See the "Updates and Patches" section in this chapter for more information.
Network	

File Management	
Command	**Description**
ip	Works on a group of commands, including **ip address**, **ip link**, and **ip route**. For example, typing the **ip address** command (**ip a** for short) shows the TCP/IP properties of all network connections. An example of this is shown after this table.
dig	Finds information about DNS. For example, **dig example.com** provides information on the IP address that comptia.org resolves to.
ping	Tests whether a device is reachable on a network by sending data packets to a specific host and measuring its response time. For example, **ping -c 4 example.com** sends four ICMP packets, marked by the **-c 4** option, to the IP address that example.com resolves to and measures the time it takes to send the echo request and receive the echo reply back in milliseconds. This is a great network diagnostic tool.
curl	Enables you to request and transfer data over a URL using various protocols such as HTTP, HTTPS, and FTP. One common use of this command is fetch data from a URL. Try it! Type **curl example.com** in your Terminal. It fetches the actual HTML code of the website. See https://www.geeksforgeeks.org/curl-command-in-linux-with-examples/ for more great uses of this command.

File Management	
Command	**Description**
traceroute	Traces a route taken by packets from a source to a destination. The output of this network diagnostic tool will show “hops” as the data packet goes through various routers to reach its destination. By default, it will only measure 30 hops, which is usually more than sufficient to reach virtually anywhere in the world. However, you can increase the number of hops if needed. Try it! In a terminal, type **traceroute example.com**. Don’t be too concerned if you see asterisks (*) along the way. They could represent an issue with the network path, such as a network time-out, but they could be a firewall setting to not allow a response from that particular router. This command is the Linux equivalent of the Windows **tracert** command. If your Linux states that the command is not found with **traceroute**, it will usually tell you what package to install to get the command working. See https://www.geeksforgeeks.org/traceroute-command-in-linux-with-examples/ for more great options with the **traceroute** command.
Informational	
df	Reports file system disk space usage. The command **df -T** includes the file system used by each partition. The command **df -h** displays the system disk usage in human-readable form.
cat	Displays the contents of text files (and configuration files) within Terminal.

File Management	
Command	**Description**
du	Displays disk usage information. You can run this command against the whole filesystem, or more likely, against specific directories. For example, type the command **du /home/*user*/Documents** and replace *user* with your username. This will give you a breakdown of the size of files in your Documents. Even better, type **du -h /home/*user*/Documents** to see the information in **-h**, or human-readable form. See this article for even more goodness: https://www.redhat.com/en/blog/du-command-options.
ps	Displays information about a process or lists running processes. For example, **ps -aux | grep firefox** lists all processes concerning the Firefox web browser that are running. You can use the **kill** command to terminate unwanted processes that are discovered with the **ps** command.
top	Displays the running Linux processes and the CPU and RAM usage for each. This is an analysis program.
man	Opens the manual page for any command. For example, **man dig** opens the manual page for the **dig** command. Manual pages give *lots* of information about the command in question. To exit the manual page, press **q** (for quit). A slimmed-down help file is also available for most commands. For example, type **dig --help** for basic information about the **dig** command. The help information is displayed directly in Terminal. This is one of the most beneficial commands to learn! Almost all Linux commands have a manual page that is packed with information. Try using **man** with all the commands you have learned so far.
Text Editors	

File Management	
Command	**Description**
nano	A text editor that can be run from Terminal. It is included in most versions of Linux.
vi	A visual text editor included by default on most Linux operating systems. It is a character-based screen editor without a GUI. We'll discuss vi (and VIM) in Chapter 62, "Basic Scripting, Part I," and Chapter 63, "Basic Scripting, Part II."

Know that when working in the Linux directory structure, you always use a slash (/) to separate directory levels. (In Windows, you use a backslash [\].) So, you might have a path such as **/Downloads/pdfs**. If there is ever any confusion as to which is the slash and which is the backslash on the keyboard, remember that the backslash (\) is the one near the backspace key (on US keyboards). Use the slash (/) for Linux, which usually shares the key with the question mark.

Note

Unlike Windows, in Terminal, capitalization matters. For example, in Windows, a file named *hello.txt* is the same as *Hello.txt*. This is not true in Linux! They would be two different files. In addition, you need to watch for case in arguments when using commands. For example, the command **ls -r** would show a list of directory contents but in reverse alphabetical order, whereas **ls -R** would show a list of the directory contents and then list subdirectories recursively. Another cool feature is the use of multiple arguments. For example, **ls -l** gives a long listing format, but you can also type **ls -lr** to give a long listing in reverse order! So many fun combinations to try!

Note

A word on text editors in Linux: Once you have opened Terminal, you can open the text editor where you will build your scripts. There

are two main options in Linux: nano and Vim.

nano is built into most Linux distributions and is the easier tool to use for those new to text-based editors. It is quite similar to Notepad in Windows (but is keyboard only by default). For example, to create and edit a file with nano, you could type **nano testscript.sh**. This command opens the nano program, and you are ready to start typing into your file. You will note several keyboard shortcuts at the bottom of the screen. To save a file and exit nano, you press Ctrl+X on the keyboard and then press y to save the changes to the file. If you want to modify the file later, you could simply repeat the entire process. As you can see, nano is easy to use. However, many technicians prefer Vim because it is heavily customizable and can provide for excellent workflow. However, it is more cryptic in its usage if you are not used to it. Vim can also do many more actions, like selecting columns and rows, that nano can't do. Do note that most Linux distributions come with vi, which is a less-powerful version of Vim but can still do most of what you want. Of course, you can easily install the full-fledged Vim!

Other useful Linux commands:

You will not see the following Linux commands on the exam, but they are good to know: **cd**, **passwd**, **shutdown**, and **poweroff**.

cd changes the directory, similar to the Windows **cd** command. Try typing **cd /etc** and look at the contents of the /etc directory.

passwd is used to update a user's password. When no user is added after the command, it will change the current user's password. However, you can type **sudo passwd user** to change someone else's password. This powerful command also lets you lock accounts, expire passwords, and more. See https://www.redhat.com/en/blog/managing-users-passwd for more examples.

shutdown/poweroff brings the system down but can be modified in a variety of ways to gracefully shut down the system, notify users, and perform many more options. To restart the system, type **reboot**.

Challenge: Use Linux Tools

Want to look like a pro? Try to access Terminal in Linux and practice the commands listed in Table 40.1. Remember that the only way to really get to know these commands is to run them in a working Linux environment. Good luck!

Now let's look at how to use a few commands. The following example includes two **ip** commands and the **su** command. Take a close look at the results:

```
sysadmin@ubuntu:/etc$ ip a
2: enp1s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_cod
state UP group default qlen 1000
    link/ether 52:54:00:f6:4c:1e brd ff:ff:ff:ff:ff:ff
    inet 10.42.0.53/16 brd 10.42.255.255 scope global enp1s0
       valid_lft forever preferred_lft forever
    inet6 fe80::5054:ff:fef6:4c1e/64 scope link
       valid_lft forever preferred_lft forever
sysadmin@ubuntu:/etc$ ip r
default via 10.42.0.1 dev enp1s0 proto static
10.42.0.0/16 dev enp1s0 proto kernel scope link src 10.42.0.53
192.168.122.0/24 dev virbr0 proto kernel scope link src
192.168.122.1 linkdown
sysadmin@ubuntu:/etc$ su - user
Password:
user@ubuntu:~$
```

In the first line, you can see that we are using a user account called *sysadmin*. You can also see that the name of the Linux system is *ubuntu*. In addition, we are currently located in the /etc directory. Finally, the first command issued is **ip a** (short for **ip address**). Normally, you would see

more information if you ran this command, but we truncated the results and are only displaying the main Ethernet network interface here. Among other things, it shows you the name of the network interface *enp1s0*, and the IP address (10.42.0.53/16). Another command you can run to find this information on this system—and many others—is the **nmcli** command. This command is not on the A+ exam objectives (yet), but it is very commonly used.

The second command is the **ip r** command (short for **ip route**). This command displays the default gateway (10.42.0.1) and any network routes available to the network interfaces.

The third command is **su - user**. Remember that the **su** command allows you to log in as someone else; in this case, it is used for the user account, but you can use it this way only if you know the password for the account! We know the password and typed it (although you can't see it, of course), and the system logged us in as *user@ubuntu*. Awesome!

When you are finished working in another account, you can end the login session by simply typing **exit** (or pressing Ctrl+D). In the preceding example, that would return us to the sysadmin login (which was always running).

The default administrative account in most versions of Linux is *root*. You can access this account by typing the **su** command. Linux will ask for the root password, and if you can supply it, you'll have full access to the system. But it's always a good idea to create a separate working administrative account and keep the root account as a backup; you should also make sure that both accounts have lengthy, complex passwords. However, know this: If you want to take administrative action when logged in as any account (other than root), you need two things: The account has to be added as an administrator of the system, *and* you have to prepend every administrative command with the **sudo** command.

For example, say you are logged in as sysadmin, and you want to change the password for the mark account. You would type **sudo passwd mark**. The **sudo** command gives sysadmin the ability to run administrative commands. The **passwd** command is used to change the password of the

currently logged-in account or other accounts. And **mark** is the account for which the password will be changed.

ExamAlert

Know your Linux file management, filesystem management, administrative, package management, and informational commands! Practice them on a distribution such as Ubuntu or Fedora.

This command-line information is accessible and available in most versions of Linux. Remember that you can learn more about most of these commands by accessing the help files or the manual pages. The manual pages are also available in several locations on the Internet.

Note

People often say that macOS is based on UNIX and related to Linux. This is true and not true. It is actually based on BSD, or Berkeley Software Distribution, which was an open-source, written mostly from scratch, copy of UNIX. UNIX was copyrighted by AT&T, so computer scientists at the University of California, Berkeley, wrote BSD to provide a free alternative while still maintaining the robustness of UNIX. The history is a little more complex than this, but this is the crux of it.

The Linux kernel, the heart of the operating system, was written by Linus Torvalds in 1991. He also modeled his operating system on UNIX-like ideals. This is why you will hear people state that macOS and Linux are related. They're not, but they're both made on UNIX-like operating systems. It is the reason that many of the same commands work in Linux, macOS, and FreeBSD.

Recovery Mode

Booting into recovery mode in Linux can be helpful for troubleshooting issues, repairing your system, or resetting passwords.

Here's a general guide, but keep in mind that the exact steps might vary slightly depending on your specific Linux distribution:

Step 1. Accessing the GRUB Menu

a. Restart your computer or virtual machine.

b. As it starts up, you'll need to interrupt the normal boot process to access the GRUB menu. This is usually done by pressing and holding or repeatedly tapping a specific key. Common keys include

- **Shift:** Often used for BIOS/MBR systems
- **Esc:** Often used for UEFI systems
- **F8:** Less common but sometimes used
- **Del:** Also less common but possible

c. If you see your Linux distribution's logo, you've likely missed the window to enter the GRUB menu. You'll need to restart and try again.

Step 2. Navigating the GRUB Menu

a. Once you're in the GRUB menu, you should see a list of boot options. This might include different kernel versions or even other operating systems if you have them installed.

b. Use the arrow keys to navigate the menu—no mouse here!

c. Look for an option that says **Advanced options for [Your Distribution Name]** (e.g., Advanced options for Ubuntu). Select it and press Enter.

Step 3. Choosing Recovery Mode

a. You'll now see a list of available kernel versions with recovery mode options.

b. Select the recovery mode option for the kernel you want to use. It will usually be labeled something like **[Kernel Version] (recovery mode)**.

c. Press Enter to boot into recovery mode.

Step 4. Using Recovery Mode

a. Once you're in recovery mode, you'll typically see a menu with various options. These options can include

- **fsck:** To check and repair file system errors
- **dpkg:** To fix broken packages
- **grub:** To reinstall or repair the bootloader
- **network:** To enable networking
- **root:** To drop to a root shell prompt

b. Use the arrow keys to navigate the menu and press Enter to select an option.

Note

Timing is crucial. You need to press the key to enter the GRUB menu at the right time during the boot process. You might need a few tries to get it right. Having Fast Boot enabled in your BIOS/UEFI settings might make it harder to access the GRUB menu. You might need to disable Fast Boot temporarily. Some Linux distributions might have slightly different methods for accessing recovery mode. Check your distribution's documentation if you have trouble.

Common Configuration Files

Unlike Windows, which stores configuration files for programs all over the place such as the Registry or AppData, Linux generally stores its configuration files in the /etc directory. This makes it extremely easy to find

the configuration files and edit them to suit your needs. Here is a list of common configuration files you should know about:

- **/etc/passwd:** Stores basic user account information, including usernames, user IDs (UIDs), group IDs (GIDs), home directories, and login shells. Previously, it stored passwords but now usually only holds a placeholder designated as an *x*.
- **/etc/shadow:** Stores the actual encrypted user passwords (usually it's actually password hashes). It has restricted permissions to protect this sensitive data.
- **/etc/hosts:** Maps hostnames to IP addresses. It's used for local name resolution, allowing you to refer to computers on your local network by name rather than IP address. Super handy!
- **/etc/fstab:** Contains information about file systems to be mounted at boot time. It specifies the device, mount point, file system type, and mount options for each file system. Remember: If you used the **mount** command, you have to add it to this configuration file if you want it to mount on a reboot!
- **/etc/resolv.conf:** Configures the system's Domain Name System (DNS) settings. It lists the IP addresses of DNS servers to use for resolving hostnames to IP addresses.

ExamAlert

Know these common configuration files in Linux and what they do.

Linux Best Practices

It's important to make sure that a Linux system is updated and secured, just like any other system. Let's discuss those concepts and some best practices that you can implement on Linux.

Updates and Patches

If a system isn't up to date, it's vulnerable to attack. It's been documented that more than 50 percent of successful attacks on Linux servers were caused by the fact that the Linux system wasn't up to date. Translation: Update your operating system!

So, how do you update Linux? The answer depends on the distribution and whether you have a desktop environment. Let's discuss the latter first.

If you have a desktop environment, such as GNOME, you usually go to the applications list and then **Software**—or a similar name, such as Software & Updates, or the Software Updater; which one you use depends on the distribution that you are using. With these programs, you can install updates for the operating system and for other software. In addition, many Linux distros tell you when updates have become available to the system and provide painless procedures to perform updates.

In addition, to work at the command line, there are a few commands you can use for updating, as shown in Table 40.2.

TABLE 40.2 **Linux Updating in the Command Line***

OS Distribution	Command	Description
Debian/Ubuntu	**apt update**	Finds out if there are any updates available for the system
	apt upgrade	Actually downloads and installs the updates
	apt install <*program*>	Installs (or upgrades) one or more applications
Fedora/RHEL	**dnf update**	Looks for updates, and if agreed to, downloads and installs them
	dnf install <*program*>	Installs (or upgrades) one or more applications

* Table 40.2 is not explicitly tested on the A+ exam; however, it is important to know these commands nonetheless. Updating a system is critical for security and performance.

Keep in mind that you *can* also use the older **apt-get** command for Debian and Ubuntu and the older **yum** command for Fedora, RHEL, and RHEL clones—and in some scenarios you may *need* to, so know both. However, **apt** and **dnf** are considered the modern replacements of **apt-get** for Debian-based operating systems and **yum** for RHEL-based operating systems. In case you were wondering, RHEL (pronounced *rell*) stands for Red Hat Enterprise Linux.

For example, let's say you want to update everything on an Ubuntu system all at once on a single command line. Using the root account, you could use something like this:

```
apt update && apt upgrade -y
```

The double ampersand allows you to string two or more commands together to be run in succession. In this case, the Ubuntu system would look for updates and then install any that are available. The **-y** means you are saying "yes" to the upgrade (because normally Linux asks you for permission before installing). However, this command is not quite secure—especially for servers. You should always check what is upgradable first before blindly running full upgrades. You can do so with this command:

```
apt list --upgradeable
```

When you use this command, you might find that you only want (or need) to patch one or more files. Perhaps the Firefox browser needs to be patched, but you don't want to do any other upgrades. You could do this with a command similar to the following:

```
apt install firefox-esr.<version_number>
```

This command will install the latest version of Firefox for Linux.

As a best practice, at the very least, make sure that all *operating system* updates are installed and check them often (or have an automated system check for you). Operating system updates include security updates, and that's what you really want. But you should also be concerned with applications, especially web browsers, because they are primary targets for attackers as well.

As mentioned, you might install updates individually. Generally, however, Linux systems such as Ubuntu, Debian, and Fedora are very careful about what updates are released; updates are tested thoroughly. So, chances are that if you run full updates of all software, the system will be more secure and will most likely behave as it should.

OS Components

The Linux boot process is the initial stage of the operating system's startup. This is the process by which the operating system loads the memory and initializes components and then prepares to execute user apps.

The Linux boot process has four main steps:

Stage 1. **BIOS.** When you power on your computer, your computer starts the Basic Input/Output System (BIOS) and performs a power-on self-test (POST). This check probes the hardware functionality of hardware components such as hard disk drives (HDDs) and solid-state drives (SSDs), keyboard, RAM, USB ports, and other hardware. If the hardware works as expected, the boot process moves on to the bootloader stage.

Stage 2. **The bootloader.** Once POST is complete, the BIOS searches for and loads the bootloader program stored in the Master Boot Record (MBR). The MBR is a 512-byte code that is usually located at /dev/sda or /dev/hda, depending on your hard drive architecture. The MBR can also be located on a live USB or DVD installation of Linux. The BIOS loads and executes this MBR code.

There are three main boot loaders in Linux: LILO, GRUB, and GRUB2. The GRUB2 (Grand Unified Bootloader) boot loader is the latest and primary boot loader in modern Linux distributions. The GRUB2 configuration file is located at /boot/grub2/grub2.cfg. Once the BIOS locates the GRUB2 boot loader, it executes and loads it into the main memory (RAM).

Stage 3. **Linux kernel initialization.** The Linux kernel is the heart of the operating system. In your Linux system, the kernel interfaces with

the hardware, controls memory management, and manages processes. The boot loader loads the selected Linux kernel. The kernel self-extracts from a compressed version and mounts the root file system. It then runs the /sbin/init program.

Stage 4. **system.** The kernel loads systemd, which is a system and service manager for Linux operating systems. System then runs all the other initialization processes. It is the first process the kernel launches because it is responsible for launching and managing all the other services. This includes the networking daemons, display managers, and background processes to make the system run well.

Three is the magic number here. It takes the bootloader, kernel, and systemd to make the magic happen!

To learn more about bootloader, kernel, and systemd, visit https://documentation.suse.com/en-us/sle-micro/6.0/html/Micro-systemd-basics/index.html.

Note

If you plan on dual-booting Windows and Linux, which is a great idea if you want the best of both worlds, you should always install Windows first and then Linux. The reason is the bootloader. If you install Linux first and then Windows, Windows will place its own bootloader in the MBR/EFI partition and overwrite Linux's bootloader with its own. Windows doesn't like to play nice and will ignore the Linux OS on the drive. However, Linux plays nice. If you install Windows first and then Linux, the GRUB bootloader will see Windows exists on the drive and make an entry for it. Consequently, if you boot in this order, you will get a boot entry for both Linux and Windows when you boot.

ExamAlert

Know the Linux OS components including the bootloader, kernel, and system. Understand how they interact in the launching of Linux.

Root Account

The root account in Linux is a special user account that wields absolute power over the entire system. It's a superuser account that grants unrestricted access to all files, directories, and commands. A root account is automatically created when you install Linux. It is similar to a Windows Administrator account. However, unlike Windows, which defaults the primary user to an Administrator account, Linux also has you set up a standard user when installing. This step is critical because the user account you use everyday should not have administrator privileges. That's a recipe for disaster! Not to mention a serious security concern.

Running as root is such a security concern because the account can do anything. Think of a hacker gaining root access to your system, which they try to do all the time. Therefore, it is best not to use root unless absolutely needed. Instead, it is always best to use the **sudo** command as described in this chapter.

ExamAlert

Know what the root account is and what the **sudo** command does.

Linux Permissions

While the A+ exam does not explicitly cover Linux permissions, it is good for you to have a basic idea about them. Linux uses file permissions to control access to files and directories. Every file has three sets of permissions: read (r), write (w), and execute (x), assigned to the owner, group, and others. These permissions dictate who can view, modify, or run a file. You can view these permissions by using the **ls -l** command, which displays a string like -rwxr-xr-x, where each set of rwx corresponds to the owner, group, and others, respectively. The first dash in **-**rwxr-xr-x means that this is a regular file. If it had a *d* there, it would mean that it's a directory.

To modify permissions, you use the **chmod** command. You can use numeric notation (such as **chmod 755** ***myfile*** to give the owner full access and the group and others read and execute permissions) or symbolic notation (such as **chmod g+w** ***myfile*** to add write permission for the group). Remember that **chmod** requires elevated permissions, so you might need to use **sudo chmod**.

For more information, you can read about Linux file permissions at https://www.redhat.com/en/blog/linux-file-permissions-explained.

Note

Interested in Linux? You might want to pursue the CompTIA Linux+ certification. It would be a great cert after you get that A+. Learn more at https://www.comptia.org/certifications/linux.

In Closing

It's important to keep in mind that Linux changes fast. The core concepts of Linux remain the same (for the most part), but new Linux kernels, security releases, and updates to Linux distributions are constantly emerging. In essence, if you want to work with Linux, be ready to learn!

Finally, one of the great things about Linux is that many of the distributions are incredibly well documented on the Internet—by very talented people. Support pages, wikis, and forums are available for most distros. Use these resources! Chances are the error you are encountering has been seen before, described online, and *solved*.

Cram Quiz

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

1. Which command in Linux shows the contents of a directory?

- **A. ls**
- **B. pwd**
- **C. cd**
- **D. mv**

2. Which command should be used to change the permissions of a file?

- **A. ps**
- **B. chown**
- **C. NTFS**
- **D. chmod**

3. You are working as a junior administrator at a midsized company. You are tasked with updating Linux system software. Which command should be used to gain the necessary permissions to update the software?

- **A. grep**
- **B. sudo**
- **C. chmod**
- **D. pwd**

4. One of your customers is trying to install a 3 TB storage drive to a Linux system. The customer wishes to use half of the drive capacity for one partition now and wants to have the option to increase the partition size later. Which file system should you recommend?

- **A.** NTFS
- **B.** FAT32
- **C.** ext4
- **D.** APFS

5. You are troubleshooting a network connectivity problem on a Linux computer. Which of the following commands will display information about the network interface?

- **A. ip a**
- **B. grep -i**
- **C. sudo**
- **D. netsh**

6. One of your customers tells you that an application in Linux will not open and gives this error:

   Only one instance of the program can be run at any time.

   You log in to the system as root and open Terminal. Which of the following commands should you run to ensure that no other instances of the program are open?

- **A. cp** and **rm**
- **B. ls** and **chown**
- **C. ps** and **kill**
- **D. pwd** and **chmod**
- **E. sudo** and **nano**

7. An administrator logs in to a Linux computer and runs the following command:

```
ps -aux | grep firefox
```

   Of the following, which best describes the functionality of this command?

- **A.** It locates and lists the processes used to run the Firefox web browser.
- **B.** It kills any running programs that start with the word *firefox*.
- **C.** It opens directories that start with the word *firefox*.

- **D.** It creates a new tab for filtering in Firefox.

8. Which command can be used to download updates and patches on a Linux workstation?

- **A. apt**
- **B. nano**
- **C. vi**
- **D. fsck**

9. Which special user account wields absolute power over the entire system and is automatically created when you install Linux?

- **A.** Superuser
- **B.** Administrator
- **C.** Standard user
- **D.** root

10. Which Linux configuration file has restricted permissions and stores the actual encrypted user passwords?

- **A.** /etc/passwd
- **B.** /etc/hosts
- **C.** /etc/resolv.conf
- **D.** /etc/shadow

11. Which of the following does the Linux kernel load that is considered a system and service manager for Linux operating systems and runs all the other initialization processes?

- **A.** The bootloader
- **B.** systemd
- **C. man**
- **D. top**

Cram Quiz Answers

1. **A. ls** will list the directory contents in Linux and macOS. It is similar to the **dir** command in Windows (which can also be used in Linux). **pwd** is used to display the full path of the working directory (for example, /home/root). **cd** is used to change directories; it is similar to the Windows command of the same name. **mv** is used to move files.

2. **D.** Use the **chmod** command to change permissions in Linux and macOS. **ps** displays information about a given process. **chown** changes ownership of a file. NTFS is the file system used by Windows that allows for file-level security assigned by a user or group.

3. **B.** Use the **sudo** command before other commands that require administrative permissions. For example, you might type

   ```
   sudo apt upgrade
   ```

   This will initiate an upgrade on a Debian-based system. Without the **sudo** command, it will not work for any user other than root. Don't forget, you can also use **apt-get** instead of **apt**. **grep** is used to search for matching information in specified files or to filter the results of a command being run. **chmod** is used to change permissions. **pwd** shows the current path that you are located in (**pwd** stands for print working directory).

4. **C.** Recommend ext4. It is the default on most Linux systems, and it has the ability to be resized at a later date. NTFS is a Windows file system, and it doesn't function well with Linux, though it does allow for dynamic resizing of disks in Windows. FAT32 can be used in Linux, and it works well for drives that need to be accessed by Linux *and* Windows systems, but it doesn't allow for resizing. APFS is the Apple File System, and it works only on macOS.

5. **A.** Use the **ip a** command (short for **ip address**) to find information about the network interface. **grep** is a search and filtering tool. If used with the **-i** option, it ignores case distinctions

(meaning uppercase and lowercase). **sudo** needs to be issued before any administrative commands. **netsh** (short for network shell) is actually a Windows command that you would run in PowerShell or the Command Prompt—tricky!

6. **C.** Use the **ps** command to see what processes are running and the **kill** command to terminate the processes as necessary. **cp** is used to copy files, and **rm** is used to remove them. **ls** lists the contents of a directory, and **chown** changes ownership of files and directories. **pwd** shows the current path, and **chmod** changes permissions on files and directories. **sudo** is used before administrative commands, and **nano** opens the built-in text editor.

7. **A.** The command will list the processes used by the Firefox web browser. To show this, you would need to have Firefox running when you type the command. You can break it down like this: The **ps** command reports a snapshot of the current running processes. It can be used with a variety of options. In this case, you use **-aux**, which will see every single process. The pipe symbol (|) is used to make a modification to the **ps** command. The **grep** command filters the results of the **ps** command, asking the system to display only results that include the word *firefox*. **ps -aux** is commonly used but is a somewhat older option. A simpler way to display process IDs for a particular program would be to use the **-e** option. For more information, visit the manual page for **ps**. As for the incorrect answers: to "kill," or terminate, programs or processes, you need the **kill** command. To open, or access, a directory, use the **cd** command. Creating new tabs in Firefox is best done in the browser itself!

   This question went a bit above and beyond what you need to know for the A+ certification, but you might see a question like this! Even if you don't need to know this for the exam, it's good knowledge for the IT field.

8. **A.** The **apt** command can be used to download and apply updates and patches to a Linux system. **nano** and **vi** are text editors that can be run from Terminal in Linux. **fsck** scans and repairs inconsistencies within a file system.

9. **D.** The root account in Linux is a special user account that wields absolute power over the entire system. It's a superuser account that grants unrestricted access to all files, directories, and commands. A root account is automatically created when you install Linux. It is similar to a Windows Administrator account. However, unlike Windows, which defaults the primary user to an Administrator account, Linux also has you set up a standard user when installing.

10. **D.** /etc/shadow stores the actual encrypted user passwords (usually it's actually password hashes). It has restricted permissions to protect sensitive data. /etc/passwd stores basic user account information, including usernames, user IDs (UIDs), group IDs (GIDs), home directories, and login shells. Previously, it stored passwords but now usually only holds a placeholder designated as an *x*. /etc/hosts maps hostnames to IP addresses. It's used for local name resolution, allowing you to refer to computers on your local network by name rather than IP address. /etc/resolv.conf configures the system's Domain Name System (DNS) settings. It lists the IP addresses of DNS servers to use for resolving hostnames to IP addresses. Know the common Linux configuration files for the exam!

11. **B.** After kernel initialization completes, the kernel loads systemd, which is a system and service manager for Linux operating systems. systemd then runs all the other initialization processes. The bootloader in Linux is often called GRUB (or Grand Unified Bootloader) and is the first software that loads after the BIOS/UEFI boots and clears POST. Once the BIOS of your computer starts and checks the major components are working, it looks for a bootloader in the Master Boot Record (MBR) or EFI system partition. The **man** command opens the manual page for any command. For example, **man dig** opens the manual page for the **dig** command. Manual pages give lots of information about the command in question. **top** is an analysis program that displays the running Linux processes and the CPU and RAM usage for each.

Phew, that ends this chapter. Excellent work! You will see questions about Linux on the A+ exams, so review this chapter *carefully*. Linux is an amazing operating system that powers most of the Internet. If you really want to learn Linux, run it! It's free after all.

"That's what makes Linux so good: you put in something, and that effort multiplies. It's a positive feedback cycle." —Linus Torvalds, creator of the Linux kernel

Chapter 41

Application Installation and Configuration Concepts

This chapter covers the following A+ 220-1202 exam objective:

- **1.10** – Given a scenario, install applications according to requirements.

Let's briefly cover some application installation and configuration concepts and a couple of best practices. This is a shorter chapter, but it is important for the exam and for the IT field. There are a lot of numbers and specifications in this chapter, so it might be a bit more of a difficult read. Take your time, and it will all be fine.

ExamAlert

Objective 1.10 focuses on system requirements for applications, OS requirements for applications, distribution methods, and impact considerations for new applications.

32-Bit vs. 64-Bit

Let's start this chapter by discussing the difference between 32-bit and 64-bit. We touched on this topic from a hardware perspective in Chapter 17, "CPUs." Now let's review what we covered in that chapter and then dig a bit deeper into this concept from a software perspective.

Almost all of today's PC-based CPUs are 64-bit; this is a type of CPU architecture that incorporates registers that are 64 bits wide. These registers, or temporary storage areas, allow the CPU to work with and process 64-bit data types and provide support for address space in the terabytes. These 64-bit CPUs have been available for PCs since 2003.

A little history: The predecessor to the 64-bit CPU was the 32-bit CPU. Intel started developing well-known 32-bit CPUs as early as 1985 with the 386DX CPU (which ran at a whopping 33 MHz!), and AMD did likewise in 1991 with the Am386. A 32-bit CPU can't support nearly as much address space as a 64-bit CPU; 32-bit is limited to 4 GB.

In your work, you will hear the terms *x86* and *x64*. The term *x86* comes from the older CPU names that ended in 86—for example, the 80386 (shortened to just 386), 486, 586, and so on. Generally, when people use the term *x36*, they are referring to the 32-bit versions of software, including operating systems and applications. The 32-bit CPUs can handle up to 4 GB of RAM (though there are some cheats that allow it to work with a bit more in practice).

Newer CPUs are referred to as *x64* (or x86-64). This is a superset of the x86 architecture, with a wider data path to handle program execution. It can run 64-bit software as well as 32-bit software and can address a default maximum of 256 TB of RAM (the real limit is higher—2^6 is a big number—but the operating system and physical limitations of the motherboards get in the way). For instance, Windows 11 Home can access only 128 GB of RAM, whereas other versions of Windows 11 can access *only* 2 TB (Pro for Workstations can access up to 6 TB). *Only* is a relative term here; we remember when 48k was a lot! Many motherboards can handle only up to 64 GB of RAM, which is less than Windows can handle, so that puts physical limits on what is available to the user.

Note

Be aware that 64-bit systems can run 32-bit software. However, if a 64-bit version of the software is available, you should always use that version. You will get better performance, stability, and memory management. The 32-bit systems can*not* run 64-bit software.

ExamAlert

Know the differences between 32-bit and 64-bit architectures. For example, remember that 32-bit CPUs can only address a maximum of 4 GB of RAM, and 64-bit CPUs can address many terabytes of RAM.

Prior to Windows 10 version 2004, Windows came in 64-bit (x64) and 32-bit (x86) versions so that users from both generations of computers could run software efficiently. But since Windows 10 version 2004, Microsoft has abandoned new 32-bit releases. However, 64-bit versions of Windows are backward compatible—meaning that they can run 32-bit Windows applications as well as 64-bit applications. The 64-bit system files and apps are stored in C:\Windows\System32, and the 32-bit system files and apps are stored in C:\Windows\SysWOW64.

Note

Yes, the pathnames are backward from what you would expect, but the reason for that is how Windows developed over time and how it progressed from a 32-bit system to a 64-bit system.

In addition, you will find that some applications are still written for the 32-bit platform. Therefore, there are also two locations for programs in Windows: 64-bit programs are stored in C:\Program Files, and 32-bit programs are stored in C:\Program Files (x86). This location makes sense because x86 means 32-bit. But keep in mind that it is preferable to use 64-bit applications if at all possible. As a result, you will spend more time in the 64-bit areas of Windows, including C:\Program Files and C:\Windows\System32.

ExamAlert

Know the locations for 64-bit and 32-bit system files and program files in Windows.

System and OS Requirements for Applications

You might find yourself involved with designing a system, or systems, to use a certain type of program, such as virtualization, programming, graphic design, CAD, A/V editing, gaming, and so on. If so, it is important to carefully analyze the main program that will be used and plan carefully for its installation and configuration, making sure that it will run properly within your hardware configuration and the operating system that is running. As with most other things in technology, planning is vital.

First, you have to plan the system and OS requirements for the application. Some applications have versions for Windows and for Mac, but it's important to think about platform compatibility regarding the main application you want to use. Many applications have a set of minimum requirements and also have a set of *recommended* requirements. With any specific applications that will be resource intensive, we suggest you go with the recommended requirements (or more); otherwise, you could experience slow performance.

Let's consider a couple of scenarios. First, we'll look at a powerful video editing program and its requirements. Then we'll look at a commonly used developer program.

Scenario 1: Video Editing Program

A powerful video editing application might *require* a 64-bit version of Windows 10/11, 10 GB of storage drive space, a dedicated Windows-compatible audio device and speakers, a display resolution of at least 1920 × 1080, and an external USB drive (acting as a hardware token) that needs to be plugged into the computer for the application to work. But those are just the minimum requirements.

The application could *recommend* more, such as a fourth-generation quad-core CPU, 16 GB of RAM, and a discrete PCIe video card that can be used for hardware acceleration. The program might even require a video card with a specific amount of onboard video RAM (VRAM), such as 4 GB or more. Remember that a discrete (or dedicated) video card is one that connects to a PCI Express slot on the motherboard, whereas an integrated video card is *part* of the motherboard—and is usually far less powerful. These dedicated graphics cards are more powerful and provide substantially more performance; video editors (and gamers) rely on the enhanced performance when rendering video. For any

custom applications that rely on video, you'll probably want a dedicated card! So, the recommended requirements can become somewhat costly.

One last thought: Sometimes even the recommended requirements might not be quite enough, depending on the system and environment. Keep this in mind as you build systems.

Note

Some specialty software will require you to use a hardware token to reduce or eliminate privacy. Most often, these hardware tokens look like USB drives and must be plugged into your device while you're using the software. These hardware tokens are easily lost, so be careful! Other software has transitioned to using a software token, where you must go online and authenticate against the manufacturer's website with a username and password before being able to use the software. Many games use this method. Either way, without the token for authentication, you either cannot use the software, or the use is severely restricted.

Scenario 2: Developer Program

Compared to a video editing program, a typical integrated development environment (IDE) program might have far less stringent *requirements*, such as Windows 10/11 (any edition) and 500 MB of storage drive space. This means that it can run on just about anything! The *recommendations* might also be less than the ones in Scenario 1—for example, a 1.6 GHz processor and 1 GB of RAM (the actual recommended specifications for Visual Studio Code [VSC] as of January 2025; see https://code.visualstudio.com/docs/supporting/requirements). As of the writing of this book, Visual Studio Code is also available for Mac (latest macOS versions), Windows 10 and 11, and Linux (Red Hat, Ubuntu, Fedora, and Debian), so you can see that it does run on almost anything. Not your toaster yet, but it's solidly cross-platform.

Note

Recommended requirements change over time, and new versions of applications are always being released, usually consuming more

resources and requiring newer operating systems. Be ready!

ExamAlert

Understand minimum requirements categories for software, including CPU, RAM, GPU (and VRAM), storage space, and OS type and edition.

Remember: Compatibility is key. And, when planning a system, you have to overengineer. Make sure you have plenty of resources (and then some) based on the *recommended* requirements of an application. Otherwise, the productivity of your users will be less than optimal.

Distribution Methods

Many applications are simply downloaded and run through the installer for Windows, macOS, or Linux. In some cases, however, the application you wish to install might be stored on physical, removable media, such as a USB flash drive or possibly even an optical disc. Perhaps it is located somewhere on the network. You might have to connect to a mapped network drive or an FTP server, and you might have to extract the content from a .zip file or another compressed group of files.

How an application will be installed should play into your planning. Be ready for multiple installation and deployment types. For instance, in the case of a program such as Microsoft 365, you might use a server to deploy the program (or a new version of the program) to multiple clients at once. Finally, know where you are installing the program. If you are using Windows, for example, a 32-bit version of the program will go to C:\Program Files (x86), and a 64-bit version of the program will be installed to C:\Program Files. In essence, you need to know the source and also the target.

Some applications (and especially operating systems) can be downloaded in .iso format. An ISO image is an optical disc image. It is a single file that is a complete representation of all the files that would be placed on an optical disc. This is the standard format for downloading operating systems from the Internet, compressed into a single file. Once downloaded, it can be mounted to an area of a storage drive or USB flash drive as the original complete set of files

to ultimately be installed to a computer. Besides using Disk Management for mounting, you could use third-party programs such as PowerISO and Rufus. (See Chapter 33, "Microsoft Operating System Features and Tools, Part II," for more information on mounting in Disk Management.)

ExamAlert

An ISO image (.iso file) is a single file that represents a complete set of files that would be placed on an optical disc. It's commonly used for operating systems and large applications.

An ISO image can also be useful for implementing over-the-network installations, and it can be used directly by a virtualization program (such as VirtualBox) to install virtual operating systems. Finally, an ISO image can be burned to an optical disc if necessary.

Note

While it is common to think of ISO images as being designed for optical media, they are also commonly used to distribute images designed for USB and SD media. Because most new devices no longer have optical drives, this makes it easy to create bootable USB-based tools. Many technicians will use such USB-based tools regularly.

Other Considerations for New Applications

Answer me these questions three: How will an application impact your computers and network? How will it impact business operations? And how should you consider security as it pertains to new applications? Let's look at the answers to these questions together now.

Application Impact

Any application that is installed will have an impact on the device or computer. Every running application—and every running process, for that matter—uses precious CPU and RAM resources.

You can see the resources being used if you view an application in the Task Manager, Resource Monitor, or Performance Monitor in Windows; the Activity Monitor in macOS; or the top program in Linux. Some applications run quietly in the background, and others might use more resources than you would like, even when they are inactive. It's important to know how to remove applications from the startup process if necessary so that resources can be freed up on the local system.

Don't forget that applications also take up space on the storage drive. Contrary to popular belief, *storage space is not infinite*! Periodically, you will need to remove apps that are not being used. You can do so from **Settings > Apps > Installed apps** in Windows 11 (**Settings > Apps > Apps & features** in Windows 10).

In many cases, an application will impact the network as well. Imagine a videotelephony program (like Zoom, Microsoft Teams, or Google Meet) or any type of application that deals with the streaming of video to the desktop. Such applications have a big impact on an individual computer's network connection and possibly the entire network—potentially slowing down other users. Can your network handle multiple users running video chat? Are your network switches up to the task? A typical video chat can use between 1 and 5 Mbps. A typical high-definition video stream can use up to 20 Mbps. Multiply that by 50 users, and your 1 Gbps switch will be in trouble. Make sure that your network's bandwidth meets the requirements of your applications, given the number of users who will be working with those apps. Implement quality of service (QoS) tweaking and set thresholds for your users either at the switch or router or locally at the computer system.

A multiuser application can also impact a business in general: its operations, productivity, and continuity—from a networking standpoint and from a security standpoint. For example, video chat programs and social media programs are known for having security and privacy issues. And let's not even mention gaming. New applications that are not coded properly can bring down systems and even entire networks, resulting in lost productivity that translates to lost revenue—and that usually means someone is headed for the unemployment line. Who? The person who installed the application. Don't be that person. Thoroughly test your potential new applications on testing systems in an isolated network before deploying them.

Safe deployment of applications also hinges on user permissions and some other security considerations. Let's briefly discuss those now.

User Permissions

When you install an application in Windows, Windows usually asks who you want to have access to the program. Quite often, the options are the user who is installing the application only or everyone on the computer. Those options can be somewhat limiting, especially if you have several users who share the system. Later, you can assign permissions to users or groups on the folder that contains the application's executable file. Be ready to navigate to C:\Program Files (x86) and C:\Program Files to do this for 32-bit and 64-bit applications, respectively.

As an administrator, you might be called upon to install a special application to a user's computer, where only that user may use the application—and even you aren't allowed to use it, regardless of the fact that you are an admin. In such a case, you have to change permissions appropriately or give the user permissions to install the application. Be ready to be called upon to make changes to ownership and permissions in Windows. We'll discuss these topics further in Chapter 45, "Windows Security Settings," and Chapter 48, "Workstation Best Practices."

Security Considerations

Please consider this: Every installed application increases the target surface of an operating system. An application could open networking connections, or open ports on the firewall, or create backdoors, all of which can be inviting to attackers. Plus, the availability of the rest of the system could be reduced by some applications that are not coded well.

Consider running evaluation versions of software on a testbed (that is, an isolated network or a VM network) before installing to live clients. Test the security of an application by scanning the system for malware, scanning for open ports, and running the application side by side with other applications to find out if there will be any conflicts. Then, check how the application updates. You may or may not want it to auto-update. If it does not auto-update, you should periodically check for updates that will address security vulnerabilities and increase the functionality of the program. Depending on your organization's policies, that could be every six months or less. The installation of the program and the program's updates could also affect the network. The larger the program, the more the network will be affected. So, after you have tested an

application thoroughly, be sure to run installations and upgrades off-hours unless they are absolutely necessary!

Cram Quiz

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

1. Which of the following are important considerations when planning the installation of a new application? (Select the three best answers.)

   - ○ **A.** CPU speed
   - ○ **B.** Windows location
   - ○ **C.** Program Files location
   - ○ **D.** User permissions
   - ○ **E.** Warranty

2. What is the name of the folder where Windows stores 64-bit system files?

   - ○ **A.** Systemroot
   - ○ **B.** System32
   - ○ **C.** SysWOW64
   - ○ **D.** Program Files (x86)

3. One of the users at your company attempts to install an application and receives the following error message:

   ```
   Not enough disk space to install...
   ```

   Which of the following was overlooked by the user?

   - ○ **A.** Operating system compatibility
   - ○ **B.** Installation method
   - ○ **C.** File permissions

- ❍ **D.** System requirements

4. A customer submits a request for a technician to install a new application on a computer. The computer has the following specifications:

CPU	Quad core (x86-64)
RAM	16 GB DDR4
Storage drive	1 TB (900 GB used)
Network	1000 Mbps Ethernet

The new application has the following minimum requirements: quad-core processor, 64-bit operating system, 8 GB of RAM, 120 GB of free space, and 1 Gbps network connection.

Which of the following will result when the technician installs the software?

- ❍ **A.** Insufficient RAM
- ❍ **B.** Network connection is too slow
- ❍ **C.** Insufficient storage
- ❍ **D.** Unknown CPU
- ❍ **E.** Incompatible system architecture

Cram Quiz Answers

1. **A, C, and D.** When installing a new application, you should consider the CPU speed (and other minimum/recommended hardware requirements), the Program Files location (64-bit or 32-bit), and user permissions. The Windows location isn't really important; by default, it will be C:\Windows, but its location doesn't really impact the installation of the application. The warranty (if there is one) can be important if there is a failure, but it doesn't play into the installation of the software.

2. **B.** System32 is the folder that Windows uses to store 64-bit system files. Systemroot is a variable used for the main Windows folder. More accurately, it is written as %systemroot%. It usually equals C:\Windows. SysWOW64 is actually the location of 32-bit system files. Program Files (x86) is the place where 32-bit versions of programs are stored.

3. **D.** The user did not pay attention to the *minimum* system requirements. Perhaps the application needed 10 GB of storage drive space, and only 8 GB were left on the partition. (Close is not good enough!) It appears that the installation started well enough, so the OS should be compatible, and the installation method is most likely correct. As long as the user has rights to run executable files, which is likely, there shouldn't be any file permissions issues.

4. **C.** The system has insufficient storage space. If the system has a 1 TB drive that has 900 GB used, that leaves 100 GB free, which is not enough for an application that requires 120 GB. The technician would first have to free up space by going to **Settings > Apps > Apps & features** and removing some unused applications. There is plenty of RAM on the system, and the network connection is fine (1000 Mbps is the same as 1 Gbps). A quad-core CPU is very common, be it Intel or AMD. Any application should be able to install to it. The system architecture should be adequate: The software requires a 64-bit system, and today's quad-core CPUs are 64-bit. The table says x86-64, which means 64-bit.

Well, that wraps up this chapter. Excellent work. Review, break, and then continue on!

Chapter 42

Cloud-Based Productivity Tools

This chapter covers the following A+ 220-1202 exam objective:

- **1.11** – Given a scenario, install and configure cloud-based productivity tools.

With the advent of anytime, anywhere Internet connectivity, many of the tools that used to be installed have instead migrated to the web. Instead of having to install and configure software locally, users now use Internet-based alternatives. These tools can be great for collaboration; for instance, this edition of the book is being written collaboratively with the author team, using the online version of Microsoft Word. This type of connectivity also brings with it some challenges. We will discuss some of these opportunities—and downfalls—in this chapter. Take your time, and it will all be fine.

ExamAlert

Objective 1.11 focuses on supporting tools that take the workload online, allowing anytime, anywhere access for users. This includes email systems, storage, collaboration tools, identity synchronization, and licensing assignment.

Email Systems

Without communication, people will have trouble getting their work done. One of the most important business communication systems is email. In nondomain environments, configuration of email is often difficult and time-consuming to support. As a result, users lose time and businesses lose money waiting for users to restore connectivity to their communications.

By moving the email system to a web-based online environment, those issues are all taken care of. Users simply log in to a web page that has been preconfigured for them. They don't need to worry about configuring anything; they only need their own user authentication (username, password, and any two-factor authentication required). Because nothing is installed locally, they can access their email from any device, anywhere they have Internet access. This anytime, anywhere access to their communications makes the modern workplace more efficient and effective and improves productivity of the workers and the support personnel.

Examples of web-based email systems include Google's Gmail and Microsoft's Outlook. Both can be used by individuals and businesses; businesses can even use their existing domains within the Gmail interface. Outlook's web interface closely mirrors that of the installed program client. Figure 42.1 shows an online Outlook window.

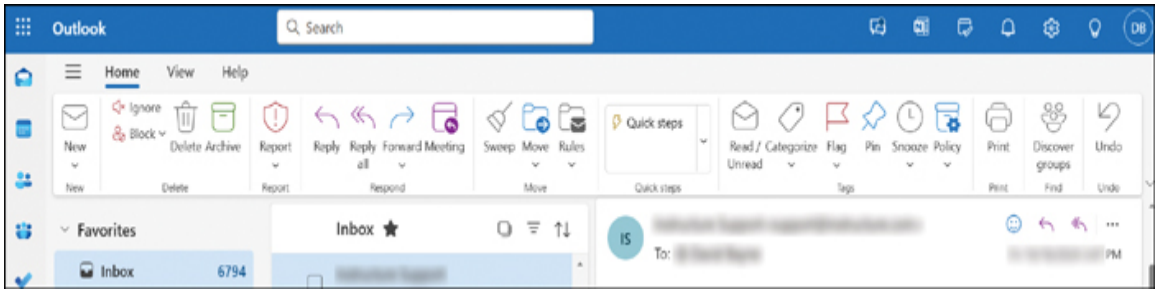


FIGURE 42.1 **Outlook Online Resembles Its Installed Counterpart**

Note

Two-factor authentication (2FA) is a security method that requires two forms of identification to log in to an account. It's the most common type of *multifactor authentication (MFA)*. We'll cover MFA in detail later in the security part of the book.

ExamAlert

Gmail and Microsoft Outlook are considered prime examples of Software as a Service (SaaS) applications because users access their email functionality through a web browser. This means that they don't need to install the software locally on their devices and can access it from anywhere with an Internet connection, making it a typical SaaS feature. More and more applications have an SaaS offering (Microsoft Office 365 and Google Docs are two additional examples although Microsoft 365 can also be installed locally).

ExamAlert

Given a scenario, be sure you know how to access and configure cloud-based email systems.

Online Storage

Because email has, for the most part, gone online as SaaS, so has storage. Microsoft's OneDrive, Google Drive, Dropbox, Box, and a multitude of other providers allow you to store your files and other documents online. This move to cloud storage has many advantages, not the least of which is disaster recovery: If your home or business is impacted by a natural disaster, the data center where you have stored your documents will likely be safe and, even if it is knocked offline, the data will very likely be backed up safely.

Many of the online storage locations can also be mounted as drives on your local device, so they will appear in Windows File Explorer just like any other location. This makes it very convenient to save directly to these online storage locations. You can also use the web interface. Figure 42.2 shows File Explorer with Microsoft OneDrive and Google Drive mounted as locations.

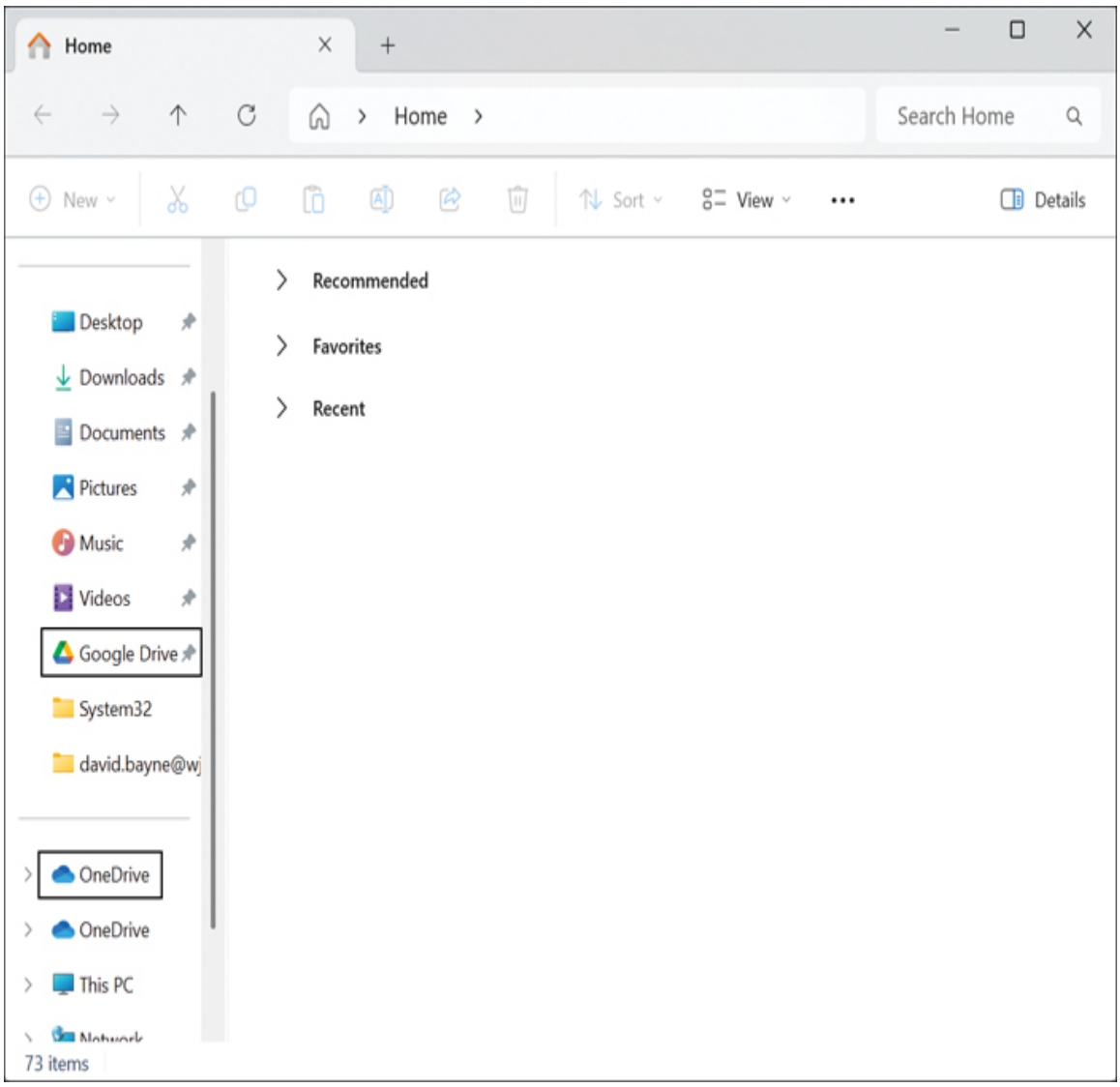


FIGURE 42.2 **Microsoft OneDrive and Google Drive in File Explorer**

You can also choose to sync folders on your local drive with the remote drive using these same tools. Any files that you place into the local drive are automatically uploaded to the remote location. Any files placed into the remote folder are automatically copied down to the local drive. This approach can even be used to create an online backup system, though you need to be careful not to run out of space on your cloud drive. Settings for this vary by cloud provider, so you should read the instructions on the

provider's website carefully; however, the whole process is designed to be easy.

Note

For more information on syncing files with OneDrive in Windows, visit https://support.microsoft.com/en-us/office/sync-files-with-onedrive-in-windows-615391c4-2bd3-4aae-a42a-858262e42a49. For more information on syncing with Google Drive, visit https://support.google.com/drive/answer/10838124?hl=en.

ExamAlert

For the exam, be sure you understand how cloud-based storage works and know how to set up folders for online syncing.

Collaboration Tools

The move to cloud-based tools has improved the concept of collaboration, allowing teams to work together more closely even when physically separated. This capability has allowed for the increase in remote work and fully remote teams, as well as other changes in workplace communication that allow flexibility of both time and location, which can help improve work–life balance. Once a user account is configured, the cloud-based provider does all of the heavy lifting of ensuring that the software is kept up to date and access is ensured.

Videoconferencing

Prior to the advent of commonplace broadband connections, videoconferencing solutions required specialized hardware and software and dedicated high-speed connections. Even as recently as 2016, it was common for companies to have dedicated videoconferencing rooms set up to facilitate any remote meetings. With the advent of adequate hardware and

speedy Internet access in many homes and even on cellular phones, having a dedicated space is no longer necessary. Instead, ordinary users have access to remote access capabilities on business-class devices at commonly available Internet speeds. This capability has allowed companies to utilize remote workers more efficiently (or at all) and has allowed the workers to flex their time and location as well to better fit their own personal needs. In addition, many medical providers offer video-based appointments, allowing patients to be seen without having to travel—a boon for those who are sick and might be contagious!

Videoconferencing is available from many providers, including Cisco Webex, Zoom, Microsoft Teams, and Google Meet. Many of the help desk ticketing systems also have videoconferencing tools built in, either by partnering with one of the larger firms or by creating their own. Most of these also have instant messaging tools built in.

Instant Messaging

Instant messaging tools allow teams and individuals to send messages to one another without having to create and send a full email. This quick communication is efficient for smaller, faster messages that might not need the longer, more formal format of an email, and can facilitate more informal conversations. In a remote environment, this conversational environment goes a long way toward building an effective team and can improve productivity.

All of the videoconference providers also have instant messaging while in a meeting. Microsoft Teams and Google also provide instant messaging outside of the messaging environment; in both cases, these are limited to users within the domain or organization, which helps reduce or eliminate spam. Slack also offers similar tools and is used by both work teams and by groups of individuals working on personal projects, games, and clubs of all sorts.

Figure 42.3 shows a Microsoft Teams window. Each icon in the left column represents a different option within Teams, including Teams videoconferencing and Chat instant messaging.

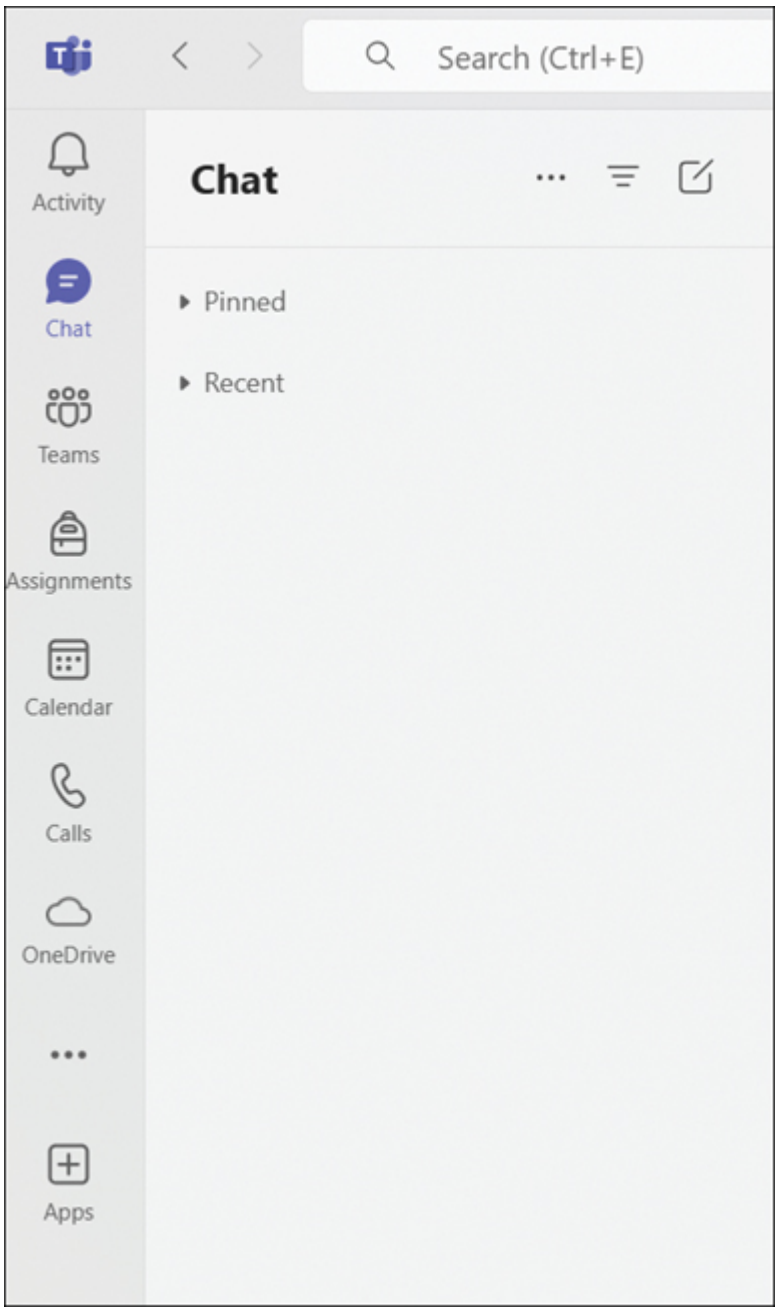


FIGURE 42.3 **Microsoft Teams Window**

Spreadsheets

Cloud-based spreadsheets allow not only anywhere, anytime access but also collaboration. Users can share their spreadsheets with other users, allowing for synchronous access and editing of the data in real time. Because the

document resides online, users always have the latest version of the files so are always up to date with the latest numbers.

Presentation Tools

Users can create and share presentations online, collaborating on the creation and editing of presentations and even with distribution. Users always have the latest version.

Some of the online presentation tools are designed to be run in kiosk mode, making their use as a remote kiosk for a visitor's center or in digital signage ideal. Because they are cloud based, content updates are easy to do remotely and quickly: Just update the presentation and, if necessary, reboot the remote devices. This flexibility of online presentation tools is a unique development of the transition to an online environment.

Word Processing Tools

Like spreadsheets and presentations, online word processing tools allow users to collaborate in an anywhere, anytime environment, and ensure that each user has the latest version of the document—even if multiple users are editing it at the same time. In fact, as with the others, you can sometimes see the other users typing in real time!

Because it is not uncommon for multiple users to collaborate on word processing documents, it is especially critical that these online documents support this functionality, and in fact, it was one of the first things that was perfected. Gone are the days of passing documents on flash drives or via email. Instead, everyone can access the shared document via a single shared drive and edit it at the same time. It really is a game changer.

Identity Synchronization

In a perfect world, users would authenticate themselves one time and not have to do so again. The system would authenticate them as needed to all new systems they need to access.

Microsoft can synchronize users' identity information within Active Directory to their Entra ID, formerly Azure Active Directory. This allows IT users and device management using Active Directory (AD) or Entra ID to enter information in only one system and have that information be in the other system, which is ideal for large organizations with assets in both systems and for users who need to be in both systems.

These systems can also be synchronized across Kerberos for use in Linux systems and with Google to provide automatic Google authentication and accounts for AD or Entra ID users. When users log in using their Entra ID or their Google login, this enables a concept called *single sign-on (SSO)*, where login and authentication information can become standardized and centralized. By using SSO, an organization can also allow users to sign in once and allow their users to use many applications without having to log in again; the SSO system handles the rest of the user authentication.

Note

Single sign-on (SSO) is a method of access in which users are given access to all the applications and systems they need when they initially log in. We'll cover SSO in more detail later in the security part of the book.

Licensing Assignment

To use a program, you must purchase a license. For Microsoft 365, licenses are assigned to individual users via their Microsoft accounts, and this information can be managed via the Microsoft 365 admin center at https://admin.microsoft.com, or via AD or Entra ID group membership, adding and deleting licenses from individual users as needed.

Your organization then can fully utilize the licenses it purchases and not "waste" them on users who don't need to use them or who have left the organization. You can assign licenses for individual programs or for entire suites of programs with this tool.

ExamAlert

Be sure you know how to install, set up, and use cloud-based productivity collaboration tools including spreadsheets, videoconferencing, presentation tools, word processing tools, instant messaging, identity synchronization, and licensing assignment.

Cram Quiz

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

1. Which of these represent reasons to move to an online email system? (Select all that apply.)

   - ○ **A.** Online email is faster than local email.
   - ○ **B.** Configuration is done for you, which reduces errors.
   - ○ **C.** Local email is always deleted immediately from the Internet.
   - ○ **D.** Email is available anytime, anywhere you have Internet access.

2. Storing data online gives which of the following advantages? (Select all that apply.)

   - ○ **A.** Anywhere, anytime access
   - ○ **B.** Automatic backup
   - ○ **C.** Sharing capabilities
   - ○ **D.** Spell check
   - ○ **E.** Storing online will protect your email

3. Documents shared online through SaaS such as Microsoft 365 or Google Docs have which of the following characteristics? (Select all that apply.)

   - ○ **A.** There is anywhere, anytime access.
   - ○ **B.** Collaboration with other users in real time is practical.
   - ○ **C.** Files are stored locally on individual machines.
   - ○ **D.** Files cannot be backed up easily.

4. Instant messaging tools can be used to communicate in which of the following ways? (Select all that apply.)

   - ○ **A.** Create short messages sent as text messages
   - ○ **B.** Create short messages that need no reply
   - ○ **C.** Create short messages for more informal communication
   - ○ **D.** Create short messages for more conversational communication

5. Videoconferencing tools allow for what type of team? (Select all that apply.)

   - ○ **A.** Remote teams
   - ○ **B.** Teams in multiple offices
   - ○ **C.** Teams in multiple countries
   - ○ **D.** Specialized hardware is required for the team

Cram Quiz Answers

1. **B and D.** Configuration is done for the end user, which eliminates errors with entry of specific server addresses. Email is available to users wherever and whenever they have Internet access. It is not necessarily any faster; they view their email in a web browser. While local email could be deleted upon downloading, this is no longer a common occurrence.

2. **A, B, and C.** You have access to your files anywhere, at any time. Your cloud provider will back up the files automatically within its system, so if a disaster were to hit, your files should be protected. You can share your files with whomever you choose, and if you have a provider who allows this, you can also collaborate on editing these documents. Spell check is available without going online, and online storage and email, while both online, are unrelated.

3. **A and B.** Files created with SaaS tools such as Microsoft 365 and Google Docs are, by default, stored online, which means that users can collaborate easily with one another, sharing the documents and even working on the documents together in real time. The files can be accessed anywhere you have Internet access, at any time of day or night. They are not generally stored on individual machines (that can be done, but it takes additional steps), and backups are automatic because the files are already online.

4. **C and D.** Instant messaging tools are used for more informal communication and can work in a more conversational manner than the more formal email format (hard to believe we're referring to email as formal!). While some can be configured to send the messages to mobile phones as text messages, this approach is uncommon.

5. **A and B.** Although the teams can be fully remote, even in different countries from one another, the key component is their remoteness, either geographically or physically. With the advent of cheap videoconferencing, teams can keep in touch while not being in the same physical location. This capability allows for better collaboration and better work-life balance.

You're doing great! If you aren't familiar with some of the concepts in this chapter, be sure to review them both online and, if you can, in person with someone who can show you how they really work. Keep up the good work!

Core 2 (220-1202)

Domain 2.0: Security

CHAPTER 43 Physical Security

CHAPTER 44 Logical Security

CHAPTER 45 Windows Security Settings

CHAPTER 46 Wireless Security and Malware

CHAPTER 47 Social Engineering, Threats, and Vulnerabilities

CHAPTER 48 Workstation Best Practices

CHAPTER 49 Mobile Device Security

CHAPTER 50 Data Destruction and Disposal

CHAPTER 51 SOHO Security

CHAPTER 52 Browser Security

Chapter 43

Physical Security

This chapter covers a portion of the following A+ 220-1202 exam objective:

- **2.1** – Summarize various security measures and their purposes.

Welcome to the first chapter on security. Everyone should have some basic knowledge of information security. Computers and computer networks are constantly under fire.

An attacker might try to break into a facility physically or hack into a system logically. This chapter and the next one cover these two concepts. Here, we use the terms *break* and *hack* loosely; the methods used to accomplish those ends can vary. The goal of this chapter is to present some basic options for securing against a person who would attempt to unlawfully enter a building or another location.

Know this: *Nothing is 100 percent secure*. It is impossible to completely secure something. Attackers and hackers are always finding ways to get around security solutions; it just takes time and persistence. So, what we are interested in is solutions that are *relatively* secure. We need powerful security methods that are within budget but not so cumbersome that they will bring our computers and networks to a crawl. That's the essence of a good security plan.

To repeat, nothing is 100 percent secure. Keep that in mind as you progress through the security chapters.

ExamAlert

This portion of **Objective 2.1** concentrates on physical security and physical access security. Chapter 44, "Logical Security," covers the logical security aspect of Objective 2.1.

Note

Remember that the CompTIA A+ certification is not a security certification. However, because security is such an important part of the IT world, it accounts for a substantial percentage of the exam. We therefore spend quite a few chapters of this book on security topics.

Physical security has to do with tangible, visible, and hands-on methods of preventing access to a home, building, server room, data center, or any other location. There are lots of ways to accomplish an acceptable level of physical security. Let's start with one of the most important—yet often overlooked—methods: using locks.

Physical Locks

The physical door lock and key are among the oldest security methods used as a deterrent against unlawful entry. In addition to locking main entrances, you should always lock server rooms, wiring closets, labs, and other technical rooms when not in use. An organization should document who has the keys to server rooms, data centers, and wiring closets. Locks should be changed out and rotated with other locks every so often. This system keeps things dynamic and harder to guess. Another type of lock, a cipher lock, requires a punch code to unlock the door. These physical methods might be used by themselves or combined with an electronic system.

It's important to use a lock for the room that the servers are in, and the servers themselves can also be locked up. Consider placing them in a well-

ventilated, lockable cabinet. Special cable locks can also be installed for PCs, laptops, and servers. Some PC cases come with built-in locks. Configure the BIOS/UEFI to log when someone opens the case of the computer. This information is logged as a chassis intrusion notification. Use a USB lock to stop people from removing USB devices or to block the physical ports.

Entry Systems

The most common electronic entry system is a key card system. Such a system uses proximity-based door access cards that you simply press against, or near, a transmitter next to the door handle. They are often RFID based. Although these systems are common, they are not the most secure option. (Smart cards can be more secure, as we will discuss in a moment.) But because they are less expensive than other systems, you might see them more often. Other electronic systems use key cards that incorporate a photo ID (such as a worker's badge). Such a card can contain information about the identity of the user, which in combination with a *badge reader* ultimately authenticates the user. While cards are common for entry systems, they can also come in smaller form factors, such as *key fobs*—similar to a vehicle's key fob—which can be attached to a user's keychain. These systems sometimes offer entry control, limiting someone's ability to enter or exit during certain times of the day and identifying and checking names against an authenticated roster, or an *entry control roster*.

Moving on to the next level of security, let's talk briefly about smart cards. A smart card has a nano-processor and can actually communicate with the authentication system. Examples of these cards include the Personal Identity Verification (PIV) card used by US government employees and contractors and the Common Access Card (CAC) used by Department of Defense (DoD) personnel. Such a card identifies the owner, authenticates them to areas of the building and to computers, and can digitally sign and encrypt files and email with the RSA encryption algorithm (using an RSA token) or another algorithm. Because these are physical items a user carries to gain access to specific systems, they are known as *hardware-based tokens*. A token might also display a code that changes, say, every minute or so; these are known as one-time password (OTP) tokens. When a person

wants access to a particular system, such as the accounting system or another confidential system, that person must type the current code that is shown on the token into the computer. This is a powerful method of authentication but can be expensive.

In addition to smart cards, there are also *mobile digital keys*. A mobile digital key is a secure digital credential stored on a mobile device that uses NFC or Bluetooth for authentication. This leverages the security features of the mobile device itself, including encryption and biometric authentication. It also allows remote management for granting or revoking access. We're seeing this technology used more and more, even for consumer devices like unlocking a car and even starting it!

An organization might use an access control vestibule (aka *mantrap*), which is an area with two locking doors. A person might get past a first door by following someone else in (tailgating/piggybacking) but might have difficulty getting past the second door, especially if there is a security guard in between the two doors. If the person doesn't have proper authentication, this person will be stranded in the access control vestibule until authorities arrive. Depending on the degree of security an organization needs, having a physical security guard (that is, a human) to check IDs and monitor entry points might be a good idea.

ExamAlert

An access control vestibule (mantrap) is used to stop and monitor people during the identification process. Know the types of physical access security devices such as key fobs, smart cards, mobile digital keys, and the biometrics protections outlined next!

Biometrics

Biometrics is the science of recognizing humans based on one or more physical characteristics. Biometrics is used as a form of authentication and access control. It is also used to identify persons who might be under surveillance.

Biometrics falls into the category of "something a person is." Examples of bodily characteristics that are measured include fingerprints, palmprints, retinal patterns, iris patterns, and even bone structure. Biometric readers (for example, fingerprint scanners) are becoming more common in door-access systems and can be found integrated with mobile devices or used as external USB devices that connect to computers. Biometric information can also be combined with smart card technology. An example of a biometric door-access system is Suprema, which has various levels of access systems, including some that incorporate smart cards and biometrics, together forming a multifactor authentication system. There are also less expensive consumer-grade biometric locks that often include a fingerprint reader as well as a key code or a key lock. One example of biometric hardware for a local computer is a USB-based fingerprint scanner, which is used to authenticate users during the login process.

Modern biometric systems, especially facial recognition technology (FRT), have made significant improvements over the years. FRT maps facial landmarks to create a digital *faceprint*, whereas voice recognition technology (VRT) analyzes vocal patterns and tone to generate a *voiceprint*. Combine this with modern machine learning, particularly with deep learning and neural network AI, and the accuracy in varying lighting conditions, angles, noise environments, and other distractors has improved dramatically. Many airports now use this new type of biometrics, in particular FRT, to scan passengers. It is truly amazing. Of course, thorough investigation and testing of a biometric system are necessary before purchase and installation.

In addition, a biometric system should be used in a multifactor authentication scheme. The more factors, the better, as long as your users can handle it. (You would be surprised what a little bit of training can do.) Voice recognition software has made great leaps and bounds since the turn of the millennium. A combination of biometrics, facial recognition, and PIN access would make for an excellent three-factor authentication system—if you can get it through budgeting!

Other Physical Security Precautions

There are myriad ways to increase security from a physical perspective. You can use, for example, fences, bollards, alarm systems, video surveillance, and security guards.

Protecting an organization's building is an important step in general security. The more security a building has, the less you have to depend on your authentication system. A building's perimeter should be surveyed for possible breaches—including all doors, windows, loading docks, and even the roof. The area around the building should be scanned for hiding places; if there are any, they should be eliminated. The area surrounding a building should be well lit at night. We can't stress enough the need for good lighting; it's an excellent deterrent. Some companies may opt to use security guards and guard dogs. It is important that they be trained properly; usually, an organization enlists the services of a third-party security company for training.

Video surveillance can also be used to track individuals' movements. Video cameras should be placed on the exterior perimeter of a building in areas that are hard to access (for example, 12 feet or higher with no lateral or climbing access). The better the cameras are hidden, the better. Video cameras can also be placed inside a building, especially in secure areas such as executive offices, wiring closets, server rooms, data centers, and research and development areas. Many organizations use closed-circuit television (CCTV), but some opt for wired/wireless IP-based solutions. In any case, the video stream may be watched and recorded, but it should not be broadcast (especially to the Internet, unless absolutely necessary). Video cameras provide an excellent way of tracking user identities. However, proper lighting is necessary inside and outside in order for the cameras to capture images well. Also, video cameras must be properly secured because they are prime targets for reverse-engineering techniques where the attacker attempts to gain access to the pan-tilt-zoom (PTZ) controls and redirect the video feed.

Alarm systems are commonplace in most buildings today. Such a system sounds a siren and alerts a central monitoring service in the event of an intrusion or a break-in. The placement of door and window sensors and motion detectors is part of a total alarm system, and should be planned out

carefully. Motion sensors are often infrared based (set off by heat) or ultrasonic based (set off by certain higher frequencies).

An organization might opt for *fencing* around parking lots or perhaps around specific areas of a building, such as the waste disposal/recycling area or any HVAC units installed on concrete pads outside. Perhaps an entire building is fenced in and has an entry gate (staffed with security guards). Another related option is bollards. A *bollard* is a short vertical post that blocks access to vehicles or protects a building or walkway. Retractable bollards are available, to allow temporary access to an area. *Magnetometers* (metal detectors) can be implemented at entry points to a building to detect metal objects, such as concealed weapons.

One great security technique is to have an employee (or a third party) attempt to access every portion of an organization's property and buildings during the day and at night as well. Monitor and track the user step by step to see what the person is able to do and what is accessible. This can be an eye-opening experience. Document what happened carefully and adjust the security plan as needed. An organization can hire third-party companies to do just this, but contracts and agreements must be judiciously carried out beforehand.

The level at which an organization implements these security methods will depend on the organization's security mindset and budget. We could go on and on about general building security, but we think you get the idea. If your organization is extremely concerned about building security and doubts that it has the knowledge to protect the building and its contents properly, consider hiring a professional.

Protecting Data Physically

Confidential documents should never be left sitting out in the open. They should either be properly filed in a lockable cabinet or shredded and disposed of when they are no longer needed. Passwords should not be written down and definitely should not be left on a desk or taped to a monitor where they can be seen. Many organizations implement a clean desk policy that states all users must remove all papers from their desks before leaving for lunch, breaks, or at the end of the day.

Anything that shows on the computer screen can be protected in a variety of ways. To protect data while a person is working, you can use a privacy screen or install a privacy filter, 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 in front of the screen can see the content shown on the screen. This helps prevent shoulder surfing where a person looks over your shoulder to see sensitive information like usernames and passwords. Many of these filters are also antiglare, helping to reduce eye stress for users.

Also, users should lock their computers whenever they leave their workstations. Windows can also be automatically set to lock after a certain amount of time, to protect the machine even if a user forgets to do so manually. A great keyboard shortcut to quickly lock your screen is ⊞ (Windows key) + L for Windows and Linux or Ctrl + ⌘ (Command key) + Q for macOS. To unlock the keyboard, simply enter your password.

Cram Quiz

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

1. Which of the following is the science of recognizing humans based on physical characteristics?

   - ○ **A.** Mantraps
   - ○ **B.** Biometrics
   - ○ **C.** Tailgating
   - ○ **D.** CAC

2. You have been tasked with preventing unwanted removal of a webcam. Which of the following tools should you implement?

   - ○ **A.** Smart card
   - ○ **B.** USB fingerprint scanner

- ○ **C.** USB lock
- ○ **D.** Privacy filter

3. You want to know if there is any intrusion to your organization's building. Which of the following should you implement? (Select the two best answers.)
   - ○ **A.** Video surveillance
   - ○ **B.** Magnetometer
   - ○ **C.** Alarm system
   - ○ **D.** Standard door lock
   - ○ **E.** Proper lighting
   - ○ **F.** Access control vestibule
4. What is the primary function of a bollard in physical security?
   - ○ **A.** To detect metal objects on individuals entering a building
   - ○ **B.** To restrict vehicle access and protect buildings or walkways
   - ○ **C.** To sound an alarm in case of unauthorized entry
   - ○ **D.** To monitor and record video footage of the premises
5. Which of the following is NOT a type of biometric authentication?
   - ○ **A.** Fingerprint scanning
   - ○ **B.** Iris scanning
   - ○ **C.** Keycard access
   - ○ **D.** Voice recognition

Cram Quiz Answers

1. **B.** Biometrics is the science of recognizing humans based on physical characteristics. In the authentication world, it falls into the

category of "something a person is." Access control vestibules (also known as mantraps) are implemented to stop tailgating. CAC, which stands for Common Access Card, is a card used by defense personnel, such as DoD employees.

2. **C.** Use a USB lock to prevent the removal of USB-based devices such as external USB storage drives, keyboards, mice, and webcams. Smart cards and USB-based fingerprint scanners are ways to authenticate a user to the computer or network. A privacy filter is used to prevent shoulder surfing—in which a person attempts to watch what a user is typing/performing in a system—by reducing the viewing angle.

3. **A and C.** Video surveillance and alarm systems can help to let you know if an intrusion occurs. However, they differ in that a video surveillance is often passive in design. It usually requires a person to actively monitor it. An alarm system, on the other hand, will trigger an alarm and then send an alert to a monitoring company, which will in turn notify the appropriate personnel at the organization that has been intruded upon. A magnetometer (metal detector) is used to detect metal objects on a person. A standard door lock is an excellent security precaution, but if it is bypassed, the lock itself won't notify you of an intrusion. Proper lighting is also a magnificent idea, but it is passive as well and won't notify of any wrongdoing unless additional sensors (or special types of lighting with sensors) are put in place. An access control vestibule (or mantrap) is used to detain people in an area with two doors—usually for authentication purposes. This by itself won't alert anyone, but access control vestibules are often equipped with video surveillance and possibly security guards (both of which could alert the organization of any wrongdoing).

4. **B.** Bollards are short, sturdy posts that are strategically placed to prevent vehicles from entering certain areas, such as pedestrian walkways or building entrances, while still allowing foot traffic to pass through. A magnetometer (metal detector) is used to detect metal objects on a person. Neither an alarm system nor a video surveillance system would include bollards.

5. **C.** Keycard access is not a type of biometric authentication because it does not rely on unique biological traits for identification. Biometric authentication methods, such as fingerprint scanning, iris scanning, and voice recognition, use distinctive biological characteristics to verify an individual's identity.

Good work! This was a shorter chapter that covers just the basics you need to know for the A+ exam. Even so, as usual, be sure to review, take a break, and then continue on.

Chapter 44
Logical Security

This chapter covers a portion of the following A+ 220-1202 exam objective:

- **2.1** – Summarize various security measures and their purposes.

As an A+ technician, you will probably be more concerned with logical security than physical security. This chapter is therefore a little longer than the last one—and also more in depth. The goal of this chapter is to present some options for securing against a person who would attempt to unlawfully gain access to a computer network and individual systems. Wow, that's a lot to cover, you might be thinking. Well, it is! However, if we stick to the fundamentals and cover just what you need to know for the CompTIA A+, everything will be just fine. Onward!

ExamAlert

This portion of **Objective 2.1** concentrates on logical security.

Logical security has to do with operating systems, programs, and data. It is less tangible than physical security. When logical and physical security are used together and implemented properly, they can provide for a high level of security. A lot of what we will discuss in this chapter is within the realm of authentication. Let's start with that.

Authentication

One major shift in authentication principles is the *zero trust model*. This principle runs on the idea of "never trust, always verify." This concept moves away from the idea that those inside certain perimeters can be trusted. Instead, zero trust mandates authentication and authorization for every access request regardless of location. This is a fundamental change in cybersecurity because it restricts those who breach the initial perimeter of a network from gaining lateral movement. It also helps to prevent insider threats—those threats that come from the inside of an organization. That topic will be discussed more in Chapter 47, "Social Engineering, Threats, and Vulnerabilities."

> **Note**
>
> Zero trust is an evolving framework that is primarily focused on protecting the resources themselves rather than placing trust in the entire network, for example, and what is already within that perimeter.

Unauthorized access can be prevented through the use of authentication, which is the verification of a person's identity. It is a preventive measure that can be broken down as the following categories:

- Something the user knows (for example, a password or PIN). These factors are known as *knowledge factors*.
- Something the user has (for example, a smart card or another security token). These factors are known as *possession factors*.
- Something the user is (for example, the biometric reading of a fingerprint or retina scan). These factors are known as *inherence factors*.
- Something the user does (for example, a signature or speaking words). These factors are known as *behavioral factors*.

- Some*where* the user is (for example, at work or at home). These factors are known as *location-based factors*.

There are more categories, but the preceding list is a good starting point for you. The first three categories (or factors) are the most common. A powerful security methodology is to combine two or more of these factors together. When this is done, it is known as *multifactor authentication (MFA)*. An example of MFA is the combination of a password (knowledge factor) and a smart card (possession factor). Another example is a combination of a fingerprint (inherence factor) with a software token that has been installed to a user's smartphone (possession factor). Both of these are two-factor authentication schemes that you might see in the field. The beauty of MFA is that if one factor is defeated or compromised by a malicious person, the second factor still stands. Think about it for a couple of minutes. Imagine some scenarios where two-factor authentication can help prevent security breaches. Of course, efficient and effective multifactor user authentication works well only if it is strong—using complex passwords, powerful biometric systems, and updated smart card systems.

Here is a brief breakdown of various multifactor authentication (MFA) methods:

- **Email** (knowledge factor/possession factor):
  - **Definition:** A one-time passcode or link is sent to a registered email address.
  - **Strengths:** Widely accessible, simple to implement.
  - **Weaknesses:** Vulnerable to email account compromise, potential for delays.
- **Hardware Token** (possession factor):
  - **Definition:** A physical device generates time-based or event-based one-time passcodes.
  - **Strengths:** Highly secure against remote attacks, independent of network connectivity.
  - **Weaknesses:** Requires carrying a separate device, potential for loss or damage.

- **Authenticator Application** (possession factor):
  - **Definition:** A software application on a mobile device generates time-based one-time passcodes (TOTPs).
  - **Strengths:** Convenient, secure, and doesn't rely on SMS or voice calls.
  - **Weaknesses:** Dependent on mobile device security, potential for device loss.
- **Short Message Service (SMS)** (possession factor):
  - **Definition:** A one-time passcode is sent to a registered mobile phone number via text message.
  - **Strengths:** Widely used, easy to implement.
  - **Weaknesses:** Vulnerable to SIM swapping, interception, and delays.
- **Voice Call** (possession factor):
  - **Definition:** A one-time passcode is delivered via an automated voice call to a registered phone number.
  - **Strengths:** Accessible to users without smartphones, can be more secure than SMS.
  - **Weaknesses:** Can be inconvenient, potential for call interception.
- **Time-Based One-Time Password (TOTP)** (possession factor):
  - **Definition:** An algorithm generates a unique, time-sensitive passcode that changes at regular intervals, often used by authenticator applications, and hardware tokens.
  - **Strengths:** Highly secure, difficult to intercept or reuse.
  - **Weaknesses:** Requires synchronized time between the device and the authentication server, potential for small time drift issues.
- **One-Time Password/Passcode (OTP)** (possession factor/knowledge factor):
  - **Definition:** A single-use code is generated and used for authentication. This can be delivered via SMS, email, voice call, or generated by an app or hardware token.

- **Strengths:** Reduces the risk of password reuse and replay attacks.
- **Weaknesses:** Delivery method vulnerabilities, or hardware token loss.

ExamAlert

When two or more authentication factors are combined, such as a password and a physical token, the result is multifactor authentication (MFA). Know the types of common MFAs.

Note

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" personal identification number (PIN).

Just-in-Time Access

Just-in-time access is a principle and practice that grants users or systems privileged access to resources only when they need it and for only as long as they need it.

Just-in-time access aligns with the principle of least privilege, which is explained more in Chapter 45, "Windows Security Settings," in relation to Windows User Account Control (UAC). The idea of just-in-time access requires users to request access only when necessary and revokes it automatically. This principle is seen in macOS when a user tries to carry out an administrative task. The OS requests a password of an administrator to carry out the task. Once the task has been performed, the elevated permissions drop away. This is also seen in Linux with the **sudo** command (see Chapter 40, "Linux," for more information on the **sudo** command).

Privileged access management (PAM) is a core cybersecurity strategy that focuses on securing and monitoring access to critical systems and data by

users with elevated permissions. Because these accounts have significant power, PAM employs techniques like credential vaulting, session recording, and, crucially, just-in-time access. This approach ensures that privileged access is granted only when needed and for the minimal duration required, drastically reducing the window of opportunity for attackers to exploit compromised credentials.

PAM strengthens security by implementing just-in-time access, which eliminates standing privileges and limits the potential for unauthorized actions. By providing temporary access rights, PAM restricts the attack surface and minimizes the risk of lateral movement within a network. Furthermore, PAM solutions often include detailed audit trails, enabling organizations to track and investigate privileged activity, which is vital for compliance and incident response. This focus on just-in-time access ensures that privileged users only gain the necessary permissions for specific tasks, enhancing overall security posture.

ExamAlert

Remember that privileged access management (PAM) is a cybersecurity strategy that protects an organization's sensitive systems and data. It uses technology, processes, and people to monitor and control access to privileged accounts.

Principle of Least Privilege

The principle of least privilege says that a user should have access to only what is required. If a user needs to update spreadsheet files and browse the Internet, that user should not be given administrative access. You might think of this policy as common sense, but it should not be taken lightly. When user accounts are created locally on a computer and especially on a domain, great care should be taken when assigning users to groups. Also, as programs are installed, they request who can use and make modifications to the program; quite often, the default is All Users. Some technicians just click Next when hastily installing a program, without realizing that a user now has full control of the program—control that the user possibly should

not have. Remember: Keep users on a need-to-know basis; give them access only to what they specifically need to do their job.

One example of a Microsoft technology that is based on this principle is User Account Control (UAC). UAC is a security component of Windows that keeps every user (besides the administrator account) in standard user mode instead of as an administrator with full administrative rights—even if the user is a member of the administrators group. It is meant to prevent unauthorized access and user error in the form of accidental changes. With UAC enabled, users perform common tasks as nonadministrators and, when necessary, as administrators, without having to switch users, log off, or use Run As.

Basically, UAC was created with two goals in mind: first, to eliminate unnecessary requests for excessive administrative-level access to Windows resources, and second, to reduce the risk of malicious software using the administrator's access control to infect operating system files. When a standard end user requires administrator privileges to perform certain tasks (such as installing an application), a small pop-up UAC window appears, notifying the user that an administrator credential is necessary. If the user has administrative rights and clicks Continue, the task will be carried out; if the user does *not* have sufficient rights (and can't provide an administrative password), the attempt fails. Note that these pop-up UAC windows do not appear if a person is logged on with the administrator account.

MDM Policies

For large organizations that have many mobile devices, a *mobile device management (MDM)* suite can be implemented. An MDM solution can take care of pushing updates and configuring hundreds of mobile devices from a central location. Decent-quality MDM software secures, monitors, manages, and supports multiple different types of mobile devices across an enterprise.

Don't forget that Windows runs on many mobile devices, and they can be administered from a centralized MDM solution such as Microsoft Intune, VMware AirWatch, Cisco Meraki, and SOTI MobiControl. Elements that you might administer and enforce include device setup, policy acceptance,

profile distribution, device tracking, roaming mitigation, remote lock, remote wipe, and so on. We'll discuss MDM further in Chapter 49, "Mobile Device Security."

More Logical Security Concepts

There are several more concepts packed into Objective 2.1. This section acts as a catch-all for the rest of the logical security concepts that we haven't gotten to yet, including authenticator applications, access control lists (ACLs), tokens, SAML/SSO, IAM/DLP, email, and SMS.

Authenticator Applications

An authenticator application is often used as a second level of security. It provides a secondary verification mechanism that is simple to use.

One example is the Google Authenticator app, which has to be installed to a person's smartphone or other mobile device running Android or iOS. Once the app is installed, the user enables two-step verification in their account. Afterward, all affected connections will require two steps of authentication. For example, a user logs in to a service/website with a username and password. The service then sends a verification code through to the Google Authenticator app on the mobile device. Only the person who possesses the mobile device will see the code and be able to type it in the appropriate security field to gain access to the website or service.

Plenty of other authenticator apps are available for mobile devices. However, an organization might just opt to use standard two-step verification by way of SMS text, phone call, or email. Most websites and services that deal with any kind of personally identifiable information (PII) or transfer of currency require this—or, at the very least, provide it as an optional feature for a person's account.

Know this: Two-step verification is *not* two-factor authentication because both steps require the same factor: knowledge. In the preceding example, it would be two pieces of knowledge (password and code), but still, it's only one *factor* of authentication. Is security improved with two-step verification? Yes. And you could argue that a person *has* a smartphone or

other mobile device. But a proper two-factor authentication scheme—such as password and biometric, or password and a hardware-based token such as a smart card—is more secure.

ExamAlert

An authenticator app uses a passcode to achieve two-step verification.

Hard Tokens vs. Soft Tokens

You will find that the term *token* is used in a lot of ways and can have several meanings. For the A+ certification, tokens are considered to be hardware- or software-based ways of providing secondary authentication codes.

Hardware-based security tokens are small, physical devices given to authorized users to help with authentication. Such a device might be attached to a keychain or might be part of a card system. Hardware-based tokens might be used as part of a door access system or as something that gives access to an individual computer or networks. For example, RSA tokens carry and generate rolling one-time passwords (OTPs), each valid for only one login session or transaction.

Software-based tokens are virtual and are installed to mobile devices and other computers. These tokens are also used to generate single-use codes when accessing various platforms (for example, the previously mentioned two-step authentication process). In comparison to hardware-based tokens, software-based tokens are more easily accessible and cheaper, there are no batteries to deal with, and they don’t have to be physically carried. However, users need to access them on mobile devices or desktop computers.

Software-based tokens are not as secure as hardware-based tokens because they can be duplicated more easily. Hardware-based tokens cannot be duplicated unless they are stolen, and even then duplication would be a difficult task.

Note

As mentioned, the term *token* can be used in different ways. For example, a crypto token is a virtual currency token that represents a tradable asset within a blockchain. The token can be used by the owner for investment purposes. Although they are not covered in the A+ objectives, we recommend learning about blockchain technologies, which are being used in many ways in the technology world. To learn more about blockchain, visit https://aws.amazon.com/what-is/blockchain/?aws-products-all.sort-by=item.additionalFields.productNameLowercase&aws-products-all.sort-order=asc.

Access Control Lists

Access control lists (ACLs) are lists of permissions attached to an object specifying the levels of access that users or groups have to that object.

There is a little bit of confusion when talking about ACLs because they can be applied to firewalls and to operating systems. But in both cases, an ACL is a set of instructions for a computer system to follow. When you're dealing with firewalls, an ACL is a set of rules that applies to a list of network names, IP addresses, and port numbers. Permissions in an ACL might allow access or deny access, depending on what systems are required to have access.

The focus of this chapter is on operating systems. When you're dealing with operating systems, an ACL specifies the permissions—such as file and printer access—that can be assigned to individual users or groups. Permissions include Read, Write, Modify, Full control, and so on. We'll discuss these permission types further in Chapter 45.

ACLs are also known as file system access control lists (FACLs or FSACLs). An ACL is a list of permissions attached to an object. In a Windows environment, ACLs are broken down into *individual access control entries (ACEs)*; for example, the user JohnT might have read access to the marketing folder. Also, Microsoft uses the term *discretionary access*

control list (DACL) to refer to an ACL that identifies trustees who are allowed or denied access to an object. It uses the term *system access control list (SACL)* to refer to an ACL that enables admins to log attempts to access a secured object.

ExamAlert

An access control list (ACL) is a list of trustees assigned to a file or folder. A trustee can be any object available to the security subsystem. The term *ACL* is also used with routers and firewall systems to refer to the list of permitted computers or users.

SAML and Single Sign-On (SSO)

Security Assertion Markup Language (*SAML)* is an open standard that is used for authentication.

SAML is based on XML, a type of styling or markup, that enables secure exchange of authentication and authorization data between an identity provider (IdP) and a service provider (SP). Imagine you want to access a cloud application (the SP), but your company already manages your login credentials (the IdP). SAML acts as the messenger, securely delivering information about your verified identity from your company's system to the cloud application. This allows the cloud application to trust that you are who you say you are, without requiring you to create a separate login for that specific application.

Single sign-on (*SSO*) is the practical application of SAML. SSO allows users to access multiple applications with a single set of credentials. When you log in to your company's network, the IdP generates a SAML assertion. This assertion is then passed to any SP you try to access, automatically logging you in. This seamless process eliminates the need for repeated logins, improving user experience and reducing the risk of weak or reused passwords. SAML is the underlying technology that makes SSO possible, providing a standardized and secure way to share user identity information across different systems.

ExamAlert

Remember that Security Assertion Markup Language (SAML) is an XML-based open standard for exchanging authentication and authorization data between identity providers (IdPs) and service providers (SPs). It enables single sign-on (SSO) authentication, allowing users to access multiple applications or services using a single set of credentials.

IAM and DLP

Identity and access management (IAM) is the system that ensures only authorized individuals can access specific digital resources. Think of it as like a digital gatekeeper: IAM verifies who a user is (authentication) and what that user is allowed to do (authorization) within a network. Central to IAM is the concept of *directory services*, which act as a digital phonebook, storing and organizing user information like usernames, passwords, and access permissions. This allows for efficient management of user identities and their access rights across various applications and systems. See Chapter 45 for more information about Active Directory, a directory service made by Microsoft.

Data loss prevention (DLP) focuses on protecting sensitive information from unauthorized access or leakage. Once IAM grants access to data, DLP steps in to control what can be done with it. DLP solutions monitor and analyze data to detect and prevent its unauthorized transfer, copying, or deletion. For example, DLP might block an employee from emailing confidential customer data to an external address. By combining IAM and DLP, organizations can create a strong security framework that controls both who accesses data and what actions they can perform with it, preventing both unauthorized access and data breaches.

ExamAlert

Know that identity and access management (IAM) comprises the policies, processes, and technologies used by organizations to

manage and control access to resources and systems based on the identities of users and entities within an organization. IAM systems typically encompass user authentication, authorization, provisioning, deprovisioning, and auditing functionalities to ensure that only authorized individuals or entities have access to the appropriate resources, data, and services. Also know that deploying a data loss prevention (DLP) solution is meant to prevent sensitive information from being sent outside of the organization.

SMS

The messaging app is a particularly devious gateway for attackers. Short Message Service (SMS) and Multimedia Messaging Service (MMS) are vulnerable to malware. Unwary users of mobile devices are especially susceptible to Trojans and phishing via SMS texts.

One way to prevent SMS-related attacks is to install mobile antimalware in the form of a mobile security suite. This endpoint protection platform needs to be updated and is best controlled using a mobile device management (MDM) solution. Another way is to use encrypted messaging apps. Yet another is to block messaging apps altogether or to use company-approved messaging apps that are deemed to be more secure. The option chosen depends on what type of mobile environment you are allowing. It will work for some mobile environments where the IT department has more control over devices but might not work for bring-your-own-device (BYOD) environments.

Email Security

Email security is a specialty all its own. You may have heard of the various attacks on email servers over the years; such attacks can filter down to each of the users in an email domain—and it can get ugly. As an A+ technician, you are not expected to secure email servers, but you should have some basic knowledge about email clients.

First, email client software should be updated as often as possible to get access to the latest security fixes. Next, educate your users about how to recognize, avoid, and quarantine malicious emails. These two things are very important! Between updates and user awareness, half the security battle is already done.

Then, it's all about security controls. For example, use encryption and digital signatures. Encryption modifies the contents of an email message, making it difficult (or even impossible) for an attacker to decipher. Digital signatures, on the other hand, use cryptographic hashing to "sign" the email, allowing a user to verify who the email came from. Also, make sure that email clients are using secure servers and ports. (Remember that they are POP3 on port 995, IMAP on port 993, and SMTP on port 465.)

Finally, think of the entire path of email. It's impossible to secure everything, but you might consider using a secure VPN for network access and ensuring that the client OS is updated and has antimalware protection.

ExamAlert

Protect email communications with encryption, digital signatures, secure ports, VPNs, and especially updates and user education.

Note

It's important to prevent spam email. Some methods include using spam filters, strong passwords, allow and deny lists, and user education!

Cram Quiz

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

1. When is a Windows computer completely secure?

- ○ **A.** When you have updated to the latest version
- ○ **B.** When you have locked down the Local Security Policy
- ○ **C.** When Microsoft releases the latest update
- ○ **D.** Never

2. You are moving up in the world and have been tasked with securing a server room. Your manager tells you to design a system that will implement two-factor authentication. Which of the following should you use as your solution to provide the best level of security for the server room?

- ○ **A.** A security guard and an entry control roster
- ○ **B.** A biometric lock and hardware tokens
- ○ **C.** A door lock and an access control vestibule
- ○ **D.** A server cabinet lock and badge readers

3. Which of the following best describes the primary purpose of just-in-time access?

- ○ **A.** Providing permanent access to all network resources
- ○ **B.** Granting temporary privileged access only when needed
- ○ **C.** Encrypting all data stored on network servers
- ○ **D.** Implementing two-factor authentication for all users

4. What is the primary function of authentication in the context of identity and access management (IAM)?

- ○ **A.** Determining what resources a user is allowed to access
- ○ **B.** Verifying a user's identity
- ○ **C.** Preventing data loss through unauthorized transfers
- ○ **D.** Monitoring network traffic for malicious activity

Cram Quiz Answers

1. **D.** Neither Windows nor any other technology is ever completely secure. Complete security is impossible. But you can reduce risk to a certain extent by configuring a system properly and by using technology wisely—ultimately providing *relative* security. Updating to the latest version is often a good idea (if done according to organization policy), but you can't rely on software updates alone. Using the Local Security Policy can help to "lock down" the system to a certain extent, but again, it is only one method. A combination of security updates, security configurations, and user education should be part of an overall security plan.

2. **B.** The most secure solution listed is the biometric lock and hardware tokens. This solution combines two factors of authentication: biometrics (something you are) and hardware tokens (something you have). While the other answers are good security methods, they do not incorporate two factors of authentication, and so they do not provide enough security for today's typical organization. Remember the phrase *defense in depth*, which means layered security. The more layers you have (within reason), the more secure your environment will be.

3. **B.** Just-in-time access is designed to minimize security risks by granting access to resources only when necessary and for the shortest possible time. This reduces the window of opportunity for attackers to exploit compromised credentials. Providing permanent access to all network resources is the opposite of just-in-time access, which seeks to eliminate standing privileges. Although encrypting all stored data is great, it's not the primary function of just-in-time access. Two-factor authentication is also great, but not the purpose of just-in-time access.

4. **B.** Verifying a user's identity is the primary function of IAM. This is typically done through passwords, biometrics, or other means. Determining what resources a user is allowed access to is *authorization*, not *authentication*. Preventing data loss through

unauthorized transfers is the role of data loss prevention (DLP). Monitoring network traffic for malicious activity is handled by intrusion detection systems and intrusion prevention systems (IDS/IPS), which are advanced firewall systems.

Okay, that was some pretty heavy reading. Stretch, review, and let's get back to it. Keep on truckin'!

Chapter 45

Windows Security Settings

This chapter covers the following A+ 220-1202 exam objective:

- **2.2** – Given a scenario, configure and apply basic Microsoft Windows OS security settings.

More security? Yes, more chapters to be sure, but it doesn't end there. You should always be thinking with your information security hat on.

This chapter gets into some fun Windows security settings such as Microsoft Defender Firewall, NTFS permissions, and BitLocker. It's important for you to know how to navigate through Windows, find these various security tools, and use them appropriately. We could discuss Windows security for days, but we have limited space, so we'll stick to the basics! Let's go!

ExamAlert

Objective 2.2 focuses on Defender Antivirus, Defender Firewall, users and groups, log-in OS options, NTFS vs. share permissions, running as administrator vs. standard user, User Account Control (UAC), BitLocker, BitLocker-To-Go, Encrypting File System (EFS), and Active Directory.

The CIA of Computer Security

The main goals of information security are to keep data ***c****onfidential* and keep the ***i****ntegrity* of data intact—all while preserving the ***a****vailability* of data. This is the *CIA triad* of computer security, and you should consider it whenever you are securing hardware, software, data, and the people who use that data. In this chapter, we'll contemplate security as it relates to OS tools, files, folders, users, permissions, and encryption. We'll start with two Windows Security tools: Defender Antivirus and the Defender Firewall.

Microsoft Defender Antivirus

Microsoft Defender Antivirus is Microsoft's built-in antivirus (and antimalware) tool. It runs automatically when Windows is installed. This tool is part of the *Windows Security* suite of programs and settings. You can access Windows Security in several ways, including

- Go to **Start > Windows Security**.
- Search for **windows security**.
- Go to **Run** and type **windowsdefender://**.
- In Windows 11, navigate to **Windows Settings > Privacy & Security > Windows Security**. Then click on the **Open Windows Security** button.
- Once you have accessed Windows Security, click **Virus & threat protection**. From there, you can run a quick scan of the system for viruses and check for updates to the Defender Antivirus program. You can also click **Manage settings** to make configuration changes to the program. For example, perhaps your organization uses a separate third-party antimalware suite. From Manage settings, you can turn off real-time protection so that the two programs do not conflict with each other. You can also enable cloud protection and modify how Windows alerts you about viruses.

Microsoft Defender Firewall

Microsoft Defender Firewall is meant to protect client computers from malicious attacks and intrusions, but sometimes it can be the culprit when certain applications fail. You can access Microsoft Defender Firewall in a couple of ways:

- The Windows Settings access method: Access **Windows Security** as described previously and then click **Firewall & network protection**.
- The Control Panel access methods:
  - Select **Control Panel > View by: Small or Large Icons > Windows Defender Firewall**.
  - Select **Run > firewall.cpl**.

> **Note**
>
> As of Spring 2025, Microsoft was in the process of renaming Windows Defender Firewall to Microsoft Defender Firewall, and both names appear in Windows. They are the same product. When we reference them in this book, either in text or in images, know that it's because the versions of Windows we're using are, like yours, updated frequently and sometimes the names change daily. Eventually we believe that the new name will become Microsoft Defender Firewall, so have attempted to standardize on that name throughout the book, but you might see the other name sometimes. For now, in Settings, it is called Microsoft Defender Firewall; however, in Control Panel, it is still Windows Defender Firewall.

From here, you can enable or disable Microsoft Defender Firewall for the private network, public network, and domain network. (In the Control Panel, you will see **Guest or public networks** instead of *domain*.) By default, these are "on," or "connected." As with Defender Antivirus, you might decide to disable Microsoft Defender Firewall and instead use the third-party firewall that your organization uses. Always verify that at least *one* firewall is enabled!

When Microsoft Defender Firewall is on, the default setting is to shield all inbound ports (effectively closing them). This is a type of default *port security*, and it means that certain applications that need to communicate with a remote host might not work properly. Or if a client computer wanted to host some services (such as FTP or a web server), the firewall would block them. That's where exceptions come in. You can still use the firewall, but you can specify applications that are exceptions to the rule. Figure 45.1 shows an example of exceptions made on a Windows 11 Pro computer. To create exceptions in Windows Security, click **Allow an app through the firewall**. To create exceptions in the Control Panel version, click **Allow an app or feature through Windows Defender Firewall**. Either method takes you to the Allowed apps window.

Figure 45.1 shows that two applications are not blocked from incoming connections. Remote Assistance is not blocked at all—not on the Private profile and not on the Public profile. Remote Desktop is allowed only on the Private profile. So, as long as the firewall is enabled, this computer can make Remote Assistance calls to other users on the Internet. But if a person wants to connect to this system through Remote Desktop without an invitation, that person must be on the LAN to succeed. With these settings, you are not sacrificing the security of the entire system. All other incoming connections will be blocked.

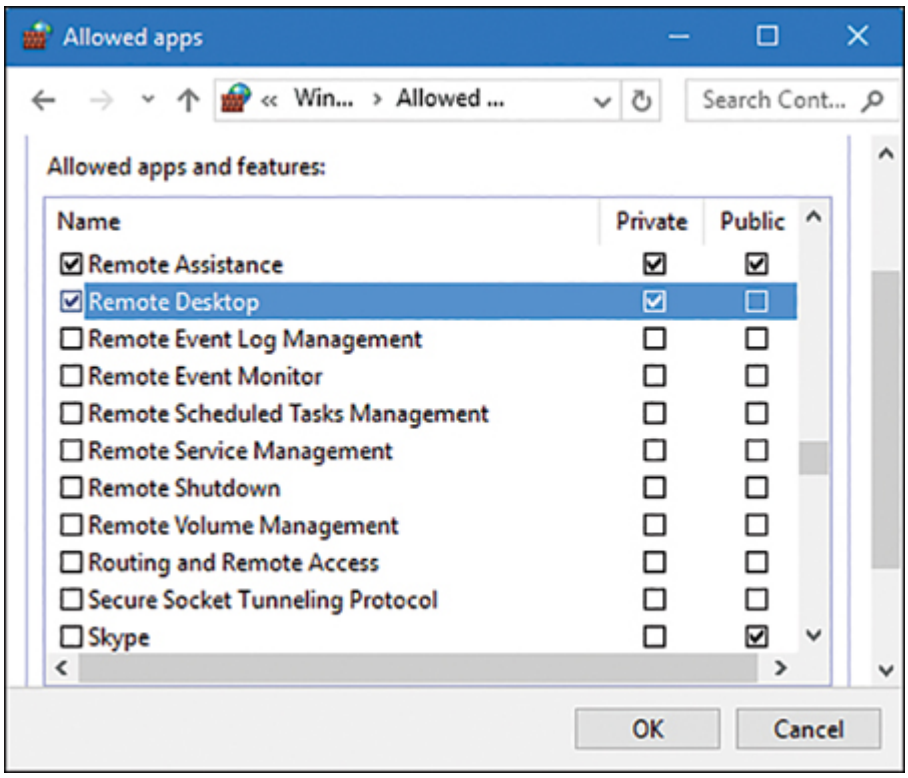


FIGURE 45.1 **Firewall Exceptions**

Let's get more in depth with the firewall settings. By clicking the **Advanced Settings** link, you can make use of Microsoft Defender Firewall with Advanced Security (also available in Windows Tools and as a snap-in in the Microsoft Management Console, MMC). You can also get to this by opening the **Run** prompt and typing **wf.msc**. From here, you can get more in depth with application restrictions. For example, you can create inbound and outbound rules for individual applications based on the private network, the public network, or both. You can also configure the firewall with the **netsh** command or within PowerShell. (For more information, see https://tinyurl.com/WFDAS.)

If Microsoft Defender Firewall gives you errors when you attempt to update the firewall settings, add exceptions, or access the advanced settings, make sure the Microsoft Defender Firewall service is enabled and running in **services.msc**.

Essentially, a firewall is a packet filter that uses *access control lists (ACLs)* to specify what packets can pass through. ACLs are composed of source

and destination IP addresses and ports, as well as the type of packets to be allowed or denied. ACLs are written differently depending on the device or program you are using. In Windows, they can be written using PowerShell or configured graphically using Microsoft Defender Firewall with Advanced Security.

Users and Groups

Users are what it's all about when it comes to Windows security. On a Windows client computer, you have two options: Microsoft accounts and local users. Microsoft accounts are accounts that are associated with email addresses. But you can also create local user accounts that do not need email addresses or Microsoft accounts. However, know that Windows 11 is heavily pushing Microsoft accounts for the initial user. While there are ways to bypass this—mainly not connecting to the Internet during initial setup and letting it default back to local accounts—it is advised to create a Microsoft account for the initial user.

Both types of user accounts have a variety of logon options for authentication purposes. You can change your authentication method by going to **Windows Settings > Accounts > Sign-in options**. The following is a partial list of sign-in options in Windows:

- **Username and password:** This is often a default setting. When you log on to Windows, you select the user account from the screen (or type the username) and then type the password. The username/password authentication method has been the industry standard for decades, but it's important to use a complex password, as we will discuss in Chapter 48, "Workstation Best Practices."
- **Personal identification number (PIN):** You can choose a numeric passcode to access Windows. You can also choose to allow letters and special characters. Initially, this seems to be just like a password, and in that thinking you should make a complex password. However, a major difference is that the PIN is tied to the specific hardware it's on. In other words, even if someone captured your pin, as opposed to your password, it would only work on that specific piece of hardware. This is part of Windows Hello.

- **Fingerprint:** If your device has a biometric reader, you can incorporate fingerprint authentication. Some laptops have these readers built in, or you could use an external USB-based fingerprint reader. This is part of Windows Hello.
- **Face:** You can use advanced facial recognition to sign in to Windows. You must have an IR camera to allow for depth sensing. This is part of Windows Hello.
- **Security key:** You can use a USB-based physical token that houses an encryption key for authentication purposes.
- **Picture password:** With this option, you select a picture to use and then "draw" on the touchscreen to have the system save your gesture. Every subsequent logon requires this gesture.

Windows Hello is a *passwordless authentication*, meaning it doesn't rely on the traditional username and password schema. Rather, with the exception of the PIN option, it uses biometric authentication. This biometric data is stored in the Trusted Platform Module (TPM) on the motherboard, so it is virtually impossible to hack. Even the PIN option, while not biometric, is still tied to the individual hardware. This is part of a larger movement across the industry to leave the traditional username/password schema that is so vulnerable to being stolen and used to gain access to people's personal accounts.

Objective 2.2 also makes mention of single sign-on (SSO). SSO means that you can use one logon to access all the systems and networks you need. To a certain extent, the Microsoft account is an example of SSO because it can allow a person access to the local computer as well as Microsoft OneDrive and other cloud-based resources. This, in combination with Windows Hello's biometric login options, makes for simple but powerful security login options.

Note

You can configure Windows users for enterprise-level single sign-on (SSO) authentication. This generally requires a domain, Microsoft Identity Manager, Azure, or OpenID Connect (and often a

combination of these). For more information, see https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-single-sign-on.

Note

The rest of this section shows how to work with local accounts.

You can accomplish basic user account creation from within Settings or the Control Panel, but in this section, we will focus on the more useful Local Users and Groups, which you can access from Computer Management or directly by going to **Run** and typing **lusrmgr.msc**.

There are six main types of user account levels you should know for the exam:

- **Administrators:** These users have full (or nearly full) control of an operating system. They are the most powerful accounts in Windows and have access to everything.
- **Standard users (also simply referred to as users):** These users are the normal accounts for people who can log on to the network. A standard user account has access to (owns) data but cannot access the data of any other user and, by default, cannot perform administrative tasks (such as installing software).
- **Local account:** This account resides solely on your specific Windows 11 device. It allows you to use the computer, install software, and personalize settings, but your data and settings are not synchronized across multiple devices. It functions independently of Microsoft's online services and is not linked to a Microsoft account.
- **Microsoft account:** This account is linked to your Microsoft online profile. It provides access to synchronized settings, files (via OneDrive), Microsoft Store apps, and other Microsoft services across multiple

devices. It requires an Internet connection for full functionality and offers features like password recovery and device tracking.

- **Guest:** These users have limited access to the system. A guest cannot install software or hardware, cannot change settings or access any data, and cannot change the password. A guest account is sometimes used for temporary workers or vendors who may need temporary access. The guest account is disabled by default.
- **Power users:** These users are included in Windows for backward compatibility with older versions of applications.

> **ExamAlert**
>
> Know the Windows user accounts and groups, including administrator, local account, Microsoft account, power user, guest, and standard user. Know what they can and cannot do!

All of these types of users are actually groups within Windows client operating systems (such as Windows 11). If you access the Local Users and Groups window and click the **Groups** folder, you will see these groups and many more (for example, Backup Operators, Remote Desktop Users, and so on). There are, however, individual administrator and guest accounts (located in the Users folder) that are built into the system.

You can create users by clicking the **Users** folder and then clicking **Action > New User** or by right-clicking in the user list work area and selecting **New User**. Either option brings up the window shown in Figure 45.2.

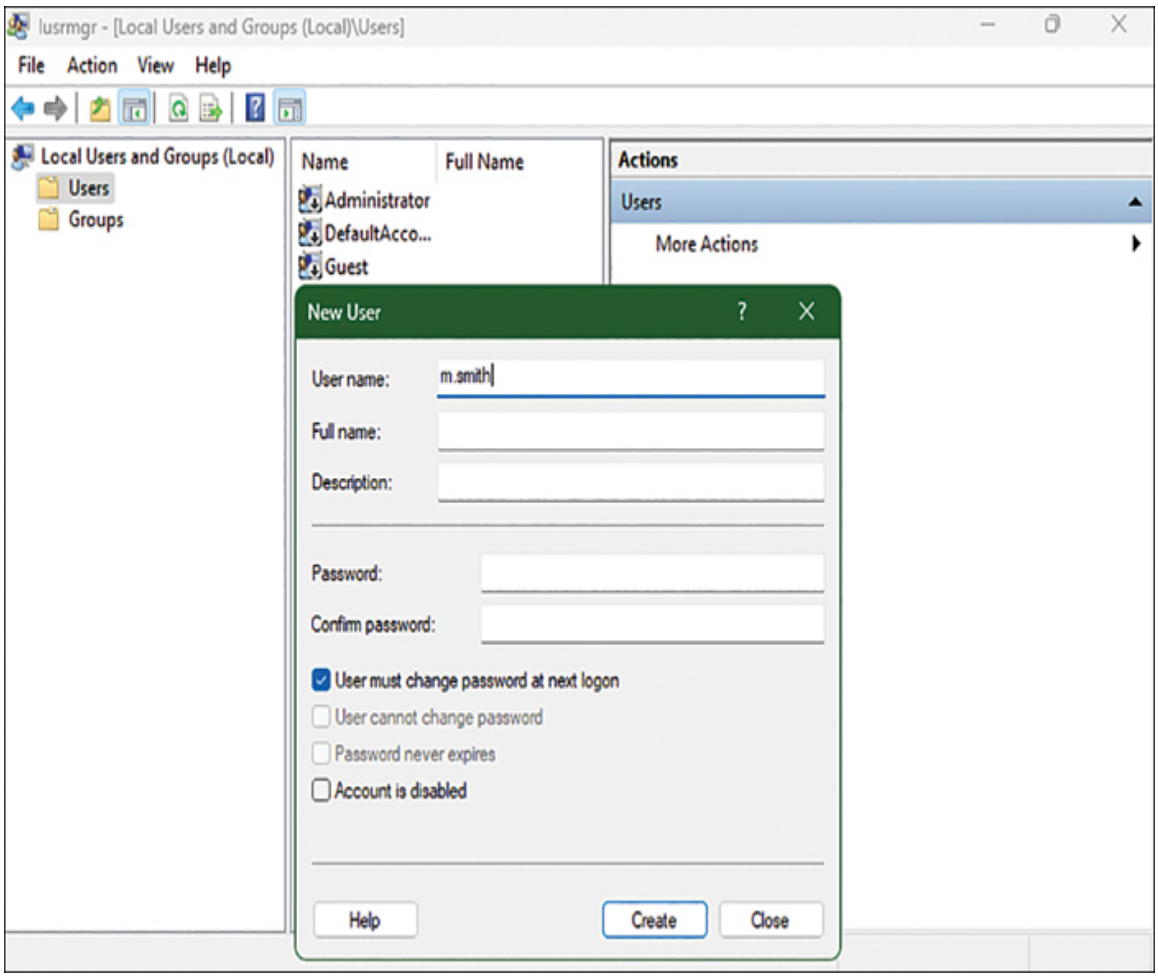


FIGURE 45.2 **New User Window**

Try going through the process now. At a bare minimum, you'll be required to type a username. You can fill out other information as well, including the user's full name and a description of the user. By default, the option **User must change password at next logon** is selected, so you don't have to select a password. In some scenarios, the system administrator supplies the password. With this option, you, as the admin, would have to type the password (and confirm it), deselect the first checkbox, and then select **User cannot change password**. The password will have to comply with any password policy that has been set (in terms of length, complexity, etc.). Keep in mind that this is not the most secure way to do things, but it might be necessary in some cases. Also note that there is a checkbox called Account is disabled. You can disable an account temporarily by using this option, but generally you would work with that setting after the account is

created (from the account **Properties** dialog box > **Account** tab). For example, if a user fails to log on with the correct password after *x* number of attempts (as set in a Group Policy), the account will become disabled, and the administrator will have to deselect the checkbox to enable the user to log on. If a person leaves an organization or is terminated, you should immediately disable the account so that the user cannot log on anymore.

By default, when a user is first created, the user is automatically given group membership to the Users group and performs as a standard user. However, you can add members to other groups if you need to (for instance, if you need to have a second administrator). To do this, right-click the user account, select **Properties**, and then click the **Member Of** tab. The Select Groups dialog box pops up, as shown in Figure 45.3, and you can either type the name of the group you want to make the user a member of or browse for it.

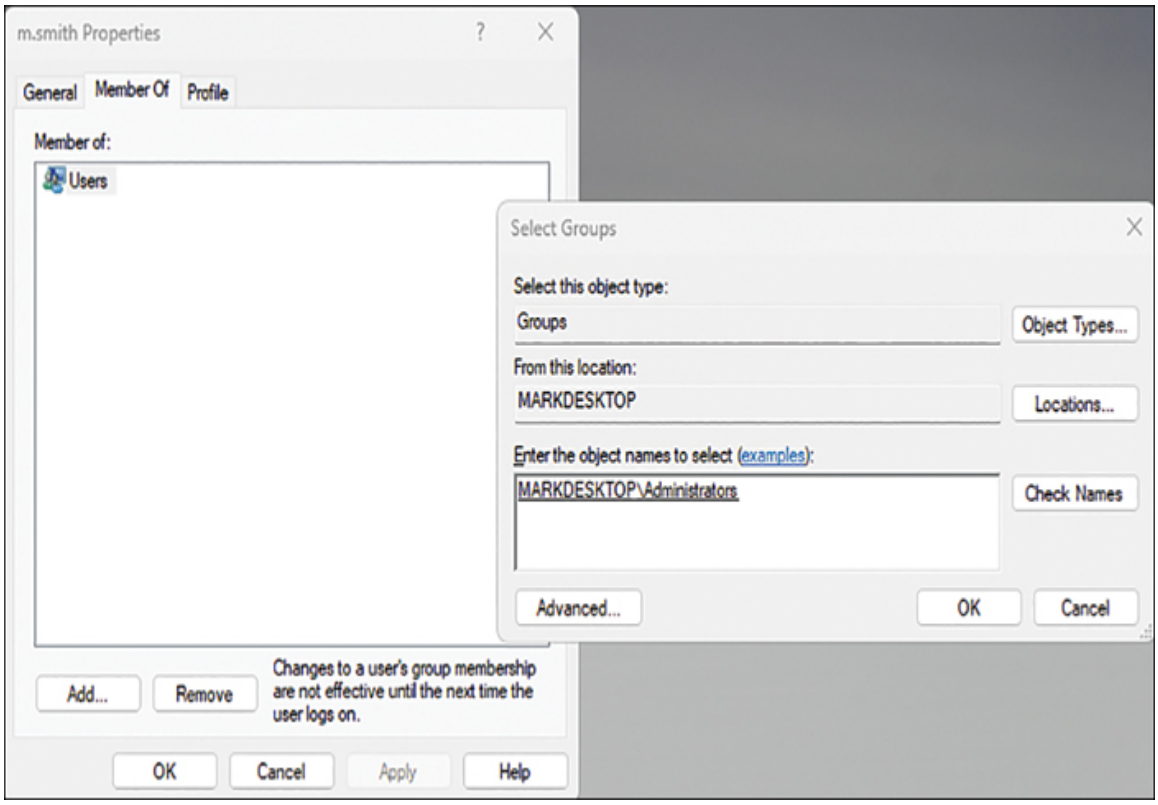


FIGURE 45.3 **Group Membership in Windows**

In Figure 45.3, the user m.smith is currently a member of the Users group, but we are in the process of adding that user to the Administrators group. Be careful who you add as an admin because that person will now get full control!

Restrict Administrator Access!

Some end users like to play with systems—which can often result in disaster. Case in point: Have you ever heard of God Mode for Windows? It displays almost every configuration window an administrator could want in one big list. It's easy to access: Just create a new folder on the desktop (or anywhere else) and rename the folder to the following:

```
GodMode.{ED7BA470-8E54-465E-825C-99712043E01C}
```

That will create the custom control panel, and you will have access to *many* functions in one window. This capability is great for actual administrators, but a typical user can use it to wreak havoc.

We can't stress enough how important it is to restrict administrative access. Typical users should *not* be administrators—period. They shouldn't be added to the administrators group, nor should they be allowed to gain administrative privileges through UAC or by knowing an admin's password. Remember the principle of least privilege. Make sure that account privileges and permissions are set so that typical users get the least access necessary!

Permissions

Folders and files can be assigned permissions, which allow users a particular level of access to the data. There are two levels of permissions, which are configured in the Properties window of a folder or a file:

- **Share permissions:** These permissions can be accessed from the Sharing tab. By default, the Everyone group has Read (read-only) access. The other two permissions available are Change and Full Control.
- **NTFS permissions:** These permissions are accessed from the Security tab. There are six default levels of permissions, from Read to Write to Full Control, as shown in Figure 45.4.

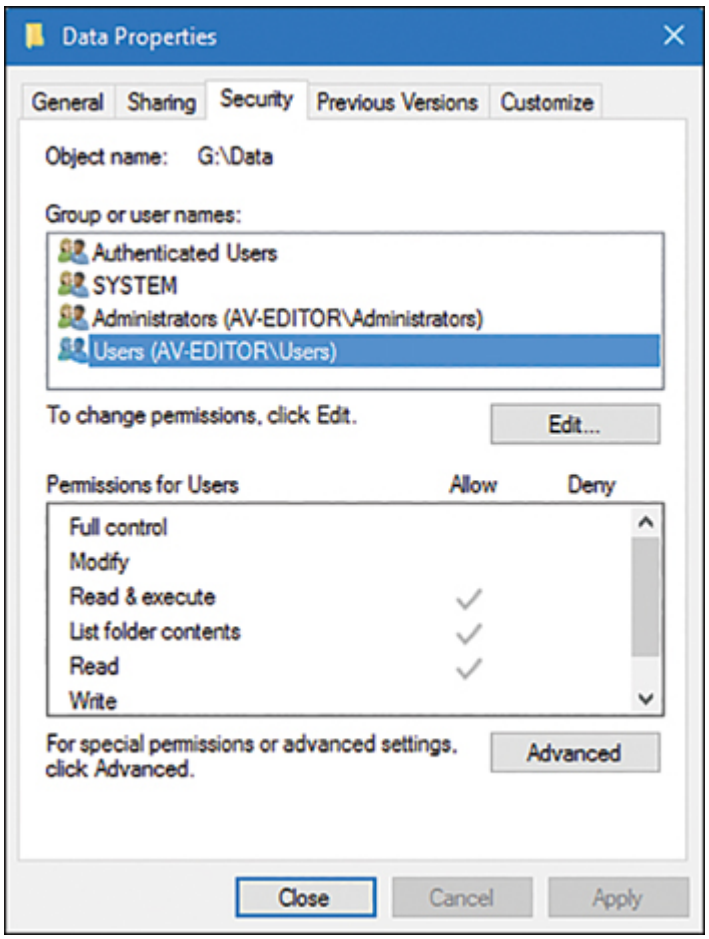


FIGURE 45.4 **Security Tab of a Folder's Properties Window**

If you happen to be using both Share and NTFS permissions, the most restrictive of the two will take precedence. So, for example, if a user was given Full Control access for Share permissions and only Read access for NTFS permissions, the user would ultimately have only the Read permission.

ExamAlert

NTFS permissions are modified in the Security tab of the folder's Properties window.

The weakest of the NTFS permissions is Read and the strongest, of course, is Full Control. Administrators have Full Control by default. Typical users have only Read, List Folder Contents, and Read & Execute by default. Note the options Allow and Deny, which can be assigned for a particular user or for a user group (hence the term *user-level security*). Generally, when you want users to have access to a folder, you add them to the list and select Allow for the appropriate permission. When you don't want to allow them access, normally you simply don't add them. But in some cases, an explicit Deny is necessary. This could be because the user is part of a larger group that already has access to a parent folder, but you don't want the specific user to have access to this particular subfolder.

Permission Inheritance and Propagation

If you create a folder, its default action is to inherit permissions from the parent folder. So any permissions that you set in the parent will be inherited by the subfolder. To view an example of this, locate any folder within an NTFS volume (besides the root folder), right-click it, select **Properties**, access the **Security** tab, and click the **Advanced** button. Figure 45.5 shows an example of this in Windows 11. (Names and navigation will be slightly different in other versions of Windows.)

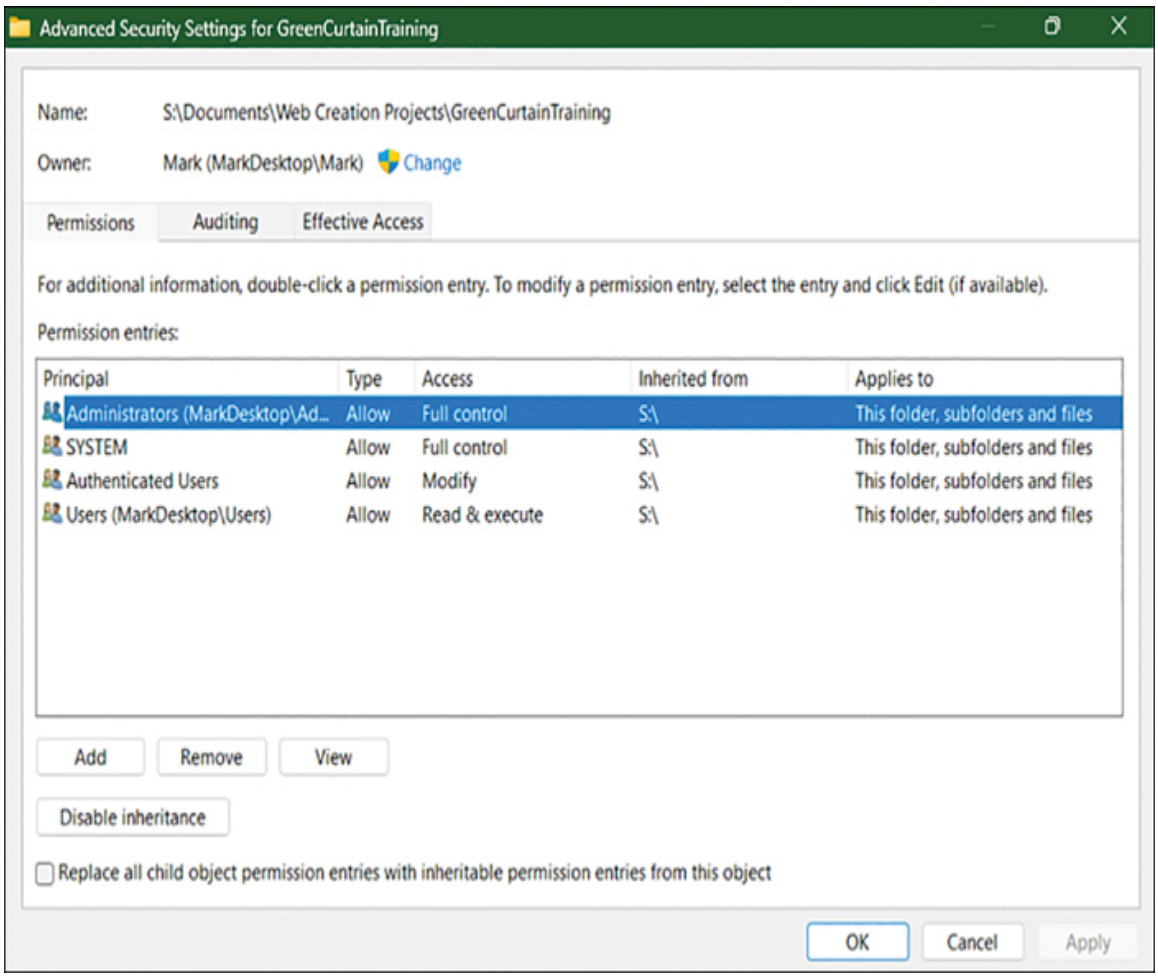


FIGURE 45.5 **Advanced Security Settings Window**

What this all means is that any permissions added or removed in the parent folder will also be added or removed in the current folder. In addition, permissions that are inherited cannot be modified in the current folder. To make modifications in this case, click the **Disable inheritance** button (or deselect the corresponding checkbox in earlier versions of Windows). When you do this, you have the option to copy the permissions from the parent to the current folder or remove them entirely. So, by default, the parent is automatically propagating permissions to the subfolder, and the subfolder is inheriting its permissions from the parent. You can also propagate permission changes to subfolders that are not inheriting from the current folder. To do so, select the **Replace all child object permission entries with inheritable permission entries from this object** checkbox. (Again, names will vary according to the version of Windows.)

This description might seem a bit confusing. You probably will not be asked many exam questions on the subject. Just remember that folders automatically inherit from the parent unless you turn off inheriting, and you can propagate permission entries to subfolders at any time by selecting the **Replace** option.

Note

One other concept you should know that is not listed in the objectives is *ownership*. By default, Windows uses discretionary access control (DAC), which means the creator of a file or folder is the owner. This means that only that person can assign permissions to that file or folder. However, an administrator can change who the owner is simply by clicking the **Change** link that is shown in Figure 45.5. So, the administrator can take ownership and subsequently change permissions if needed.

Moving and Copying Folders and Files

This subject (like the previous one) is actually an advanced Microsoft Windows concept, so we'll try to keep this section simple. *Moving* and *copying* folders and files have different results when it comes to permissions. Basically, it breaks down like this:

- When you copy a folder or file on the same volume or to a different volume, it *inherits* the permissions of the parent folder it was copied to (known as the target directory).
- When you move a folder or file to a different location on the same volume, it *retains* the original permissions.
- When you move a file to another volume, it *inherits* the permissions of the parent folder.

Note

Keep in mind that when you move data within a partition, the data isn't actually relocated; instead, the pointer to the file or folder is modified.

File Security

Files can be assigned four different attributes in Windows: read-only, hidden, compression, and encryption. To access these attributes, right-click any file and select **Properties**. On the General tab, you will see the Read-only checkbox; if this is checked, no one can save modifications to the file, but a new file can be saved with the changes. Checking the **Hidden** checkbox makes the file invisible to all users except the user who created the file. Admins can unhide files individually or for an entire system, as we will explain in a moment. When you click the **Advanced** button, you see two checkboxes: **Compress contents to save disk space**, which allows you to convert the file to a smaller size that takes up less space on the drive, and **Encrypt contents to secure data**, which scrambles the file content so only the user who created the file can read it. We'll discuss encryption later in this chapter.

Note

The **attrib** command at the Command Prompt can modify the read-only, archive, system, and hidden attributes for files and display the attributes for each file. This older command is still available in Windows but is not used often. For more information about this command, see https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/attrib.

System files and folders are hidden from view by the OS to protect the system. In some cases, you can simply click the **Show the contents of this folder** link, but to permanently configure the system to show hidden files and folders, you need to navigate to the File Explorer Options dialog box. (An example of this is shown in Figure 36.2 in Chapter 36, "Windows

Control Panel Utilities.") Then select the **View** tab and, under Hidden files and folders, select the **Show hidden files, folders, and drives** radio button. To configure the system to show protected system files, deselect the **Hide protected operating system files** checkbox, located below Show hidden files and folders. This enables you to view files such as bootmgr, pagefile.sys, and hiberfil.sys.

ExamAlert

To view files such as bootmgr, pagefile.sys, and hiberfil.sys, select the **Show hidden files** radio button and deselect the **Hide protected operating system files** checkbox.

Administrative Shares

Folders and files need to be shared so that other users on the local computer and on the network can gain access to them. Windows operating systems use an access control model for securable objects such as folders. This model takes care of rights and permissions, usually through discretionary access control lists (DACLs) that contain individual access control entries (ACEs). You can find all the shared folders by navigating to **Computer Management > System Tools > Shared Folders > Shares** or directly by going to **Run** and typing **compmgmt.msc**. In Figure 45.6, you can see that we have shared a folder named Data, which is also known as a local share.

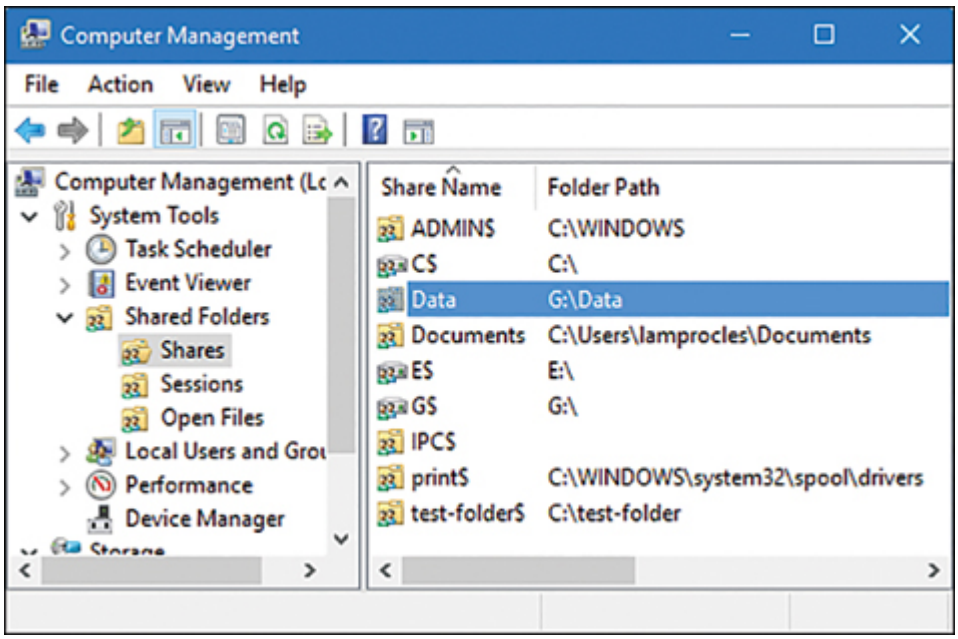


FIGURE 45.6 **Windows Shares**

Here, you can also see the hidden administrative shares, which can be identified by the $ on the end of the share name. These shares cannot be seen by standard users when browsing to the computer over the network; they are meant for administrative use. Note that every volume (C:, E:, and G:, for example) has an administrative share. Although it is possible to remove these shares by editing the registry, this is not recommended because it might cause other networking issues. You should be aware that only administrators should have access to these shares. Hidden shares can be created by simply adding *$* to the end of the share name when enabling the share. Administrative/hidden shares can be accessed only if the user knows the exact network path to the folder and has permissions to access it.

ExamAlert

Hidden/administrative shares can be identified by the $ on the end of the share name.

Encrypting File System

Encryption is the process of converting information with the use of a cipher (algorithm), making it unreadable by other users unless they have the correct "key" to the information. Cryptography is the process of hiding information. In a cryptosystem, information is protected by being disguised.

A few different encryption technologies are used in Windows. For example, whenever you log on to a Windows network, that authentication is secured with the Kerberos protocol. As another example, when you want to encrypt one or more files or folders, Windows uses Encrypting File System (EFS), a component of NTFS. Follow these steps to encrypt a file in Windows:

1. Locate the file you want to encrypt, right-click it, and select **Properties**. This brings up the General tab within the file's Properties window.
2. At the bottom of the General tab, click the **Advanced** button. This brings up the Advanced Attributes window.
3. Check the box labeled **Encrypt contents to secure data**.
4. Click **OK** for both windows. (When you do so, the system should ask whether you want to encrypt the parent folder and the file or just the file. It's recommended that the file's parent folder be encrypted as well.)

To unencrypt the file and return it to normal, simply deselect the **Encrypt contents to secure data** checkbox.

Note

You can color-code encrypted and compressed NTFS files. You do this in the Folder Options dialog box by clicking the **View** tab and selecting **Show encrypted or compressed NTFS files in color**. After you select that option, a green filename indicates an encrypted file, and a blue filename indicates a compressed file.

If a file needs to be decrypted and the original user (the owner of the key or certificate) isn't available, an EFS recovery agent needs to be used. In many

cases, the default recovery agent is the built-in administrator account. It is important to note a couple more items: EFS isn't designed to protect data while it is transferred from one computer to another; in addition, EFS is not designed to encrypt an entire drive.

BitLocker Encryption

To encrypt an entire disk, you need some kind of full disk encryption software. Several options are currently available on the market. One of them, developed by Microsoft, is called BitLocker, and it is available only on select editions of Windows (such as Pro, Pro for Workstations, and Enterprise). BitLocker uses a type of encryption known as *data-at-rest*. This means data that is stored on the local computer and not being transmitted through the network.

> **Note**
>
> Data-at-rest is data that is stored or retained in a persistent storage medium, such as a hard disk drive (HDD), solid-state drive (SSD), tape drive, or optical disc, and is not actively being accessed or transmitted.

BitLocker software can encrypt an entire disk, which, after it's completed, is transparent to the user. However, there are some requirements for this. You need either of the following:

- A Trusted Platform Module (TPM) chip, which is a chip residing on the motherboard that actually stores the encrypted keys.
- An external USB key to store the encrypted keys and a storage drive with two volumes, preferably created during the installation of Windows. One volume (most likely C:) is for the operating system that will be encrypted; the other is the active volume that remains unencrypted so that the computer can boot. If a second volume needs to be created, that can be done in Disk Management, and the volume can then be accessed by BitLocker.

ExamAlert

Know the components necessary for BitLocker: a TPM or USB key.

To use BitLocker, you can search for it in Windows Settings or go to **All Control Panel Items > BitLocker Drive Encryption**. BitLocker software (like EFS) is based on Advanced Encryption Standard (AES) and uses a 128-bit key by default, though it can be increased to 256-bit in the Group Policy Editor. Keep in mind that a drive encrypted with BitLocker usually suffers in terms of performance compared to a nonencrypted drive and could have a shorter shelf life as well. By default, BitLocker is used to encrypt the internal drive of a system. However, you can also encrypt USB drives and other removable devices by using BitLocker-To-Go. This is also done in the same place that BitLocker is used. Once inserted, a USB drive or other removable media will be recognized by the program automatically.

Note

Need to increase BitLocker's AES cipher strength to 256-bit? Open the Local Group Policy Editor (**Run > gpedit.msc**) and go to **Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption** and enable and configure the policy for your version of Windows.

Run As

Remember that standard users can't do very much in Windows. You need to run a lot of these configuration programs as an administrator—meaning in elevated mode. Generally, right-clicking an app and selecting **Run as administrator** is enough. For more options, see Chapter 34, "Microsoft Command-Line Tools, Part I." Also, Objective 2.2 makes mention of User Account Control (UAC), and we discuss UAC briefly in Chapter 44, "Logical Security."

Active Directory

We don't cover too much concerning servers in this book, but this section is an exception. Get ready for a crash course on Active Directory (AD)!

A Microsoft *domain* is a network of Windows computers that is controlled by a Windows Server that has Active Directory installed; that server is a *domain controller*. Active Directory is a Microsoft directory service that centralizes the management of user accounts, computer accounts, and so on for a domain.

ExamAlert

Know that a domain is Microsoft's implementation of a client/server network. It centralizes the management of users and computers.

For a user to log on to the domain, that person must have a user account on the domain controller, and the user must know the username, password, and the domain to be logged on to (for example, dpro42.com). In addition, the Windows client computer must have been previously configured to connect to the domain.

The user account is stored within the domain in one of two places: within the Users folder (which is the default) or within an organizational unit that the administrator has created. Take a moment to analyze Figure 45.7.

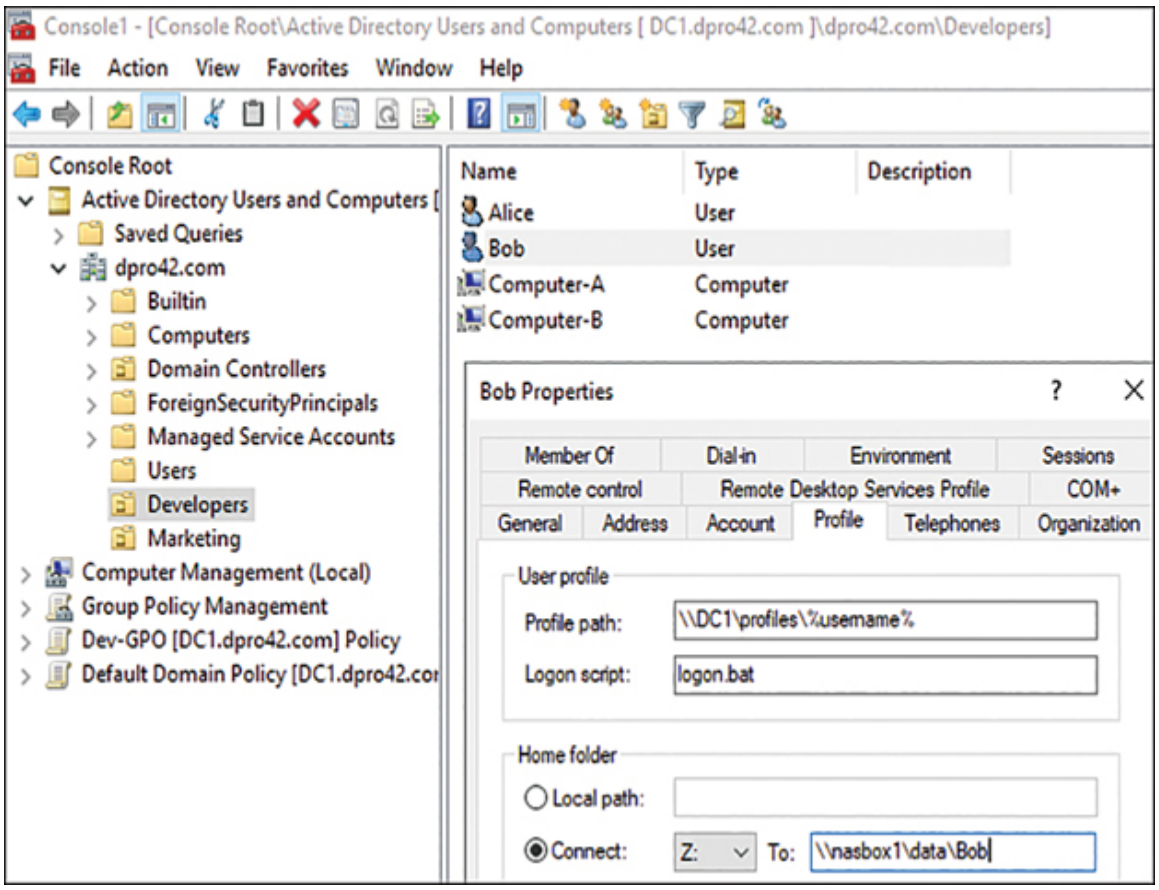


FIGURE 45.7 **User Account Stored on a Domain Controller in Active Directory**

We packed a lot of stuff into Figure 45.7. Here, you see a Windows server that is acting as a domain controller (which means it has AD installed). It shows Active Directory Users and Computers, which, as the name implies, is where you go to add, remove, and configure user accounts and computer accounts. (We actually added it to an MMC along with a few other snap-ins.)

By default, users are created within the Users folder, which you can find by following the path **Active Directory Users and Computers > *Domain Name* > Users**. dpro42.com is the domain name we chose for this Microsoft network. Note that you do not have to own the domain if it is only used as an internal network, so name it whatever you want! The Users folder has lots of built-in users and groups to work with. However, as mentioned, you can also add users to an *organizational unit (OU)*, which is a container that

you can use to categorize users and computers. Also, you can apply separate group policies for different OUs. This allows you to configure different rules for each set of users, groups, and computers, from one OU to the next. There's a *lot* more to it, but this should suffice for the A+ exam.

Generally, we set up OUs to mimic an organization's departments. So, Figure 45.7 shows that we've created two OUs: Developers and Marketing. The Developers OU is selected, and on the right you can see two users and two computers within that OU: Alice, Bob, Computer-A, and Computer-B (all of which we created).

Furthermore, the user account Bob is selected, and you can see that we have opened the Properties dialog box for Bob. In this figure, you can see the Profile tab. This is where you can set up a profile path, logon script, and home folder for the account. Let's discuss each of these briefly.

User Profiles

Every user account gets a profile, which is a group of folders and settings based on how users configure their desktop environment: Start menu options, desktop icons, background color, and so on. By default, when a user first logs on to a computer, a *local* profile is created and stored on that computer. For example, in Windows 11, this profile is stored in C:\Users*%userprofile%*, where *%userprofile%* is a variable for whichever user is currently logged on. You can get to the currently logged-on user's profile folder by going to **Run** and typing **%userprofile%** or **%homepath%**. Windows displays the profile folders and—if you are showing hidden files—the NTUSER.DAT file, which is what Windows actually uses to store the profile data.

Now, if you would like a user's profile to follow the user from one computer to the next on a domain, you want a *roaming* profile. That's a profile that is stored on a server. And that's where the Profile path field in Figure 45.7 comes in. The figure shows the location of this user's roaming profile configured as \\DC1\profiles\%username%. *DC1* is the computer where the profile is stored. In this case, it is the domain controller that is being used, but it might be stored somewhere else, and it's probably a good idea to store it elsewhere. *profiles* is the share name for the folder where all

the user profiles are stored. *%username%* is another variable, which takes the place of the account name. (We could have used Bob if we'd wanted to, with the same result, but you can appreciate the power of a variable, especially if you will be working with a lot of accounts.) As long as the path to the profile is valid, the domain controller will store it there, and the user can log on to various computers on the network, and the profile will follow the user around.

Logon Script

A logon script (referred to as a *log-in* script in A+ Objective 2.2) is used to assign tasks that are executed when the user logs on to the domain. It could assign tasks like running programs, mapping network drives, setting variables, updating antimalware applications, running commands, and calling other scripts. The idea is to automate the configuration process for a user's environment and workflow so that the user can simply sit down, log on, and start working. In Figure 45.7, the script is called logon.bat. Who knows, maybe some command-line functionality is included in the script; for example, perhaps a particular program such as Excel is opened up, or maybe the user receives a welcome message when logging on. Imagine the power of scripting! In the figure, logon.bat is the name, which means it is a batch file, but you often use PowerShell to create scripts too. (PowerShell scripts use the .ps1 extension.) Whatever you use, the file has to be stored—either in the default location on the server (NETLOGON) or elsewhere, in which case the path to the file location must be entered into the field in addition to the filename.

In Windows Active Directory, assigning a log-in script automates tasks upon user login. This is primarily done through Group Policy Objects (GPOs).

1. Scripts, often batch files (.bat) or PowerShell scripts (.ps1), are placed in the Netlogon share on a domain controller.
2. Using the Group Policy Management Console, you edit a GPO that applies to the desired users or organizational units (OUs).

3. Within the GPO's User Configuration, under Windows Settings, you'll find the Scripts (Logon/Logoff) section.
4. Here, you specify the path to your script, which will then execute when the targeted users log on. This allows for tasks like mapping network drives or setting printer configurations.

Home Folder

The home folder is where a user stores documents by default. Look again at Figure 45.7. If you select the **Local path** option, stored documents will end up at the local computer where the user is sitting. However, the idea behind having a Microsoft domain is that it enables you to centrally store files. So, in many cases, you will select **Connect:** and use a mapped network drive (such as Z:) to a path. This is known as *folder redirection*.

In Figure 45.7, Z: is mapped to *nasbox1*, which has a share called *data*, and finally to a folder named *Bob*. This way, regardless of what computer Bob logs on to, data will be stored to the Z: drive.

Note

The last three concepts (profile, logon script, and home folder) can be used on a local Windows system as well. Just go to **Local Users and Groups > Users**, right-click the user in question, select **Properties**, and then go to the **Profile** tab. The same options are there, but they are limited when there is no domain in use. The whole concept here is that having a domain allows you to centralize data, profiles, and home folders; everything is more organized and more easily monitored, and that *usually* equates to more security. By the way, Local Users and Groups can be added to an MMC or can be accessed from Computer Management.

Group Policy

Group policies are part of Windows, whether you are working at a local system or within a domain. They house all of the rules that users must abide by within the OS—for example, what programs they can use, and when passwords have to be changed. There are hundreds of policies that can be modified to secure a system. In a domain environment, there is a default domain policy, which is stored on the domain controller; it affects all typical users that are created. However, you can create separate policies for users that are organized into OUs. In the left pane in Figure 45.7 you can see a policy named Dev-GPO [DC1.dpro42.com] Policy. That is a policy that we created just for the Developers OU, with its two users and two computers. It could be that we want those users to have even longer passwords than the rest of the users on the domain. We can ensure that by modifying the Dev-GPO Policy.

On the local system, you can modify the group policy by going to **Run** and typing **gpedit.msc**, which opens the Local Group Policy Editor. Two of the policies that you will most commonly modify are the Password Policy and Account Lockout Policy. These can be accessed quickly by going to **Run** and typing **secpol.msc**, which brings you to the Local Security Policy console window, a subset of the entire Group Policy. Figure 45.8 shows an example of this window on a Windows 11 Pro computer, with the Password Policy opened. Policy modification is essentially the same, regardless of whether the policy is stored on a local Windows client or on a Windows domain controller.

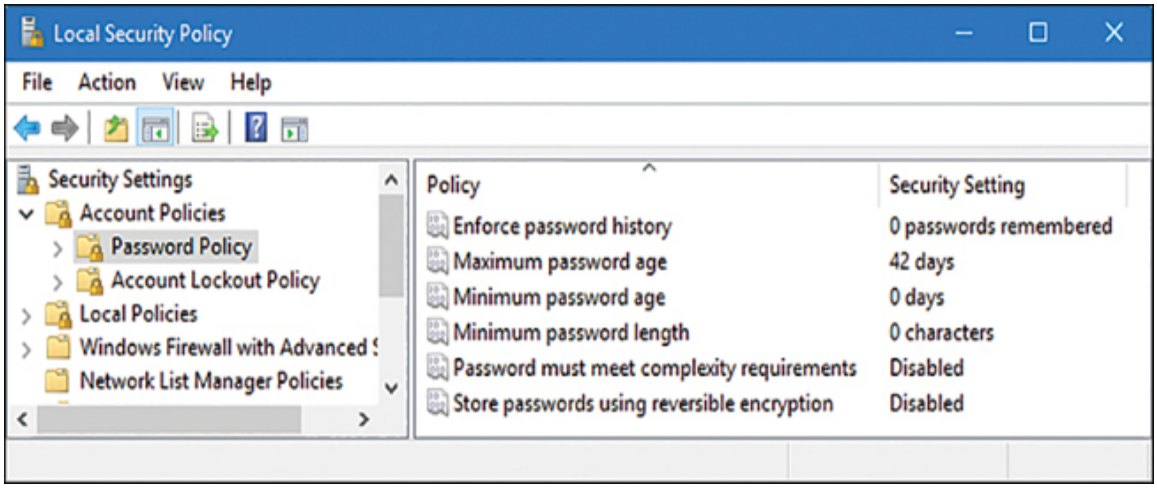


FIGURE 45.8 **Local Security Policy Opened to the Password Policy**

ExamAlert

Know how to access and configure the Group Policy Editor (**gpedit.msc**) and the Local Security Policy (**secpol.msc**).

Some changes take effect immediately, but some require further action. So, when you are finished configuring group policy, you should either log off and back on or restart the computer or, better yet, run the **gpupdate** command so that the group policy entries are updated in the operating system.

Security Groups

Security groups in Active Directory provide an efficient way to set permissions and assign access to resources in a Windows domain.

You can build custom security groups, but to leverage Active Directory out of the box, you use the built-in security groups. One example of a built-in security group is the Domain Admins group. This group is created automatically when you create a Windows domain by installing Active Directory on a Windows server. Members of the Domain Admins group have full control of the Windows domain but do not have full control over local Windows computer systems. (That responsibility lies with the administrator account locally on each computer.)

Another example is the Backup Operators group. Members of this security group can perform backup operations on domain controllers but are quite limited in other respects within the domain.

There are a lot of other default security groups in Active Directory, including Account Operators, DNSAdmins, Enterprise Admins, and Domain Users. Each of these security groups has different levels of built-in permissions to resources. For example, the Domain Users group is designed to house the bulk of your typical users, who intentionally have very little access to programs, data, and the domain. In fact, if you were to create a user in Active Directory, that user account would be assigned to the Domain

Users group by default. If none of the plethora of built-in groups have the level of security you want, you (as a domain admin) can then create new security groups for the domain. For more information on security groups, see https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/active-directory-security-groups.

A Quick Word About AD

This discussion is just the tip of the iceberg when it comes to Active Directory, and there are loads of Microsoft certifications dealing with Windows Server. What you have learned here should be enough for the A+ exam, but if you are interested in learning more, we recommend that you check out the following links:

- **Getting Started with Windows Server:** https://docs.microsoft.com/en-us/windows-server/get-started/get-started-with-windows-server
- **Windows Server Free Trial:** https://www.microsoft.com/en-us/windows-server/trial

Cram Quiz

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

1. You have been tasked with setting up encryption for a Windows computer. You are required to encrypt several shared folders within a partition so that they can't be read by other users. What tool should you use?

   - **A.** BitLocker
   - **B.** TPM
   - **C.** Administrative share
   - **D.** EFS

2. One of the users on your network is trying to access files shared on a remote computer. The file's share permissions allow the user Full Control, but the NTFS permissions allow the user Read access. Which of the following will be the resulting access for the user?

- ○ **A.** Full Control
- ○ **B.** Modify
- ○ **C.** Read
- ○ **D.** Write

3. You are the administrator for your network, and you set up an administrative share called Data$. Which of the following are necessary for another user to access this share? (Select the two best answers.)

- ○ **A.** The user must have permissions to access the share.
- ○ **B.** The user must know the decryption key.
- ○ **C.** The user must know the exact network path to the share.
- ○ **D.** The user must enable File Sharing in the Network and Sharing Center.

4. You are tasked with encrypting several laptops using BitLocker. However, some of the laptops do not have a built-in TPM chip. What should you implement to enable BitLocker on those laptops?

- ○ **A.** Firmware update
- ○ **B.** MFA
- ○ **C.** USB key
- ○ **D.** Encryption on the local drive

5. Which Windows account would you create for someone who needs to regularly install software, change settings, and take ownership?

- ○ **A.** Power user
- ○ **B.** Standard user

- ○ **C.** Guest
- ○ **D.** Root
- ○ **E.** Administrator

6. Which of the following is a built-in security component of Windows?

- ○ **A.** UAC
- ○ **B.** Firefox
- ○ **C.** Active Directory
- ○ **D.** MFA

7. You have been tasked with configuring a user account so that its folders and settings will follow the user to whatever computer the user logs on to within the domain. Which of the following should you configure?

- ○ **A.** OU
- ○ **B.** Roaming profile
- ○ **C.** Logon script
- ○ **D.** Home folder mapped to a network drive

8. You need to block users from installing programs in Windows. Of the following, what tool should you use?

- ○ **A. wf.msc**
- ○ **B.** Principle of least privilege
- ○ **C.** Digital signature
- ○ **D. gpedit.msc**

9. What is the primary function of Windows Hello?

- ○ **A.** To encrypt an entire disk
- ○ **B.** To manage user accounts and computer accounts

- ○ **C.** To provide passwordless authentication using biometrics or a PIN
- ○ **D.** To set up a firewall for network protection

10. What is the purpose of a roaming profile in Active Directory?
    - ○ **A.** To allow users to access their files from any computer on the network
    - ○ **B.** To execute specific tasks when a user logs on to the domain
    - ○ **C.** To provide a centralized location for storing user documents
    - ○ **D.** To store user settings and preferences on a server, allowing them to access a consistent profile from any computer on the domain

Cram Quiz Answers

1. **D.** Use Encrypting File System (EFS). This is easily done: Right-click the folder(s), select **Properties**, click the **Advanced** button, and check **Encrypt contents to secure data**. At this point, other users will not be able to read the files contained in those folders. BitLocker is used to encrypt an entire storage drive (or volume), but in the scenario, you only need to encrypt several folders. A Trusted Platform Module (TPM) chip is a chip that is required for using BitLocker, but it is not necessary for EFS. By creating an administrator share, you will effectively hide the contents from typical users, unless they know the admin password. If they do know the password, then they can read the files. Regardless, administrative shares do not encrypt data.

2. **C.** The user will get only Read access. If you are using both sets of permissions, the most restrictive set will take precedence. In this case, NTFS permissions are more restrictive than share permissions.

3. **A and C.** The user needs to have permissions to the share and must know the exact path to the network share because it is an administrative share. The question does not mention whether the file is encrypted. The user doesn't need to enable sharing; the person is trying to access a share.

4. **C.** If the laptops don't have a TPM chip, use a USB key to provide the encryption required by BitLocker. A firmware update won't help in this scenario; the TPM chip is an actual piece of hardware that is integrated to the motherboard. MFA stands for multifactor authentication. While MFA is a good idea, this question deals with encryption, not authentication. Encrypting the local drive is the task at hand, but you need to get BitLocker to work first!

5. **E.** Administrators have full control of an operating system. Power users are included in Windows for backward compatibility with older versions and are seldom used. Standard users are the normal default accounts for people who can log on to the network. Guests have limited access to the system. A guest cannot install software or hardware, cannot change settings, cannot access any data, and cannot change the password.

6. **A.** User Account Control (UAC) adds a layer of security to Windows to protect against malware and user error. Firefox is considered by many to be a secure web browser, but it is not included in Windows, nor can it be called a "security component"; it is a browser. Active Directory runs on Windows Server (though it can be accessed remotely from a Windows client); while it can increase the security of an organization's Windows network, it isn't a security component per se. With multifactor authentication (MFA), two or more types of identification are required for a user to be authenticated to a system, network, or facility. MFA is not a built-in security component of Windows, but it can be accomplished on a Windows system—for example, by using the default username/password scheme (something the person knows), adding a USB-based fingerprint scanner (something the person is), and configuring them to both be used during logon to Windows.

7. **B.** Configure a roaming profile for the user. The roaming profile is configured at the domain controller and allows the user to move from one computer to the next, and the user profile follows—as long as the user is logging on with the same username and password and logging on to the domain. Organizational units (OUs) provide a way of organizing users, computers, and policies. A logon script is designed to execute programs, features, and actions when a user logs on. As long as a user logs on to the domain, this script will be initiated. The home folder is the default location where a user will save and download files; it can be either local or mapped to a network drive, the latter of which is preferred on a domain.

8. **D.** Use the Group Policy Editor (**Run > gpedit.msc**) to make modifications to how (and whether) programs are installed to Windows. (There are a variety of other ways as well.) **Run > wf.msc** brings up Microsoft Defender Firewall with Advanced Security. The principle of least privilege is not a tool but a concept, which states that a user (or program) should only be given the access required to complete a task—and no more. Digital signatures are used to cryptographically "sign" emails so that users can verify that the emails came from known good sources.

9. **C.** Windows Hello is a feature that allows users to sign in to Windows using biometrics like fingerprint or facial recognition, or a PIN. It is a passwordless authentication method that aims to improve security and convenience. BitLocker is used for disk encryption, Active Directory is used for managing user accounts and computer accounts, and Microsoft Defender Firewall is used for network protection.

10. **D.** A roaming profile is a user profile stored on a server, allowing users to access their personalized settings and preferences from any computer on the domain. Home folders are used to store user documents, logon scripts execute tasks upon user login, and file sharing allows users to access files from other computers. Yes, allowing users to access their documents across computers connected to AD is a benefit of a roaming profile, but the primary

purpose is to access one’s personalized settings and preferences across computers in the domain.

Remember, with great power comes great responsibility. In short, leave it to the admins. Continue!

Chapter 46

Wireless Security and Malware

This chapter covers the following A+ 220-1202 exam objectives:

- **2.3** – Compare and contrast wireless security protocols and authentication methods.
- **2.4** – Summarize types of malware and tools/methods for detection, removal, and prevention.

You can't get enough security! That's because, as mentioned earlier in the book, nothing is ever 100 percent secure. However, you need to temper your vigilance and security aggressiveness by using prioritization. Always be thinking in terms of the most urgent threats and vulnerabilities to your organization and continue the list of risks from there. Secure them accordingly, starting from the top.

This chapter continues the security journey by discussing wireless security and authentication and how to prevent malware. It's a bit of a catch-all chapter due to the number of varying concepts covered, but we'll try to make it as pleasant as possible by breaking it up into manageable sections. Let's go!

Comparing and Contrasting Wireless Security Protocols and Authentication Methods

ExamAlert

Objective 2.3 concentrates on the following: protocols and encryption (WPA2, WPA3, TKIP, and AES) and authentication (RADIUS, TACACS+, Kerberos, and multifactor).

Wi-Fi connections are used by PCs, laptops, tablets, smartphones, industrial devices, and the list goes on. However, with ease of use comes additional security considerations. The plain truth is that a signal traveling in the air is going to be more insecure than a signal traversing a cable. So, you need to use proper wireless protocols and encryption protocols. Let's talk about some of them now.

Wireless and Encryption Protocols

We discussed various wireless protocols in Chapter 5, "Wireless Technologies," but we didn't discuss wireless encryption protocols. Let's review those important protocols now. Table 46.1 shows the wireless encryption protocols you should know for the exam.

TABLE 46.1 **Wireless Encryption Methods**

Wireless Protocol	Description	Encryption Level
WPA2	Wi-Fi Protected Access version 2. While WPA2 is still considered a secure option and widely used, WPA3 is generally recommended as the more secure choice if your devices are compatible because it offers improved encryption and protection against newer vulnerabilities compared to WPA2; however, if your devices don't support WPA3, then WPA2 remains a viable option.	128-bit

Wireless Protocol	Description	Encryption Level
WPA3	Wi-Fi Protected Access version 3. This secure wireless data encryption method is based on 802.11i, which replaces WPA2. The WPA3 standard replaces the preshared key (PSK) exchange with Simultaneous Authentication of Equals (SAE).	192-bit. WPA3 uses a minimum of 128-bit encryption in personal mode but can reach up to 192-bit encryption in enterprise mode, meaning the encryption strength can vary depending on the usage, with 192 bits being the strongest option available in WPA3.
TKIP	Temporal Key Integrity Protocol (deprecated encryption protocol used with WEP or WPA).	128-bit
AES	Advanced Encryption Standard (encryption protocol used with WPA2/WPA3). This encryption algorithm is used for securing sensitive networks used by US government agencies. It has become the encryption standard for corporate networks.	128-, 192-, and 256-bit

ExamAlert

Know the differences between WPA2, WPA3, TKIP, and AES.

At the writing of this book (2025), the best option is to go with WPA3 for wireless connectivity—if it is available—and AES for data encryption over that wireless connection. In fact, AES may be your only option, depending on the client used. For example, in Windows 11 Pro, if you select WPA2

(Personal or Enterprise), you will be forced to use AES. Figure 46.1 shows an example of this.

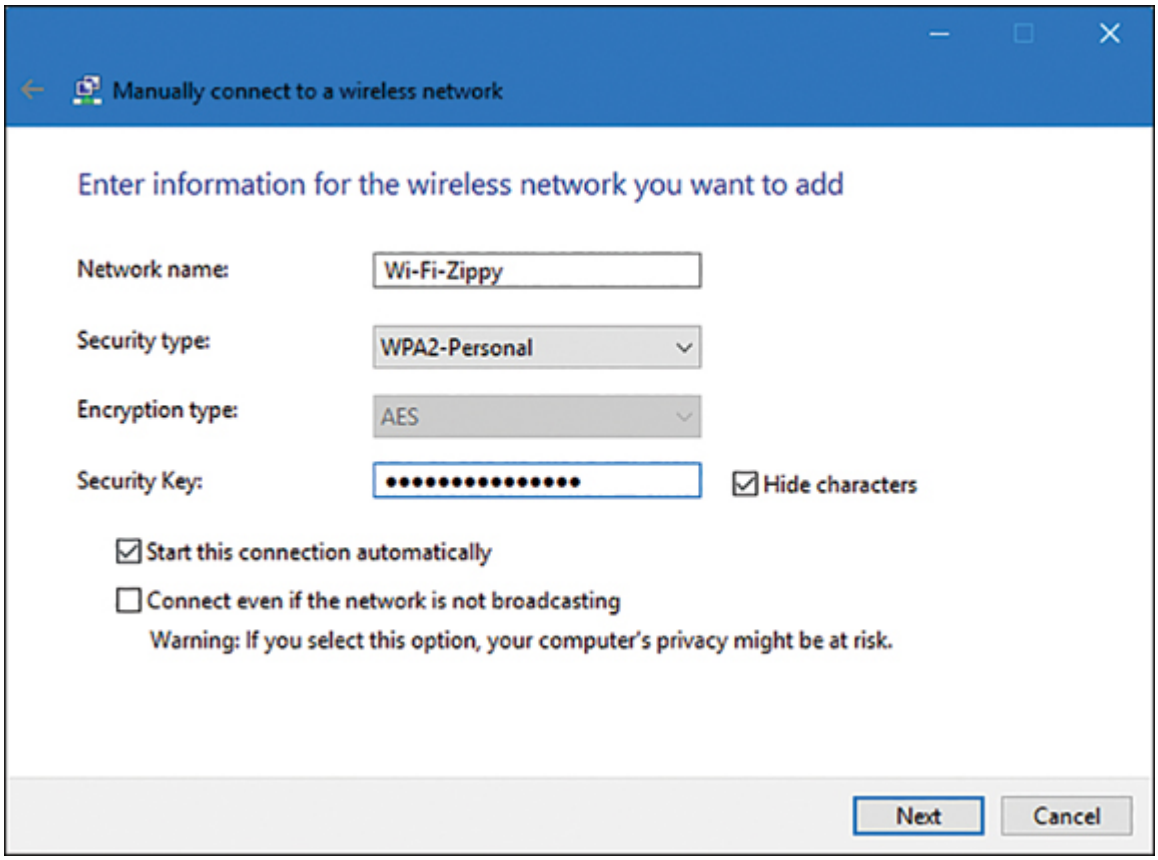


FIGURE 46.1 **Manual Wireless Network Connection in Windows**

Note

You can get to the window shown in Figure 46.1 by navigating to the **Network and Sharing Center** and clicking the **Set up a new connection or network** link.

The Encryption type field is grayed out, and although you could modify that in the Group Policy Editor or in the Registry Editor, doing so is usually not wise. What would be wise is to check the **Hide characters** checkbox for the Security Key; by default on some systems, the box is not checked, and the Security Key field displays what is typed.

In the figure, the security type specified is WPA2-Personal. This means that we are connecting to a basic Wi-Fi access point, and a preshared key (PSK) allows access. The PSK is stored on the access point. However, there are other options—some less secure and some more secure. The no authentication (Open) option has no key and no security, but you might use it to temporarily make a network connection and download the required software. Many larger organizations disable this option so that users and admins cannot connect without encryption. WEP may also be listed; WEP is not recommended because it can be compromised.

The more secure options include WPA2-Enterprise and 802.1X. WPA2-Enterprise, as the name implies, is designed for larger networks—ones that use an authentication server of some sort. Note that if your router and end device support it, choose WPA3 if it's an option! That could be a RADIUS server or a Terminal Access Controller Access-Control System Plus (TACACS+) server, which we'll discuss more in just a bit. These can be used as centralized authentication platforms for wireless connections and a variety of other authentication purposes, and they can be used as single sign-on (SSO) servers as well.

ExamAlert

RADIUS servers can be used to provide secure SSO access for Wi-Fi and network resources.

RADIUS and TACACS+

Remote Authentication Dial-In User Service (RADIUS) provides centralized administration of dial-up, VPN, and wireless authentication and can be used with 802.1X as well. It uses ports 1812 and 1813 by default, and when connecting to a RADIUS server from a wireless client, you often need to enter the port (1812) and the IP address of the server. Figure 46.2 shows an example of an access point that has been configured to redirect authentication requests to a RADIUS server using the IP address 172.18.0.13 on the default port 1812.

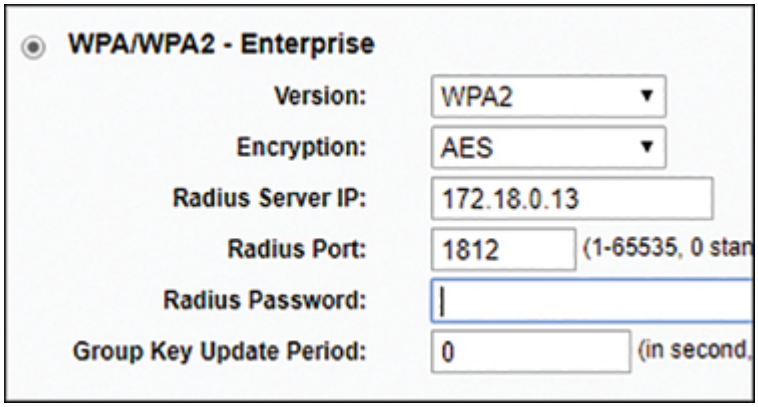


FIGURE 46.2 **WPA2-Enterprise Configuration on an AP**

ExamAlert

Know how to connect a wireless client to a RADIUS server using WPA2-Enterprise and port 1812.

RADIUS can be run on a variety of devices and servers, including Windows Server devices. RADIUS can also be used as a multifactor authentication (MFA) tool or as part of an MFA scheme. This can be much more secure than using a single-factor authentication scheme such as a typical WPA2-PSK connection.

Note

802.1X is an IEEE standard that defines port-based network access control (PNAC). Not to be confused with 802.11x WLAN standards, 802.1X is an authentication technology used to connect hosts to a LAN or WLAN. 802.1X allows you to apply a security control that ties physical ports to end-device MAC addresses and prevents additional devices from being connected to the network. It is a good way of implementing port security—better than simply setting up MAC address filtering.

TACACS+ (pronounced *tack-ax plus*) is really the pinnacle of confusing computer acronyms. TACACS+ is developed by Cisco and uses inbound port 49; however, it uses TCP as the transport mechanism instead of UDP.

There are a few differences between RADIUS and TACACS+. Whereas RADIUS uses UDP as its transport layer protocol, TACACS+ uses TCP as its transport layer protocol, and TCP is usually seen as a more reliable transport protocol than UDP (though each has its own unique set of advantages). Also, RADIUS combines the authentication and authorization functions when dealing with users; however, TACACS+ separates these two functions into two separate operations—introducing another layer of security. This means that you can run separate commands on a Cisco device for the individual authentication and authorization functions. TACACS+ also separates the accounting function into its own operation. Finally, TACACS+ provides for more types of authentication requests than does RADIUS.

ExamAlert

RADIUS uses port 1812 and UDP. TACACS+ uses port 49 and TCP.

Note

Authentication, authorization, and accounting are collectively known as AAA. RADIUS and TACACS+ servers are often referred to as AAA servers.

Kerberos

Kerberos is an authentication protocol designed at MIT that enables computers to prove their identity to each other in a secure manner. It is used most often in client/server environments, where the client and the server both verify each other's identity. This is known as two-way authentication, or mutual authentication. Often, Kerberos protects a network server from

illegitimate login attempts; it is named after Cerberus, the mythological three-headed guard dog who guards Hades. Pretty cool name, right?!

A common implementation of Kerberos occurs when a user logs on to a Microsoft domain. (Note: We are not implying that Microsoft domains are analogous to Hades!) The domain controller in the Microsoft domain is known as the key distribution center (KDC). This server works with tickets that prove the identity of users. The KDC is composed of two logical parts: the authentication server and the ticket-granting server. Basically, a client computer attempts to authenticate itself to the authentication server portion of the KDC. When it does so successfully, the client receives a ticket. This is actually a ticket to get other tickets—known as a ticket-granting ticket (TGT). The client uses this preliminary ticket to demonstrate its identity to a ticket-granting server in the hopes of ultimately getting access to a service—for example, making a connection to Active Directory on a domain controller. The domain controller running Kerberos will have inbound port 88 open to the service logon requests from clients. Kerberos goes hand in hand with the modified LDAP service used by Active Directory (which, by the way, uses port 389 by default and port 636 for secure LDAP).

Know this: Active Directory is the most commonly used directory services solution, but it's not the only game in town. Kerberos can be used with any directory services solution, including the open-source FreeIPA and its cousin Red Hat Identity Management. However, the A+ exam will most likely focus on Active Directory.

ExamAlert

Kerberos uses mutual authentication to provide security for clients attempting to connect to Active Directory domain controllers. It uses inbound port 88.

Cram Quiz

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

1. Which of the following is the strongest form of wireless encryption?

   - **A.** WPA3
   - **B.** WPA
   - **C.** AES
   - **D.** TKIP

2. You have been tasked with connecting wireless clients to a server that supports SSO and 802.1X. Which of the following technologies should you implement? (Select the two best answers.)

   - **A.** WPA2-PSK
   - **B.** WPA2-ENT
   - **C.** WEP
   - **D.** TKIP
   - **E.** RADIUS
   - **F.** Kerberos

3. What is the primary advantage of TACACS+ over RADIUS for authentication?

   - **A.** TACACS+ uses UDP, which is considered more reliable than TCP used by RADIUS.
   - **B.** TACACS+ combines authentication and authorization for greater efficiency.
   - **C.** TACACS+ separates authentication and authorization, providing an additional layer of security.
   - **D.** TACACS+ operates on ports 1812 and 1813, which are more secure than the port used by RADIUS.

4. Which of the following wireless encryption protocols offers 256-bit encryption?

   - **A.** AES
   - **B.** TKIP
   - **C.** WPA2
   - **D.** WPA3

Cram Quiz Answers

1. **C.** Of the list of options, Advanced Encryption Standard (AES) is the strongest form of wireless encryption. WPA is a wireless encryption protocol, but it is deprecated; WPA2 or WPA3 is recommended. TKIP is deprecated and has been compromised; it should be avoided. Use TKIP, WEP, or the no authentication only option if you are temporarily connecting a device to a Wi-Fi network in an attempt to update it to a newer protocol or if you are initiating testing. Even then, use extreme caution!

2. **B and E.** To take advantage of single sign-on (SSO) and 802.1X, you would need a special authentication system (such as RADIUS) on the server side and WPA2-Enterprise on the client side (sometimes abbreviated as WPA2-ENT). And what port does RADIUS use by default? Do you remember? WPA2-PSK uses a preshared key that is stored on the AP, and it doesn't support the other technologies. WEP and TKIP are outdated and should be avoided. Kerberos is a mutual authentication protocol used by Active Directory and other directory services programs.

3. **C.** TACACS+ enhances security by separating authentication and authorization into distinct operations, unlike RADIUS, which combines them. This separation allows for more granular control and can prevent unauthorized access even if one factor is compromised. TACACS+ actually uses TCP, which is generally considered more reliable than UDP used by RADIUS, so that answer is just wrong. Also, RADIUS combines authentication and

authorization, whereas TACACS+ separates them. TACACS+ uses port 49, whereas RADIUS uses ports 1812 and 1813. The security of the port is not directly related to its number.

4. **A.** This a tricky one! Advanced Encryption Standard (AES) can be used with WPA2 and WPA3. It is the encryption algorithm used by US government agencies and can offer up to 256-bit encryption! TKIP is an old encryption protocol used with WEP and WPA and should not be used anymore. Normally, WPA2 uses standard 128-bit AES encryption, but you can configure it to use 256-bit AES encryption. Likewise, WPA3 Personal utilizes 128-bit encryption and 192-bit in enterprise mode by default. However, you can enable 256-bit AES encryption in WPA3 Enterprise mode. So, yes, WPA2 and WPA3 can use 256-bit AES encryption, but it's AES itself that can do 256-bit encryption.

Detecting, Removing, and Preventing Malware Using the Appropriate Tools and Methods

ExamAlert

Objective 2.4 focuses on malware (Trojans, rootkits, viruses, spyware, ransomware, keyloggers, boot sector viruses, cryptominers, stalkerware, and fileless malware), adware, and the tools and methods used to mitigate malware issues (recovery console, endpoint detection and response, managed detection and response, extended detection and response, antivirus, antimalware, email security gateways, software firewalls, user education regarding common threats, and OS reinstallation).

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, Trojan horses, spyware, ransomware, rootkits, keyloggers, and other types of undesirable software.

Malicious Software Types

Of course, we don't want malware to infect our computer systems, but to defend against it, we first need to define it and categorize it. Then we can put preventive measures into place. It's also important to locate and remove/quarantine malware from a computer system in the event that it shows up. Table 46.2 summarizes the various malware threats you should know for the exam.

TABLE 46.2 **Malware Types**

Malware Threat	Definition
Virus	Code that runs on a computer without the user's knowledge; it infects the computer when the code is accessed and executed. This requires human interaction to spread, such as opening an infected email attachment or running an infected program.
Worm	A piece of malware that can replicate itself and spread automatically through networks. This very dangerous piece of malware is the reason that you should never stick random USB flash drives in your system! See the following site for a notorious look back at a worm: https://www.fbi.gov/history/famous-cases/morris-worm.

Malware Threat	Definition
Trojan horse	Malicious software that appears to perform desired functions, like the Greek Trojan horse, but is actually performing malicious functions behind the scenes. It is similar to a virus but doesn't spread by infecting other files. Instead, this type of malware executes malicious actions like stealing sensitive data such as usernames and passwords, creating backdoors to gain access later, and other nefarious actions! The name stems from the infamous Trojan horse of Greek lore where the seemingly defeated Greeks gave the victorious Trojans a gift at the end—a giant wooden horse. Yet, those Trojans didn't realize that Greek soldiers hid inside the horse when they brought their "present" inside the Trojan walls. During the night of Trojan revelry, the Greeks dropped out of the horse and killed all the Trojans in the city. Wow, Odysseus, just wow.

Malware Threat	Definition
Spyware	Malicious software either downloaded unwittingly from a website or installed along with some other third-party software that spies on the user's work. This type of spying is usually the gathering of user data like browsing history, location data, and even username and passwords! This malware is often deployed as a Trojan, but its main purpose is the gathering of data. The less invasive form of spyware is *adware*, which is primarily designed to display unwanted advertisements through pop-ups and banners in your browser. However, while adware is usually more benign, it's an easy crossover into full-blown spyware. Adware is often labeled as a *PUP*, or *potentially unwanted program*, by antimalware scanners. PUPs are often installed alongside other software, especially those free programs often called *freeware*. You might think twice before installing that "free" YouTube downloader program! Like spyware, there is also *stalkerware*. While the intent of spyware generally is financial gain or data collection for marketing, stalkerware, as a subset of spyware, is more personal and invasive. Its intent is to control, harass, or surveil a specific individual.
Rootkit	Software that is designed to gain administrator-level control over a computer system without being detected. Traditionally, a rootkit executes after the operating system has loaded, but often these are used with a *boot sector virus,* which loads during the startup process in the boot sector. So, the boot sector virus will load during the start of the OS loading procedure, and it will hand off to a rootkit. Rootkits are highly dangerous because they often load and carry out their payload before the operating systems' antimalware program has even loaded!

Malware Threat	Definition
Ransomware	Malicious software that restricts access to a computer system or locks the system until a ransom is paid, often with a bitcoin wallet address. Some ransomware even includes directions on how to create a bitcoin wallet and fund it! So polite…not! Ransomware is often propagated by Trojans, and it uses RSA encryption keys to "lock" the files. This type of attack has increased substantially over the years and often targets government organizations, school districts, medical facilities, and others where the "locking" of data is catastrophic. See this website for more information: https://www.cisa.gov/stopransomware/ransomware-101.
Keylogger	A program or device that captures all the keystrokes made by a user on a computer keyboard. A software-based keylogger may be loaded into a computer knowingly or without the user's knowledge using a Trojan. A hardware-based keylogger may be connected physically to a keyboard's cable so it can store data and possibly transmit it wirelessly.
Cryptominer	Hardware or software that is designed to "mine" for cryptocurrencies and can be legitimate or illegitimate. An illegitimately placed software-based cryptominer uses up the resources of a computer. The computer is also compromised because the existence of the cryptominer proves that someone has gained access to the system in some way.

Malware Threat	Definition
Fileless	A very dangerous type of malware that operates without having the traditional executable files of other types. Instead, this type can exploit legitimate system tools and processes such as PowerShell or Windows Management Instrumentation (WMI). This allows the malicious code to run directly in RAM, which makes it harder for traditional antivirus software to detect. See this website for more information: https://www.crowdstrike.com/en-us/cybersecurity-101/malware/fileless-malware.

ExamAlert

Know the difference between viruses, Trojan horses, spyware, adware, rootkits, ransomware, keyloggers, stalkerware cryptominers, and fileless malware.

Malware can be spread in a variety of ways, including via removable media, email attachments, downloaded programs, malicious hyperlinks, and the dreaded botnet. A *botnet* is a group of compromised computers that are controlled by a main computer (somewhere) that directs them to attack particular servers and routers on the Internet. It is called a botnet because it is a network of computers—robots, or bots for short—that work as a collective. Usually, the computer is infected with a Trojan that contains the code to connect the system to the botnet. Unless the antimalware program detects it, the user has no knowledge of it happening; it all occurs behind the scenes. You'll learn more about botnets in Chapter 47, "Social Engineering, Threats, and Vulnerabilities."

Preventing Malicious Software

Now that you know the types of malware, let's talk about how to stop them before they happen.

In a nutshell, you can prevent malware infection by using antimalware programs, updating the OS and apps, scanning the system, implementing policies, and educating users. But that's just in a nutshell. Let's dive a little deeper.

Preventing Viruses and Trojans

There is some confusion about the differences between viruses, worms, and Trojans; even some hackers and antivirus software developers are confused about the differences. That's because there are literally thousands of strains of malware (and possibly many more), and they can be quite difficult to classify. To a certain extent, the distinction doesn't matter. The bottom line is that for the most part, prevention is the same for viruses, worms, and Trojans.

You can do several things to protect a computer system from these types of malware. First, every computer should have *antivirus (AV)* software running on it. Better yet, every computer should have *antimalware* software on it. The name change is more than just a word. Traditional antivirus software just looked at virus definitions to match up, whereas antimalware software takes a more holistic approach and looks at definitions and heuristic scanning that analyzes files and programs. Many new antimalware companies are even incorporating artificial intelligence to detect malware.

Companies that provide antivirus and antimalware solutions often call them *endpoint protection platforms*. *EPPs* leverage signature-based detection, heuristics, and machine learning to prevent known and zero-day malware from executing on endpoints. They block malicious files and processes by analyzing their characteristics before they can cause harm. *Endpoint detection and response (EDR)* agents continuously monitor endpoint activity, collecting detailed telemetry like process executions, network connections, and file modifications. This data is analyzed to detect unexpected behavior and potential threats, providing security analysts with context for incident response. *Managed detection and response (MDR)* services augment EDR by providing 24/7 monitoring, threat hunting, and

incident response performed by security experts. These experts use the EDR data to investigate alerts, contain threats, and provide remediation guidance. *Extended detection and response (XDR)* unifies security data from various sources, including endpoints, networks, cloud workloads, and email, into a centralized platform. It employs advanced analytics and automation to correlate events, detect complex threats, and orchestrate automated responses across the entire security platform, providing a more holistic and proactive security approach. Remember, your endpoint is the client devices like your computer!

Additionally, many companies also imply an *email security gateway*. It acts as a protective barrier for email communication, sitting between your organization's mail server and the Internet. It scrutinizes incoming and outgoing emails for threats like spam, malware, and phishing attempts, using various techniques to filter and block malicious content. By inspecting attachments, links, and email content, it safeguards sensitive data and prevents cyberattacks from infiltrating your network through email.

Furthermore, software should be updated. If AV/AM software is bundled with the OS—for example, Windows Security (previously known as Microsoft Defender Antivirus)—then OS updates will also update the AV software. Third-party AV software requires a current license and must be renewed yearly with most providers. Or if it is free AV software, you need to periodically check if it is still a full version of the software. If it isn't already set to auto-update, set the AV software to automatically update at periodic intervals (for example, every day or every week). It's a good idea to schedule regular full scans of the system within the AV software or within the Windows Task Scheduler. Remember, some new computers come with free trial antimalware programs. While this is fine, it is important to either pay for the subscription once the trial runs out, or uninstall it and let the native Windows Security take over. The reason is that an out-of-date antimalware program can actually be more dangerous because it blocks the built-in Windows antimalware program—leaving your computer more at risk!

As long as the definitions have been updated, antivirus systems will usually locate viruses along with worms and Trojans. However, these systems usually do not locate rootkit activity unless it specifically has that feature,

which usually requires you to restart your OS to scan for rootkits on startup. Keep in mind that antimalware software is important, but it is not a cure-all.

You also need to make sure a computer has the latest updates available. This goes for the operating system and applications such as Microsoft 365. Backdoors into operating systems and other applications are not uncommon, and OS manufacturers often release fixes for these breaches of security. For example, Windows offers the Windows Update program. It should be enabled, and by default, it will update your system automatically; however, you should manually verify that the system is up to date and that updates are turned on. It might be that your organization has rules governing how Windows Update will function. If so, configure Automatic Updates according to your company's policy.

It's also important to consider boot sector viruses. When it comes to boot sector viruses, your antimalware software is still the best bet. The antimalware software might use a bootable USB flash drive to accomplish scanning of the boot sector, or it might have boot shielding built in. Some BIOS/UEFI programs have the capability to scan the boot sector of the storage drive at startup; this might need to be enabled in the BIOS setup first. You can also use recovery environments and the command line to repair the boot sector.

A *recovery console*—or in Windows, the Windows Recovery Environment (WinRE)—is a set of tools that operate outside of the normal Windows environment, designed to diagnose and repair system issues that prevent Windows from starting correctly. It provides access to command-line utilities and other diagnostic tools, allowing users to fix corrupted system files, repair boot sectors, or restore from backups. If Windows can start, you can access WinRE through the Settings app by navigating to **Update & Security > Recovery > Advanced startup** and clicking **Restart now**, or by using a Windows installation media.

Within WinRE, users can choose from several recovery modes:

- **Startup Repair:** This mode automatically diagnoses and attempts to fix common startup problems, such as missing or corrupted system files, driver issues, or boot sector errors.

- **System Restore:** This mode allows users to revert their system to a previous state saved as a restore point. This capability can be helpful to undo recent changes that may have caused instability or errors.
- **Command Prompt:** This mode provides advanced users with access to a command-line interface, allowing them to manually execute commands for troubleshooting and repair. It can be used to fix issues not addressed by the automated tools.
- **System Image Recovery:** This mode allows users to restore their entire system from a previously created system image backup, including the operating system, applications, and user files. This is a comprehensive recovery option for major system failures.

See this website for more information on this extremely important tool: https://learn.microsoft.com/en-us/windows-hardware/manufacture/desktop/windows-recovery-environment--windows-re--technical-reference?view=windows-11.

It's vital to make sure that a firewall is available, enabled, and updated. A firewall closes all the inbound ports to your computer (or network) in an attempt to block intruders. Microsoft Defender Firewall is a built-in feature of Windows, and you might also have a SOHO router with a built-in firewall. By using both, you have two layers of protection from viruses and other attacks. You can access Microsoft Defender Firewall by going to **Run > firewall.cpl**. Keep in mind that you might need to set exceptions for programs that need to access the Internet. You might do this based on the program or the port used by the protocol, enabling specific applications to communicate through the firewall while keeping the rest of the ports closed.

Note

Another good technique when trying to prevent viruses (and just about any other malware) is to disable AutoPlay/AutoRun for USB-connected devices and optical drives. Plus, remember to disable these devices in the BIOS/UEFI! We'll discuss this more in Chapter 48, "Workstation Best Practices."

From a more generalized perspective, malware is prevented through the use of a concept called *defense in depth*, or layering of security, and through monitoring the system and end-user education.

Educate users about how viruses can infect a system. Consider implementing an antiphishing educational campaign. By using simulations, you can help users know how to identify phishing attacks. (You'll learn more about phishing in Chapter 47.) A great quiz to start with is Google's Phishing quiz at https://phishingquiz.withgoogle.com/. You should also look at Google's Safe Browsing page if making websites: https://safebrowsing.google.com/.

Instruct users on how to screen (or filter) their emails, text messages, and other communications, and tell them not to open unknown attachments. Show them how to scan removable media before copying files to their computers or set up the computers to scan removable media automatically. Sometimes user education works; sometimes it doesn't. One way to make user education more effective is to have a technical trainer educate your users instead of doing it yourself. This can provide for a more engaging learning environment. During this training, you might opt to define an organization's acceptable use policy (AUP). This is a document that stipulates constraints and practices that a user must agree to before being granted access to a corporate network or the Internet. Sometimes an AUP can be a bit difficult for the average non-techie to understand. However, an AUP is usually designed to not only stipulate constraints but also educate the user, so it is in the user's best interest to learn what policies are covered in the AUP.

By using these methods, you can severely reduce virus infection. However, if a computer is infected by a virus, you want to know what to do to troubleshoot the problem. We'll get into that as well as the CompTIA A+ malware removal process in Chapter 56, "Troubleshooting PC Security Issues."

You can prevent and troubleshoot Trojans in much the same manner as viruses. There are scanners for Trojans as well (for example, Microsoft's Malicious Software Removal Tool). In some cases, antimalware software scans for worms and Trojans in addition to viruses. Both of these tools can easily detect *known* Trojans, regardless of whether it is the actual attacker's

application or any .exe files that are part of the application and are used at the victim computer. However, if a Trojan or worm is brand new, a hot fix or an individual scanner might become available from your antimalware provider. New Trojans and variants of Trojans are created every day. Until the antimalware provider finds out about them, they are known as zero-day attacks (as discussed in more detail in Chapter 47). The only way to prevent these attacks is to stick to the fundamentals discussed throughout this section.

Preventing and Troubleshooting Spyware

You can prevent spyware in much the same manner that you prevent viruses in that spyware prevention includes updating the operating system and using a firewall. Also, because spyware has become much more common, antivirus companies have begun adding antispyware components to their software. Here are a few more things you can do to protect your computer in the hopes of preventing spyware:

- Download and install antispyware protection software (which might be included in your antimalware suite). Be sure to keep the antispyware software updated.
- If you are using Windows, consider enabling SmartScreen for Microsoft Edge, which checks web content and protects against malicious sites and downloads.
- Adjust web browser security settings in the following ways:
  - Enable a phishing filter if you have one and turn on automatic website checking.
  - Enable checking of certificates. If a certificate (that is, a secure encrypted connection on the web) has been revoked or is otherwise invalid, you want to know about it; a message such as “invalid certificate (trusted root CA)” will only be received when the browser is checking for it. If the browser is not protecting you in this way, you could inadvertently stumble onto a disreputable website.
  - Check for unwanted proxy connections. (For more information on proxy connections, see Chapter 38, “Windows Networking.”)

- Uninstall unnecessary applications and turn off superfluous services (for example, Telnet and FTP if they are not used).
- Educate users on how to surf the Web safely. Remember: User education is the number-one method of preventing malware!
- Consider technologies that discourage spyware. For example, use a browser that is less susceptible to spyware. For example, Mozilla's Firefox prides itself on limiting spyware.

Preventing Rootkits

A successfully installed rootkit enables unauthorized users to gain access to a system, acting as the root or administrator user. A rootkit is copied to a computer as a binary file; this binary file can be detected by signature-based and heuristic-based antivirus programs. However, after a rootkit is executed, it can be difficult to detect. The reason is that most rootkits are collections of programs working together that can make many modifications to the system. When the operating system is subverted, the OS can't be trusted, and it is difficult to tell whether your antivirus programs run properly or whether any of your other efforts have any effect. Although security software manufacturers attempt to detect running rootkits, they are not always successful.

One good way to identify a rootkit is to use rescue removable media (such as a USB flash drive) to boot the computer. This way, the operating system is not running, which means the rootkit is not running, making the rootkit much easier for the external media to detect.

Unfortunately, because of the difficulty involved in removing rootkits, sometimes the best way to combat a rootkit is to wipe the drive and reinstall the operating system and all software. You might hear this process referred to as "reimaging the machine." Generally, upon detecting a rootkit, a PC technician will do this because it usually is quicker than attempting to fix all the rootkit issues, and it can verify that the rootkit has been removed completely. See this page for more information on how to reset a PC, with the option to save your data: https://support.microsoft.com/en-us/windows/fix-issues-by-reinstalling-the-current-version-of-windows-497ac6da-7cac-4641-82a5-f50398d879a0.

Software isn't the only method of defense and repair when it comes to rootkits. Newer motherboards equipped with UEFI take advantage of Secure Boot technology, which can help protect the preboot process against rootkit attacks. It means that a rootkit can potentially be stopped *before* it actually causes any damage.

Backup/Restore and Recovery Environments

A good security plan includes not only prevention methods but also solid backup procedures. Back up as often as you can. This could be done on a file-by-file basis, using built-in Windows programs such as File History as well as third-party programs; it can also include the imaging of storage drives and creation of a single file that incorporates the entire storage drive and all of its contents. Snapshots can be taken as well to mark a point in time (for example, by using System Restore). For any system that has important data on it, you should have a backup plan. Consider this whenever you build or deploy new systems. We'll discuss backup plans further in Chapter 58, "Change Management and Backup Methods."

In the event that malware does infect a system, you have to quarantine it, remove it, and recover the system. A great way to do this is to think outside the box and boot the system to some type of recovery environment. This could be a Linux-based repair disc/drive, or you could use the built-in Windows Recovery Environment (WinRE).

Cram Quiz

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

1. Which of the following types of malware is designed to gain administrative-level control of a system?

   - ○ **A.** Ransomware
   - ○ **B.** Keylogger

- ○ **C.** Rootkit
- ○ **D.** Spyware

2. You have been tasked with implementing a virus prevention plan on a group of Windows client computers. Which of the following should you carry out? (Select all that apply.)

- ○ **A.** Update antimalware software.
- ○ **B.** Configure File History.
- ○ **C.** Update Microsoft 365.
- ○ **D.** Install a rootkit scanner.
- ○ **E.** Verify that a firewall is installed.

3. One of your customers complains of a problem: When browsing the Internet, multiple browser pages start opening automatically. You notice that the computer is performing poorly, even when not connected to the Internet. What should you do?

- ○ **A.** Enable a pop-up blocker.
- ○ **B.** Reboot the computer.
- ○ **C.** Install/scan with an antimalware tool.
- ○ **D.** Update the antivirus definitions.

4. Which security solution focuses on unifying security data from various sources, including endpoints, networks, cloud workloads, and email, into a centralized platform for a holistic and proactive security approach?

- ○ **A.** Endpoint protection platform (EPP)
- ○ **B.** Endpoint detection and response (EDR)
- ○ **C.** Managed detection and response (MDR)
- ○ **D.** Extended detection and response (XDR)

5. Which Windows Recovery Environment (WinRE) mode would be most suitable for a user who wants to undo recent software installations that have caused the system to become unstable?

   - **A.** Startup Repair
   - **B.** System Restore
   - **C.** Command Prompt
   - **D.** System Image Recovery

Cram Quiz Answers

1. **C.** A rootkit is designed to get administrative control of a computer system. The word *root* is synonymous with *administrator* in some systems (such as Linux and UNIX). Ransomware is malware that encrypts a person's files so that they are not accessible. Keyloggers capture the keystrokes a person makes on a keyboard. They are used to steal passwords and other confidential information. Spyware is malware that is used to watch (and possibly record) what a person is doing on a system and on the Internet.

2. **A, C, and E.** First of all, update everything. Then verify that antimalware software and a firewall are installed and updated. Be sure to update the OS and apps as well. Microsoft 365 is especially susceptible to malware, so if you run it, you have to keep a close eye on it. Configuring File History or any other backup methods won't prevent malware from occurring, but it is important to do this nonetheless. Remember, backup is not prevention. A rootkit scanner won't scan for viruses and won't prevent them; in fact, it won't prevent rootkits, but it might find them.

3. **C.** Chances are that the customer's computer does not have an antivirus or antimalware program running. Install one (or enable one if it already exists). However, the problem is probably worse than that, and the system likely needs to be remediated (isolated, scanned, and so on). These are probably not just pop-ups; you normally see only one legitimate pop-up at a time. Plus, the

computer is performing poorly, even when not connected to the Internet. Rebooting the computer can fix some issues, but it won't fix a malware-infected system. Updating the antivirus software is always a good idea, but the problem might not be caused by a virus. It is more likely that the system has no antimalware program running. Note: If you ever determine that a system is infected with malware, it should be disconnected from the network right away and placed in isolation until it is repaired properly!

4. **D.** XDR is the only solution that collects and correlates security data from various sources beyond just endpoints. It provides a centralized platform for a more comprehensive and proactive security approach. EPP focuses on preventing known and zero-day malware from executing on endpoints. EDR monitors endpoint activity and collects telemetry data for analysis and threat detection. MDR augments EDR with 24/7 monitoring and incident response by security experts.

5. **B.** System Restore allows users to revert their system to a previous state, effectively undoing any recent changes that may have caused instability or errors. In this scenario, where software installations have led to instability, using System Restore to roll back the system to a point before the installations would be the most appropriate solution. Startup Repair mode is designed to fix common startup problems, such as missing or corrupted system files, but it may not address issues caused by software installations. Command Prompt mode provides a command-line interface for manual troubleshooting, but it requires advanced knowledge and may not be the most efficient solution for this scenario. System Image Recovery mode restores the entire system from a backup, which is a more drastic measure than necessary for addressing instability caused by software installations!

Another chapter on security is in the books! Review your notes, jump up and do a quick silly dance, and continue on!

“It takes 20 years to build a reputation and five minutes to ruin it.” — Warren Buffett

Chapter 47

Social Engineering, Threats, and Vulnerabilities

This chapter covers the following A+ 220-1202 exam objective:

- **2.5** – Compare and contrast common social engineering attacks, threats, and vulnerabilities.

When it comes to information security, it's not just about technical attacks. We need to worry about people too. One great way to improve your organization's security mindset is to employ the following epigram: "To know your Enemy, you must become your Enemy" (Sun Tzu). This means knowing your attacker's methods, techniques, and purpose.

This chapter embarks on a journey through some of the various social engineering methods as well as some technical attacks that you should know for the exam.

ExamAlert

Objective 2.5 concentrates on the following: social engineering (such as phishing and shoulder surfing), threats (such as DDoS and zero-day attacks), and vulnerabilities (such as unpatched systems and EOL systems).

Social Engineering

Social engineering is the act of manipulating users into revealing confidential information or performing other actions that are detrimental to users. Almost everyone gets emails from unknown entities making false claims or asking for personal information (or money!); this is one example of social engineering. But there are a plethora of other ways to extract information from unwitting users. Let's examine some of them now.

Phishing

Phishing is an attempt to fraudulently obtain private information. A phisher usually masquerades as someone else, perhaps another entity. Phishing is usually done via electronic communication. Little information about the target is necessary. A phisher may target thousands of individuals without much concern as to their backgrounds. An example of phishing would be an email that requests verification of private information. Clicking a link in the email will probably lead to a malicious website that is designed to give individuals a false sense of security and fraudulently obtain information from them. Such a website often looks like a legitimate website. A common phishing technique is to pose as a vendor (such as an online retailer or a domain registrar) and send individuals email confirmations of orders that they supposedly placed.

Specific groups of people might be targeted with more streamlined phishing campaigns; this is known as *spear phishing*. A campaign can even target specific individuals. A form of spear fishing, known as *whaling*, targets senior executives of corporations, though con artists use other techniques in addition to phishing when targeting a "whale."

Phishing is also sometimes attempted by telephone. Phone phishing, known as *vishing*, works in the same manner as phishing but is initiated via a phone call, often using an automated VoIP system or home-brewed private branch exchange (PBX). The phone call often sounds like a prerecorded message from a legitimate institution (bank, online retailer, donation collector, and so on). The message asks the unsuspecting person for confidential information such as name, bank account numbers, and codes under the guise of needing to verify information for the person's protection.

It's really the opposite, of course, and many people are caught unawares by these types of scams every day. By using automated systems (such as the ones that telemarketers use), vishing can be perpetrated on large groups of people with little effort.

Like vishing, a new type of phishing called *smishing* has gained in popularity. Instead of phishing phone calls, these are phishing text messages. Because many users are wary of unsolicited phone calls, scammers have resorted to smishing. This type of social engineering is often seen during holidays with messages that state your order has a problem and to click here or during tax season with messages supposedly from the IRS stating that you need to verify tax information. Don't do it!

Okay, really, phishing, vishing, and smishing? What will scammers think of next to carry out their phishing expeditions? *QR code phishing*, or *quishing*, is one. In this type of social engineering, scammers place malicious QR codes to redirect to fake websites to gain sensitive information such as login credentials or payment information. In California, many cities, especially beach cities, have QR codes posted for people to pay for parking permits. Scammers stick new QR codes over the official city ones to redirect to fake websites to steal credit card information. So, unsuspecting visitors leave with sand on their feet and a stolen credit card! Be careful scanning those QR codes, my friends!

As you can imagine, several different types of social engineering are often lumped into what is referred to as phishing, but actual phishing for private information is normally limited to email and websites. To defend against this, a phishing filter or add-on should be installed and enabled on a web browser. Also, individuals should be trained to realize that reputable institutions and businesses will not call or email, requesting private information. If individuals are not sure whether they're being targeted, they should hang up the phone or simply delete the email. A quick way to find out if an email is phishing for information is to hover over a link (but don't click it!). You will see a URL domain name that is far different from the institution that the phisher is claiming to be—probably a URL located in a distant country. Unfortunately, some smaller banks might call or text you if your account has been compromised. If this happens to you, ask for their extension, hang up, and call the number on the back of your card or a

known good number and punch in their extension. If the call is legitimate, you can resolve your issue. If the caller doesn't want to give you their extension or immediately asks for your Social Security number, think twice!

Shoulder Surfing

With *shoulder surfing*, a person uses direct observation to find out a target's password, PIN, or other authentication information. The simple resolution to prevent this type of social engineering is for the user to physically shield the screen, keypad, or other authentication-requesting devices. A technical method is to use a screen filter. A more aggressive approach is to courteously ask an assumed shoulder surfer to move along. Also, private information should never be left on a desk or out in the open. In fact, many organizations have a "clean desk policy" that states this explicitly. Computers should be locked or logged off when the user is not in the immediate area. Shoulder surfing and the methods described in the following several sections are examples of no-tech hacking.

ExamAlert

Use a screen filter to protect against shoulder surfing.

Piggybacking/Tailgating

With *piggybacking*, an unauthorized person tags along with an authorized person to gain entry to a restricted area—usually with the person's consent. *Tailgating* is essentially the same but with one difference: It usually occurs *without* the authorized person's consent. Both of these types of intrusions can be defeated through the use of access control vestibules (also known as mantraps). Remember that this is a small space that can usually fit only one person. It has two sets of interlocking doors; the first set must be closed before the other will open, creating somewhat of a waiting room where people are identified (and cannot escape). Think twice before entering your

building with that stranger fumbling for their keys behind you and asking if you can hold the door for them!

Multifactor authentication (MFA) is often used in conjunction with an access control vestibule. With MFA, two or more types of authentication are used for user access control (for example, using a proximity card and PIN at the first door and then using a biometric scan at the second). An access control vestibule is an example of a preventive security control. Turnstiles, double entry doors, and security guards are other less expensive solutions to the problem of piggybacking and tailgating and help address confidentiality in general.

Dumpster Diving

With *dumpster diving*, a person scavenges for private information in garbage and recycling containers. Any sensitive documents should be stored in a safe place as long as possible. When they are no longer necessary, they should be shredded. (Some organizations incinerate their documents.) Information might be found not only on paper but also on storage drives or removable media. Company policy should document proper recycling and/or destruction of storage drives, and employees should be educated on proper disposal methods. Chapter 50, "Data Destruction and Disposal," will cover these policies and procedures in more detail. Another way to deter a person from attempting dumpster diving is to use security cameras and good lighting in the area where the dumpsters are located; some organizations keep their dumpsters indoors in a warehouse or similar area.

Impersonation

Impersonation involves presenting oneself as another person, imitating that other person's characteristics. By impersonating the appropriate personnel or third-party entities, a person hopes to obtain records about an organization, its data, and its personnel. IT people and employees should always be on the lookout for impersonators and should always ask for identification. If there is any doubt, the issue should be escalated to a supervisor and/or a call should be made to the authorities. Impersonation is

often a key element in *pretexting*, in which someone invents a scenario and attempts to get a key person to reveal confidential information. Impersonation is so common that there are memes about it—a guy showing up in a truck with a ladder on it saying he's there to fix something and allowed in without ever having to show identification. Heck, the meme implies that a person can just wear an orange safety vest and get in about anywhere. Don't fall for this!

Note

Objective 2.5 covers more than just social engineering, but the following techniques are sometimes used by attackers and malicious insiders in addition to social engineering, and they are therefore somewhat related.

Threats and Vulnerabilities

Because there are so many types of threats and vulnerabilities in today's computers and networks, there are many types of attacks as well. Let's briefly examine some more types of attacks and common vulnerabilities that a typical organization might have to face.

Network-Based Attacks

Network-based attacks include spoofing, on-path attacks, zero-day attacks and various denial-of-service attacks. Let's consider them now.

In a *spoofing attack*, an attacker masquerades as another person by falsifying information. This can be done as a social engineering attack, as in the previously mentioned phishing method, or it can be performed as a more technical attack, such as the on-path attack. In an *on-path attack*, an attacker intercepts data between a client and a server. It is a type of active interception. If the attack is successful, all communications are diverted to the attacking computer. The computer can, at this point, modify the data, insert code, and send it to the receiving computer. This type of

eavesdropping is successful only when the attacker can properly impersonate each endpoint.

Some attacks exploit vulnerabilities that haven't even been discovered yet or that have been discovered but have not been disclosed through the proper channels so that security administrators can become aware of them. These are known as *zero-day attacks*. In this type of attack, an attacker exploits a vulnerability in an operating system or a network security device in such a way that makes it almost impossible to defend against. Because of this, zero-day attacks are a severe threat. Actually, most vulnerabilities are discovered through zero-day attacks, and the first group of systems that are attacked have very little defense. But once such an attack is detected, the development of a solution is not far behind (it could be days or even hours); the vulnerability (and attack) becomes known and is no longer a zero-day threat.

ExamAlert

Remember that a zero-day attack or threat is a computer threat that tries to exploit computer application vulnerabilities that are unknown to others or possibly even the software developer. (Those weaknesses are also called zero-day vulnerabilities.)

Most of the attacks and malware we have reviewed so far can be initiated by *zombies*—computers that distribute malware or participate in attacks without the knowledge of the owner. Zombies (also called robots or bots) can be grouped together by a central attacker to form a *botnet*. This is done to perpetuate large-scale attacks against particular servers. Distributed denial of service (DDoS) is an example of an attack committed by a botnet; it is designed to bring down a server or website. Let's talk about denial-of-service attacks a little more.

DoS

Denial of service (DoS) is a broad term applied to many different types of network attacks that attempt to make computer resources unavailable.

Generally, it is done to servers but can also be perpetrated against routers and other hosts. Examples of DoS attacks include ping floods, Smurf attacks, SYN floods, pings of death, and fork bombs.

DDoS

An attacker (or group of attackers) may make use of a *distributed denial-of-service (DDoS)* attack. In this type of attack, a group of compromised systems attacks a single target, causing denial of service at that host.

A DDoS attack often utilizes a botnet, which is a large group of computers, known as *robots* or simply *bots*. Often, these are systems owned by unsuspecting users. The computers in a botnet that act as attackers are known as *zombies*. An attacker starts a DDoS attack by exploiting a single vulnerability in a computer system and making that computer the zombie controller, or DDoS controller. This controlling system communicates with the other systems in the botnet. The attacker often loads malicious software on many computers (zombies). The attacker can launch a flood of attacks by all zombies in the botnet with a single command. DDoS attacks and botnets are often associated with exploit kits and ransomware.

DoS and DDoS attacks are difficult to defend against. These attacks can be prevented to some extent by keeping stateful firewalls, switches, and routers updated, and implementing access control lists, intrusion prevention systems (IPSs), and proactive testing. Several companies offer products that simulate DoS and DDoS attacks. By creating a test server and assessing its vulnerabilities with simulated DoS tests, you can find holes in the security of a server before you take it live. An organization could also opt for a "clean pipe," which attempts to weed out DDoS and other attacks. This solution is offered as a service by some ISPs and other companies. Manual protection of servers can be a difficult task; to implement proper DDoS mitigation, your organization might want to consider anti-DDoS technology and emergency response from an outside source or from a cloud-based provider. Finally, if you realize that a DDoS attack is being carried out on your network, call your ISP and request that the traffic be redirected.

ExamAlert

In a DDoS attack, multiple systems are used to attack a server, website, or network.

Password Cracking

One way that attackers attempt to gain access to systems is through password cracking. This is usually done with the aid of password-cracking software. Two common methods of password cracking are the dictionary attack and the brute-force attack.

A *dictionary attack* uses a prearranged list of likely words, trying them all, one at a time. A dictionary attack can be used for cracking passwords, passphrases, and keys. It works best with weak passwords and when targeting multiple systems. The power of a dictionary attack depends on the strength of the dictionary used by the password-cracking program.

In a *brute-force attack*, a threat actor tries every possible password. This type of attack is often a last resort because of the amount of CPU resources it can require. It works best on shorter passwords but can theoretically break any password, given enough time and CPU power.

Using complex and long passwords is the best way to prevent these types of attacks from succeeding. But a system and its network should also be protected with the Internet security appliances mentioned previously.

Cryptanalysis Attacks

A *cryptanalysis attack* uses a considerable set of precalculated encrypted passwords located in a lookup table. Such a table is known as a *rainbow table*, and this type of password attack uses a *precomputation*, where all words in the dictionary (or a specific set of possible passwords) are hashed and stored. The goal of a cryptanalysis attack is to recover passwords more quickly. This type of attack can be defeated by implementing *salting*, which is the randomization of the hashing process. It usually incorporates key stretching, which means adding bits of information to a password to make it stronger.

ExamAlert

Know the differences between dictionary and brute-force attacks.

Evil Twin

An *evil twin* is a rogue, counterfeit, and unauthorized wireless access point that uses the same SSID name as a nearby wireless network, often a public hotspot.

Like an evil twin antagonist in a sci-fi book, the device is identical in almost all respects to the authorized wireless access point (WAP). While the antagonist in the sci-fi book usually has a beard or goatee, the WAP is controlled by a person with the same types of motives as the bearded evil twin. One of these motives is phishing.

For example, an attacker might attempt to fool wireless users at an Internet café to connect to a counterfeit WAP to gain valuable information and passwords from those users. If a user is unlucky enough to connect to the evil twin, all the information within the session can easily be recorded and digested later by the attacker. This type of attack can also be enacted on organizations. To protect against this, virtual private networks (VPNs) can be implemented and require external authentication outside the WAP. Administrators should scan the network often with wireless site survey software for rogue APs that might be evil twins. In general, users should be trained not to send passwords, credit card numbers, and other sensitive information over wireless networks.

ExamAlert

Rogue access points can also serve as a type of on-path attack (formerly known as man-in-the-middle, or MITM, attack), referred to as an evil twin.

Additional Security Threats

There are some more security threats that you should know for the exam, including insider threats, business email compromise (BEC), supply chain/pipeline attack, cross-site scripting (XSS), and SQL injection. Let's start with insider threats.

Insider Threat

A malicious insider is one of the most insidious threats. Instead of impersonating personnel, as is done in pretexting, the person actually becomes personnel!

This attack is often used as part of a corporate espionage plan. Think that all IT techs are 100 percent honorable? In high tech, you will find an assortment of atrocities, including malicious insider threats. The insider might have been sent by a competing organization to obtain a job or consulting position with a certain company, or perhaps the person may be approached by the competing organization while already working for the company that is the target. Such an attack is often initiated by organizations from another country. Once an insider is situated, that person can easily get access to secure data, personally identifiable information (PII), financials, engineering plans, and so on and pass that information on to the infiltrating organization. Of course, the penalties for this behavior are high, but the potential rewards can be quite enticing to properly "motivated" individuals. Companies therefore often run thorough background checks and credit checks and have human resources put a potential employee through a set of psychological questions. Then, when a person is hired, there is a sort of trial period during which the person is allowed very little access to secure data and secure environments.

Now, a malicious insider doesn't necessarily have to be a person. It could be a device or a bug that was inserted into the organization by a person using social engineering skills—for example, rogue PIN pad devices, audio and video sensors (bugs), keyloggers, and so on. Planting such devices requires physical access to the building in one way or another, so identification and authentication are of paramount importance.

While there are insiders who purposely sabotage a company, there are also insiders who do so unintentionally. For example, an employee who falls for

a phishing email could be inadvertently exposing the entire company to malware through a malicious link. A friendly company employee who holds the door for a stranger fumbling for their keys might be letting in a criminal who now has physical access to electronic equipment. Unfortunately, the term *insider threat* was developed because it is one of the top ways organizations have been infected with malware. The unintentional insider can pose just as great a risk as an intentional insider!

Business Email Compromise and Supply Chain/Pipeline Attacks

Business email compromise (BEC) is a sophisticated scam where attackers impersonate trusted individuals, like executives or vendors, via email to trick employees into transferring funds or divulging sensitive information. *Supply chain/pipeline attacks* target vulnerabilities in third-party software, hardware, or services that an organization relies on. Attackers compromise these external components and then use them as a stepping stone to infiltrate the target's network, potentially disrupting operations or stealing data. In pipeline attacks, the target is specifically a software delivery process, where malicious code is inserted into the software build or update process.

Cross-Site Scripting (XSS)

One web application vulnerability to watch out for is *cross-site scripting (XSS)*. XSS holes are vulnerabilities that can be exploited with a type of code injection. *Code injection* involves exploiting a computer programming bug or flaw by inserting and processing invalid information; it is used to change how a program executes data. In the case of an XSS attack, an attacker inserts malicious scripts into a web page in the hopes of gaining elevated privileges and access to session cookies and other information stored by a user's web browser. This code (often JavaScript) is usually injected from a separate "attack site." It can also manifest as an embedded JavaScript image tag, header manipulation (as in manipulated HTTP response headers), or other HTML-embedded image objects within emails (that are web-based).

Programmers can often defeat XSS attacks through the use of output encoding (JavaScript escaping, CSS escaping, and URL encoding) by preventing the use of HTML tags and with input validation (for example, checking forms and confirming that input from users does not contain hypertext). On the user side, the possibility of an XSS attack's success can be reduced by increasing cookie security and by disabling scripts. If XSS attacks via email are a concern, a user could opt to set the email client to text only.

SQL Injection

Databases are just as vulnerable as other computer systems. The most common kind of database is a relational database, which is administered by a relational database management system (RDBMS). These systems are usually written in Structured Query Language (SQL). An example of a SQL database is Microsoft's SQL Server; it can act as the back end for a program written in Visual Basic or Visual C++. Another example is MySQL, a free, open-source relational database program often used in conjunction with websites that employ PHP pages.

One concern with SQL is *SQL injection attacks*, which occur in databases, ASP.NET applications, and blogging software (such as WordPress) that use MySQL as a back end. In these attacks, user input in web forms is not filtered correctly and is executed improperly; as a result, an attacker is able to gain access to resources or change data.

For example, the login form for a web page that uses a SQL back end (such as a WordPress login page) may be insecure, especially if the front-end application is not updated. An attacker may attempt to access the database (from a form or in a variety of other ways), query the database, find a username, and then inject code into the password portion of the SQL code —perhaps something as simple as X = X . This will allow any password to be used for the user account. If the login script was written properly (and validated properly), it should deflect this injected code. But if it wasn't, or if the application being used is not updated, such an attack could work.

It is possible to defend against SQL injection threats by constraining user input, filtering user input, and using stored procedures such as input-

validation forms.

> **Note**
>
> Injection attacks are on OWASP's "top 10 web application security risks" list. Learn more about these risks at https://owasp.org/www-project-top-ten/.

Vulnerabilities and Security Best Practices

Most organizations have policies regarding security best practices. The biggest vulnerability to an organization is the violation of those best practices (namely, noncompliant systems).

For example, an organization might have rules stating that all systems—operating systems, antimalware applications, and so on—must be updated at particular intervals. If a single computer fails to be updated, it is no longer in compliance with policy. This one computer could be used by a hacker or malicious insider to cause all kinds of harm, even on systems that are updated, simply because the nonupdated system is behind the firewall (on the LAN) with the rest of the computers.

When updating systems, double-check that everything has indeed been updated. Use scanning software to find all systems on the network and review network documentation to make sure no systems have "fallen through the cracks." If you find some rogue systems, make sure they are legitimate systems. Verify that these systems have some kind of antimalware program installed and that the program has been updated.

While you're scanning through a network of systems, it's also vital to check for outdated software. Remember that in Chapter 29, "Common Operating Systems," we talked about the end-of-life (EOL) date for operating systems such as Windows and macOS. If a computer on your network has passed the EOL date, then it most likely does not receive security updates anymore, and it is therefore a vulnerability to the entire network and infrastructure.

Finally, let's discuss some bring-your-own-device (BYOD) concerns. Around 2011, organizations began to allow employees to bring their own mobile devices into work and connect them to the organization's network (for work purposes only, of course). This BYOD concept has since grown into a popular method of computing for many organizations. It is enticing from a budgeting standpoint, but it can be very difficult on the security administrator—and possibly on the user as well.

For a BYOD implementation to be successful, the key is to implement storage segmentation—a clear separation of organizational and personal information, applications, and other content. The data ownership line must be unmistakable.

For networks with a lot of users, consider third-party offerings from companies that make use of mobile device management (MDM) platforms. These are centralized software solutions that can control, configure, update, and secure remote mobile devices that run Android, iOS, iPadOS, and Chrome OS, all from one administrative console. MDM software can be run from a server within the organization or administered within the cloud. It makes the job of a mobile IT security administrator at least manageable. From the central location, the security administrator can carry out tasks related to application management, content management, and patch management in a simplified manner and to multiple devices all at once. This reduces the risks related to vulnerable systems on the network, increases the efficiency of devices, reduces the footprint of devices, and, ultimately, makes devices more secure.

Note

That last section is a bit of a catch-all. Remember that the CompTIA A+ is not a security exam, but it does require that you know some basic security concepts.

Cram Quiz

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

1. Which of the following is an attempt to guess a password by using a combination of letters and numbers?

   - ○ **A.** Brute-force
   - ○ **B.** Social engineering
   - ○ **C.** Dictionary
   - ○ **D.** Zero-day

2. A user clicked a link in an email that appeared to be from his bank. The link led him to a page that requested he change his password to access his bank account. It turns out that the web page was fraudulent. This is an example of which of the following?

   - ○ **A.** Impersonation
   - ○ **B.** Dumpster diving
   - ○ **C.** Phishing
   - ○ **D.** Shoulder surfing

3. Several hundred infected computers simultaneously attacked your organization's server, rendering it useless to legitimate users. This is an example of what kind of attack?

   - ○ **A.** Botnet
   - ○ **B.** On-path attack
   - ○ **C.** Tailgating
   - ○ **D.** DDoS attack
   - ○ **E.** Rainbow table

4. A hacker executed a coded attack against a vulnerability that has not yet been addressed by anyone. This is an example of what kind of attack?

- **A.** DDoS attack
- **B.** Spoofing attack
- **C.** Zero-day attack
- **D.** Brute-force attack

5. What is the primary method used in vishing to deceive individuals?
   - **A.** Sending fraudulent emails
   - **B.** Distributing infected software
   - **C.** Making phone calls with automated messages
   - **D.** Creating fake websites
6. What is the primary function of an evil twin in a wireless network attack?
   - **A.** To distribute malicious software through email attachments
   - **B.** To impersonate a legitimate access point and capture user data
   - **C.** To physically damage network hardware
   - **D.** To manipulate employee behavior through social engineering tactics

Cram Quiz Answers

1. **A.** A brute-force attack uses a combination of letters, numbers, and symbols to guess passwords, PINs, and passcodes. In contrast, a dictionary attack uses a list of words. Social engineering is an attempt to manipulate people into providing confidential information. A zero-day attack is an attack that has not yet been seen or documented, and it is very difficult to prepare for such attacks.

2. **C.** This is an example of phishing. Phishers use email to trick a person into divulging confidential information. While it could be said that the website that was accessed is impersonating the actual banking website, that would be more of a spoof; with true impersonation, a person mimics another person. Dumpster diving involves a person hunting through garbage or recycling to find confidential information. With shoulder surfing, a person attempts to get information by sight by, for example, looking over a person's shoulder as that person types in a password.

3. **D.** In a distributed denial-of-service (DDoS) attack, many computers (zombies) work together in an attempt to bring down a server or router. While it makes use of a botnet, not all botnets are necessarily bad, nor is a botnet an attack. An on-path attack is a type of spoof in which a person uses a computer to intercept and either use or change data that is captured. Tailgating is a type of social engineering attack in which a person attempts to enter a secure area by following another person without that person's knowledge. A rainbow table is a set of precalculated encrypted passwords located in a lookup table.

4. **C.** A zero-day attack is an attack that exploits vulnerabilities that have not yet been discovered (besides by the attacker, that is). A DDoS attack is an attack that incorporates many systems in a collective attack against a server or network device. A spoofing attack involves technical impersonation; for example, a computer system sitting between a client and a server may impersonate the server in an attempt to retrieve user data. A brute-force attack is a password-based attack in which every conceivable password is attempted.

5. **C.** Vishing is initiated via a phone call, often using an automated VoIP system or home-brewed private branch exchange (PBX). These calls frequently use prerecorded messages to mimic legitimate institutions. Sending fraudulent emails is the method used in standard phishing, not vishing. Distributing infected software, while a cyber threat, is not the core method of vishing.

Creating fake websites is also a method of standard phishing, not vishing.

6. **B.** An evil twin is a rogue, counterfeit, and unauthorized wireless access point that uses the same SSID name as a nearby wireless network to gain valuable information and passwords from those users. Distributing malicious software through email attachments describes a Trojan horse, for example, not an evil twin. Physically damaging network hardware is not the main purpose of an evil twin attack. While social engineering can be used in conjunction with an evil twin, the core function is the impersonation of a wireless access point, not direct social manipulation.

It's easy to become paranoid when learning about cybersecurity attacks, but they are out there and you need to be prepared. Be a little paranoid, but don't completely wrap your head in tin foil quite yet. Let's continue!

Chapter 48

Workstation Best Practices

This chapter covers the following A+ 220-1202 exam objective:

- **2.7** – Given a scenario, apply workstation security options and hardening techniques.

As a system administrator, you have to make sure that users can get access to only what they need and that no one else can masquerade as a legitimate user. User accounts can be secured by using a combination of strong passwords, password policies, restrictions, account lockouts, and, in general, good account management, which requires not only solid configuration but also monitoring and auditing of user accounts. While many of the techniques in this chapter are designed for Windows, some of the concepts can be easily incorporated into any operating system.

ExamAlert

Objective 2.7 concentrates on data-at-rest encryption, password best practices, BIOS/UEFI passwords, end-user best practices, account management, changing the default administrator's user account/password, disabling AutoRun/AutoPlay, and disabling unused services.

Usernames and Passwords

The username/password combination is the most common type of authentication for gaining access to computers. The username is known to all parties involved and can be seen as plaintext when typed. In some cases, the user has no control over their username; in other cases, the username might be a name or an email address or might be selected by the user. For example, you might use a sign-in to access the Microsoft Store for apps; in this case, it is typical to use your email address as your username. You can see this username, it shows up on the screen, and you can be identified by it. The password is either set by the user or created automatically for the user. This password, however, is not something anyone else should know or see.

It is common knowledge that a strong password is important for protecting a user account, whether the account is with a bank, at work, or elsewhere. But what is a strong password? Many organizations define a strong password as a password with at least 10 characters, including at least 1 uppercase letter, 1 number, and 1 special character. The best passwords have similar requirements but are 16 characters or more. Many password-checker programs on the Web can help you get an idea of what is considered "strong." Table 48.1 shows a strong password and a "best" password.

TABLE 48.1 **Strong and Stronger Passwords**

Password	Strength of Password
|Ocrian7	Strong
This1sV#ryS3cure	Very strong, or "best"

Notice that the first password in the table uses the | (pipe) symbol instead of the letter L. This is a special character that shares the \ (backslash) key on the keyboard. The second password uses 16 characters, including 3 capital letters, 2 numbers, and a partridge in a pear tree…um, we mean 1 special character. (Just checking whether you're still with us!) Although a partridge wouldn't help your password security, the other methods make for an extremely strong password that would take a supercomputer a long time to crack. (Of course, the passwords in the table are now weak because they

have been mass printed and are *known*. They are just examples and should not be used on a system.)

According to the latest National Institute of Standards and Technology (NIST) guidelines, the new recommended password practice is to prioritize longer password lengths over complex character combinations, meaning users should create passwords that are at least 12–16 characters long, with a focus on using unique phrases or random character strings rather than enforcing specific character types like uppercase, lowercase, numbers, and symbols; additionally, most recent guidelines recommend against mandatory password expiration, only changing passwords when a breach is suspected, and strongly encourage using multifactor authentication (MFA).

Key points of the updated password guidelines are as follows:

- **Length is key:** Prioritize password length over complexity, aiming for at least 12–16 characters.
- **No more forced complexity:** Avoid requiring specific character types (uppercase, lowercase, numbers, symbols) in passwords.
- **Passphrases encouraged:** Use memorable phrases as passwords, ensuring they are long and unique.
- **No mandatory expiration:** Don't force users to change passwords at regular intervals unless there is evidence of a breach.
- **Use a password manager:** Utilize a password manager to generate and store strong, unique passwords for each account.
- **MFA is essential:** Always enable multi-factor authentication for added security.

Password length can even go beyond 16 characters. In fact, NIST says the longer the better, as long as your users are set up with a secure method of either remembering those passwords/passphrases or pasting them from a password vault. In fact, in 2024, NIST actually recommended passwords with at least 64 characters! They also stated that if you are not using a password manager to remember these crazy, long passwords, then you should use modified, nonsensical sentences with various character types. For example, change the sentence *I desire purple rainbows showering white*

stars on me to *1D3s1r3Purpl3Ra1nb0wsSh0w3r1ngWh1t3St@rs0nMe**. Wow, that's quite a password, but it's unique, has a long character count, is complex, and, while nonsensical, can be memorized if not using a password vault/manager. Just remember: Because this example is printed now, don't use it!

Note

Recent NIST guidelines have shifted the focus of password security from complexity to length, recommending passwords or passphrases of at least 64 characters for maximum protection. This approach emphasizes using longer, unique phrases or random strings rather than enforcing complex character combinations. Furthermore, mandatory password expiration is discouraged, advocating for changes only when a breach is suspected. Crucially, the guidelines strongly promote the use of password managers for generating and securely storing strong, unique passwords, and mandate the implementation of multifactor authentication (MFA) as an essential security measure.

Password Vaults/Managers

Remembering passwords can be hard, and writing them down is not a good option. Luckily, there is built-in credential storage in every major operating system, or you can use dedicated password manager applications.

Windows:

Credential Manager

- Windows has a built-in Credential Manager that stores login credentials for websites, applications, and networks. While it stores passwords, it lacks the full feature set of a dedicated password manager.

- For a more robust solution, consider using third-party password manager applications that offer features like password generation, secure sharing, and cross-platform syncing. Popular third-party applications are 1Password and Bitwarden.

macOS:

Keychain and FileVault

- macOS utilizes Keychain to store passwords, certificates, and other sensitive information. FileVault encrypts the entire disk, adding an extra layer of security. iCloud Keychain allows syncing passwords across Apple devices.
- Again, for more cross platform options, third-party applications are highly recommended; 1Password and Bitwarden work on macOS too!

Linux:

- Linux distributions often rely on various keyring services, such as GNOME Keyring or KWallet, to store credentials.
- Because of the wide variety of Linux distributions, there is not one single password storage system. Dedicated password managers like 1Password or Bitwarden—yep, the same two have cross-platform support—are popular choices for Linux users, providing strong encryption and cross-platform compatibility.

BIOS/UEFI Passwords

BIOS and UEFI passwords serve as crucial security barriers, safeguarding a computer's firmware settings from unauthorized modifications. The *system password* acts as a gatekeeper, demanding authentication before the operating system initiates, effectively preventing unauthorized bootups. Conversely, the *supervisor password* restricts access to the BIOS/UEFI setup utility itself, ensuring that critical firmware configurations, such as boot order or hardware settings, cannot be altered without proper authorization. These two password types work in tandem to protect the system at its most fundamental level, thwarting attempts to bypass security

measures or introduce malicious changes. See Chapter 16, "Motherboards and Add-on Cards," for more information.

ExamAlert

Understand what is required for a strong, complex password.

Password Policies

A password might need to meet certain requirements, or it might need to be changed at regular intervals, among other policies. Figure 48.1 shows an example of the default password policy in the Local Security Policy window on a Windows computer. To open the Local Security Policy window, go to **Administrative Tools** or go to **Run > secpol.msc**. Then navigate to **Security Settings > Account Policies > Password Policy**.

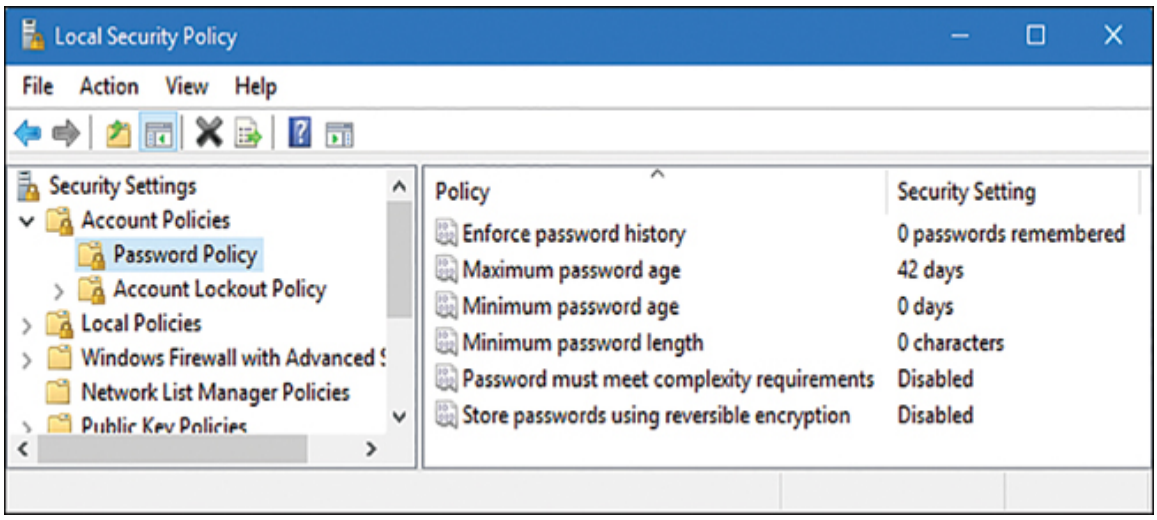


FIGURE 48.1 **Default Password Policy in Windows**

As shown in the figure, there are several items that you can configure (or that can be configured by the network administrator centrally if the computer is part of a domain). The important ones for the exam include the following:

- **Enforce password history:** When this policy is defined, users cannot use any of the passwords that are remembered in the history. If you set the history to 3, the last three passwords cannot be used again when it is time to change the password.
- **Maximum password age** and **Minimum password age:** These settings define exactly how long a password can be used. This is also known as password expiration. The maximum is initially set to 42 days but does not affect the default administrator account. To enforce an effective password history, the minimum must be higher than 0 days.
- **Minimum password length:** This setting requires that the password must be at least the specified number of characters. For a strong password policy, set this to between 10 and 16 (at least!). Better yet, follow the new NIST guidelines and make it 64 characters.
- **Password must meet complexity requirements:** This means that passwords must meet three of these four criteria: uppercase characters, lowercase characters, digits between 0 and 9, and nonalphabetic characters (special characters).

> **Note**
>
> For more information on some password best practices, see https://www.microsoft.com/en-us/research/publication/password-guidance/ and the NIST special publication SP 800-63B: Digital Identity Guidelines: https://pages.nist.gov/800-63-3/sp800-63b.html.

Account Management and End-User Best Practices

Now that you know more about secure passwords and password policies, let's talk about securing user accounts for Windows. To access user accounts in Windows 11, you can use the Settings app or the Command Prompt.

To use the Settings app, follow these steps:

1. Open Settings by pressing Windows+I or right-clicking the Windows button and selecting **Settings**.
2. Select **Accounts** from the left sidebar.
3. Select **Other Users** in the Account Settings section.
4. To view family accounts, select **Family**.

To use the Command Prompt, follow these steps:

1. Open the Command Prompt by pressing Windows+R and typing **CMD**.
2. Type the **net user** command and press Enter.
3. To view more details about user accounts, type the **wmic useraccount get** command and press Enter.

For more information on managing user accounts in Windows, see https://support.microsoft.com/en-us/windows/manage-user-accounts-in-windows-104dc19f-6430-4b49-6a2b-e4dbd1dcdf32.

There are a few things you can do to secure passwords and password policies, as described here. (Refer to Figure 48.2 while reading through the list.)

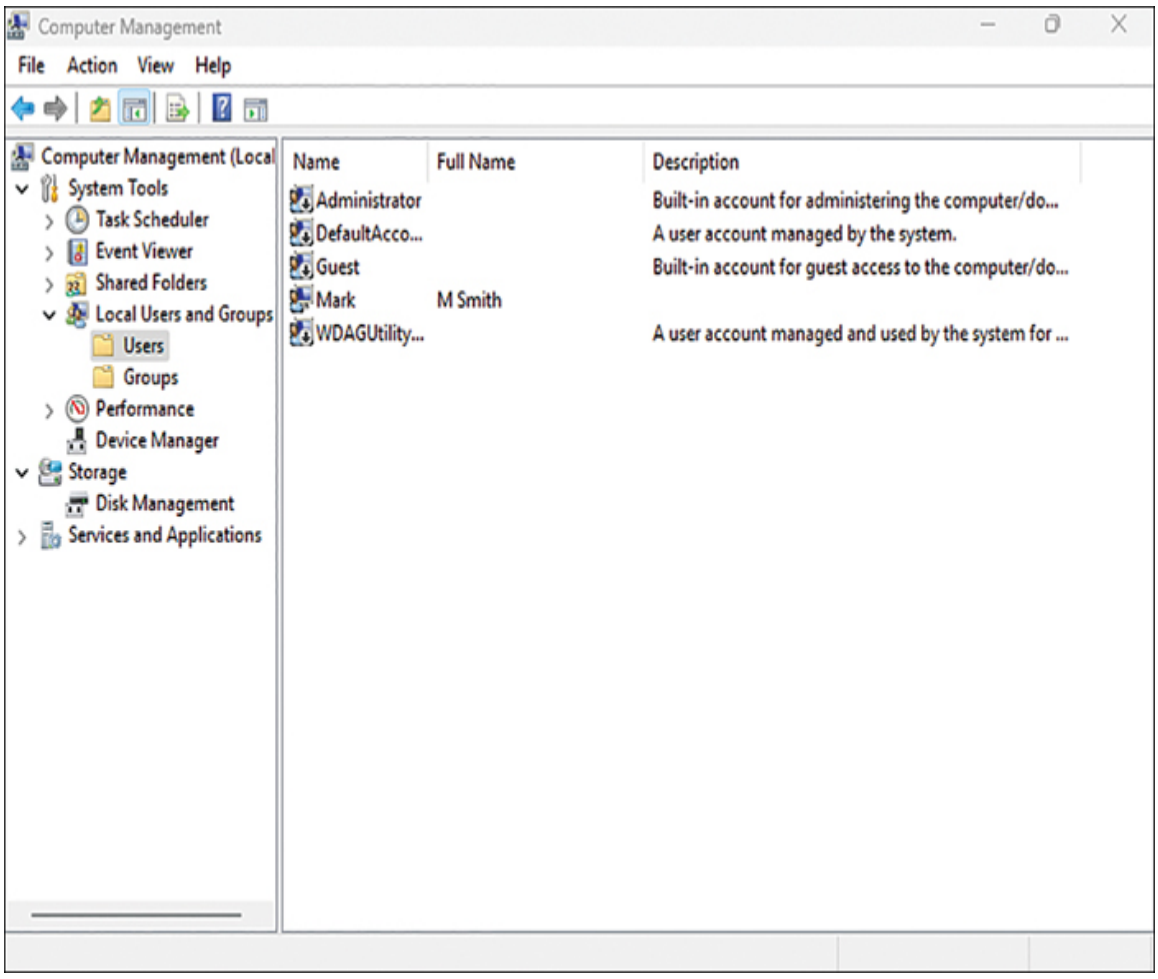


FIGURE 48.2 **Computer Management Window, Showing Users**

- **Rename and password protect the Administrator account:** To configure this account, navigate to **Computer Management > System Tools > Local Users and Groups > Users** and locate the Administrator account. Right-click the account to open a drop-down menu in which you can rename the account and/or give it a password. (Just remember the new username and password!) It's great to have this additional Administrator account on the shelf just in case the primary account fails. Many organizations do just this and disable the original Administrator account. If the account is disabled, you can enable it if necessary. Right-click the account and select **Properties**. In the **General** tab, deselect the **Account is disabled** checkbox. Alternatively, open PowerShell or the Command Prompt (as an admin) and type **net**

user administrator /active:yes. Of course, you have to have administrative privileges to perform these actions.

- **Verify that the Guest account and other unnecessary accounts are disabled:** Navigate again to **Local Users and Groups > Users**, right-click the account in question, select **Properties**, and then select the **Account is disabled** checkbox (which is disabled by default in most versions of Windows). You can tell that it is disabled if it has a black down arrow over the account icon. You can also delete accounts (aside from built-in accounts, such as the Guest account); however, companies usually opt to have them disabled so that they can retain auditing information that is linked to those accounts.
- **Restrict user permissions:** Users are created as standard users by default, but it's always a good idea to audit the user accounts and make sure that they don't have any unnecessary group memberships that could give them more power than they require. This is part of the principle of least privilege: The less a user can do, the more secure the system will be.
- **Set logon time and computer restrictions:** In a Windows domain, you can allow and disallow certain hours of the day that a user can log on to the network. In the user's Properties dialog box, go to the **Account** tab and click the **Logon Hours** button. From there, you can configure when the user is allowed to log on. For example, in Figure 48.3, user Bob can only log on to the domain Monday through Friday from 8 a.m. to 6 p.m. You can also specify individual computers that the user can log on to by clicking the **Log On To** button in the Properties dialog box. For temporary employees and contractors, it's a good idea to configure account expiration, which is at the bottom of the Account tab.

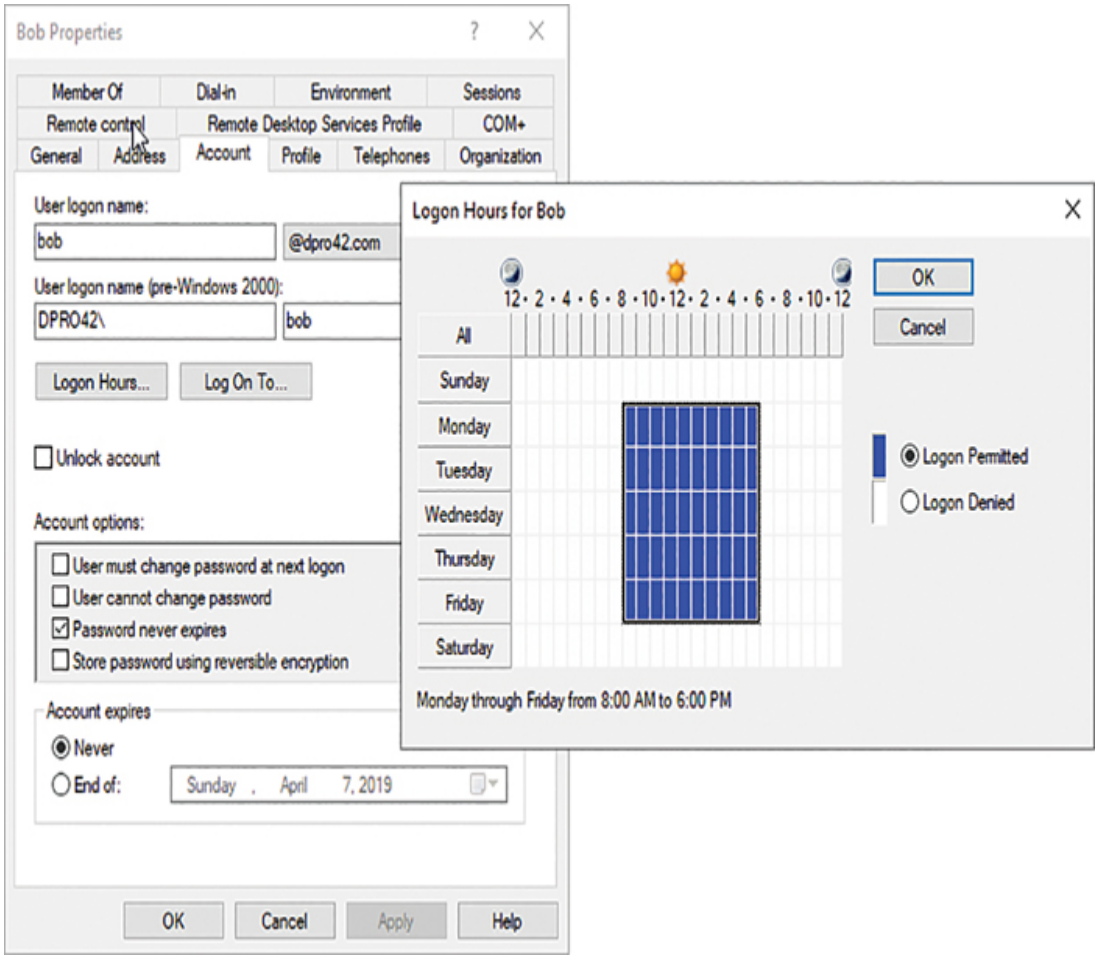


FIGURE 48.3 **Logon Hours Setting**

- **Set the account lockout threshold:** If a user attempts to log on to a system and is unsuccessful (after a specified number of attempts), that user will be locked out of the system. The settings and thresholds for logon can be configured in the Local Security Policy window. Navigate to **Security Settings > Account Policies > Account Lockout Policy**. From here, you can set the account lockout threshold to a certain number of invalid logons, set how long the user will be locked out, and set the amount of time until the lockout counter is reset. If an account is locked out and you need to unlock it immediately, follow one of the options at the end of the first bullet.
- **Set account expiration dates:** Note that while NIST now suggests only setting these dates in the case of a breach, it is still important to know. In Windows 11, account expiration dates are managed through the Local

Users and Groups management console. To access it, press the Windows key, type **lusrmgr.msc**, and press Enter. Navigate to the Users folder, right-click the desired user account, and select **Properties**. On the Account tab, you'll find the Account Expires option. Here, you can select a specific date from the calendar to set the account's expiration. After you select the date and click **Apply** or **OK**, the account will automatically be disabled on the chosen expiration date. Note that this feature is primarily available in Windows 11 Pro, Enterprise, and Education editions, not in the Home edition.

- **Use password managers:** Whether you're using the operating system's built-in credential manager or third-party applications, it is suggested to use some sort of password manager. See the previous section, "Password Vaults/Managers," for more information.

ExamAlert

Know how to enable/disable accounts, reset passwords, and modify password policy!

Note

Lockouts due to forgotten passwords are common in organizations. Sometimes a user will use several passwords to gain access to various systems, making the problem worse. Having several complex passwords can be confusing to a user and may lead to many tech support calls requiring accounts to be unlocked. To combat this situation, use *single sign-on (SSO)*, or federated identity management. Remember that with SSO, a user needs only one password to gain access to two or more systems.

It's important to note that when logging on to a Microsoft network, the logon process is secured by the Kerberos protocol, which is run by the Active Directory domain controller. This adds a layer of protection for the username and password as they are being authenticated across the network.

Regardless of whether or not a user is part of a domain, when the user takes a break or leaves for lunch, that user should either log off or lock the computer. The computer can be locked by pressing Windows+L. The operating system then goes into a locked state, and the only way to unlock the computer is to enter the username and password of the person who is logged in to the computer. The difference between locking and logging out is that a locked computer leaves all the session's applications and files open; logging out closes all open applications and files.

Aside from locking a computer manually, a user can opt to put the computer to sleep after a certain period of time or enable a password-protected screensaver, both of which will force the user to log on when returning to the computer. Sleep settings can be accessed in Windows 11 by navigating to **Settings > System > Power** or by navigating to **Control Panel > All Control Panel Items > Power Options > Edit Plan Settings**. Further configuration can be performed within the Power Options dialog box by clicking the **Change advanced power settings** link. To set the screen saver to require a password when the system resumes in Windows, for example, go to **Settings > Personalization** (or right-click the desktop and select **Personalize**). Then go to **Lock screen > Screen saver settings**. In the dialog box, check **On resume, display logon screen**.

Finally, end users should be educated about securing critical hardware and personally identifiable information (PII). For example, a laptop could be secured with a cable lock or, at the very least, put away in a laptop bag out of sight. And PII such as passwords, ID cards, and so on should not be left out on a desk or under a keyboard. Users should follow a company clean desk policy. These are the first places malicious insiders and other con artists will look. Anything that can be traced back to the end user or the organization should be secured.

Disabling Unused Services

Disabling unused services on Windows 11 enhances security and performance. Unnecessary services consume system resources, potentially creating vulnerabilities for attackers to exploit. By reducing the attack surface, you minimize the risk of unauthorized access. Furthermore,

disabling background processes frees up RAM and CPU, leading to improved responsiveness and faster boot times.

To disable services, press Windows+R, type **services.msc**, and press Enter. Locate the service you want to disable, right-click it, and select **Properties**. In the **Startup type** drop-down, choose **Disabled** or **Manual** (if you might need it occasionally). Be cautious, because disabling critical services can cause system instability. Research unfamiliar services before disabling them, and consider creating a system restore point beforehand.

Disabling AutoPlay/AutoRun

If you disable AutoPlay, removable media won't automatically start its AutoRun application (if it has one), and any embedded malware won't have a chance to infect the system before you scan the media. To disable AutoPlay/AutoRun in Windows, you have a couple of options.

One way to do this in Windows 11 is to open **Settings** and then click **Bluetooth & devices**. Next, select **AutoPlay** from the right side. Finally, set the AutoPlay slider button to **Off**.

Or, to use the Group Policy Editor, complete the following steps:

1. Go to the Run prompt and type **gpedit.msc**. The Local Group Policy Editor appears. (This is not available in some editions of Windows.)
2. Navigate to **Computer Configuration > Administrative Templates > Windows Components > AutoPlay Policies**. From here, you can modify how AutoPlay and AutoRun function.
3. Double-click the **Turn off AutoPlay** setting. This displays the Turn off AutoPlay configuration window.
4. Click the **Enabled** radio button and then click **OK**. When you do this, you are actually enabling the policy named Turn off AutoPlay.

ExamAlert

Know how to disable AutoPlay in Windows Settings and the Group Policy Editor.

Note

We discussed data encryption further in Chapter 45, "Windows Security Settings." When you enable BitLocker encryption as described in Chapter 45, this is known as *data-at-rest encryption*. It encrypts the data stored on a physical device in the event of physical theft rather than when it's actively being used, such as data-in-transit or data-in-use encryption—think SSL/TLS encryption for that.

The Information Security Field Is Enormous

As you can see, you could configure security for Windows all day—and still have more to do. This is one of the reasons the computer security field is so massive—and this is just Windows. Remember that these last couple of chapters have given an overview of how to secure Windows and Windows networks. Keep reading and learning because there is a lot of work to do when it comes to computer and data security!

Cram Quiz

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

1. Which of the following is the strongest password?

- ○ **A.** |ocrian#
- ○ **B.** Marqu1sD3S0d
- ○ **C.** This1sV#ryS3cure
- ○ **D.** Thisisverysecure

2. Your boss is concerned that people who have been terminated will come back in the building and attempt to log on to the network using passwords that they used in the past. What should you do to help protect against this? (Select the two best answers.)

- ○ **A.** Set up a password length policy.
- ○ **B.** Configure an account lockout threshold.
- ○ **C.** Immediately disable the accounts of people who have been terminated.
- ○ **D.** Set logon time restrictions.
- ○ **E.** Disable the Guest account.

3. A customer complains that while he was away at lunch, someone used his computer to send emails to other coworkers without his knowledge. Which of the following should you recommend that the user do?

- ○ **A.** Enable a screensaver.
- ○ **B.** Unplug the network cable before leaving for lunch.
- ○ **C.** Use the Windows lock feature.
- ○ **D.** Enable the out-of-office message in email when leaving for lunch.

4. Which of the following best describes encryption?

- ○ **A.** Prevents unauthorized users from viewing or reading data
- ○ **B.** Prevents unauthorized users from deleting data
- ○ **C.** Prevents unauthorized users from posing as the original source sending data
- ○ **D.** Prevents unauthorized users from decompressing files

5. How can you prevent applications from automatically executing and possibly infecting a computer with malware when removable media is inserted?

- ○ **A.** Enable the account lockout threshold policy.
- ○ **B.** Turn on BitLocker.
- ○ **C.** Turn off BitLocker-To-Go.
- ○ **D.** Disable AutoPlay.

6. Which of the following account settings is used to limit the time of day a user is allowed to log on to a Windows system?
   - ○ **A.** Account Lockout Threshold
   - ○ **B.** Logon Hours
   - ○ **C.** Account Expiration
   - ○ **D.** User Permissions
7. Which of the following is a built-in credential storage option in macOS?
   - ○ **A.** Credential Manager
   - ○ **B.** GNOME Keyring
   - ○ **C.** Keychain
   - ○ **D.** KWallet

Cram Quiz Answers

1. **C.** This1sV#ryS3cure incorporates uppercase and lowercase letters, numbers, and special characters, and it is 16 characters long. That makes it the strongest password of the listed options. |ocrian# has special characters but is missing uppercase letters and numerals—and it is only 8 characters long. Marqu1sD3S0d does not have any special characters. Thisisverysecure is 16 characters long and has 1 capital letter but does not have any numerals or special characters.
2. **B and C.** The best answers are to configure an account lockout threshold and immediately disable the accounts of anyone who has

been terminated. A common method is to use the "three strikes and you're out" rule for account lockout, meaning that a person can attempt to log on three times before the account is locked out. But, more importantly, you should disable (or lock) the accounts of people who have been offboarded or terminated. The other options are all good security options in general but won't help much with disgruntled former employees who are attempting to get into the system. Also, some type of authentication system should be in place so that these people cannot get access to the building.

3. **C.** Tell the customer to lock the computer (by pressing Windows+L or by using the Start menu) before leaving for lunch. As long as there is a strong password, other coworkers should not be able to access the system. Screensavers by themselves do not secure systems, but a user can enable the password-protected screensaver feature (but should be aware that there is a delay before the screensaver turns on). Unplugging the network cable is not a legitimate answer; plus, it can always be plugged back in. The out-of-office message will reply only to people emailing the user; it won't stop outgoing emails.

4. **A.** Encryption prevents unauthorized users from viewing or reading data. Properly configured permissions prevent unauthorized users from deleting data or attempting to decompress files. A strong logon password prevents unauthorized users from posing as the original source sending data.

5. **D.** If you disable AutoPlay, removable media won't automatically start its AutoRun application (if it has one), and any embedded malware won't have a chance to infect the system before you scan the media. The account lockout threshold specifies the number of times a user can attempt to log on to Windows before being logged off. BitLocker and BitLocker-To-Go are used for encryption, not for blocking removable media from automatically executing files.

6. **B.** Logon Hours allows or disallows certain hours of the day that a user can log on to the network. You configure this setting in the user's Properties dialog box under the Account tab by clicking the

Logon Hours button. The Account Lockout Threshold setting is related to the number of unsuccessful logon attempts before an account is locked out. The Account Expiration setting is for setting a date when an account is automatically disabled. User Permissions defines what a user can do on the system (such as read, write, or execute files).

7. **C.** macOS utilizes Keychain to store passwords, certificates, and other sensitive information. Credential Manager is the built-in credential storage option for Windows. GNOME Keyring is a keyring service commonly used in Linux distributions using the GNOME GUI, while KWallet is another keyring service used in Linux distributions using KDE.

Awesome! You're doing "Grrreat" in the words of Tony the Tiger. This important chapter wraps up Windows security. Be sure to review the chapter and your notes, take a break, and then continue!

Chapter 49

Mobile Device Security

This chapter covers the following A+ 220-1202 exam objective:

- **2.8** – Given a scenario, apply common methods for securing mobile devices.

Mobile devices need to be secured just like any other computing devices. But due to their transportable nature, some of the security techniques will be a bit different and can be more challenging for a system administrator. We recommend that you prepare for the possibility of a stolen, lost, damaged, or compromised device. The methods in this chapter can help you recover from such problems and also aid you in preventing them from happening.

ExamAlert

Objective 2.8 focuses on hardening techniques, patch management, endpoint security software, locator applications, remote wipes, remote backup applications, failed log-in attempt restrictions, and policies and procedures.

Hardening Techniques

Mobile device hardening strengthens security through various techniques. Device encryption is critical, rendering data unreadable without the correct passcode, safeguarding sensitive information in case of loss or theft. iOS employs hardware-based encryption using a dedicated Secure Enclave, which isolates cryptographic keys from the main processor, whereas Android utilizes file-based encryption or full-disk encryption, depending on the device and Android version, leveraging hardware acceleration when available.

Configuration profiles, often deployed via *mobile device management (MDM)* systems, enforce security policies. These profiles can restrict app installations, enforce strong passwords, disable unnecessary features like Bluetooth or location services when not needed, and configure VPNs for secure network access. Combining robust encryption with tailored configuration profiles minimizes vulnerabilities and significantly reduces the risk of data breaches on mobile devices. We'll cover more details on MDM and configuration profiles later in this chapter.

Screen Locks

Because mobile devices are expensive and could contain confidential data, they are often targeted by thieves. Plus, they are small and easy to conceal, making them easy to steal. However, there are some things you can do to prevent theft or loss, protect data, and attempt to get a mobile device back in the event that it is *misplaced*.

The first thing a user should do when receiving a mobile device is to configure a screen lock. Locking the device makes it inaccessible to everyone except experienced hackers (or someone who knows your unlock method). To unlock the device, the user has to be authenticated in one of several ways. There are several types of screen locks that a user can choose from to be authenticated. The screen lock can be something a user *knows*, such as a PIN or a password. It could also be based on something the person *is*; it might use fingerprint, voice, or facial recognition technology, which are collectively known as *biometrics*. Or, it could be something the person *does*, such as a basic swipe (which has no inherent security by itself), or a pattern that is drawn on the display, or a series of taps or knocks on the phone. Finally, in a secure environment, it could be a combination of these

different methods, which is known as *multifactor authentication (MFA)*. Figure 49.1 shows an example of an Android smartphone's screen lock options.

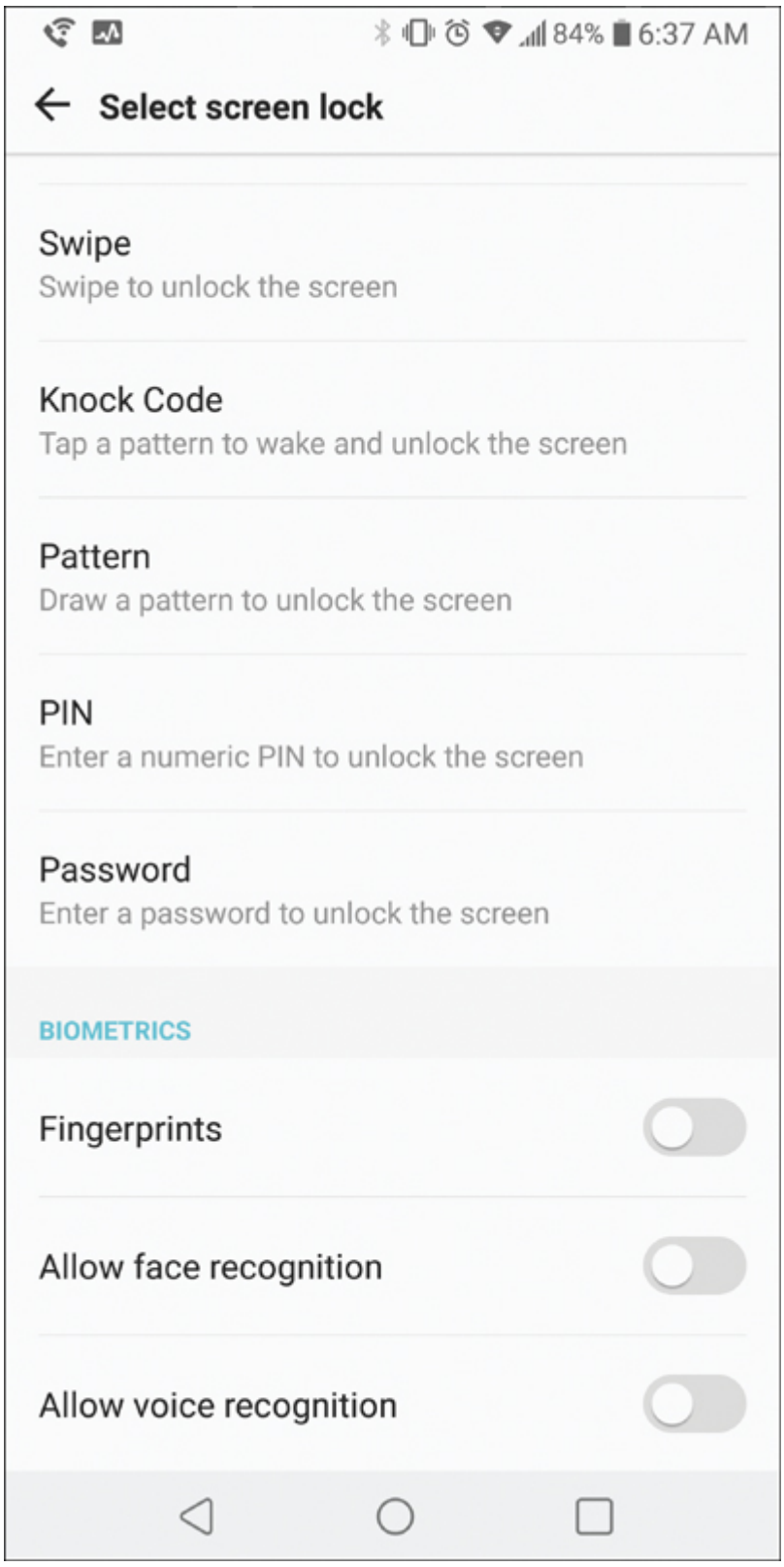


FIGURE 49.1 **Android Screen Lock Options**

A complex password is often used as a secure form of screen lock. See Chapter 48, "Workstation Best Practices," for more information about complex passwords. You can also select how long the device will wait after inactivity to lock (as part of the screen timeout). In a confidential environment, you might set this to the lowest setting—10 or 15 seconds.

Speaking of passwords, some devices have the option to make the password visible (or to make the last character typed visible). Doing so is almost never recommended because it makes the mobile device vulnerable to shoulder surfers (people looking over your shoulder to find out your password); this option should be deselected so that only asterisks (*) are shown when the user types a password.

ExamAlert

Know how to configure a screen lock using fingerprint, face, swipe, pattern, and password locks. Also know how to disable visible passwords.

Aside from the default timeout, devices can also be locked by pressing the power button quickly. If 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 may have an account lockout threshold. This means that if a user fails to be authenticated after a certain number of attempts (typically three or five), the device locks temporarily, and the user has to wait a certain amount of time before attempting to authenticate again. After that, if the user fails to be authenticated again, the timeout increases (on most devices). After a certain number of attempts, the device either needs to be connected to the computer it was last synced to or must be restored to factory condition with a hard reset (which can wipe the data). Many companies utilize a mobile device management solution. In an MDM-controlled environment, the device and/or account might be locked in this scenario, and only an administrator will be able to unlock it.

ExamAlert

Understand the consequences of entering an incorrect passcode or other authentication information too many times.

Some devices have a setting to erase the device automatically after a certain number of incorrect authentication attempts—most notably Apple iOS devices. There are also third-party apps available for download for most mobile devices that can wipe the data after a specified number of attempts. Some apps configure a device to automatically take a picture of the user after three failed attempts and email the picture to the owner of the device.

Authenticator Applications

Authenticator apps can be installed to a mobile device to help in the process of authenticating an individual. They might be used as the only method of authentication or as part of a *two-step authentication* process. The latter is common.

For example, say that you are logging in to a service provider, such as Google. Further suppose that you have initiated two-step authentication, and you have to supply not only a username and password but also, in the second step, a code that is sent to you (often by way of text message or email). The authenticator app can be used to take the place of that second step by giving you a QR code, a numeric code, or something similar. The code is preinstalled to the mobile device, but it can allow a person to log on to a service or be otherwise authenticated to something even if Internet access is not currently available on the mobile device.

Two-Step Authentication

Two-step authentication is quite common, but it is not necessarily the most secure authentication. Don't mistake two-*step* authentication with two-*factor* authentication. Two-step authentication normally requires that the person logging in have two pieces of information that the person *knows*. True multifactor authentication requires two or more different *factors* of information, such as something a person *knows* and something a person *is*.

Theft and Loss of Mobile Devices

There's an app for virtually everything. Imagine that a device is lost or stolen. If the user previously installed a *locator application* and the GPS/location service is enabled on the device, the user can track where the device is, and the organization can decide whether to get the police involved. One example is Google's *Find My Device* or Apple's *Find My*.

Even if you track your mobile device and find it, you might be too late: A hacker might be able to get past passcodes and other screen locks. It's just a matter of time before the hacker has access to the data. So, an organization with confidential information should consider installing a *remote wipe* program on mobile devices, which both Google's *Find My Device* and Apple's *Find My* services already have. As long as a mobile device still has access to the Internet, the remote wipe program can be initiated from a desktop or laptop computer, deleting all the contents of the mobile device remotely. In some cases, the command that starts the remote wipe must be issued from an MDM server.

You should also have a backup plan in place so that data on a mobile device is backed up to a secure location at regular intervals. This way, if the data needs to be wiped, you are secure in the fact that most of the data can be recovered. The type of remote wipe program, the backup program, and policies regarding how these are implemented will vary from one organization to the next. Be sure to read up on your organization's policies to see exactly what is allowed from a mobile security standpoint.

ExamAlert

Know what locator/tracker applications are and how remote wipes are used to erase confidential data in the event that a device is stolen.

Compromised and Damaged Devices

Theft and loss aren't the only risks a mobile device faces. You should protect against the chance that a mobile device will be damaged or that its security will be compromised. The device could be the victim of unauthorized account access, root access, leaked files, location tracking, camera/microphone activation, and so on. These problems could be due to a rogue application, malware installation, or other hijacking of the mobile device. You need to be prepared before such things happen.

Backups

Many organizations implement backup and remote backup policies.

Both Apple and Google provide robust remote backup and synchronization services for their respective mobile operating systems. Apple's iCloud seamlessly backs up device data, photos, and settings, allowing for easy restoration or access across Apple devices. Google's Google One subscription service offers similar capabilities for Android, backing up data, photos, and app settings to Google's cloud, accessible across various devices. Various manufacturers of Android devices also have their own proprietary cloud backup programs. Beyond backups, both companies offer integrated productivity suites: Apple's iWork and Google's Workspace, enabling document creation, collaboration, and cloud storage, further enhancing data accessibility and continuity. Additionally, both companies provide device location services, allowing users to remotely locate, lock, or wipe their devices in case of loss or theft, enhancing security and data protection. If you don't want to use Google or Apple products, there are other third-party apps that will allow you to back up your data to a PC or to the cloud as well.

Updates

One way to protect mobile devices from compromise is to patch or update the operating system. This is called *patch management*. By default, you will be 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, this is generally the About Device

section, though actual navigation can change from version to version. You are usually notified of updates in the notification panel/status screen.

If you find that system updates or security updates are available for download, you should probably install them right away. Security patches account for a large percentage of system updates because a lot of attackers around the world are trying to compromise the Android operating system. But let's be real: Attackers will go for any OS if it catches their fancy, be it Android or iOS or any other operating system! Updates for iOS can be located at **Settings > General > Software Update** (or a similar path).

Note

Remember that the exact path to the update feature in a mobile OS can be different from one manufacturer to the next and from one device to the next. In addition, new versions of the software are constantly being released, resulting in changed paths and modified setting names. However, you can find out the path you need by consulting the software manufacturer's website (visit the following links), by going to the device manufacturer's website, or even by going to your cellular provider's website:

- **iOS:** https://support.apple.com/ios
- **Android:** https://support.google.com/android

ExamAlert

Know how to check for, and perform, Android and iOS updates.

In addition to system updates, you should also update your applications. An out-of-date application, or app, can cause serious security concerns. Updating apps on iOS and Android is straightforward. On iOS, navigate to the App Store, tap your profile icon, and scroll to see pending updates; tap **Update All** or individual app updates. On Android, open the Google Play

Store, tap your profile icon, go to Manage Apps & Device, and select **Updates available**; tap **Update all** or individual app updates. Both platforms also offer automatic updates: on iOS, enable App Updates in **Settings > App Store**, and on Android, enable Auto-Update Apps in the Play Store's settings. Regularly updating apps is crucial for security patches and new features.

Antivirus/Antimalware/Firewalls

Updates are great, but they are not created to specifically battle viruses and other malware. So, just as there is antivirus/firewall software for PCs, there is antivirus/firewall software, called *endpoint security software*, for mobile devices. A number of third-party applications can be downloaded (and possibly paid for) and installed on a mobile device. Some examples for Android include F-Secure Mobile Security, McAfee, Avast, Bitdefender, and Sophos. Different terms are used to describe the various protective software that is installed to a mobile device: antivirus, antimalware, firewall, content filtering, endpoint protection platform, and mobile intrusion prevention system (MIPS). Be ready to install and configure any of these on mobile devices.

iOS, on the other hand, is a tightly controlled operating system. One of the benefits of being a closed-source OS is that it can be more difficult to write viruses for it; however, there is no OS that can't be compromised. For the longest time, there was no antivirus software for iOS—that is, until 2011, when a type of jailbreaking software called *jailbreakme* used a simple PDF to move insecure code to the root of a device, causing a jailbreak. Ever since, antivirus software has been a reality for iOS-based devices.

iOS *jailbreaking* is the process of removing the limitations that Apple imposes on its devices that run iOS. Jailbreaking enables users to gain root access to the system and allows the download of previously unavailable applications and software not authorized by Apple.

In the Android world, the act of gaining "superuser" privileges is known as *rooting*. Note that performing either rooting or jailbreaking could be a breach of the end-user license agreement (EULA). It can also be dangerous. These types of hacks might require a user to wipe out the device completely

and/or install a special application that may or may not be trustworthy. Many phones are rendered useless or are compromised when attempting such a procedure. Applications that have anything to do with rooting or jailbreaking should generally be avoided.

You also should be aware of *sideloading*. Sideloading apps on Android, installing apps from sources outside the Google Play Store, poses significant security risks. These apps bypass Google's security checks, potentially containing malware or vulnerabilities that could compromise your device and data. This behavior differs from rooting, which grants administrative-level access to the operating system, allowing deep customization but also increasing vulnerability to attacks. Recently, iOS has introduced limited sideloading in certain regions, allowing installation from approved third-party app stores. This practice contrasts with jailbreaking, which removes iOS's built-in restrictions, granting extensive access and customization but drastically weakening security. While iOS sideloading undergoes some level of vetting from Apple, it still increases the attack surface compared to app store–only installations, but unlike jailbreaking, it does not give complete access to the underlying OS.

ExamAlert

Understand the terms *jailbreaking, sideloading,* and *rooting*.

MDM and MAM

Any antivirus software for Android or iOS should be checked regularly for updates—if the device is not configured to automatically download updates, that is. Also, as previously mentioned, for large organizations that have many mobile devices, a mobile device management suite can be implemented. An MDM server can take care of pushing updates and configuring hundreds of mobile devices from a central location. Decent-quality MDM software will secure, monitor, manage, and support different types of mobile devices across the enterprise.

MDM deals mostly with the device itself and the operating system. Contrast this with mobile *application* management (MAM), which concerns corporate-owned software and apps. Sometimes you will see MDM and MAM combined as *enterprise mobility management (EMM)*.

ExamAlert

Remember that MDM is software that is used to update and secure mobile devices from a central location. MAM focuses on managing specific corporate mobile applications.

Full Device Encryption

If a device is stolen or lost, and the authentication method is defeated, then the attacker (or another person) will have access to the data unless some kind of remote wipe is initiated. However, sometimes remote wipe will not function; for example, if the device is out of range of a radio tower, or if the attacker takes it into a shielded area such as a Faraday cage. This is when encryption can help avoid data loss.

Some mobile device manufacturers allow for encryption of the entire storage area for select devices. In other cases, you will have the option to encrypt the SD card only. Encryption is something to consider when deciding on the type of mobile devices to use in your organization. Careful planning is required when implementing encryption—not only planning the selection of the software to be used but also planning the process and knowing what to do in the event that decryption is necessary. For example, in many cases, if you encrypt an entire smartphone, the encryption process can be lengthy, taking up to an hour or two—depending on the speed of the device, the software used, and the amount of data to encrypt. One way around this issue is to encrypt only new data instead of all the data, as shown in Figure 49.2. That might be a viable time saver in a bring-your-own-device (BYOD) environment. Another consideration: It's important not to interrupt the encryption process because interruptions could cause files to be corrupted. You'll often simply encrypt new devices before they are given to a user, but that's not always the case; in any case, you should

have a device fully charged before starting the process. Finally, if files need to be decrypted, you might need to initiate a factory reset or provide the key to the data, so be sure to have a decryption plan in place.

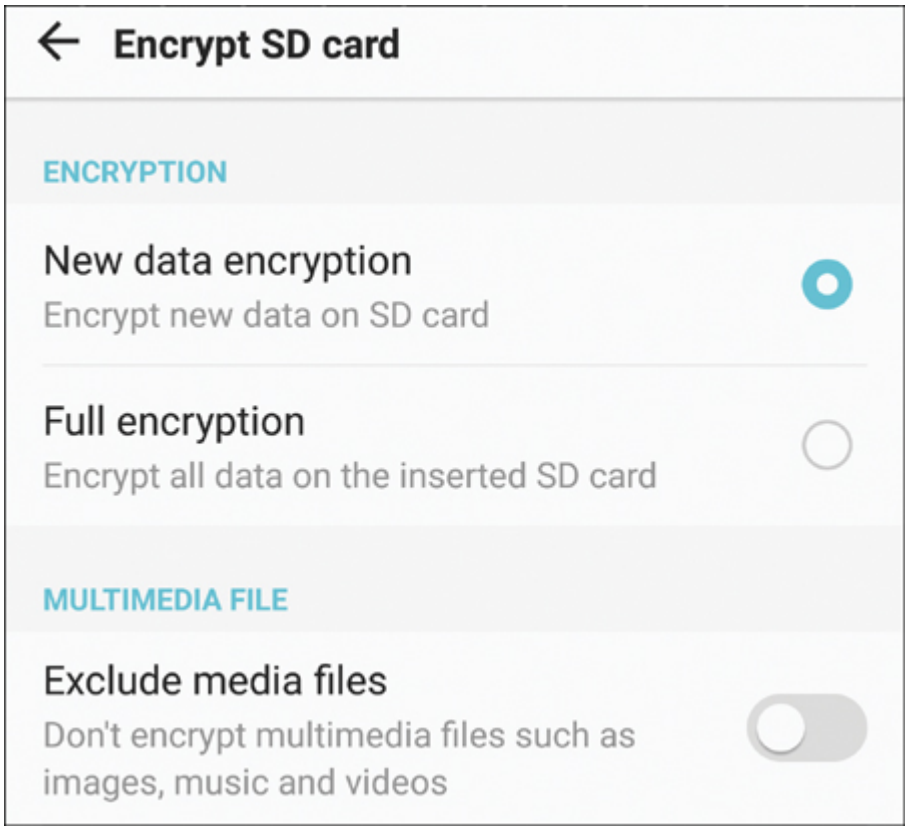


FIGURE 49.2 **SD Card Encryption Screen on an Android-Based Smartphone**

The beauty of encryption is that it makes it very difficult for hackers to make sense of the files. If the proper encryption methods are used—for instance, AES-256—then hackers would need a team of supercomputers working for a nearly infinite number of years to crack the cipher and decrypt the content (as of the writing of this book, of course). So, it is unlikely that hackers will attempt to decrypt files unless they guess that a weak or compromised cipher has been employed. Instead, the hackers will use…*other* methods. (The *nearly infinite* might be completely turned on its head if quantum computing becomes a reality, but for now, we're good.)

ExamAlert

BitLocker is a full disk encryption (FDE) feature included with Microsoft Windows operating systems. It is designed to protect data by providing encryption for entire volumes. By default, BitLocker uses the Advanced Encryption Standard (AES) encryption algorithm.

Remember that encryption and any other techniques used to secure a device or data are not foolproof. A good security person will create a *threat model*—in essence, determine what the threats and vulnerabilities are within a particular system or data set and prioritize them from most threatening to least. After the threat model has been established, you can decide on the security techniques to implement.

Note

If you liked that last paragraph, then you might be interested in pursuing the CompTIA Security+ certification or other computer security–related certifications. For more information on CompTIA Security+, see https://www.comptia.org/certifications/security.

IoT Security

Although it's no longer being tested on the 220-1202 exam, it is still important to know about securing Internet of Things (IoT) devices. The Internet of Things is a realm of technologies that is growing at an estimated rate of 1 million devices per day, and it has an economic impact measured in the trillions of dollars. In the home or at work, IoT devices need to be secured because they are potential targets for attackers. The reason is partially that many of them are easily accessible and partially that many IoT devices are not built with security in mind; this means that, out of the box, many of these devices are inherently insecure.

A lot of the techniques that we established in the previous several chapters can also be used for IoT devices: lengthy and complex

passwords/passphrases, encryption, multifactor authentication, and so on. But because of the lack of built-in security, IoT devices need a little more.

Speaking generally, we can do a few things to increase IoT security. First, we need to be able to *see* the various IoT devices because some can easily go unnoticed. Next, we should attempt to segment the devices based on their risk levels. Finally, we need to protect through monitoring, policies, and periodic testing.

From a more technical standpoint, we can employ some specific security controls—for example, avoiding the built-in defaults, using the best password managers/vaults, keeping software (and firmware) up to date and considering automating that process, encrypting network connections (data in motion), and super-securing the Internet connection and connections to other network segments. That's right, *super-secure* it: the Internet connection, associated network cables, and any routers, cable modems, and other Internet-related devices. In fact, putting your IoT devices on a separate network, like a VLAN, away from your desktop and other vital end devices is a great way to secure them. Have a guest network option on your home router? Use that to separate out your IoT devices. Remember this: The weakest link in your security chain is actually your strongest link. What we mean by this is that it only takes one weak link to allow an intruder access to your network. And don't forget to layer your security: Have a *defense-in-depth* mindset.

For larger environments, you have to think realistically. How in the world can one admin, or even a group of admins, spare the time to monitor and protect the cornucopia of IoT devices that potentially exist? In many enterprise environments, it's just not feasible. That's where third-party IoT infrastructure management tools and services come in. They use network access control (NAC) methods to see all devices, monitor the devices, and control access to and from the network. That last part goes well beyond the CompTIA A+, but it's something to consider as you progress in the IT world!

Note

For more information on IoT security, see https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program.

Policies and Procedures

Well, at some point, we had to talk about rules and who sets them. Sometimes it's the system administrator, and many times, it is an executive, upper management, or a committee. Whoever it is, you can bet that there will be policies and procedures to follow at your organization. Generally, these are designed to be helpful, but they can be somewhat challenging in a BYOD environment.

Note

Remember, BYOD = bring your own device.

In BYOD environments, people can use their personal mobile devices for work purposes. As you can imagine, this policy can create a lot of logistical problems. For example, an organization adopting BYOD has to carefully plan how data is to be separated; devices require different partitions, data access policies, data loss prevention (DLP) methods, and so on—not to mention data encryption. User agreements must be drawn up and signed by employees to acknowledge that they understand what they can and can't do with their devices while on company premises or during work hours. The organization should consider use of an MDM for the addition and removal of devices.

From a user perspective, the greatest concern is the loss of employee privacy. From a company perspective, the greatest concern is the leakage of data and any other security breaches related to mobile devices. As an entry point to a network, mobile devices have historically been less secure than typical workstation computers. That's a generalized statement, but what we are suggesting is being cautious when configuring mobile devices. There

are a lot of other issues that can present whenever you mix business and personal. However, what is more important is what you can do about it.

First, we mentioned using an MDM solution, which can be used to remotely administer a host of devices. It gives the administrator the ability to lock down devices and create those separate partitions, perhaps virtual partitions, or use containerization. Such a solution should completely separate the work data *and* apps from the personal data and apps. An MDM solution can also be used to limit how and when a user works, defining the time and the place where work can be done. In addition, an organization needs to have a user agreement, in which it clearly explains that the work data on a mobile device can be accessed and monitored by the organization at any time. Organization is also important. Keep a log of all the BYOD devices on the network; it should be kept separate from any MDM software that is running to limit mobile device sprawl. Then, enact the best practices we have talked about in this book, such as complex passwords, automatic locks, DLP, encryption, MFA, and so on. Finally, carefully decide on who will be administering the devices and keep that list short!

Note

There are also corporate-owned personally enabled (COPE) devices. In a COPE environment, the order is reversed: Instead of a person bringing in a device that is already in use and having it adjusted for work, with COPE the organization owns the device, prepares it for work, and then offers it for personal use as well. It's similar to the idea of a company car.

Note

When an employee is terminated, retires, or quits, segregating and retrieving organizational data and applications might be difficult during the offboarding process. The bring-your-own-device (BYOD), choose-your-own-device (CYOD), or corporate-owned personally enabled (COPE) policies should address how data and corporate-owned applications will be retrieved in these situations.

Profile Security Requirements

For mobile device security, a good practice is to create *security profiles*, or templates that you can use on multiple devices, as long as they are on the same platform. Then you can create a template (or set of templates) for each type of mobile device. For the most part, this means using an MDM solution. MDMs often come with prebuilt profiles for administration, but they are usually not secured, especially for your organization's particular needs. So, it's best to start with a built-in profile and then build out the security from there, based on your overall security plan, threat model, and vulnerability assessment.

Once you have begun creating a profile, start configuring it securely. For example, choose the mode that it will use, such as authenticated (which might use Transport Layer Security [TLS]) or encrypted (which might use TLS and AES). Then select a certificate that will be used when the mobile device communicates with the MDM server; be sure that it is a valid certificate with the proper encryption bit level. Configure endpoint protection, which might include Microsoft Defender Antivirus and BitLocker (for Microsoft devices) or other endpoint protection software. Your organization might also require that identity protection services be installed on the mobile devices. Think about kiosk settings (such as allow lists) to limit what a user can do on the mobile device and give the user access to the functionality that is required. Then, it's all about securely configuring services that we have talked about previously: email, VPN, Wi-Fi, DLP, and certificates. For example, Microsoft Intune supports Simple Certificate Enrollment Protocol (SCEP) and Public Key Cryptography Standards (PKCS) certificates to help with the authentication of users via Wi-Fi and VPN. Profiles can also be configured to govern how people utilize data through a cellular provider and whether or not hot spots can be created.

As mentioned, you can initiate allow lists and deny lists to either allow certain programs or disallow certain programs, respectively. Plus, consider configuring trusted and untrusted application sources for mobile devices. For example, an administrator might configure an Android-based profile

that only allows users to download apps from Google Play or, better yet, doesn't allow users to install apps *at all*. Ultimately, the idea is to lock down the devices as much as possible but still allow users to perform their work. The more you can automate this process through the use of templates and scripts, the better.

> **Note**
>
> We'll discuss policies and procedures further in the operational procedures section later in this book.

Cram Quiz

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

1. You want to prevent a user from accessing your phone while you step away from your desk. What should you do?

   - ○ **A.** Implement remote backup.
   - ○ **B.** Set up a remote wipe program.
   - ○ **C.** Configure a screen lock.
   - ○ **D.** Install a locator application.

2. Which of the following can be described as removing limitations in iOS?

   - ○ **A.** Rooting
   - ○ **B.** Jailbreaking
   - ○ **C.** Geotracking
   - ○ **D.** Antivirus software

3. Your organization is concerned about a potential scenario involving a mobile device containing confidential data being stolen. Which of the following should be recommended first? (Select the best answer.)

- ○ **A.** Remote backup application
- ○ **B.** Remote wipe program
- ○ **C.** Passcode locks
- ○ **D.** Locator application

4. You are concerned about the possibility of jailbreaks on your organization's iPhones and viruses on the Android-based devices. Which of the following should you implement? (Select the two best answers.)

- ○ **A.** Antivirus software
- ○ **B.** Firewall
- ○ **C.** Mobile device management
- ○ **D.** Device reset

5. Android-based smartphones in your organization are part of the BYOD infrastructure. They need to be able to connect to the LAN remotely using a VPN. Which of the following should you incorporate into the MDM profile for the smartphones to connect to the VPN securely? (Select the best answer.)

- ○ **A.** Antivirus software
- ○ **B.** Certificate
- ○ **C.** Remote wipe
- ○ **D.** Authenticator app
- ○ **E.** Microsoft Intune

6. Which of the following is a primary function of a mobile device management (MDM) suite?

- **A.** Primarily managing corporate-owned software and applications on mobile devices
- **B.** Securing, monitoring, managing, and supporting different types of mobile devices across an enterprise from a central location
- **C.** Focusing on separating personal data and applications from work data on employee-owned devices
- **D.** Primarily addressing the logistical problems associated with employees using personal devices for work purposes

7. What is a significant concern for organizations when implementing a bring-your-own-device (BYOD) policy?

- **A.** The potential difficulty in managing updates for a variety of device operating systems
- **B.** The loss of employee privacy due to organizational monitoring of personal devices
- **C.** The increased risk of data leakage and other security breaches related to mobile devices
- **D.** The complexity of initially configuring personal devices for work use

Cram Quiz Answers

1. **C.** You should configure a screen lock (either a pattern drawn on the screen, a PIN, a password, biometric recognition, or something else). Remote backup, remote wipe, and locator applications will not prevent someone from accessing the phone.

2. **B.** Jailbreaking is the process of removing the limitations of an iOS-based device so that the user gets superuser abilities. Rooting is a similar technique used on Android mobile devices. Geotracking is the practice of tracking a device over time. Antivirus software is used to combat malware.

3. **B.** The remote wipe program is the most important option listed. This will prevent a thief from accessing the data on the device. Afterward, you might recommend a backup program (in case the data needs to be wiped), as well as passcode locks and a locator application.

4. **A and C.** You should implement antivirus software on the local mobile devices and consider MDM for deploying antivirus updates to multiple mobile devices remotely. This can protect against viruses and other malware as well as jailbreaks on Apple devices. As of the writing of this book, firewalls for mobile devices are not common, but that could change in the future. Device resets are used to restart mobile devices or to reset them to factory condition, depending on the type of reset and the manufacturer of a device. We'll discuss those more in Chapter 54, "Troubleshooting Mobile Operating Systems and Applications."

5. **B.** Use an encryption certificate to secure the VPN connection process from the mobile devices to the LAN. Consider powerful VPN technologies such as OpenVPN, IKEv2, RADIUS servers, and so on. Antivirus software is important for mobile devices, but it won't impact secure VPN connectivity. Remote wipe is an important theft/loss solution. Authenticator apps are used to verify a user to a system and are often used in place of the second step of two-factor authentication, but they are not as secure as using a certificate. Microsoft Intune can be used to administer mobile devices, but it is not inherently secure; the profiles therein need to be configured in a secure way.

6. **B.** Decent-quality MDM software will secure, monitor, manage, and support different types of mobile devices across the enterprise. An MDM server can take care of pushing updates and configuring hundreds of mobile devices from a central location. Contrast this with mobile application management (MAM), which concerns corporate-owned software and apps. While MDM can be used to create separate partitions or containers, this is just one capability within its broader functions, not its primary focus. While MDM can help manage BYOD devices, the logistical problems

themselves are broader and include user agreements and data loss prevention strategies, which aren't solely the domain of MDM.

7. **C.** From a company perspective, the greatest concern is the leakage of data and any other security breaches related to mobile devices. While managing updates can be a challenge in a BYOD environment, MDM is a solution for pushing updates, suggesting it's a manageable issue. The "greatest concern" from a company perspective is explicitly stated as data leakage. The loss of employee privacy as "the greatest concern" is from a user perspective, not necessarily the primary concern for the organization. While initial configuration can be complex, data leakage is a more prominent concern for the organization.

Yes! You've made it to the end of another chapter. Know this: Learning never ends! Onward!

Chapter 50

Data Destruction and Disposal

This chapter covers the following A+ 220-1202 exam objective:

- **2.9** – Compare and contrast common data destruction and disposal methods.

In this chapter, we'll cover how to properly repurpose, recycle, dispose of, and destroy storage devices. By the way, we'll focus on internal storage drives, but some of the methods herein can be applied to other devices that store data: USB flash drives, memory sticks, and so on. Be ready to protect all data, wherever it exists! There's lots to do, so *let's go already*!

ExamAlert

Objective 2.9 focuses on physical destruction, recycling and repurposing best practices, outsourcing concepts, and regulatory and environmental requirements.

Data Security 101

Storage drives that contain an organization's data can be a security threat. When a drive is removed from a computer, it needs to be either stored, repurposed within the company, recycled for use by another entity, or

disposed of in a proper manner. Sanitizing the drive is a common way of removing data, but it's not the only way. The manner in which data is removed might vary depending on the proposed final destination of the device. Proper data removal goes far beyond file deletion or the formatting of digital media. The problem with high-level formats done within the operating system is the data remanence (or residue) that is left behind; with the help of third-party software, that residue can be used to re-create files. So, you have to plan how a drive will be repurposed and use some quality tools to make sure any existing data has been removed properly.

Caution

The tools and procedures described in the following sections will either remove all data on a drive or render a storage drive unusable. Proceed with extreme caution and at your own risk! Consider using virtual machines for testing.

Formatting Drives

Recall that we talked about formatting back in Chapter 33, "Microsoft Operating System Features and Tools, Part II." As mentioned in that chapter, Windows can perform quick formats and full formats; both of these are known as *high-level* formats, but they have different results. A quick format in Windows simply removes access to the files, but a full format writes zeros to the entire partition (zeroing out the drive). So, for repurposing a drive, the full format is the better option because it is a form of overwriting.

However, the CompTIA A+ objectives use the term *low-level format*. Also known as a physical format, a low-level format is something that is done to mechanical drives by the manufacturer. Modern hard disk drives are low-level formatted at the factory, and this technique should be done to a drive only once under normal circumstances; it physically creates the tracks and sectors on a hard disk drive. Older hard disk drives (from the 1980s and 1990s) could be low-level formatted from the BIOS in an effort to extend the lifespan of those drives, but low-level formatting can be damaging to a

drive. Today, the term *low-level format (LLF)* has taken on a little more meaning for some people. Some consider commands such as **dd** (which can zero out the drive) and **hdparm**, programs such as GParted, and some other third-party tools to be LLF tools. However, the reality is that they either zero out a drive or simply remove and create partitions, so they are not really low-level formatting the drive. However, some of these tools *can* be more effective than a basic Windows format.

Regardless, all of these processes have to be performed from outside the partition and file system that is to be formatted or overwritten. So, for example, to rewrite a Windows system partition, you could boot a computer to a live Linux flash drive (running Ubuntu or another distro) and run the command or program required on the target Windows system partition.

Overwriting Drives

Let's talk about deleting versus overwriting for a moment. If you delete a file on a drive, the OS will not be able to access it anymore. However, in most systems, the file remains until it is overwritten, either by another file or through another process. So, deleting data is not nearly enough to secure a drive that will be repurposed or recycled. Overwriting is a better option. This can be done with programs that write various data to the drive, but a common method is to *zero out* the drive. This means writing binary zeros over every sector and all the data on the drive.

You can zero out a drive in Windows in a few ways. First, you can use the full format option in the GUI that we mentioned previously. Second, you can use the **format** command in PowerShell or the Command Prompt. For example, the following command will format the E: drive as NTFS and zero out every sector of the drive in two passes, meaning that it will run the process twice. You have to be in elevated mode to perform this procedure:

```
format E: /fs:NTFS /p:2
```

You can increase the number of passes by changing the parameter **p:2** to whatever number you wish. A company may require a particular number of passes—perhaps three—depending on the organization and the policies that

have been put in place. But remember that the more passes, the more time it will take, and the more stress that will be put on the drive.

> **Note**
>
> For more information about the **format** command and all of its parameters, type **format /?** at the command line and/or see https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/format.

The third option is to use **diskpart**, but this utility wipes the entire drive, including any existing partitions, leaving you with unallocated space. To use this utility, enter **diskpart** (in elevated mode), list the disks (with the **list disk** command), select the disk you want to zero out (for example, **select disk 1**), and then type **clean all**. (You also have to type the name of the volume to proceed.) If you want to use the drive again, it will have to be initialized, partitioned, and formatted.

For all three of these options, the process can be very lengthy, depending on the size of the drive, the speed of the drive, and the amount of data on it. To test these commands quickly, use a virtual machine with a small secondary virtual drive that is around, say, 8 GB. Remember, you have to be outside the partition or drive that you want to zero out. So, for example, if you want to zero out the E: partition, you can do it from C:.

You can also zero out a drive in Linux and macOS. We mentioned that it can be done graphically with the GParted application (which has to be installed first), but you can also do it in Terminal with the **dd** command. For example:

```
sudo dd if=/dev/zero of=/dev/sdb1
```

Here, you replace *sdb1* with whatever drive and partition you want to zero out. This particular command will zero out the first partition of the drive *sdb* (a second drive in the system). The process can take a long time, and it gives you no warnings. To watch the progress of the procedure, use the **status=progress** parameter. Afterward, you will have to reformat the

partition to the file system of your choice. Be very careful not to zero out the system partition. Use this method with extreme caution!

Zeroing out the drive can be a potentially secure way of overwriting all the data so that the drive can be repurposed within an organization. But what if a drive is to be recycled for use by another organization, or what if you want to sell a personal computer? You might want to go further. And if your organization has highly sensitive data or stores personally identifiable information (PII), then a higher standard should be employed.

For example, the DoD 5220.22-M standard specifies *sanitizing* a drive. One implementation of this standard is to perform three passes: first, overwriting the entire drive with binary zeros; second, overwriting the entire drive with binary ones; and third, overwriting the entire drive with a random bit pattern and verifying that final overwrite and logging that verification.

However, other standards are more secure, such as NIST 800-88 Rev. 1, *Guidelines for Media Sanitization* (published in 2014). 800-88 is actually broken down into three categories: clear, purge, and destroy. The 220-1202 updated objectives do not focus on the clearing and purging of media sanitization; however, it is important to know them regardless.

Note

Clearing and purging are methods for removing data from storage media. Clearing aims to make data difficult to recover but acknowledges it's possible with specialized techniques. This method, which includes zeroing out drives or using bit-erasure software, is suitable for repurposing media within an organization but not recommended for sensitive information. Purging, on the other hand, is recommended for sensitive data and media leaving the organization. It involves methods like Secure Erase (accessible via firmware or manufacturer tools) or degaussing. Secure Erase leaves the drive functional, while degaussing, primarily for magnetic drives, renders the data unreadable and often the drive unusable. Organizations should adhere to their own data destruction policies, and when uncertain, purging is the safer approach.

Physical Destruction

Storage media can be physically destroyed in a very basic way by using a hammer or similar tool or by drilling holes through the platters. For drives containing sensitive data, you should employ a more robust destruction technique. Electromagnetic *degaussing* is one option that is often used in conjunction with a complete physical destruction process, such as *incineration* or the more common *drive shredding* (also known as pulverization). At this point, the remnants of the drive can be disposed of in accordance with municipal guidelines.

Some organizations require a certificate of destruction to show that a drive has indeed been destroyed; in fact, the certificate is often required by data privacy laws. A destruction certificate is obtained from the third party that performs the drive destruction. A typical organization does not have the equipment necessary to perform proper destruction. That's why an outside vendor is usually contracted to do the work; those third-party vendors have mechanical *degaussers* and drive shredders designed specifically to meet NIST and DoD standards. Some of these vendors come onsite to perform the process of destruction in front of the appropriate company personnel. Then the personnel sign off on the procedure. It's not recommended that drives be mailed or otherwise transported to a vendor, but if they are, the organization should use properly insured and tracked postal options or secure couriers, and the entire process should be documented utilizing a chain of custody or similar process.

ExamAlert

Know how to physically destroy a hard drive: drilling, shredding, degaussing, and incineration.

The type of data removal used will be dictated by the data stored on the drive. If there is no PII or other sensitive information, the drive might simply be cleared. But in many cases, organizations will specify purging of data if the drive is to leave the building and be reused. In cases where a drive previously contained confidential or top-secret data, the drive will

usually be destroyed. Again, always follow the policies that have been developed by your organization. If they are unclear, ask for additional interpretation from the appropriate personnel.

Note

The NIST SP 800-88 document concerning *Guidelines for Media Sanitization* can be obtained from https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final.

Regulatory and Environmental Requirements

Data destruction and disposal must adhere to regulatory and environmental requirements, ensuring sensitive information is irretrievable and hazardous materials are handled responsibly. Regulations like the Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), and National Institute of Standards and Technology (NIST) standards mandate secure data erasure or physical destruction of drives to prevent unauthorized access. Methods include overwriting, degaussing, and physical shredding or disintegration as previously discussed. Environmentally, disposal must comply with e-waste regulations, preventing toxic materials from contaminating landfills. Please see the previous note for the NIST link to Special Publication 800-88.

Cram Quiz

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

1. A drive needs to be disposed of in such a way that no one can access the data. Which method should be used?

   ○ **A. format E:**

   ○ **B.** Clearing

- ○ **C. diskpart**
- ○ **D.** Destruction

2. A drive is to be repurposed within your company. You have been tasked with zeroing out the drive three times from within Windows. Which of the following methods will accomplish this?

- ○ **A.** Degaussing
- ○ **B. format C: /fs:fat32 /p:3**
- ○ **C. diskpart > select disk 1 > clean all**
- ○ **D. dd if=/dev/zero of=/dev/sda1**

3. You have been tasked with purging a drive so that it can be recycled to a sister company. Which of the following should you perform before sending out the drive?

- ○ **A.** Clear the drive.
- ○ **B.** Degauss the drive.
- ○ **C.** Run Secure Erase on the drive.
- ○ **D.** Pulverize the drive.

4. What is the primary reason that regulations like HIPAA and GDPR necessitate secure data destruction?

- ○ **A.** To ensure that organizations are using the most cost-effective methods for disposing of old hardware
- ○ **B.** To standardize the physical dimensions of storage devices being discarded
- ○ **C.** To prevent unauthorized individuals from accessing sensitive information stored on the devices
- ○ **D.** To encourage organizations to reuse old storage devices whenever possible

5. Why might an organization require a certificate of destruction when disposing of storage drives?

- ○ **A.** To ensure that the third-party vendor is using the latest technology for data erasure
- ○ **B.** To have proof that the drives were destroyed in compliance with data privacy laws
- ○ **C.** To document the chain of custody if the drives are transported offsite for destruction
- ○ **D.** To verify the resale value of the destroyed materials for accounting purposes

Cram Quiz Answers

1. **D.** You should destroy the drive. You could do this with the use of a tool (such as a drive shredder), by incinerating it, or by degaussing it, although the first option is usually preferred. The **format E:** command will only format the drive to a new file system; that is not secure enough if the data has to be removed altogether. Clearing is the removal of data from a drive that is to be repurposed and used again within the organization. The **diskpart** utility can be used to clear the drive, but it is not appropriate for drive disposal.

2. **B.** The only option listed that will zero out the drive three times (from Windows) is **format C: /fs:fat32 /p:3**. This procedure formats the drive as FAT32 and runs the process three times (**p:3**). Degaussing a hard disk drive will render the data unreadable and, in most cases, will make the drive unusable. By default, the **diskpart** and **dd** processes listed will only zero out the drive once. They would have to be run with an additional parameter or run manually two more times to meet the criteria. Also, **dd** is run from Linux, not from Windows, so that is another reason that answer is incorrect. But be very careful: Note that the drive listed in the **dd** command is sda1. That will most likely be the system drive; if the command is run on that drive, the OS will be erased, which is what you want in this case. Just remember to use caution when erasing drives. Double-check what you are doing before you run any commands.

3. **C.** At a bare minimum, run the Secure Erase program (or a comparable program) to sanitize the drive; it needs to be completely wiped if it is to be reused. The rest of the answers are not examples of sanitizing or purging. Clearing the drive by formatting or zeroing out does not meet the requirements for sending the drive out to another company as standardized by NIST and the DoD. Degaussing the drive will render it useless. Pulverizing the drive (shredding it) will destroy it and will also render it unusable.

4. **C**. Regulations like HIPAA and GDPR mandate secure data erasure or physical destruction of drives to prevent unauthorized access. HIPAA focuses on protecting patient health data in the US. GDPR protects personal data of EU citizens. While cost-effectiveness might be a consideration for organizations, the security aspect is mandated by regulations, not the cost. Standardizing the physical dimensions of the devices being disposed of makes no sense! If you incinerate your drives, you will just have a little pile of ash. While reuse might be possible after clearing, the regulations mentioned are concerned with *destruction* to prevent access.

5. **B.** Many organizations require a certificate of destruction to show that a drive has indeed been destroyed; the certificate is often required by data privacy laws. While using appropriate technology is important, the certificate primarily serves as proof of destruction, not necessarily a guarantee of the latest technology being used. Chain of custody is important for tracking the drives during transport, but the certificate of destruction is a separate document confirming the completion of the destruction process. If you destroy your drives, there's a very low market for resale!

You need to know how to recycle, reuse, and if necessary, destroy storage drives. Go with standardized processes, and all will be well. Continue!

Chapter 51
SOHO Security

This chapter covers the following A+ 220-1202 exam objectives:

- **2.6** – Given a scenario, implement procedures for basic small office/home office (SOHO) malware removal.
- **2.10** – Given a scenario, apply security settings on SOHO wireless and wired networks.

A small office/home office (SOHO) network is easy to set up. But if you don't secure it, you might as well just call up a hacker and ask that person to invade the network. The core of a SOHO network is the SOHO router. This device actually acts as a switch, router, firewall, and wireless access point (WAP). For the rest of this section, we'll describe how to secure this device, and we'll refer to it simply as a *router*. Before you make any security configurations, it is highly recommended that you back up your settings and update the firmware. And don't forget to save the configuration when you're done!

Note

You can access online emulators for several different kinds of routers. It's good practice to run through these configurations on your own router or an emulator of some sort.

Removing SOHO Malware

Before diving into the specifics of how to apply security settings in your SOHO environment, you should also know a systematic procedure to remove malware if infected.

ExamAlert

Objective 2.6 lists a specific 10-step procedure to remove malware from a SOHO environment. Know the following steps!

Step 1. **Investigate and Verify Malware Symptoms:** Don't jump to conclusions! First, carefully observe the symptoms. Is the computer running unusually slow? Are there strange pop-ups or error messages? Is the Internet behavior odd? Check system logs for unusual activity. This investigation helps you understand the potential malware and the extent of the infection.

Step 2. **Quarantine the Infected System:** Isolate the affected computer from the rest of your network. Disconnect it from the Internet and any shared drives. This prevents the malware from spreading or leaking data.

Step 3. **Disable System Restore in Windows Home:** In Windows Home editions, System Restore can sometimes interfere with malware removal. Temporarily disable it to prevent the malware from being restored from a previous restore point. You can usually find System Restore settings by searching for "Create a restore point" in the Windows search bar.

Step 4. **Remediate Infected Systems:** For this step, move on to steps 5–7, with step 7 being a last resort. When you're finished, continue on with step 8.

Step 5. **Update Antimalware Software:** Ensure your antivirus and antimalware programs are fully updated with the latest definitions.

This gives you the best chance of detecting and removing the malware.

Step 6. **Use Scan and Removal Techniques:** Boot into the Safe Mode/preinstallation environment to limit malware activity during the scan. If necessary, use a preinstallation environment like a bootable USB drive with antivirus software to scan the system from outside the infected Windows environment.

Step 7. **Reimage/Reinstall:** If all else fails, consider reinstalling Windows. This is the most drastic step but ensures a clean system free of persistent malware. Back up important data before doing this!

Step 8. **Schedule Scans and Run Updates:** After the malware is removed, schedule regular full system scans with your antivirus software. Also, keep your operating system, applications, and browser extensions updated to patch vulnerabilities and prevent future infections.

Step 9. **Enable System Restore and Create a Restore Point in Windows Home:** Once the system is clean, re-enable System Restore and create a new restore point. This provides a fallback in case of future issues.

Step 10. **Educate the End User:** Perhaps the most crucial step! Explain to the user how the infection likely occurred (such as clicking a malicious link or downloading an infected file) and how to avoid similar situations in the future. Emphasize safe browsing habits, email security, and the importance of software updates.

Cram Quiz

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

1. Why is it important to disable System Restore in Windows Home during malware removal?

- ○ **A.** It speeds up the scanning process.
- ○ **B.** It prevents malware from being restored from a backup.
- ○ **C.** It frees up disk space for the antimalware software to operate.
- ○ **D.** It forces the malware to become active, making it easier to detect.

2. Which of the following is the most drastic step in malware removal but also ensures a completely clean system?

- ○ **A.** Running a full system scan in Safe Mode
- ○ **B.** Using a dedicated malware removal tool
- ○ **C.** Disabling suspicious startup programs
- ○ **D.** Reimaging or reinstalling the operating system

Cram Quiz Answers

1. **B.** Disabling System Restore during malware removal prevents malware from being restored from a backup. System Restore points can inadvertently contain malware. Disabling System Restore prevents the malware from being reintroduced during the recovery process. Disabling System Restore doesn't necessarily speed up the scanning, nor does it directly affect free disk space. Malware doesn't need to be active to be detected.

2. **D.** The most drastic step in malware removal is reimaging or reinstalling the operating system. Doing so completely wipes the hard drive and installs a fresh copy of Windows, eliminating any deeply embedded malware. Safe Mode scans are helpful but might not remove all malware, and dedicated tools are useful but not always guaranteed to remove everything. Disabling startup programs might not address the root cause of the infection.

Applying Security Settings on SOHO Wireless and Wired Networks

Now let's dive into securing those small office/home office networks. We're talking routers, Wi-Fi, and firewalls here, so buckle up. This section focuses on getting your home router locked down, covering everything from basic password changes to the nitty-gritty of wireless settings and firewall configurations. It's all about making sure your SOHO setup is as tight as possible.

ExamAlert

Objective 2.10 concentrates on home router settings, wireless-specific settings, and firewall settings.

Changing Default Passwords

The first thing you should do to secure a router is to change the password. Some routers require that you change the password when you first log in. Other routers come with a blank password or have a basic password, such as *admin*. You need to connect to the router by opening up your favorite browser (your favorite should be the most secure one), typing the IP address of the router (for example, 192.168.0.1 or 192.168.1.1), and logging in. If the router has the option to create another admin account (or at least change the name), do it—and keep the original administrator account as the backup. No matter what router you're using, you will definitely be able to change the password—and you should change it! Make it something complex, based on the rules we discussed in Chapter 48, "Workstation Best Practices." Save the settings (which will log you out) and then log in with the new password to make sure your new settings have taken effect.

Note

If you don't know the IP address of your router, open a Command Prompt in Windows and type **ipconfig /all**. Then look under the

adapter you're using and look for *Default Gateway*. That's the IP address to your router. On Linux or macOS, type **netstat -nr | grep 'default'**. Some newer mesh network routers will require you to use their app to make changes; however, they will usually tell you this when you try to go to the default gateway page on your browser.

ExamAlert

Remember to change the router admin password first before you do anything else!

A router may also have a user password. Change it as well, but change it to a different password than you used for the admin account. In addition, make sure you have *secure management access* turned on in your router. This policy ensures that your login credentials and data are not transmitted in plaintext and often uses a secure protocol like HTTPS when you're logging in to your router. This will help to protect from anyone "listening" in on your network traffic.

Using Wireless-Specific Security Settings

Now we'll move on to some core wireless-specific radio and broadcasting security concepts, including the SSID, encryption, antennas, radio power levels, and WPS.

Changing and Disabling the SSID

The service set identifier (SSID) is used to name a wireless network. Default SSIDs are usually basic, so it is wise to change the name of the wireless network before enabling wireless on the router. Names that include uppercase letters, lowercase letters, and numbers will be more challenging for casual wireless passersby to memorize.

After all wireless clients are connected to the network, consider disabling the SSID. Although this is not a perfect solution, it will mask part of the SSID broadcast, making it impossible to see with normal wireless locating software. Figure 51.1 shows a modified SSID named *Neptune8Network* and that it is not enabled.

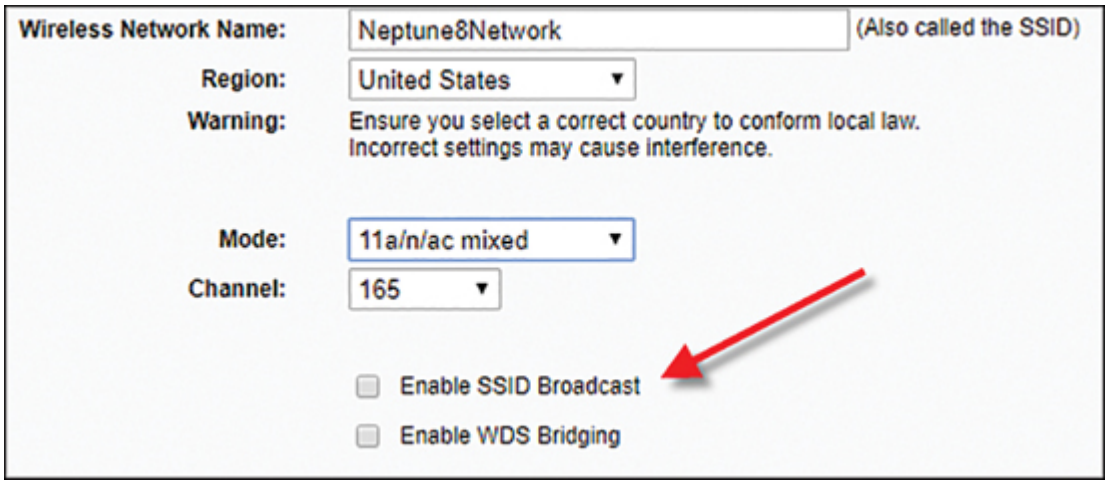


FIGURE 51.1 **Renamed and Disabled SSID**

When the SSID is disabled, wireless clients won't see the SSID name when they scan for wireless networks. If you need to connect additional wireless clients, you will either have to enable the SSID broadcast or enter the wireless SSID manually when connecting. For example, to connect manually in Windows, open the Network and Sharing Center and select **Set up a new connection or network**. Then select **Manually connect to a wireless network**. (The wireless adapter must be installed with correct drivers for you to see this link.) You will have to type the SSID (also known as the *network name*), the security type, the encryption type, and the security key to get into the network. Note that hiding your SSID is a type of security through obscurity. This means that it's not a real security measure because many network scanners are readily available as software apps and can find these "hidden" networks, but hiding SSIDs keeps basic devices from seeing them by default.

Note

By the way, given the channel and mode listed in Figure 51.1, what frequency is this router transmitting on? The channel is 165, so its center frequency is 5.825 GHz. If a channel overlaps with a neighbor, consider changing the channel to one that is farther away.

Setting Antennas and Radio Power Levels

Strategically placing your access point (AP) is important. Usually, the best place for an AP is in the center of the building, if at all possible. This way, equal access can be given to everyone on the perimeter of the organization's property, and there is the least chance of the signal bleeding over outside the organization. Also, moving your AP higher up, such as on top of a bookcase in an office or the ceiling if separate from the router, will help with the umbrella-like spread of the Wi-Fi signal.

If you need to reduce the broadcast range of the AP, you can attempt to reduce the transmission power levels of the antenna. For example, Figure 51.2 shows the transmission power of an AP set to Low, which for small offices is usually enough. The other options are Medium and High, or you might actually get a numeric option on some routers (measured in dBm). Test the signal strength by connecting with a laptop or another mobile device and moving to the perimeter of the building. If the lowest setting still allows access from the mobile device—with a decent data transfer rate—then there is no need to increase the power level.

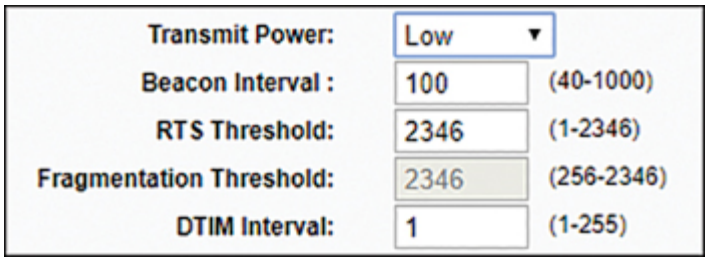


FIGURE 51.2 **AP Power Level Set to Low**

Also, to avoid interference in the form of electromagnetic interference (EMI) or radio frequency interference (RFI), keep WAPs away from any electrical panels, cables, devices, motors, or other pieces of equipment that

might give off an electromagnetic (EM) field. If necessary, shield any device that is creating an EM field.

An AP's antennas can be rotated so that they are parallel to each other or at an angle to each other. For example, if you have two antennas, then 180 degrees is often a good orientation to sweep the area for wireless transmissions. The more antennas, the better (usually)—especially if they incorporate MIMO technology (described in Chapter 5, "Wireless Technologies") to combine multiple data streams.

By placing the AP and adjusting the antennas appropriately and lowering the radio power levels as far as possible, you can further secure your wireless network while still providing decent service to your users.

To place wireless antennas, consider these recommendations:

- **Line of Sight:** Ensure a clear path between transmitter and receiver antennas.
- **Distance:** Keep antennas at least a quarter wavelength apart, ideally a full wavelength.
- **Orientation:** Align receiving antennas in the same plane as the transmitting antenna.
- **Height:** Mount antennas above people and obstacles.
- **Location:** Avoid placing antennas near metal objects, walls, and sources of interference.
- **Antenna Type:** Use the correct receiver antenna for the frequency band.
- **Antenna Separation:** Maintain suitable distance between diversity receiver antennas.
- **Antenna Orientation (Routers):** Point antennas vertically for best coverage on the same level.

Note

For more information regarding proper WAP placement, see https://kb.netgear.com/000065251/Where-should-I-put-my-

NETGEAR-wireless-access-point-for-optimal-WiFi-network-performance. For more information on antenna diversity, see https://lightyear.ai/tips/what-is-antenna-diversity.

ExamAlert

Strategically place your access points and know how to adjust radio power levels and AP antennas.

Using Guest Networks

Wireless guest networks can be a great convenience for people who are visiting your home or place of work. A guest network allows those people access to the Internet but does not allow access to any internal resources or other wireless clients on the main wireless networks. Using a guest network is a good way to isolate your guests. It's also a good way to isolate Internet of Things (IoT) devices such as video cameras and music devices (which can be inherently insecure). However, the guest network can be a liability in and of itself, especially if it doesn't use strong passphrases or encryption. For many organizations, the policy is to disable the wireless guest network altogether unless it is absolutely necessary. Instead, if your organization has individuals who need guest access, install a completely different wireless access point used just for guests. You can also use a *captive portal*, which is a web page that intercepts and redirects users' web traffic when they attempt to access a Wi-Fi guest network. At the captive portal page, users may be required to log in, accept terms of service by acknowledging an acceptable use policy (AUP), make a payment, or provide other information before gaining access to the Internet.

Disabling WPS

Wi-Fi Protected Setup (WPS) was originally intended to make connecting to a wireless access point easier for the average user. However, anything that is made simpler is often less secure as well. Case in point: WPS is

vulnerable to brute-force attacks, which can lead to intrusions on the network. In a brute-force attack, threat actors try to guess passwords and codes by trying combinations of letters, numbers, and symbols. A WPS code is usually 8 to 10 digits long, which is not very difficult to crack. So, your best bet is to disable WPS altogether.

Enabling MAC Filtering and IP Filtering

You also might be able to configure a wireless access point for MAC filtering and IP filtering, which are basic forms of network access control. MAC/IP filtering can filter out which computers can (or cannot) access the wireless network (and wired network). An AP does this by consulting a list of MAC addresses or IP addresses that have been previously entered.

In some cases, a device might broadcast this MAC or IP table. If this is the case, look for an update for the firmware of the access point and attempt to fine-tune the broadcast range of the device so that it does not leak out to other organizations. Because MAC/IP filtering and a disabled SSID can be fairly easily circumvented using a network sniffer, it is important to also use strong encryption and possibly to consider other types of network access control (such as 802.1X) and external authentication methods (such as RADIUS).

ExamAlert

MAC filtering and IP filtering can be used to specify which computers are allowed or denied access to the wireless network (and wired network).

Assigning Static IP Addresses

A SOHO router can be set to limit the number of DHCP addresses it hands out. If there are not enough addresses to go around, you might find that certain hosts (such as servers or printers) lose connectivity when there are more client computers on the network. First, consider increasing the scope

of addresses that the router is configured to hand out to clients. Second, try assigning static IP addresses to the servers and printers—essentially, any hosts that share information or services. This way, if more clients obtaining dynamic addresses are added in the future, the servers and printers will not be affected.

By default, a SOHO router itself uses a static IP address on the LAN side; however, on the WAN side, it is usually set to obtain an IP address from an ISP dynamically, although you can change this to a static address if you wish. If you have servers that a SOHO router is port forwarding to, and if you have clients connecting to those servers from the Internet, you might consider requesting a bank of static IP addresses from your ISP and configuring the SOHO router's WAN port to use one of those static IP addresses. Or, at the very least, you might use a service such as DynDNS to forward your Internet domain name to your SOHO router's dynamically assigned IP address. This way, clients will be able to connect by domain name, even if the IP address changes over time. If you have clients connecting via a virtual private network (VPN) through your SOHO router, using PPTP, L2TP, or OpenVPN, then the use of a static IP address is recommended, and it might even be required.

Adjusting Firewall Settings and Additional Configurations

A SOHO router usually has a built-in firewall with some basic security functionality. Let's discuss a few of the common features you might find in such a router:

- **NAT:** Network Address Translation (NAT) is the process of transforming IP addresses as data crosses a router. NAT hides an entire IP address space on the LAN (for example, 192.168.1.1 through 192.168.1.255). If an IP address on the LAN needs to communicate with the Internet, the IP address is converted to the public IP address of the router.
- **Port forwarding/mapping:** This process maps an external network port to an internal IP address and port, enabling you to have a web server,

FTP server, and other servers—but you need to have only one port for each of them open on the WAN side of the router. It can be any port you like; of course, you need to tell people which port they need to connect to if it is not a standard one. Some devices use *virtual servers* to make the process a lot more user-friendly. So, for example, you might have an FTP server running internally on your LAN; its IP address and port might be 192.168.0.100:21 (notice that the colon separates the IP address from the port), but you would have users on the Internet connect to your router's WAN address (for example, 65.43.18.1) and any port you want. The router takes care of the rest, and the typical user won't notice the forwarding. Port forwarding is also referred to as destination NAT (DNAT).

- **Screened subnet:** A screened subnet, also known as a demilitarized zone (DMZ), is an area that is not quite on the Internet and not quite part of your LAN. It's a sort of middle ground that, for the most part, is protected by a firewall, but particular traffic will be let through. A screened subnet is a good place for web servers, email servers, and FTP servers because these are services required by users on the Internet. The beauty of a screened subnet is that users can access it without having access to your LAN—if it is configured correctly, of course. Quite often, a screened subnet is set up as the third leg of a firewall. The first leg connects to the LAN, the second leg connects to the Internet, and the third connects to the screened subnet. You need to know the ports that your servers will use, and you need to create rules within the firewall (or an all-in-one device, such as a SOHO router) to allow only the required traffic into the screened subnet.
- **UPnP:** Universal Plug and Play (UPnP) is a group of networking protocols that allows computers, printers, and other Internet-ready devices to discover each other on the network. It is a consumer-level technology designed to make networking easier for the user. For example, if you want easier accessibility and connectivity of a PC, a smartphone, and a printer that are all connected to the SOHO router, UPnP can provide that. However, it is often recommended to disable this function, if you are concerned about security, and manually configure port forwarding.

Using Content Filtering/Parental Controls

Most SOHO routers come with a parental control section where content can be filtered on a very basic level. The "parent" can select the MAC address of a particular computer and specify what domain names that computer is allowed to connect to—and when. Figure 51.3 shows an example.

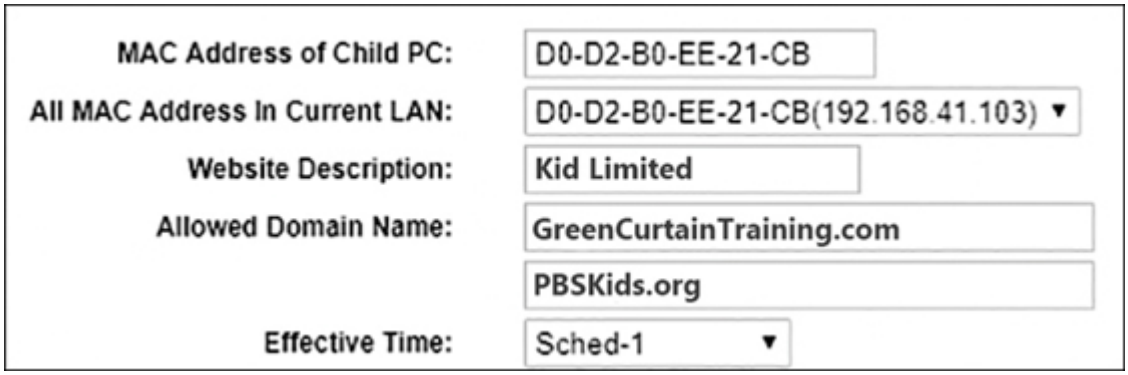


FIGURE 51.3 **Parental Control Entry**

In the figure, you can see that the MAC address D0-D2-B0-EE-21-CB has access to two domains (GreenCurtainTraining.com and PBSKids.org) and that Effective Time is set to Sched-1, a schedule we preconfigured that allows the "child" to connect from 8 a.m. to 4 p.m. on weekdays; scheduling is usually a component of parental control.

Because the MAC address of a computer can't be changed (by a typical user), this configuration follows the computer, even if it gets a new IP address later. This uses the same concept as MAC filtering, and in fact, some parental control sections have MAC filtering built in.

Disabling Physical Ports and More Physical Security

A router might come with the capability to disable the physical ports on the switch portion of the device. Disabling physical ports is a wise precaution. If you disable unused physical ports, a rogue computer can be plugged into the router physically but won't have any hopes of accessing the network. This concept is a policy in most organizations. Unused router or switch

ports are disabled so that a person can't connect a laptop to any old RJ-45 jack on the premises.

ExamAlert

Disable any physical ports that are not in use!

Consider the physical security of a SOHO router as well. Can anyone in the building put their hands on it? That would be inappropriate, so you need to physically secure the device, which means keeping it in a locked area such as a wiring closet or, if that is not possible, above a drop ceiling (mounted properly) or against the ceiling if there is no drop ceiling. This way, the device will at least be more difficult to reach—as long as you don't have a ladder lying around. Anyone who uses a SOHO router is unlikely to have a server room, but a server room would be an optimal location.

A Final Word on SOHO Routers

Make sure that a router's firmware is kept up to date. Also, make sure the built-in firewall is always enabled. This firewall is going to be much more important than the Windows firewalls on the individual computers, though both are recommended. Most routers' firewalls are on by default, but you should check. If you do any kind of port forwarding, port triggering, screened subnet configuration, or remote connections, make sure the firewall is allowing traffic only through the specific port or ports you require and that all others are blocked. Check for updates every month or so, and while you are at it, change the administrator password for good measure.

ExamAlert

You will likely see many questions about wireless on the exam. Make sure you know how to apply the following settings on a SOHO wireless/wired network:

- **Router settings**
  - Changing default passwords
  - Setting IP filtering
  - Making firmware updates
  - Content filtering
  - Ensuring physical placement/secure locations
  - Using Universal Plug and Play (UPnP)
  - Using screened subnets
  - Configuring secure management access
- **Wireless specific**
  - Changing the service set identifier (SSID)
  - Disabling SSID broadcast
  - Changing encryption settings
  - Configuring guest access
- **Firewall settings**
  - Disabling unused ports
  - Using port forwarding/mapping

Cram Quiz

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

1. Which of the following helps to secure a SOHO router? (Select the three best answers.)

   ○ **A.** Change default passwords.

- **B.** Enable SSID.
- **C.** Enable MAC filtering.
- **D.** Enable WPS.
- **E.** Enable WPA3.

2. You want to prevent rogue employees from connecting a laptop to the SOHO router and accessing the network. How can you accomplish this? (Select the two best answers.)
   - **A.** Enable MAC filtering.
   - **B.** Create a screened subnet.
   - **C.** Configure a complex SSID.
   - **D.** Disable physical ports.
3. You want to prevent certain users from accessing particular websites. What should you configure on the SOHO router?
   - **A.** MAC filtering
   - **B.** Disable unused ports
   - **C.** Port forwarding
   - **D.** Content filtering
   - **E.** Power levels

Cram Quiz Answers

1. **A, C, and E.** Changing default passwords, enabling MAC filtering, and enabling the latest version of WPA can all increase the security of a SOHO router. Enabling SSID broadcast makes a router visible. Enabling WPS makes it easier to connect to the router but has security implications.
2. **A and D.** By enabling MAC filtering, you can create a list of MAC addresses that a SOHO router will accept. Any other computers with different MAC addresses will not be allowed

access to the network. This works for wired and wireless connections. You can also disable physical ports on the router; this blocks any physical signal from being sent to those unused ports. (You might also try reducing the transmitting power of the wireless channel being used.) A screened subnet (also known as a DMZ) is used to host servers and acts as a separate area between the LAN and the Internet. A complex SSID is great but won't matter to a user connecting a laptop physically to the router because the SSID affects only wireless access.

3. **D.** By enabling content filtering (and parental controls), you can select computers—by MAC address—and select what websites (domains) those computers are allowed to connect to. MAC filtering by itself simply allows or denies computers access to the router based on the MAC address of the computer. Disabling unused ports is a good idea, but it will simply stop a computer from accessing the SOHO router if it is connected on that port. Port forwarding involves configuring a router to forward Internet-based IP addresses and ports to a computer or server that is on the LAN or the screened subnet. Power levels refer to the broadcasting power of an AP's radio. The lower, the better—as long as people on the perimeter of the building can still communicate with the router.

In this chapter, you read a lot about router security. If you employ these methods, you'll be on your way to a *super-secure* Internet experience! Only one more chapter on security to go. You've got this!

Chapter 52

Browser Security

This chapter covers the following A+ 220-1202 exam objective:

- **2.11** – Given a scenario, configure relevant security settings in a browser.

Web browsers—everyone uses them. And they connect us to the Internet. Do we have to stress the need for web browser security? This chapter describes some basic techniques used to secure the most common browsers and shows how to safeguard users' browsing habits. In this chapter, we'll focus mostly on Microsoft Edge and Google Chrome, but most everything applies to the Mozilla Firefox as well.

Hey! This is the last chapter on security. Or is it? We should always be thinking in terms of security, as you will see as you progress through the rest of the book. But as far as Domain 2.0: Security is concerned, this is the last chapter.

ExamAlert

Objective 2.11 focuses on browser download/installation, browser patching, extensions and plug-ins, password managers, secure connections/sites and valid certificates, settings, and browser feature management.

Browser Download/Installation

As you work with different operating systems, you will see that each of them favors a certain web browser that is installed as part of the system and works by default whenever you need to connect to the Internet.

For example, Windows has Microsoft Edge built in. Apple products have the Safari browser. Linux distributions often use Firefox. And Chromebooks use Chrome. You will find that end users and many organizations also use Chrome heavily as their main web browser. There are other web browsers, but these are the four you should know for the exam, with Microsoft Edge and Chrome at the top of the list.

If you use the default browser that comes with an operating system, then no download or installation is necessary; the browser just works. However, if you want to use a different browser, you need to download it, install it, and then set it as the default within the operating system. So, for example, if you are working in Windows 11 and want to use Chrome as the default web browser, you need to do the following:

1. **Search for the Chrome web browser:** A simple search in any Internet search engine for "Chrome web browser" will suffice. (Generally speaking, we recommend skipping through any ads displayed in the search results.) Click the download button or link.
2. **Download and install:** After you click **Download**, the installation usually begins automatically, regardless of the OS you're using. The installation of most web browsers is so user-friendly that it happens almost like magic.
3. **Set Chrome as the default web browser:** A web browser often asks if you want to set it as the default web browser, and clicking **Yes** makes it so. You can also perform this action in the browser settings. Or, you can change the default browser in Windows. For example, in Windows 11, you go to **Windows Settings** > **Apps** > **Default Apps**. Then, scroll down to and click the web browser you want to be the default and change it to be the default for .htm and .html.

For other web browsers, you might need to use slightly different download and installation methods. The important thing to know for the exam is how to change the default web browser in Windows.

ExamAlert

To change the default web browser (or other default programs) in Windows, go to **Windows Settings > Apps > Default Apps**.

Table 52.1 lists the download links for some popular web browsers.

TABLE 52.1 **Web Browser Download Links**

Browser	Link
Microsoft Edge	https://www.microsoft.com/en-us/edge
Chrome	https://www.google.com/chrome/
Firefox	https://www.mozilla.org/en-US/firefox/new/
Safari	https://support.apple.com/downloads/safari (macOS only)
Opera	https://www.opera.com/download
Chromium	https://www.chromium.org/getting-involved/download-chromium

All of the web browser links listed in Table 52.1 are considered to be trusted sources. It's important to download programs and files from trusted sources—that is, sources that you know are legitimate. However, keep in mind that the level of trust in a source may depend on the policy of your organization. Any website or app can be put on an untrusted list, and sometimes browsers are banned. For example, hackers tend to prefer browsers such as Chromium and Opera to do their dirty work. This might prompt an administrator to eliminate the ability to install those web browsers and place them on the untrusted list. We'll discuss trusted and untrusted sources more later in the chapter.

Note

Firefox has been the standard in privacy for a long time. But you might also be interested in the Tor browser or Brave, as well as search engines such as DuckDuckGo or Startpage.

Hashing

In your travels, you will encounter file downloads that incorporate *signatures*. A signature allows you to check whether a file has been tampered with while in transit between the web server and your local computer. A signature could be considered a summary of a file to be downloaded. It is created using a cryptographic hashing technique.

Commonly used browsers such as Microsoft Edge and Google Chrome do not use signatures to verify the browser installation files. Instead, they rely on the mandatory usage of secure HTTPS connections before downloads can be initiated. However, other less commonly used web browsers might use signatures. A signature might also be referred to as a *hash* or as a *checksum*. Essentially, you need to check the downloaded file's signature against the signature that is stored on the website. If the two match, then you can be relatively sure that your download has not been tampered with during transit. Of course, the process is more technical than that. Step-by-step processes are readily available on the Internet for hashing technologies such as SHA and PGP.

Browser patching is essential to fix security vulnerabilities and improve performance. Chrome, Edge, and Firefox typically update automatically in the background, downloading and installing patches seamlessly. You can also manually check for updates in the browser's settings menu. Safari updates are managed through the macOS system update mechanism, ensuring the browser is patched along with the operating system. These updates often include critical security fixes, performance enhancements, and new features, making regular patching crucial for a safe and optimal browsing experience.

Settings

It's important to know how to access the settings for web browsers. Table 52.2 shows ways to get to the settings for Edge, Chrome, Firefox, and Safari.

TABLE 52.2 **Web Browser Settings Pages**

Browser	How to Get to Settings
Edge	▶ Click the menu button (three horizontal dots) in the upper-right corner of the screen and click **Settings**. ▶ Type **edge://settings** in the address bar.
Chrome	▶ Click the menu button (three vertical dots) in the upper-right corner of the screen and click **Settings**. ▶ Type **chrome://settings** in the address bar.
Firefox	▶ Click the menu button (three horizontal lines) in the upper-right corner of the screen and click **Preferences**. ▶ Type **about:preferences** in the address bar.
Safari	▶ On the menu, click **Safari** > **Preferences**

ExamAlert

Know how to access settings in Edge and Chrome.

Extensions and Plug-ins

To customize web browsers, you can use extensions and plug-ins. For the most part, Microsoft Edge and Google Chrome focus on *extensions* and have done away with the term *plug-ins*. Firefox has streamlined extensions and plug-ins to the term *add-ons*; however, the add-ons enable you to install extensions.

Extensions are software programs that add functionality to a browser. They can be good or bad. The good ones make the browser better and don't use too much more of your computer's resources. The bad ones often use a lot of system resources, cause system failures, collect data, or perform malicious actions behind the scenes.

Some examples of extensions for Microsoft Edge and Google Chrome include Office Online, Adblock Plus, 1Password, Save to Pocket, and Dark Mode. These all add different types of functionality to the web browser. These extensions, once installed, are easily accessible from the main browser application.

To see what extensions are installed to Microsoft Edge, type **edge://extensions** in the Edge address bar. To see what extensions are installed to Chrome, type **chrome://extensions** in the Chrome address bar. From these locations, you can also search extensions and, most importantly, enable or disable them. Enabling or disabling extensions, plug-ins, and browser features is referred to as *browser feature management*.

Once again, it's important to use a trusted source when obtaining extensions. In the Microsoft Edge extensions page, you can click the **Get extensions for Microsoft Edge** link. Doing so opens a new tab that brings you to the Edge Add-ons web page. For Google Chrome, use the Chrome Web Store.

To work with extensions in Firefox, click the menu button and select **Add-ons** (or press Ctrl+Shift+A). Then select **Extensions**. Or go to https://addons.mozilla.org/en-US/firefox/extensions/. The Firefox Add-ons page also shows plug-ins. While using an extension is the more common way to modify the Firefox browser, a plug-in might still be used, such as for a decryption module or a video codec for playback of certain types of video files.

Often, a web browser will warn you when you try to install an extension from an untrusted source. This is an example of a failsafe. Educate your users to read the messages that show up onscreen because these messages are often security-related. An extension that comes from an untrusted source could cause system instability or could compromise the system altogether.

ExamAlert

The term *trusted source* refers to a reliable provider of information, like a reputable news website or an established expert, where the accuracy and credibility of the content are considered high, whereas an *untrusted source* is a source that lacks credibility, could be inaccurate, or has a history of providing misleading information, like an anonymous online forum or a website with a known bias.

Password Managers

Beware! Passwords can be stored in a variety of places. The most common place is within some kind of *password manager*, which is a program that stores all the passwords that you use for various websites and services. There are several types of password managers (or *password vaults*, as they are sometimes called). They can exist as locally run programs or as third-party Internet-based services. You could use Credential Manager (Windows) or Keychain (macOS) to store web credentials *and* OS credentials. Password managers also exist within most of today's web browsers. Because this chapter is about browser security, we'll focus on web browser–based password managers.

By default, when you type a password to access a website, most web browsers ask you if you want the browser to save the password. If you click **Yes**, your machine will save it within the browser application in Settings, where you can later copy and paste them to the various websites you need to access. Some browsers may also offer to fill in passwords automatically when you next access websites. Depending on the browser and the settings, you might also have the option to have a password saved to your *account*. This means that the password is stored in the cloud with your user account (if you are logged in). The password can then move with you to other devices using the same browser and user account. All of the browsers will use encryption for the username and password.

A home user might like to let the browser manage passwords. Really, who can remember all those pesky complex passwords today? However, most

organizations frown upon this practice because they deem it too great a security risk. So, you should know how to disable it. That means disabling two functions: the browser offering to save a password and the ability for the browser to autofill the password in the future. To disable these settings in Edge, go to **Settings > Profiles > Passwords** (or type **edge://settings/passwords**). To disable them in Chrome, go to **Settings > Autofill > Passwords** (or type **chrome://settings/passwords**).

ExamAlert

Know how to disable the password manager in Edge and in Chrome.

Banning Web Browser Password Managers

If an organization bans web browser password managers, what are organizational users to do with their passwords? Well, there are a few options.

First, there are third-party password manager programs, such as 1Password, Bitwarden, Dashlane, and ProtonPass. An organization might consider using one of these programs as a more secure solution than storing passwords in a web browser. These programs typically encrypt passwords in a vault locally on the system. However, some of them can also integrate with the web browser. Some store passwords in the cloud to allow access from multiple devices. The key (pun intended) is to have a super-lengthy and complex passphrase that allows access to the entire vault. That's the *one* password that needs to be memorized. If that password is compromised, all the user's other passwords are compromised. Some password managers, such as 1Password, also have a Secret Key in addition to the primary password. This offers a sort of two-factor authentication. Just don't lose either!

Second, an organization might choose to build its own password manager, using the programming language and cipher of its choice. An organization might build from scratch or—more likely—build on other work. For example, programs such as Bitwarden are open source, and the source code can be freely downloaded and modified at will.

Third, an organization might say *no* to passwords altogether, instead relying on other forms of authentication. Or the organization might simply disallow users from logging in to anything other than the organization's infrastructure. Technically, this would probably be accomplished using a single sign-on (SSO) system and various types of filtering. Fundamentally, this method would rely on the principle of least privilege, which, ultimately, reduces risk and simplifies the situation in one stroke.

Secure Connections

If an Internet session isn't secure, then clients, servers, and data in motion are all at risk. Let's examine a couple of technologies and options for securing connections.

TLS

The first thing to consider is the type of connection made when connecting to a website. To secure a connection, you need to encrypt it. There are various ways to do this. The most common way is to use Transport Layer Security (TLS).

TLS is a cryptographic protocol that provides secure Internet communications such as web browsing, instant messaging, email, and VoIP. This protocol relies on a public key infrastructure (PKI) for obtaining and validating certificates.

Note

A public key infrastructure (PKI) is an entire system of hardware and software, policies and procedures, and people. It is used to create, distribute, manage, store, and revoke digital certificates. If you have connected to a secure website in the past, you have been a part of a PKI! But a PKI can be used for other things as well, such as secure email transmissions and secure connections to remote computers and remote networks. A PKI is all encompassing: It includes users, client computers, servers, services, and, most of all, encryption.

Many people refer to the secure connections they make to websites as SSL, but actually most of them are TLS. TLS is a newer and more secure solution, and Secure Sockets Layer (SSL) has been deprecated. As of the writing of this book, the latest version of TLS is 1.3 (defined in 2018), though you might still see version 1.2 in use. However, what you should be most interested in is the strength of the cipher—which is something to keep

in mind when inquiring as to TLS certificates. Let's look at essentially how TLS works. Two types of keys are required when any two computers attempt to communicate with TLS: a public key and a session key. Asymmetric encryption is used to encrypt and share session keys, and symmetric encryption is used to encrypt the session data. A session key used by a protocol such as TLS is used only once; a separate session key is used for every connection.

ExamAlert

To learn more about cryptography, see https://www.nist.gov/cryptography.

Now, you might be called upon to verify that specific versions of TLS are enabled (or disabled) in the web browser settings. To do this for Edge/Internet Explorer, open the Internet Properties dialog box (**Run > inetcpl.cpl**), go to the Advanced tab, scroll all the way down to the TLS settings, and select/deselect the various versions of TLS. As of the writing of this book, TLS 1.3 is no longer considered experimental in Windows 11 and Windows Server 2022 and is enabled by default. Also, Google Chrome piggybacks the Windows settings for TLS, so you go to the same location for Chrome as for Edge.

ExamAlert

Know how to check the TLS version in Edge and in Chrome.

You might also work with specific security functions for TLS 1.3 and other security features. The Advanced tab is the place to be in this respect. In Chrome, there is another option: Open a new tab by clicking the plus symbol at the top of the browser or pressing Ctrl+T. Then type **chrome://flags** in the address bar. Search for "TLS 1.3" (or something similar), and you will see the option to enable/disable it. To do the same

thing in Firefox, open a new tab and type **about:config** in the address bar. Search for "TLS" and look for the **security.tls.version.min** setting.

From a user education standpoint, you should instruct people not to enter any personally identifiable information (PII) on a website that does not have a secure connection. The easiest way for a user to tell if the connection is secure is to look for the padlock in the address bar (and possibly the HTTPS protocol). If there is no padlock or if it's clear that HTTPS is not in use, the user should close the tab. To get even more information about a connection, a user could right-click the padlock and view the details of the certificate used for the encrypted connection. The drop-down menu that appears when you right-click the padlock will state whether the certificate is secure. You can then view the details of the certificate. The details include the connection protocol (for instance, TLS), the certificate encryption type (for example, RSA), and the cryptographic hash (for example, SHA256), among other things. Viewing the details of the certificate goes a little beyond the A+, but it's something we recommend you look at when you get a chance.

Secure Sites and Tracking

You can modify the security level for a browser to affect which sites are accessed and the ways the browser allows those sites to track users.

For example, in Edge, go to **Settings > Privacy, search, and services** (or **edge://settings/privacy**) and locate the Tracking Prevention section. For some organizations, the default Balanced option might not be secure enough, and you might be instructed to set this to Strict instead. Better yet, you can do this on multiple systems automatically with group policy (discussed in a little bit). You can also set exceptions for sites that you want to allow.

The Privacy section of Edge is the place to be if you are concerned about security. It has a *ton* of stuff for you to consider. Spend 5 or 10 minutes browsing that portion of Settings. For example, scroll down to the Security section and click **Manage Certificates** to bring up the Certificates window, where you can import, export, and further manipulate certificates. You can view and *really* manage certificates by going to **Run > certmgr.msc** to bring up the Certificate Manager window. Try navigating to **Trusted Root**

Certification Authorities > Certificates to see all of the certificate issuers for the system.

In addition, other settings are scattered around Edge, such as the Cookies and site permissions section, where you can set the cookies you want to allow from web servers and view permissions for sites that have been visited.

> **Note**
>
> For a secure Internet browsing experience, you might also implement a proxy server or a virtual private network (VPN).

More Settings

You've already seen how to access some settings in Edge and Chrome. Remember **edge://settings** and **chrome://settings**? Table 52.3 shows some examples of browser settings, what they mean, and where to configure them in Edge and Chrome (using address bar paths).

TABLE 52.3 **Web Browser Configurations**

Setting	Meaning	Configuration
Pop-up blocker	Blocks unwanted windows that appear when a user clicks on a web page element.	**edge://settings/content > Pop-ups and redirects** **chrome://settings/content > Pop-ups and redirects**
Clear browsing data	Removes all website-based temporary files stored on the local system, such as browsing history, cookies, passwords, and cache.	**edge://settings/privacy > Clear browsing data** **chrome://settings/privacy > Clear browsing data**

Setting	Meaning	Configuration
Sign-in/data synchronization	If enabled, synchronizes logon and data across devices.	**edge://settings/profiles/sync** **chrome://settings/syncSetup**
Trusted/untrusted sites	Allows you to configure which websites the browser is allowed to connect to.	**Run > inetcpl.cpl > Security tab**

A user who doesn't want information about a browsing session to be stored locally can use private browsing, also known as *incognito mode*. In this mode, the browser disregards any cached information, logins, synchronized data, and so forth. And, by default, web caching, cookies, and so on are disabled (at least for that "private" session).

To enter private browsing mode, right-click the browser icon and select **New InPrivate window** (Edge) or **New Incognito window** (Chrome). Or, from within the browser, use the Ctrl+Shift+N shortcut (Edge/Chrome) or Ctrl+Shift+P (Firefox).

ExamAlert

Know how to initiate private browsing mode in Edge and in Chrome.

Note

Does private browsing mode mean the browsing history isn't stored anywhere? Not on your life! Know this: Just about everything today is tracked one way or another. Enough said.

Want to configure these settings in a policy-oriented system? Of course, you do! Use the Local Group Policy Editor. Go to **Run > gpedit.msc** and

navigate to **User Configuration > Administrative Templates > Windows Components > Microsoft Edge**. There you will find more policy settings than you could dream of. We recommend that you take a few minutes to explore these settings. You will discover that you can configure browser settings (and Windows settings in general) more efficiently with the Local Group Policy Editor, especially if you need more advanced control and want to configure policies for multiple users/computers (for example, using the Active Directory group policy).

General Browser Security Procedures

An organization should implement some general procedures, regardless of the browser it uses. These concepts can be applied to desktop browsers as well as mobile browsers:

- **Implement policies:** The policy could be handwritten, configured at the browser, implemented within the computer operating system, or, better yet, configured on a server centrally. Policies can be configured to manage add-ons and disallow access to websites that are known to be malicious. Or, a policy might state that all web browsers should be configured to delete all cookies and content daily. Another policy might state that if there is a browser misconfiguration, a technician should reset the browser to default settings and start fresh.
- **Train users:** User training is important when it comes to helping users know which websites to access, how to use search engines, and what to do if pop-ups appear onscreen. The more users you can reach with your wisdom, the better!
- **Use a proxy and content filter:** An HTTP proxy (also known as a proxy server) acts as a go-between for the clients on a network and the Internet. Basically, it caches website information for clients and thus reduces the number of requests that need to be forwarded to the corresponding web server on the Internet. An HTTP proxy is used to save time, make more efficient use of bandwidth, and help secure client connections. When a content filter is used in combination with an HTTP proxy, specific websites can be filtered out, especially ones that may potentially be malicious that can waste users' time (you know what we're talking about!).

- **Secure against malicious code:** Depending on your company's policies and procedures, you might need to configure an increased level of security concerning ActiveX controls, Java, JavaScript, audio/video media, phishing, and much more. Always be on the lookout!
- **Use ad blockers:** Consider using ad blockers to stop ads from gaining personal information about your browsing habits. This can also help stop adware, as discussed in Chapter 46, "Wireless Security and Malware." Many websites offer free content because of those ads, so blocking those ads might take away from revenue streams. This is why many websites are resorting to paywalls to force the users to subscribe to see content. You will also see more aggressive anti-ad-blocker measures being taken, including the use of Admiral's Anti-Adblock solution, which is a private company whose solutions many websites employ to block ad-blocker technology.
- **Use secure DNS:** By default, DNS requests are not encrypted. Lately, there has been a move to encrypt those DNS requests. Secure DNS encrypts your DNS requests, preventing eavesdropping and manipulation by third parties, enhancing privacy and security. To implement it, you can either change your DNS settings in your operating system's network configuration to use a secure DNS provider like Cloudflare or Google Public DNS, or enable DNS over HTTPS (DoH) in your web browser's settings.

Cram Quiz

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

1. You have been tasked with implementing ad-blocking functionality within a web browser. Which of the following should you add to make ad blocking a reality?

   ○ **A.** Extension

- ○ **B.** Valid certificate
- ○ **C.** Pop-up blocker
- ○ **D.** Password manager

2. A user's computer is running very slow. You investigate and find out that there are many, many temporary files, caused by *excessive* browsing. Where would you go in Microsoft Edge to fix the problem?

- ○ **A. edge://settings/profiles/sync**
- ○ **B. chrome://extensions**
- ○ **C. edge://settings/privacy**
- ○ **D. edge://settings/content**

3. You want to verify that Google Chrome will connect to websites in a secure manner. Where should you go to confirm this? (Select the two best answers.)

- ○ **A.** PGP key
- ○ **B.** TLS setting (1.2 or higher)
- ○ **C.** Installation file signature from a trusted source
- ○ **D.** Incognito mode
- ○ **E.** Trusted zones in **Internet Properties > Security**

4. You are working for Geeks of the Future, a company that solves home user technology issues. One customer's computer is suffering from slow performance as well as browser crashes. These issues began after the customer clicked a "repair" pop-up while browsing the Web. Which of the following should you perform *first* to resolve the issue? (Select the two best answers.)

- ○ **A.** Enable the web browser's pop-up blocker.
- ○ **B.** Scan the storage drive's boot sector and RAM with an antivirus program.

- ❍ **C.** Initiate a cold shutdown and then turn on the computer.
- ❍ **D.** Uninstall any recently installed suspicious programs and browser extensions.
- ❍ **E.** Run SFC and replace changed files with the original system files.

5. How are updates for the Safari web browser typically managed?

- ❍ **A.** Through the browser's built-in settings menu, similar to Chrome and Firefox
- ❍ **B.** Independently by downloading patch files directly from Apple's website
- ❍ **C.** As part of the macOS system update process
- ❍ **D.** By manually installing updates prompted by the browser itself

6. What is the primary security benefit of using Secure DNS?

- ❍ **A.** It speeds up website loading times by caching DNS requests.
- ❍ **B.** It prevents third parties from intercepting and manipulating DNS requests.
- ❍ **C.** It blocks advertisements and prevents tracking of browsing habits.
- ❍ **D.** It automatically updates web browsers to the latest secure versions.

Cram Quiz Answers

1. **A.** Add an extension for the ad blocker of your choice. (Make sure it's relatively secure!) A valid certificate is required before a web browser establishes a session with a web server. Pop-up blockers are different from ad blockers in that they block pop-up windows in general; an ad blocker might happen to block some pop-up

windows but only because they are ad based. A password manager stores passwords in an encrypted fashion within a vault on the local computer.

2. **C.** In the address bar, go to **edge://settings/privacy** and then click **Clear browsing data**. This will remove all of the temporary files that are potentially slowing down the system. **edge://settings/profiles/sync** is used for sign-in and data synchronization. **chrome://extensions** is where you would go to enable or disable extensions in Chrome, not Microsoft Edge. **edge://settings/content** is for blocking pop-ups.

3. **B and E.** Check the TLS setting in **Internet Properties > Advanced**. In most cases, you want to make sure that it is TLS 1.2 or higher. That is the secure protocol that launches the session. Also, check out the trusted zones section of **Internet Properties > Security**. This is where you can select the level of security and specify custom levels, if necessary. Both of these will work for Edge and for Chrome. Using a PGP key (or an installation file signature) is a good idea when you are installing a less-well-known browser; it lets you verify whether the installation file was tampered with during transit. Incognito mode, which is Chrome's private browsing mode, is great to use when you want to avoid having browser session information stored locally.

4. **A and D.** The *first* things you should do are to enable the web browser's pop-up blocker and uninstall any recently installed suspicious programs and browser extensions. The problem occurred when the customer clicked on a fake repair pop-up while browsing the Internet. Pop-ups should be disabled on today's web browsers by default, but users have a way of disabling that which protects them most! The act of clicking the pop-up probably initiated more problems—for example, the installation of unwanted browser extensions (which is common) or perhaps even undesirable programs. These extensions and/or programs are most likely causing the system to behave slowly because they are reaching out to the Internet to do malicious things. They should be removed. However, you should also scan the system for malware

—not just the boot sector of the storage drive but the entire system and not just with anti*virus* software but with a full-fledged anti*malware* program. And the *very* first thing you should do if malware is even a remote consideration is to quarantine or isolate the system. If you suspect malware, you might also need to run System File Checker (SFC) to repair OS files. (You might also opt to simply reimage the system, though that can be a tough sell with a home user.) Finally, doing a cold shutdown and boot is also known as a *graceful shutdown*, and it can help with various hardware and software issues; it is generally a good idea to perform a graceful shutdown as a final step when you are done troubleshooting a system.

5. **C.** Safari updates are managed through the macOS system update mechanism, ensuring the browser is patched along with the operating system. However, Chrome and Firefox update automatically or via their settings menus. Apple does macOS system updates and usually does not offer patch file updates.

6. **B.** Secure DNS encrypts your DNS requests to prevent eavesdropping and manipulation by third parties to enhance privacy and security. Yes, caching DNS requests can speed up website load times, but note that is not the security benefit. Many third-party DNS services do block advertisements and prevent tracking, which is great but again not necessarily a security benefit. DNS is just to look up domain names to IP addresses; it doesn't update your browser.

You have finished this chapter and also the security section of this book. Well done! But remember, you should always have security on your mind! For a technician, security should be a primary consideration with any technology. Review your notes for this chapter and for the entire domain. Take a nice break, and we'll "see" you at the next chapter!

"Companies spend millions of dollars on firewalls, encryption, and secure access devices, and it's money wasted; none of these measures address the

weakest link in the security chain. The people who use, administer, and operate computer systems.” —Kevin Mitnick

Core 2 (220-1202)

Domain 3.0: Software Troubleshooting

CHAPTER 53 Troubleshooting Microsoft Windows

CHAPTER 54 Troubleshooting Mobile Operating Systems and Applications

CHAPTER 55 Troubleshooting Mobile Operating Systems' Security Issues

CHAPTER 56 Troubleshooting PC Security Issues

Chapter 53
Troubleshooting Microsoft Windows

This chapter covers the following A+ 220-1202 exam objective:

- **3.1** – Given a scenario, troubleshoot common Windows OS issues.

Welcome to the first chapter of Domain 3.0: Software Troubleshooting.

Now it's time for the toughest part of working with Windows: troubleshooting. Troubleshooting is probably the most important skill for a computer technician to possess.

Many different things can go wrong with a computer, and the majority of them are software-related. This vital chapter endeavors to give you the tools, utilities, and skills necessary to troubleshoot the various boot errors, stop errors, and other Windows problems you might encounter.

This is one of the longer chapters in the book. Take breaks as you go and review your notes often.

ExamAlert

Objective 3.1 concentrates on common symptoms and common troubleshooting steps in Windows.

Windows Recovery

There are many tools included with Windows that are designed to help you troubleshoot and repair just about any issue that might come up. Before getting into the exact issues you might face, let's look at some of the repair and preinstallation environment repair tools, what they do, and where you can access them. We'll start with the Windows Recovery Environment.

Windows Recovery Environment (Windows RE)

Windows RE (or WinRE for short), also referred to as Advanced Startup Options, is a set of tools included in Windows whose purpose is to recover Windows from errors that prevent it

from booting. These tools can also be instrumental in fixing issues that cause a computer to "freeze up."

In Windows, you access WinRE through the Advanced Startup menu. You can get to Advanced Startup in a variety of ways, including the following:

- Hold the Shift key while selecting **Restart**. (This works with most power option locations in Windows.)
- In PowerShell or the Command Prompt, type **shutdown /r /o** and then press Enter.
- Go to **Start > Settings > System > Recovery** (**Start > Settings > Update & security > Recovery** in Windows 10) and, next to Advanced Startup, click **Restart now**.
- Boot to the appropriate recovery media. This could include a USB drive, a CD/DVD if equipped, a network if you have one set up, or most often, the Windows Recovery Partition on your hard drive. For USB or CD/DVD options, you will need to configure these ahead of time (before you need them or from a different computer). For the Windows Recovery Partition, these are created by the manufacturer for just this situation. Refer to your manufacturer's instructions for details.

> **Note**
>
> Windows recovery drives are invaluable tools. See https://support.microsoft.com/en-us/windows/recovery-drive-abb4691b-5324-6d4a-8766-73fab304c246 for information on how to create a recovery USB drive and use it to recover a Windows system.

- If your device is equipped with one, press the hardware recovery button or the button combination designated by the maker of the device.

Once the system has rebooted, you should see the Choose an option screen. Select **Troubleshoot**, and you can access several options, including

- **Reset your PC:** This option enables you to keep personal files *or* remove everything.

  To reset Windows 11, you can use the Settings app to go to **System > Recovery** and select **Reset PC**, as shown in Figure 53.1. You can also boot into the Advanced Startup Options menu and select **Reset this PC**.

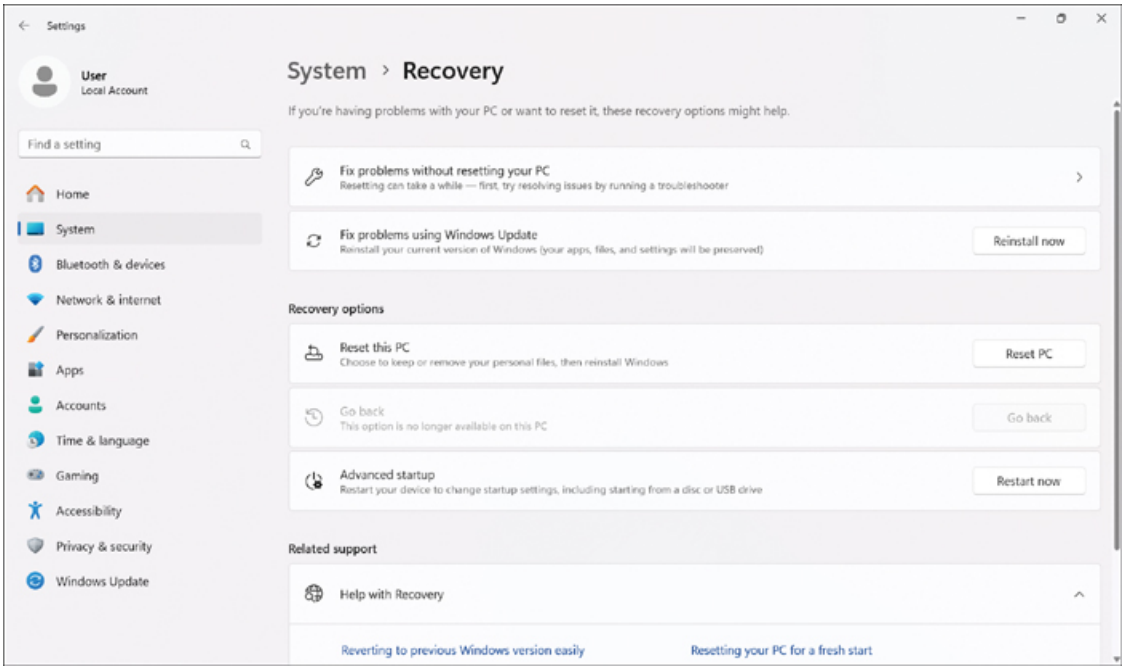


FIGURE 53.1 **System > Recovery Window in Windows 11**

- **Advanced Options:** This option brings up the Advanced options screen, which shows the main tools that you can use to troubleshoot a system. Figure 53.2 shows the Advanced options screen that appears in Windows 11 when you restart into Advanced Startup mode. The options might be listed differently, depending on your version of Windows. Table 53.1 describes the options you will encounter in Advanced options, as well as other options that you can't see in the figure. Note that not all versions of Windows will have all options.

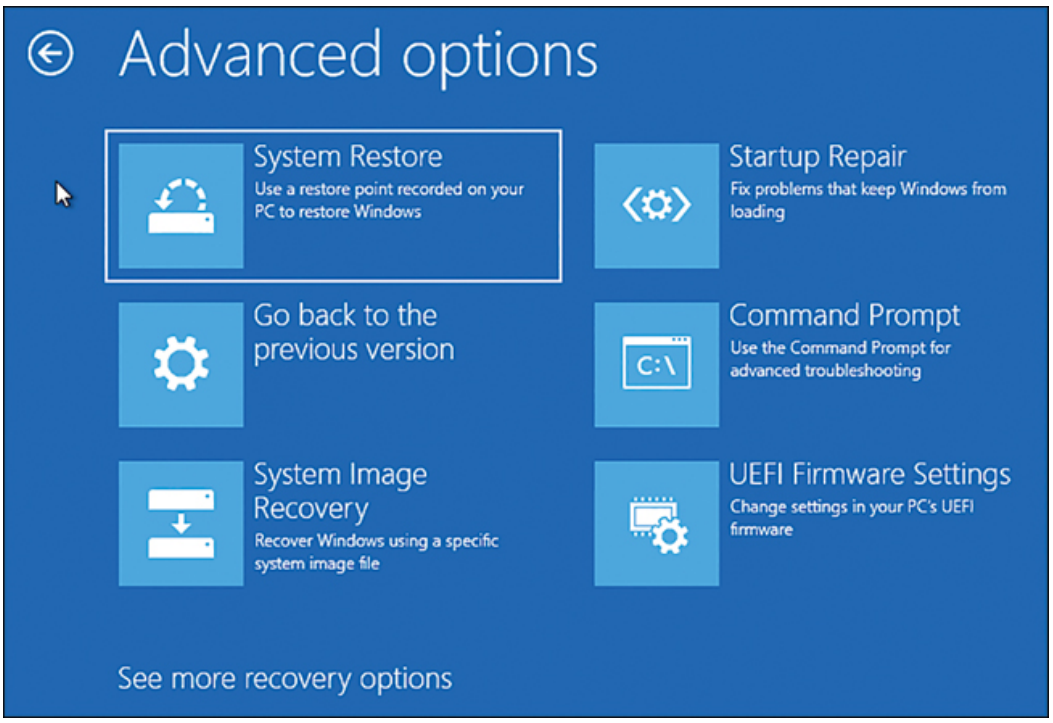


FIGURE 53.2 **The Windows Advanced Options Screen**

TABLE 53.1 **Windows Recovery Advanced Options**

Recovery Option	Description
System Restore	This option restores the computer's system files to an earlier point in time. The option allows you to undo system changes to a computer without affecting the personal files on the computer, such as email, documents, or photos. Note: If you use System Restore when a computer is in Safe Mode, you cannot undo the restore operation. However, you can run System Restore again and choose a different restore point, if one exists. We'll discuss System Restore further later in this chapter.
Go back to the previous version/Go back to the previous build	This option, which is available for only a limited time after an upgrade, allows you to go back to an earlier build of Windows. You can also do this from Settings in Windows. Go to **Start > Settings > System > Recovery** and choose **Go back** if it is available. Windows Update has a related tool. To use it, go to **Settings > Windows Update > Update history > Uninstall updates**, and it will enable you to uninstall updates that were recently installed. If you think a recent update caused a problem, you can quickly and easily uninstall it and get your system up and running again.

Recovery Option	Description
System Image Recovery	These programs are used to restore a storage drive from a backup in select editions of Windows.
Startup Repair	This option automatically fixes certain problems, such as missing or damaged system files that might prevent Windows from starting correctly. This option can help with general system instability. Startup Repair scans your computer for the problem and then tries to fix it so that your computer can start correctly. Most of the time, this is a great place to start when troubleshooting.
Command Prompt	Advanced users can use the Command Prompt to perform recovery-related operations and also run other command-line tools for diagnosing and troubleshooting problems. To use it, you must log on as an administrator.
UEFI Firmware Settings (not available in Windows 11)	This option allows a user to access the UEFI from the OS to make changes. (It requires UEFI-compatible BIOS.)
Startup Settings	This option enables you to boot to a variety of modes that are explained later in this chapter. To access this in Windows 10, you might have to click **See more recovery options**.

ExamAlert

Memorize the different WinRE options.

Note

To learn more about WinRE, see https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/windows-recovery-environment--windows-re--technical-reference.

Keep in mind that Windows attempts to do a self-repair if it senses a boot issue. This occurs first when you start, or restart, the system. If this automatic repair does not fix the problem, using WinRE is your next stop. However, in some cases, you need to boot the system in a different *way* to fix a problem. Let's discuss advanced booting now.

Startup Settings

If Windows is not functioning properly, the culprit might be a video driver, a new configuration, or another system issue. The Startup Settings portion of WinRE has several startup options—such as Safe Mode—that can aid you in fixing such problems.

F8

Historically, you accessed the Startup Settings options by pressing the F8 key immediately after the computer started up. For example, in Windows 7, pressing F8 would bring up the Windows Advanced Boot Options menu, which has many of the same options as shown in Figure 53.1 but with slight differences in names and arrangement.

While Microsoft still supports the F8 keypress, it does not work in Windows 10/11 by default. To enable F8 functionality in Windows 10/11, type the following in the Command Prompt (as an admin):

```
bcdedit /set {default} bootmenupolicy legacy
```

This command effectively replaces the Startup Settings version. To disable it and go back to the Startup Settings version in WinRE, use the same command but replace **legacy** with **standard**.

The Startup Settings window and the Advanced Options menu have essentially the same options, with one difference: The Advanced Options menu includes the Startup Repair option, which automatically attempts to fix Windows issues for you. This option is not included in the Startup Settings window because there are several automated repair options elsewhere in WinRE. You will most likely use Startup Settings more often, so we'll focus on that.

ExamAlert

Know the various settings under Windows Startup Settings (such as Safe Mode) and know what they do. If you have a chance, practice on real equipment to see what each does (be sure to re-enable anything you shut off and be careful to not reset your system!)

System Restore

The System Restore tool can be used to create a snapshot of the state of the operating system and store it for later retrieval. It can be very helpful when you're troubleshooting a system.

System Restore can fix issues caused by defective hardware or software by reverting to an earlier point in time. Registry changes made by hardware or software are reversed in an attempt to force the computer to work the way it did previously. Restore points can be created manually and are also created automatically by the operating system before new hardware, updates, or applications are installed.

To create a restore point in Windows, follow these steps:

1. Open the System Properties dialog box to the System Protection tab by selecting **Run** and typing either **systempropertiesprotection** or **sysdm.cpl ,4** (see Figure 53.3). For

more information on the System Properties dialog box, refer to Chapter 37, "Windows Settings."

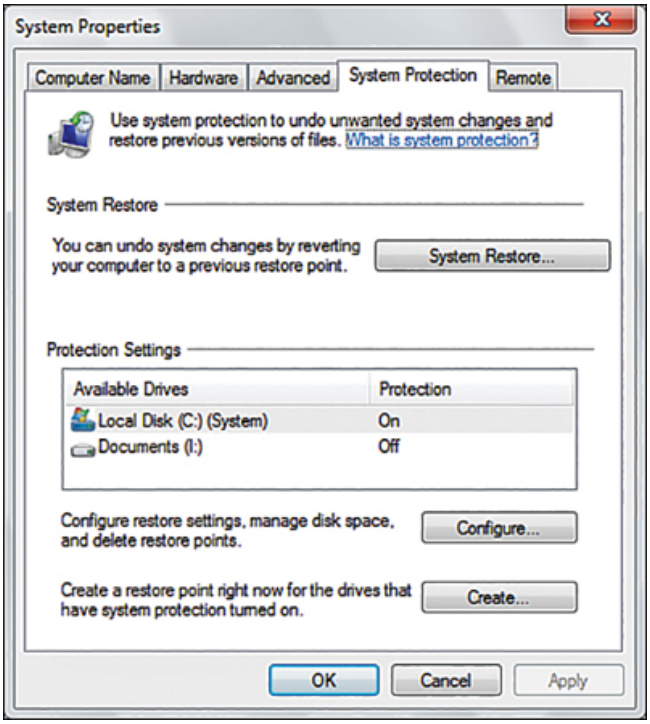


FIGURE 53.3 **The System Protection Tab of the System Properties Dialog Box**

2. Click the **Create** button. The System Protection dialog box appears.
3. Type a name for the restore point and then click **Create**.

If System Restore is not available, it might be turned off. There are several reasons a user might turn it off (for example, if the system had been scanned for viruses recently).

To enable or disable System Restore in Windows, click the **Configure** button on the System Protection tab of the System Properties dialog box. Then click the **Turn on system protection** radio button.

Using System Restore is kind of like using a time machine (if one actually existed). It allows you to reset a computer to an earlier configuration—hopefully, one that functioned properly. To actually restore a computer to an earlier point in time, just click the **System Restore** button on the System Properties/System Protection dialog box and then follow the instructions. But beware: Some applications might be removed, and drivers might be uninstalled.

System Restore is disabled by default in Windows 10 and Windows 11. You can enable it, but in practice Windows will automatically create a restore point for you, regardless of the settings in System Restore, if you have enough free space remaining in your system drive. Although this tool was once very useful, and is moderately useful now, we cannot predict whether a particular tool will still exist in the future. A better choice is, as always, making full backups of all data files.

Note

If a system won't boot normally, you can attempt to run System Restore from Safe Mode, or you can use WinRE or System Recovery Options.

ExamAlert

Understand how to enable and disable System Restore, how to create restore points, and how to restore a system to an earlier point in time.

Improper, Spontaneous, and Frequent Shutdowns

You've probably seen a Windows computer fail and reboot with a message such as "Windows was shut down improperly." Improper and spontaneous shutdowns can happen for a variety of reasons, including brownouts or blackouts, power surges, hardware failures, a user inadvertently unplugging the computer, or perhaps a virus or other malware. This phenomenon can be disturbing to users, and it may have been going on for a while before a user got you involved, so it is especially important to be patient with the user (and the computer) when troubleshooting this problem.

Some of the methods you can use to troubleshoot improper and spontaneous shutdowns include the following:

- **Check the Event Viewer:** Look in the System log to see if there are any alerts about hardware failures, service failures, and so on. If there is an alert, consider upgrading the driver for the affected hardware or upgrading the software that the service is dependent on. Ensure that the computer is running the latest updates.
- **Use MSConfig (the System Configuration utility):** On the General tab, select the **Selective startup** checkbox and the **Load startup items** checkbox. To weed out third-party program issues, click the **Services** tab, click the **Hide all Microsoft services** checkbox, and then click **Disable all**. Restart the system and see if the same issues return or if events are still written to the Event Viewer. Remember to restore Normal startup in MSConfig when you finish troubleshooting.
- **Boot into Safe Mode:** Use Safe Mode to further investigate the problem. Safe Mode uses only the most basic drivers, so if a driver issue is causing the problems, Safe Mode could help you find out about it. Don't forget that you can also access Safe boot from MSConfig.
- **Run a virus scan:** Run a scan for malware and quarantine anything unusual. Update the antivirus/antimalware software before you start and when you are finished.
- **Check power:** Make sure the AC outlet is wired properly and is supplying clean power. Verify that the power plug is firmly secured to the computer. If necessary, you might have to check the power supply. Intermittent and unexplained shutdowns can sometimes be linked to power supplies or other hardware failures.

- **Use WinRE:** If necessary, use the Windows Recovery Environment to troubleshoot spontaneous shutdowns.

Blue Screen of Death (BSOD) Stop Errors

A stop error (also known as a blue screen of death [BSOD]) is the worst type of error that can happen while Windows is operating. It completely halts the operating system and displays a blue screen with various text and code. You might also see a sad face with a QR code and/or hexadecimal text, among other things.

Anything you were working on when you get a BSOD is, for the most part, lost. In some cases, Windows reboots the computer after a memory dump has been initiated. (This is also known as auto-restart.) If not, you need to physically turn off the computer by pressing the power button and then turn it back on. A BSOD may happen only once, and if that is the case, you need not worry too much. But if it happens two or three times or more, you should investigate. Quite often these errors are due to hardware issues, such as improperly seated memory or a corrupt driver file. If you see two columns of information on a BSOD with a list of drivers and other files, a driver issue could be the culprit. Look at the bottom of the second (or last) column and identify the driver that has failed (for example, ntfs.sys). Drivers can become corrupt for a variety of reasons, and those that are corrupt need to be replaced when you boot into Windows. Or, if you can't boot into Windows and Windows does not auto-repair the file, you can replace the driver within WinRE's Command Prompt. Less commonly, a BSOD might be caused by a memory error, and the screen will show additional code that you can research on Microsoft's websites: support.microsoft.com and docs.microsoft.com.

By default, three things happen when a stop error occurs:

1. An event is usually written to the System log within the Event Viewer, if that option has been selected in the Startup and Recovery window, as shown in Figure 53.4. When a stop error is written to the System log, it may be listed as an Information entry, not as an Error entry. The stop error will be listed as "The computer has rebooted from a bugcheck. The bugcheck was: *error number*." Use the error number to look up the problem—and hopefully find a solution—at one of Microsoft's support sites.

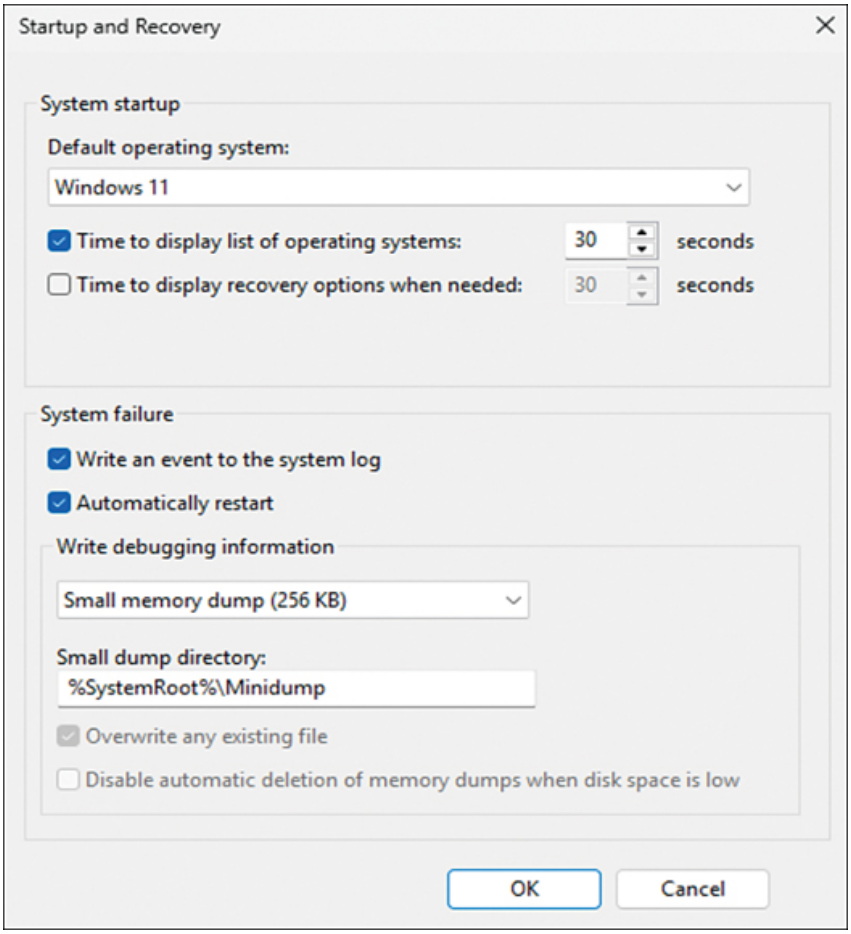


FIGURE 53.4 **The Startup and Recovery Window**

The settings shown in Figure 53.4 can be accessed from the Advanced tab in the System Properties dialog box (which you can access directly via **Run > SystemPropertiesAdvanced.exe**). Click the **Settings** button in the Startup and Recovery area to access the Startup and Recovery window.

2. Windows writes debugging information to the storage drive for later analysis with memory dump debugging programs; this debugging information is essentially the contents of RAM. The default setting in Windows is to only write a portion of the contents of RAM; this is known as a *kernel memory dump*. The kernel memory dump is saved as the file %SystemRoot%\Memory.dmp. You can also select to create a small memory dump, which is written to %SystemRoot%\Minidump. Windows also enables you to do a complete memory dump, which dumps the entire contents of RAM to a file named Memory.dmp. To support a complete memory dump, the paging file must be large enough to hold all the physical RAM plus 1 MB.

Note

For more information about the various dump files, visit https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/varieties-of-kernel-mode-dump-files.

3. The computer automatically restarts (if the Automatically restart option is selected, which is the default in Windows).

ExamAlert

Know how to stop errors from occurring and how memory dumps function.

How to Restore Windows

There actually is something worse than a stop error. With a complete system failure, a system cannot be repaired. When this happens, the only options are to reinstall Windows or to restore Windows. There are several methods for restoring Windows, including

- **Repair option:** Boot to the Windows installation media (Recovery partition, USB flash drive, DVD, etc.) and click the repair option. In the main Windows RE Advanced options (or System Recovery Options) window, select **System Image Recovery**. Provide backup media.
- **Reset the image:** Reset the system to a factory image stored on a separate partition of the storage drive. This commonly needs to occur on laptops, especially ones that do not have optical drives. You can also use third-party tools such as Ghost or Acronis True Image. Remember that the image needs to be created *before* the disaster!

There are various other ways to access the utilities mentioned. Refer to earlier parts of this chapter for details or refer to the documentation that came with your third-party software.

Common Windows Symptoms and Solutions

We have already discussed a lot of issues and solutions, but there are a good number of other symptoms that you will encounter when working on Windows. What makes troubleshooting difficult is that there are often several potential solutions to a problem. Let's fill the gaps by listing some of those symptoms and potential solutions in Table 53.2.

ExamAlert

You will likely be tested on the common symptoms and solutions listed in Table 53.2. Given a scenario, know how to troubleshoot Windows OS problems well for the exam and in the field!

TABLE 53.2 **Windows Symptoms and Solutions**

Symptom	Potential Solutions
Slow or sluggish performance/slow bootup	▶ Use the built-in Windows Troubleshooter: Go to **Settings > Update & Security > Troubleshoot**. Note: In Windows 11, you can find the troubleshooters in **Settings > System > Troubleshoot**. Or Go to **Control Panel > System and Security** and click the **Troubleshoot common computer problems** link under Security and Maintenance. Then click **Additional Troubleshooters**. From there, you can run a variety of troubleshooting tools. Note: You can also see individual troubleshooting tools by navigating to **Control Panel > All Control Panel Items > Troubleshooting**. ▶ Clean up and defragment the storage drive. ▶ Reboot often. ▶ Watch for numerous tabs opened in a web browser. ▶ Uninstall unused programs. ▶ Limit programs that run at startup. View the notification area to see what is running. Use **Task Manager > Startup** to disable programs. ▶ Scan for malware. ▶ End tasks in **Task Manager > Processes** (or with the **taskkill** command). Also, if you receive a “low memory” error: ▶ Increase RAM (if possible). ▶ If it is not possible to increase RAM, increase the virtual memory: **Run > systempropertiesadvanced.exe > Advanced** and click the **Settings** button under Performance to open the Performance Options dialog box, where you select the **Advanced** tab and click the **Change** button.

Symptom	Potential Solutions
Limited or no network connectivity	▶ Restart the system. ▶ Reboot the router, or modem, or gateway. ▶ Update the network settings, including the IP address and gateway address, and run **ipconfig /release** and **ipconfig /renew**. ▶ Update the wireless network settings: SSID, encryption type, and so on. ▶ Ensure that the system is not in airplane mode. ▶ If necessary, boot into Safe Mode (or Safe boot) and roll back the network driver in the Device Manager. ▶ Check the patch cable and look for a link light. ▶ Go to **Settings > Update & Security > Troubleshoot > Additional troubleshooters > Internet Connections**. Note: In Windows 11, go to **Settings > System > Troubleshoot > Other Troubleshooters > Network and Internet**.
No OS found/failure to boot	▶ Update the BIOS/UEFI boot order. ▶ Repair the GPT or MBR or boot files in the system partition. (See the various repair options earlier in this chapter.) ▶ Check hardware connections (drive cables, etc.). If necessary, roll back any changes or reimage/reload the OS.
Bootmgr is missing	If the Windows Boot Manager file is missing or corrupt, try the following: ▶ Boot to WinRE and select **Startup Repair** to automatically repair the system. ▶ Rebuild the Boot Configuration Data (BCD) store by entering **bootrec /rebuildbcd** in the Command Prompt in WinRE (not Windows!). (Do a System Restore, if needed.) ▶ Ensure that the C: partition is set to **active**. See this site for advanced troubleshooting of Windows boot problems: https://docs.microsoft.com/en-us/windows/client-management/advanced-troubleshooting-boot-problems.
Boot sector issues	Enter **bootrec /fixboot** at the WinRE Command Prompt.

Symptom	Potential Solutions
Application/OS won't install or won't run	▶ Verify the requirements for the application or OS. ▶ Add resources (CPU cores, RAM, storage space, etc.). Note: If there is a RAM issue, run the Windows Memory Diagnostic program to troubleshoot it: **Run > mdsched**.
Application crashes	▶ Apply updates to the OS. ▶ Apply updates to the application. ▶ Repair the application: **Control Panel > All Control Panel Items > Programs and Features** and then right-click the application in question and select **Repair** (or reinstall if necessary). ▶ Run the application in program compatibility mode. Use the Program Compatibility Troubleshooter: Go to **Settings > Update & Security > Troubleshoot > Additional troubleshooters > Program Compatibility Troubleshooter**. (In Windows 11, open Settings and type **Program Compatibility** in the search box.) Note that the Program Compatibility Troubleshooter and other troubleshooters are scheduled to be retired soon. See https://support.microsoft.com/en-us/windows/deprecation-of-microsoft-support-diagnostic-tool-msdt-and-msdt-troubleshooters-0c5ac9a2-1600-4539-b9d0-069e71f9040a for details. ▶ You can also right-click the program executable link/button and change the compatibility settings. ▶ Temporarily disable the application from startup if it is interfering with other programs and the OS: **Task Manager > Startup**.
Missing or corrupt system files	▶ Use the System File Checker (**sfc**) tool. To run SFC, open the Command Prompt and type **sfc** with the appropriate switch. A typical option is **sfc /scannow**, which scans all protected files immediately and repairs files. ▶ Use the **chkdsk** tool. Open the Command Prompt. From there, run **chkdsk** with either the **/F** switch (which fixes errors on the drive) or the **/R** switch (which locates bad sectors and recovers data)—or run both.
Blue screen/black screen	See the sections "Windows Recovery" and "Blue Screen of Death (BSOD) Stop Errors," earlier in this chapter.

Symptom	Potential Solutions
Printing issues	▶ Go to **Settings > Update & Security > Troubleshoot > Additional troubleshooters > Printer**. Note: In Windows 11, go to **Settings > System > Troubleshoot > Other troubleshooters > Printer**. ▶ Configure settings in **Control Panel > All Control Panel Items > Devices and Printers**. ▶ Roll back device drivers for any devices that fail in Windows. (See Chapter 28, "Troubleshooting Printers," for more information.)
Device issues	▶ Use the Troubleshooter. ▶ Use the Device Manager to troubleshoot (**Run > devmgmt.msc**). Know the Device Manager icons: ▶ Black downward-pointing arrow = Device is disabled. Simply reenable it to use the device. In rare cases, a hardware conflict can be caused by I/O settings or interrupt requests (IRQs); for example, serial COM ports. ▶ Exclamation point = Incorrect driver or hardware conflict. Try removing the device and let Windows reinstall it. If that does not work, download correct drivers from the manufacturer's website. To troubleshoot further, open the Properties window for the device and locate the error code on the General tab or the Events tab. Cross-reference the code with the codes listed at https://support.microsoft.com/en-us/help/310123/error-codes-in-device-manager-in-windows.
USB controller resource warnings	When you get warnings such as "Not Enough USB Controller Resources," try the following: ▶ Manage and rearrange devices connected to USB ports. ▶ Reserve USB 3.0 ports for USB 3.0 devices only; older devices should be connected to USB 2.0 ports. ▶ Use a USB dock. ▶ Add a USB adapter card. ▶ Reinstall the USB Controller drivers in the Device Manager.

Symptom	Potential Solutions
Services fail to start	▶ Start or restart services: **Run > services.msc**, right-click the service in question and choose **Properties**, and stop and start it within the Properties window. Or use the **net start** and **net stop** commands. Check for issues with other services that the affected service is dependent on. Also try modifying services in **MSConfig > Settings** or with the **Restart-Service** cmdlet in PowerShell. (See the following site for more information on this cmdlet: https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.management/restart-service?view=powershell-7.2.) ▶ Verify that the services have not been disabled in MSConfig or the Services console window.
Time drift	Time drift (or "clock drift") occurs when Windows is not synchronized to a time server properly, and the clock slowly drifts away from standard time. It might then synchronize to the motherboard's Real Time Clock (RTC). Try the following: ▶ Use Network Time Protocol (NTP) to synchronize the Windows system to a time server. ▶ Synchronize the Windows system to the domain controller (if the system is a member of a domain). For more information, see https://learn.microsoft.com/en-us/windows-server/networking/windows-time-service/windows-time-service-tools-and-settings?tabs=config.

Symptom	Potential Solutions
Slow profile load	Slow profile loading is often due to a bloated user profile (especially roaming profiles). Check the following: ▶ Clean up temp files and cookies with cleanup programs and manually. For example: C:\Users\%username%\AppData\Local\Microsoft\Windows\Temporary Internet Files C:\Users\%username%\AppData\Roaming\Microsoft\Windows\Cookies ▶ Verify that the workstation's time is synchronized to the domain controller (if on a domain). Use the **net time** command. For example, log on locally and type **net time *domaincontroller*/set**. ▶ Check the User Profile service for issues. ▶ Watch for too many programs loading at startup. ▶ Configure policies via **gpedit.msc**: **Computer Configuration > Administrative Templates > System > Group Policy** (and similar policies). ▶ Run the Windows Troubleshooter. ▶ Roll back updates (if necessary).
Corrupted profile	▶ Copy the profile to a new account. Do this at **Run > systempropertiesadvanced.exe** and click the **Settings** button in the User Profiles section. Or copy the entire folder or just the ntuser.dat file, as required. ▶ Repair the user profile within the Registry Editor. ▶ Remove, rename, and/or rebuild the profile.

ExamAlert

Know how to get to the troubleshooters in Windows (**Settings > Update & Security > Troubleshoot > Additional troubleshooters**; in Windows 11, go to **Settings > System > Troubleshoot**) and know the various troubleshooting tools, such as those for Internet connections, playing audio, printers, and so on.

Note

You can also use "God Mode" for troubleshooting. See Chapter 45, "Windows Security Settings," for a refresher. When you open that control panel, search "troubleshooting"

or scroll way down to see all of the Windows troubleshooters.

A Final Word on Windows Troubleshooting

Here's the thing about troubleshooting: It goes on and on. Many problems may occur, and there are usually multiple potential solutions to each problem. What works today on one version of Windows might not work tomorrow on another version of Windows. Be ready to think outside the box and use that six-step troubleshooting methodology as a guide while prioritizing the probable causes and potential solutions. Also, visit https://support.microsoft.com and https://docs.microsoft.comoften.

Cram Quiz

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

1. Which option starts the operating system with a minimal set of drivers?

- ○ **A.** Windows RE
- ○ **B.** System Restore
- ○ **C.** Safe Mode
- ○ **D.** Debugging Mode

2. Which tool should be used if you want to use Startup Repair in Windows?

- ○ **A.** File History
- ○ **B.** Windows RE
- ○ **C.** System Restore
- ○ **D.** Safe Mode

3. Jack, an end user at your company, copied files from a USB thumb drive to his PC. When he was done, he updated his computer and restarted it. Then he received the error message "NO OS FOUND." Which of the following should you try *first* to fix the problem?

- ○ **A.** Reboot the computer.
- ○ **B.** Check the SATA cables.
- ○ **C.** Check the BIOS/UEFI boot order.
- ○ **D.** Uninstall, reinstall, and update applications.
- ○ **E.** Perform a hardware diagnostics check.

4. One of your customers updated the software for a wireless adapter on a PC. After rebooting, the user logged in, and the computer displayed a blue screen. What should you do?

- ○ **A.** Install the device on a known good computer.
- ○ **B.** Reboot the computer and access debugging mode.
- ○ **C.** Purchase a new wireless adapter.
- ○ **D.** Roll back the device drivers in Safe Mode.

5. A technician suspects protected Windows system files may be corrupt. What should the tech do first to verify these suspicions and fix any potential problems?

- ○ **A.** Run a system file check.
- ○ **B.** Roll back updates.
- ○ **C.** Restart all services.
- ○ **D.** Rebuild Windows profiles.

6. A stop error in Windows could manifest as which of the following?

- ○ **A.** A BSOD
- ○ **B.** An Event Viewer error
- ○ **C.** An Action Center notification
- ○ **D.** An Edge error

7. Which tool can be used to restore a computer?

- ○ **A. bootrec /fixboot**
- ○ **B.** System Restore
- ○ **C.** Windows Troubleshooter
- ○ **D.** MSConfig

8. Which of the following might cause a blue screen?

- ○ **A.** A faulty USB port
- ○ **B.** A CPU without a fan
- ○ **C.** Bad drivers
- ○ **D.** A program compatibility issue

9. You are tasked with repairing an issue with a Windows client computer that is attempting to log on to a domain. The user informs you that it takes 5 minutes to log on to the domain, but logging in to the local machine takes only 15 seconds. What steps should you take to fix the problem? (Select the two best answers.)

- **A.** Clean up temp files.
- **B.** Disable unnecessary services in MSConfig.
- **C.** Update the BIOS/UEFI boot order.
- **D.** Synchronize the Windows client's time to the domain.
- **E.** Run **ipconfig /release** and **ipconfig /renew**.

Cram Quiz Answers

1. **C.** Safe Mode starts the operating system with a minimal set of drivers. Windows RE (WinRE) is the recovery environment used to repair Windows; it exists outside the operating system. System Restore is used to revert the OS to an earlier point in time. Debugging mode is one of the Advanced boot options.

2. **B.** Windows RE includes Startup Repair. File History is the backup and restore feature of Windows. Safe Mode is part of the Startup Settings screen. System Restore is a different tool that is also available in Windows RE; it can be used to restore a computer's settings to a previous point in time.

3. **C.** Check the BIOS/UEFI boot order first. In the scenario, it is likely that the user left the USB flash drive in the USB port of the computer when he restarted the system. If USB is set first in the BIOS boot order, the system could not boot to the main storage drive that houses the OS. While this could also be fixed by simply disconnecting the USB drive, the BIOS boot order should be changed immediately because having USB first is a security issue. Rebooting the computer is fine, but only if the USB drive has been removed first. Opening the computer and checking cables should be further down the troubleshooting list because these steps take time (and are most likely not the issue here), and an end user should not be doing this. Uninstalling, reinstalling, and updating all applications could take an enormous amount of time, and this approach has very little to do with the problem. If removing the USB flash drive and modifying the BIOS boot order don't fix the problem, a hardware diagnostics check might be necessary.

4. **D.** You should boot into Safe Mode and roll back the drivers of the device in the Device Manager. The drivers that the customer installed were probably corrupt and caused the stop error. There's no need to remove the device and install it anywhere just yet. Debugging mode probably won't be necessary for this; it is more commonly used to analyze issues during boot. Never purchase new equipment until you have exhausted all other ideas!

5. **A.** The technician should first run System File Check (SFC) to verify whether or not operating system files are corrupt. The technician might also be tempted to check the physical integrity of the disk with the **chkdsk** command, but this is different from checking protected Windows system files. Rolling back updates might be necessary but could cause more issues than it solves. Plus, the idea here is to *check* the system files first without actually *doing* anything. Restarting all services would seem to be a

bit extreme for this scenario, but it could be done in **MSConfig > Services** or with the PowerShell **Restart-Service** cmdlet. However, it would probably be wiser to focus on a few select services first instead of restarting all of them. Windows profiles are separate from the protected system files; the technician should rebuild these files if she suspects that there are problems with user accounts.

6. **A.** A BSOD (blue screen of death) results from a stop error in Windows. The proper name for it is a stop error.

7. **B.** System Restore is the tool used to restore a computer to an earlier point in time. While it doesn't completely restore from an image, it is still a form of restoration. The command **bootrec /fixboot** is used to repair the boot sector of the storage drive. The Windows Troubleshooter is a group of troubleshooting tools that can repair issues related to the Internet connection, printers, and so on. MSConfig is used to modify how Windows boots and which services are run.

8. **C.** Bad drivers could cause a blue screen error (stop error). Blue screens could also be caused by improperly seated RAM, among other hardware issues. A faulty USB port should not cause a blue screen. A CPU installed without a fan would overheat, causing the system to shut down. Incompatible programs simply don't run.

9. **A and D.** Apparently, the user's roaming profile is loading slowly, and the local profile is fine. This could be caused by a variety of things, including a bloated roaming profile or the client not being synchronized to the domain properly. So, first try cleaning up temp files and cookies (either with a cleanup program or manually), cleaning up the login script, and otherwise reducing the size of the profile. Then make sure that the client computer's time is synchronized to the domain controller (which can also help with *time drift*). Do this with the **net time** (or **w32tm**) command. Disabling unnecessary services is always a good idea, but it is unlikely that doing so will improve the logon process to the domain very much, especially if the local logon is quick. Updating the BIOS/UEFI boot order isn't necessary because the system is booting to Windows just fine. Releasing and renewing the IP address shouldn't be necessary in this scenario, but it can be helpful when troubleshooting no (or limited) connectivity issues.

Remember that troubleshooting is what we technicians do. It's all about persistence: Keep searching for answers!

Chapter 54

Troubleshooting Mobile Operating Systems and Applications

This chapter covers the following A+ 220-1202 exam objective:

- **3.2** – Given a scenario, troubleshoot common mobile OS and application issues.

The number of mobile devices in the workplace continues to grow steadily and shows no signs of slowing down. With more devices come more problems that will need your attention. There is a bit of overlap between this chapter and Chapter 2, "Mobile Device Accessories and Connectivity Options," and Chapter 3, "Mobile Device Network Connectivity and Application Support." That's because the hardware and the software of a mobile device are very closely linked; a problem that occurs could be due to software, hardware, or both! You might want to refer to those chapters to get a little refresher on mobile device hardware and communications. Let's get troubleshooting!

ExamAlert

Objective 3.2 focuses on the following common symptoms of mobile operating system and application issues: application fails to launch, application fails to close/crashes, application fails to update, slow to respond, OS fails to update, application fails to install,

battery life issues, random reboots, connectivity issues, and screen does not autorotate.

Note

We discuss mobile device batteries elsewhere in the book, and mobile battery troubleshooting specifically in Chapter 26, "Troubleshooting Mobile Devices."

Wireless Troubleshooting

Wireless difficulties and other connectivity issues make up a good percentage of the total problems you will face when it comes to mobile devices. After all, if your mobile device has no network connection, its usefulness is severely impacted. This section goes into some detail about Wi-Fi, Bluetooth, and NFC.

Wi-Fi Troubleshooting

Failed Wi-Fi can cause all kinds of issues, from applications not working, to Internet access failures, to problems updating the OS on a device. When troubleshooting mobile device wireless connections, always perform the following basic wireless troubleshooting techniques:

- Check whether the device is within range of the Wi-Fi network.
- Ensure that your Wi-Fi card is turned on (surprisingly, this affects an awful lot of people; they unintentionally turn off their Wi-Fi, usually by going into Airplane mode, and forget to turn it back on).
- Ensure that the correct SSID is entered.
- Ensure that the device supports the encryption protocol of the wireless network.

- Make sure the user didn't inadvertently connect to an unintended Wi-Fi network. This scenario happens more often than you might think, given the number of open Wi-Fi networks available today. And let's not forget about rogue access points and evil twins; these fraudulent access points are troublesome at best and malicious at worst, and are designed to hijack connections and other data from unsuspecting users.
- Watch for tethering and mobile hot spots. Make sure they are not conflicting with the wireless connection.
- Check whether the cellular connection is conflicting with the wireless connection.

If you still have trouble, here are a few more methods you can try to connect or reconnect to a wireless network:

- Power cycle the mobile device.
- Power cycle the wireless access point (WAP).
- Remove, or "forget," the particular wireless network and then attempt to connect to it again.
- Consider using a Wi-Fi analyzer app to locate the wireless network in question. Sometimes these analysis apps can give you more information that can help to solve the connectivity problem. They're also great security tools for checking your own WAP. Just be careful because some of them use up a good deal of system resources and could possibly cause the battery to run hot.
- Access the advanced settings and check whether there is a Wi-Fi sleep policy, whether Wi-Fi scanning has been turned off, whether there is a proxy configuration, or whether a static IP address is used. Also, Wi-Fi Direct and Wi-Fi Protected Setup (WPS) might need to be configured properly or disabled. Any of these could possibly cause conflicts. You might also try renewing the lease of an IP address, if the device is obtaining addresses from a DHCP server (which it most likely is). Some devices also have the option Best Wi-Fi Performance, which uses more power but might help when connecting to distant WAPs. Another possibility is that the mobile device needs to have an encryption certificate installed, which is usually done from here as well. The

advanced settings will vary from device to device, but an example is shown in Figure 54.1. Note that the IP address and MAC address are shown at the bottom of the figure; if you ever need to know either of those addresses, this is a good place to go.

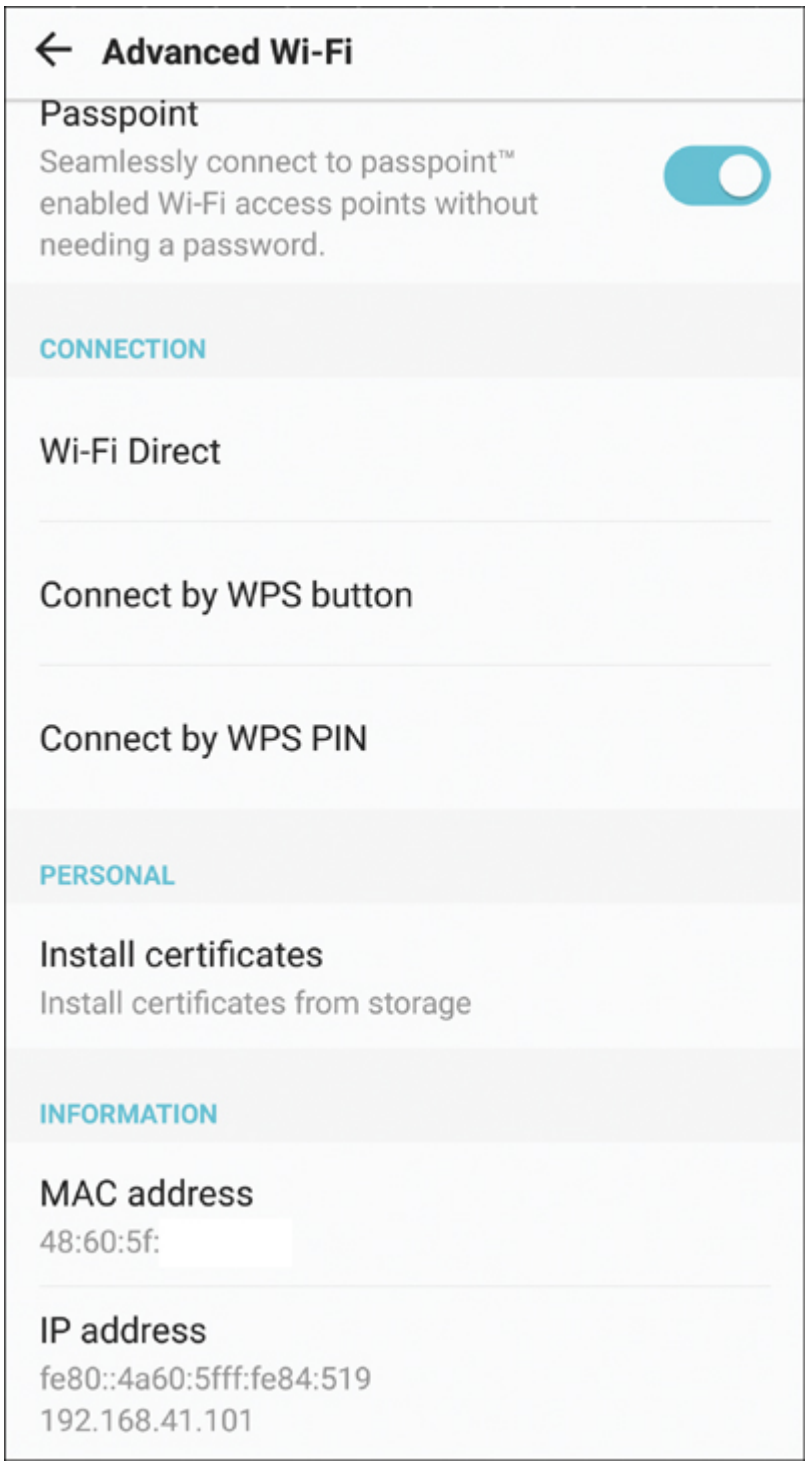


FIGURE 54.1 **Advanced Wireless Settings**

One of these methods usually works when troubleshooting a wireless connection, but if all else fails, a hard reset can bring the device back to factory settings. (Remember: Always back up all data and settings before performing a hard reset!) And if the mobile device still can't connect to any of several known good wireless networks, consider accessing the Developer options and the *super* advanced wireless settings (more on Developer options later) or take the device to an authorized service center.

You might also encounter issues where a device can connect to Wi-Fi but has a slow connection. In such a case, check the signal strength, the distance to the nearest WAP, whether or not the device is connecting to the *correct* WAP (if there is more than one option), and whether there are any obstructions.

ExamAlert

Know your Wi-Fi troubleshooting techniques!

Bluetooth Troubleshooting

If you have trouble pairing a Bluetooth device and connecting or reconnecting to Bluetooth devices or personal area networks (PANs), try some of the following methods:

- Make sure the phone or other mobile device is Bluetooth capable.
- Verify whether Bluetooth is enabled on the mobile device (the device might be in Airplane mode, which shuts off all antennas, including Bluetooth). Also, verify whether it is enabled on the target device (for example, an automobile sound system).
- Verify whether your devices, especially Bluetooth headsets, are fully charged.

- Check whether you are within range. For example, Class 2 Bluetooth devices have a range of 10 meters (approximately 32 feet).
- Restart the mobile device and attempt to reconnect.
- Verify that the devices are paired properly (see Chapter 2 for more information).
- Check for conflicting Wi-Fi frequencies. Consider changing the channel used by the Wi-Fi network (if it is on 2.4 GHz).
- Use a known good Bluetooth device with the mobile device to make sure that the mobile device's Bluetooth is functional.
- Remove, or "forget," the particular Bluetooth device, turn off Bluetooth in general, restart the mobile device, and then attempt to reconnect.
- Check that the user didn't make an unintended Bluetooth connection. If a Bluetooth device doesn't have a passcode or other security methods implemented, it can easily be connected to another mobile device and vice versa.

Note

Many Bluetooth issues arise from pairing problems. See Chapter 2 for more information about pairing.

Note

For help fixing Bluetooth problems on Android, see https://support.google.com/android/answer/9769184?hl=en.

For help connecting a Bluetooth accessory to an iPhone or iPad, see https://support.apple.com/en-us/111804.

ExamAlert

Know your Bluetooth troubleshooting techniques!

NFC Troubleshooting

Another close-proximity wireless technology that can cause headaches is near-field communication (NFC), which includes several different technologies under several names. Collectively, we will refer to all of these as *NFC* in this section.

As mentioned in Chapter 2, NFC enables mobile devices to communicate with each other when the devices touch or are in close proximity to each other. If NFC fails to perform for a user, you can try a couple of things:

- Check whether the two NFC-compliant devices are in close proximity.
- Check whether the device is in airplane mode.
- Turn off NFC, wait 5 seconds, and turn it back on again.
- Try restarting the device.
- Attempt to clear any NFC cached data.
- Download updates for NFC or for the OS.
- Make sure the device is actually NFC compliant; it might not be, and if this is the case, the user will have to transfer data using other means.
- Hold the device so that the NFC antenna is facing the correct direction.
- Remove third-party cases. Some third-party cases can interfere with the NFC antenna.
- Make sure the card is not expired and that it’s compatible with the phone’s NFC technology.
- Make sure the phone and the card are aligned correctly.

- If the user is attempting to pay using NFC, ensure that the device is NFC compliant and that the payment system is configured correctly within the mobile operating system. Pay special attention to the error messages received both on the mobile device and on the payment system screen, because the information on both devices is critical to resolving the issue.

ExamAlert

Given a scenario, be able to troubleshoot common Wi-Fi, Bluetooth, and NFC issues!

Troubleshooting and Stopping Applications

Sometimes applications fail to launch, close unexpectedly, or fail to update properly. As is so often the case, a first step is often to restart your device to see if the problem goes away. In other cases, an application might need to be uninstalled and reinstalled; in this case, make sure that all data pertaining to the application is backed up accordingly.

You might encounter applications that continue to run in the background even after you close them. That behavior will continue unless you specifically turn off the apps within the OS.

There are several reasons why an app might be slow to respond but not totally lock up. Things to check include network connections, because poor network connections can appear as lagging apps. Out-of-date apps can also run slow and sometimes be buggy; updates are often released that will speed up the apps and reduce the bugginess. Sometimes incompatibility with the phone operating system can be a problem, and updating the phone OS is the solution. If your device is running low on storage space, which can occur if you have a lot of apps installed or have taken a lot of pictures or video, that can cause slowdowns with the apps. If too many apps are running at once, that can cause slowdowns. Finally, malware can infect your device and cause slowdowns. Checking for malware on your device can help you find any malware that might have inadvertently infected your

device. Clearing the app cache can also help speed slowly running or unstable apps.

To turn off apps (or services) that are running on a typical Android-based system, go to App Info or the Application Manager (or similar name). That screen displays all the currently running applications and services, though the services portion might be within a different tab of that screen. Like applications on PCs, mobile device apps use RAM. The more RAM that is used by a mobile device, the worse it will perform; high RAM usage not only makes a device slow to respond but also eats up battery power. To close an app, you simply locate it on the list, tap it, and, on the next screen, tap **Force stop**. Figure 54.2 shows an app info screen with the Force stop option on the right side. You can also stop services or processes in this manner. If you are not absolutely sure what a service is, do not initiate a stop because it could possibly cause system instability. In the past, due to that instability, force stops were reserved for services; they are now an option on many devices for applications as well. Just remember that force stops can cause the OS to behave erratically.

You can also clear the storage data and cache by tapping **Storage & cache**, as shown in Figure 54.2. By clearing the data and cache, you can fix a lot of issues with applications.

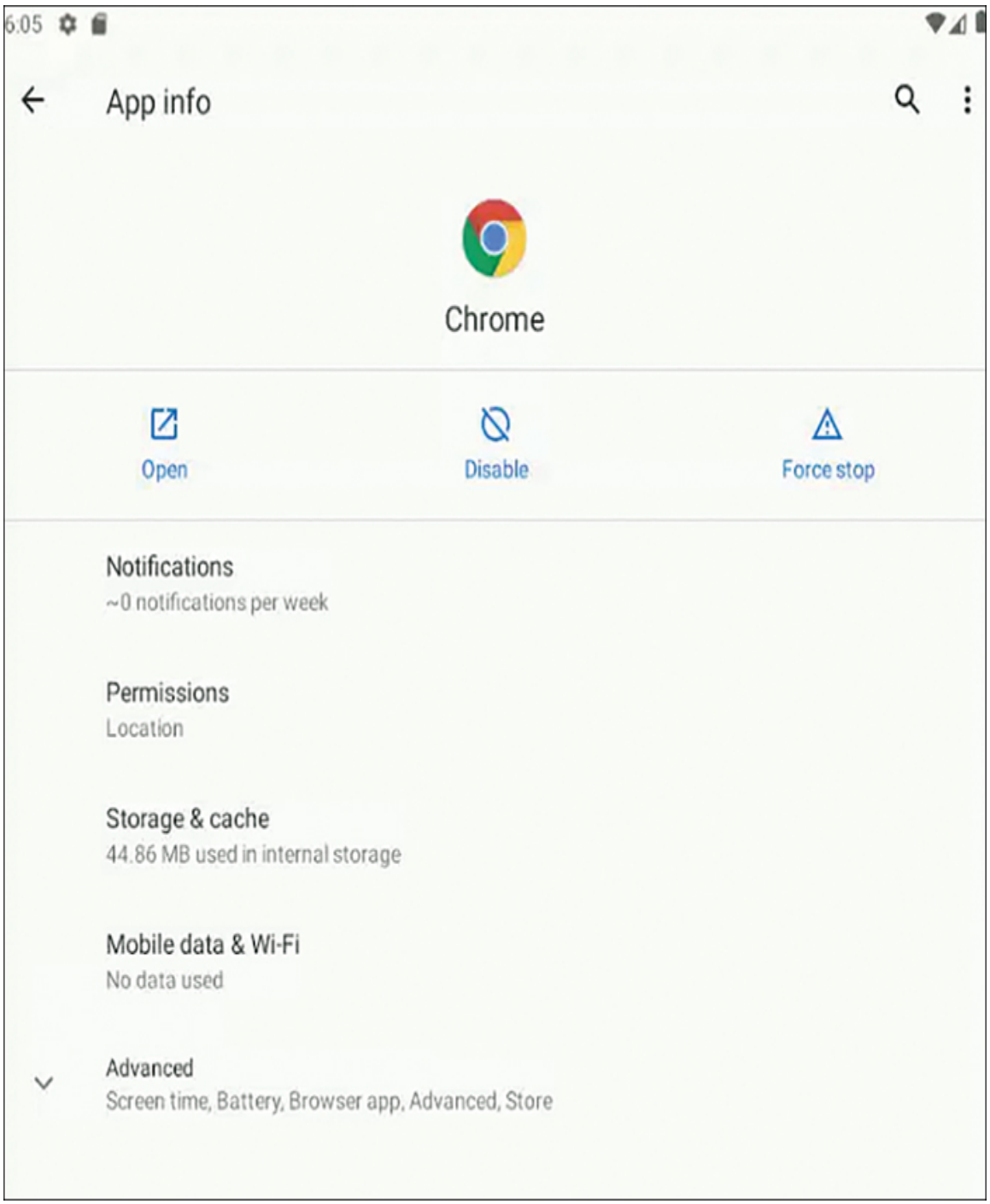


FIGURE 54.2 **The Force Stop Option in Android**

To force quit an app on an iOS-based device, follow these steps:

1. From the Home screen, swipe up from the bottom of the screen and pause slightly in the middle of the screen.
2. Swipe right or left to find the app that you want to close.
3. Swipe up on the app's preview to close the app.

ExamAlert

Understand how to force stop apps on Android and Apple devices.

There are third-party apps that can close down all the apps in one shot if you need to save time. However, these third-party solutions can cause erratic behavior. Finally, if an application is causing a device to lock up and you can't stop the app normally or through a force stop, then a soft reset or a hard reset will be necessary.

If the app fails to install at all, the first thing to check is your Internet connection—after all, without a stable Internet connect you can't go online to download the installer at all. Check to ensure that you have enough storage space; the general rule is that you need enough for the app itself plus 1 GB of free space. Cheap Android devices often have little free space available, so you might have to offload pictures, videos, or other apps to make space available. Finally, make sure that the app is compatible with your device, including the device itself and the operating system you have installed. Nothing will work if your device is not compatible.

Initiating Resets

The screen on a mobile device may freeze, so tapping on the screen and pressing any buttons have no effect. To fix this problem, consider a soft reset. A *soft reset* is done by simply powering off the mobile device and powering it back on. (You might have to hold the power button for longer than usual.) This resets the drivers and the OS. Soft resets are similar to shutting down a PC and powering it back up. Some technicians will also call this a *power cycle*. A soft reset can help when certain applications are

not functioning properly or when network connectivity is failing. If a smartphone is still locked up after it is restarted, attempt a hard reset.

iOS-based devices can do a variety of more advanced software resets beyond a simple power cycle, such as Reset and Erase All Content and Settings. These options are available by tapping **Settings > General > Transfer or Reset iPhone**.

A *hard reset* should be initiated only when things have gone terribly wrong—for example, when hardware or software has been compromised or has failed and a soft reset does not fix the problem. You need to make sure that all data is backed up before performing a hard reset because some hard resets will reset the mobile device back to the original factory condition.

Caution

All data will be wiped when a hard reset is initiated!

Hard resets (and forced restarts) vary from one device to the next. They can be initiated from within the OS, or they can be initiated by pressing a special combination of buttons, possibly while restarting the device.

Note

For more information on how to restart an iPhone, visit https://support.apple.com/en-us/HT201559.

For more information on how to restore an iPhone or iPad to factory settings, visit https://support.apple.com/en-us/HT201252.

For more information on how to reset or restart an Android phone, visit https://www.plug.tech/blogs/plug-university/how-do-i-reset-or-restart-my-android-phone.

For more information on how to back up or restore an Android device, visit https://support.google.com/android/answer/2819582.

More Mobile Application and OS Troubleshooting

The operating system and the loaded applications can give mobile device users some heartache—especially given how some people truly *love* their smartphones and tablets.

Updates: The Good and the Bad

We talked about keeping a device updated; in general, this is a good idea, especially for antimalware applications. But sometimes an update is not a good idea. For example, the latest version of a mobile OS might not work well on your device (even if the experts say it will). The older the device, the slower the CPU; and the newer the OS version, the more CPU resources it requires. Ultimately, the new version of an OS will not function as well on an older device. The same goes for the latest versions of apps, though not to such an extent.

If a device is updated and starts to work sluggishly, a downgrade might be necessary. This means going back to the original factory image for the device and usually requires a USB connection to a desktop computer. Some Android devices require you to enter developer mode, which can be done, for example, by tapping the build number (in About) seven times or using some other similar technique. Once you are in developer mode, you can enable USB debugging from Settings. Other devices allow you to select USB debugging when you first plug in the device via USB. You'll need to have a full battery before initiating a downgrade. Check your device documentation for more information or go to the manufacturer's website to find out how to enable USB debugging for a specific device.

Application Issues

Applications can also cause a mobile device OS to perform slowly or freeze the system altogether. If this happens, first restart the device. If that does not work, consider force stopping the application in question, uninstalling unnecessary apps, and possibly resetting the device. If you have previously enabled developer mode, you can access that and see a list of all running services and modify them from there.

Apps might also fail to load or might load very slowly. That could occur when too many apps are open or when the web browser has too many tabs open. It could also be a sign that there is no space left on the device. Close apps, close browser tabs, and remove and/or relocate apps to see if any of those actions fix the problem.

On most Android devices, you can also clear the cache memory for the system and for individual apps. To clear the system cache, reboot the device into recovery mode (usually with a simultaneous button combination, such as power, volume up, and home) and then select **wipe cache partition** or an option with a similar name. Just be very careful not to select the factory reset option! It is often very close in proximity on the menu. The individual app cache (and app data) can be cleared on the same screen where force stops are performed.

Random Reboots

A device might randomly reboot. To troubleshoot this problem, try the following:

- Make sure the OS is up to date.
- Check storage and clear space, if needed.
- Close apps that are not being used.
- Remove the case and external batteries, if they are being used.
- Disable auto-restart.
- Check for bad apps, such as banned games or faulty untrusted apps, and uninstall them.
- Update apps with newer versions; older versions might be unstable.
- Scan the device with an antimalware program.
- Be sure the battery is fully charged.

- If the problem just started occurring, uninstall whatever app you just installed; that app might be the problem, either because it is unstable, incompatible with something else on your device, or for some other reason.
- Check your device for overheating. Remove it from direct sunlight and allow it to cool down before continuing to use. This is especially true on warm days and when using resource-intensive apps such as GPS.
- If all else fails, you might need to contact support, but try these first because eventually YOU will be support.

Poor Battery Life Issues

We discussed battery life in depth in Chapter 26, but it deserves a mention here too. Poor battery life in smartphones may be attributed to the following:

- The battery is old (which often means the battery gets hot quite easily).
- The battery is damaged.
- Powerful applications are siphoning battery power (possibly running in the background).
- The battery is not charging properly. Check the charging cable and port.
- The phone is too hot. Powerful applications, GPS programs, and games could cause this and can make it more difficult for the battery to charge. If the device is in the sun this is also an issue. Be sure to keep your device in the shade, especially when charging and when using GPS and other resource-intensive applications.
- The phone has wireless issues. For example, if it is in a signal dead spot, the phone will constantly attempt to search for a signal, which causes the battery to drain. Additional wireless technologies such as GPS, Bluetooth, and NFC, if running concurrently, can drain the battery. Try running your device in Airplane mode, which shuts off all of the antennas; you can turn on just the services you need (such as Wi-Fi or Bluetooth), which will help conserve battery life.

See Chapter 26 for more information on how to conserve battery power.

In addition, mobile device random reboots are often related to battery issues. To preserve a mobile device's battery life, you can adjust your screen brightness, charge your device strategically, and use battery saver mode.

Start by adjusting your screen brightness:

- Dim your screen or turn on auto-brightness.
- Enable a darker display theme.
- Use battery saver mode.
- Turn on battery saver mode manually or set a schedule.
- Note that battery saver mode slows down your device to save power.

Other tips when running low on power include the following:

- Turn off keyboard vibrations and haptic feedback.
- Set your screen to turn off sooner after you stop using it.
- Use Wi-Fi instead of data.
- Turn off location services.
- Use airplane mode strategically.

ExamAlert

The 220-1202 Exam Objective 3.2 specifically calls out application fails to launch, application fails to close/crashes, application fails to update, application fails to install, slow to respond, OS fails to update, battery life issues, and random reboots. Be sure you know how to troubleshoot these common mobile OS and application issues!

Addressing Video Issues

If we had a dollar for every person who approached us with a video issue, we'd be rich. From dim displays to no display, damage to the screen, missing pixels, and blinking screen, mobile devices can experience a number of video issues. Luckily, mobile device displays are more resilient today than they once were, but there are still some common issues that you should consider.

First is auto-rotate. It's amazing how easy it is to disable this function accidentally; users do it all the time. If a user is working on photos, videos, or apps that require auto-rotate, being without this function can be very frustrating. The good news is that this particular fix is usually easy. For Android users, the solution is usually directly within the quick settings panel that can be swiped down from the top of the screen. In Android, this option is often called Rotation. In iOS, it is called Portrait Orientation Lock.

ExamAlert

Know what to do if a device screen does not auto-rotate.

Earlier in the book, we said you can connect anything to anything else if you have the right adapter. That advice also holds true for mobile devices. However, some adapters are made better than others. For example, it is wise to use an adapter made by Apple for connecting, say, an iPad's USB-C or Lightning port to an HDMI input. For Android devices, seek out quality adapters for connecting from USB-C–equipped Android devices to HDMI or to the USB port of an automobile. For both iOS and Android, make sure there is a solid connection and that you are using the correct adapter. Generally, this adapter just works out of the box, even if screen sharing or screen mirroring is turned off, because it relies on a cabled connection, not a wireless connection. The troubleshooting side of it is usually at the TV, monitor, or projector where the image is to be mirrored. Always remember to check the input option being used; it is usually part of the onscreen display (OSD).

Note

We discuss mobile video hardware and ports in the 220-1201 portion of this book.

On the software side of things, make sure that screen mirroring is enabled. Different Android devices have this setting in different places. One example is to go to **Network > Screen Sharing** (though Screen Sharing could also be in General, Display, or elsewhere, depending on the device). Verify that screen sharing is enabled. On the other end, make sure the device that is being shared to is accepting the connection. A passcode could be required if you are connecting to some kind of casting device (Amazon Fire TV, Google Chromecast, Apple TV, and so on). Don't forget to check the volume on the mobile device as well. iOS devices use the Screen Mirroring option, which connects to Apple TV and any other AirPlay devices, including third-party software offerings that can allow iOS devices to mirror to computer systems. Screen Mirroring can easily be found in the Control Center by swiping down from the top right of the display.

Note

If a physical cable connects an iOS device to an external display, the Screen Mirroring name changes to Dock Connector. If you were to press **Stop mirroring**, you might need to restart the iOS device to enable mirroring again.

Cram Quiz

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

1. An application won't close on an Android smartphone. You've tried to force stop it—to no avail. What should you do?

   ○ **A.** Hard reset the device.

- ○ **B.** Stop the underlying service in Running Services.
- ○ **C.** Soft reset the device.
- ○ **D.** Take the device to an authorized service center.

2. Which of the following are valid Wi-Fi troubleshooting methods? (Select the two best answers.)

- ○ **A.** Power cycle the device.
- ○ **B.** Restart Bluetooth.
- ○ **C.** Use a static IP address.
- ○ **D.** Make sure the device is within range.
- ○ **E.** Rename the SSID of the WAP.

3. A technician has turned the Portrait Orientation Lock off for an iPhone user. Which common mobile OS problem does this rectify?

- ○ **A.** The Camera app fails to launch.
- ○ **B.** The screen does not auto-rotate.
- ○ **C.** The OS fails to update.
- ○ **D.** The battery fails to hold a charge.

4. A user has upgraded to a new mobile device and is preparing to give the old device away. What should the user do before giving it away to ensure that the data is protected?

- ○ **A.** Nothing; the data is already protected.
- ○ **B.** Perform a soft reset of the device.
- ○ **C.** Perform a hard reset of the device.
- ○ **D.** Charge the battery.

5. If an application stops responding, which of the following actions can you do to help get your system operating again?

- ○ **A.** Force stop the application.

- ○ **B.** Wait for the application to start working again.
- ○ **C.** Do a full reset of your mobile device.
- ○ **D.** Charge your device.

6. What can you do to help improve battery life?
   - ○ **A.** Ensure that you always charge your battery to 100 percent.
   - ○ **B.** Keep your mobile device on a charger.
   - ○ **C.** Dim the screen.
   - ○ **D.** Turn on airplane mode.

Cram Quiz Answers

1. **C.** If you've already tried to stop the application within Running Services, attempt a soft reset. Hard resets on Android devices should be used only as a last resort because a hard reset will return a device to factory condition—wiping all the data. The question indicates that the application won't close, not that a service won't stop, though you could try finding an underlying service that might be the culprit. But you should try resetting the device before doing this or taking it to an authorized service center.

2. **A and D.** Valid Wi-Fi troubleshooting methods include power cycling the device and making sure the mobile device is within range of the wireless access point. Bluetooth could possibly cause a conflict with Wi-Fi. If you suspect that Bluetooth is interfering, simply turn off Bluetooth. Static IP addresses are one thing you can check for when troubleshooting. Normally, the mobile device should obtain an IP address dynamically from a DHCP server. Renaming the SSID of the access point could cause problems for all clients trying to connect. However, you should make sure that the correct SSID was typed if the connection was made manually.

3. **B.** If an iPhone's or iPad's screen won't auto-rotate, the reason is probably that the Portrait Orientation Lock setting is on and locking the display in place. Turning it off unlocks the option,

allowing the screen to rotate. In Android, this is simply known as rotation. If the Camera app fails to launch, you might need to restart and/or update the app or restart the phone. If the OS fails to update, you need to troubleshoot the Wi-Fi connection. If the battery fails to hold a charge, it will most likely need to be serviced.

4. **C.** Perform a hard reset, sometimes called a factory reset. This will erase all data on the device and reset it to factory settings. By doing this, all of the user's personal information will be erased from the device, and it will be ready for the next user. A soft reset will not only restart the device but will leave all of the data in place.

5. **A.** A force stop (force quit in iOS) will quit the application, allowing you to get back to your work right away. While you could wait, a truly locked-up app may never come back (or it may take a long, long time). A full reset of your mobile device is overkill. Although your mobile battery may be part of the problem, and you should always monitor the charge, just having a low battery does not cause an app to lock up.

6. **C and D.** Dimming the screen turns down the backlight, which will use less power. Turning on airplane mode turns off all of the radios in a device (you can turn on individual radios, such as Bluetooth or Wi-Fi, as needed), so the device draws less power. Keeping your device plugged in is actually counterproductive because keeping the battery topped up shortens battery life.

Excellent. Two more troubleshooting chapters to go! Review and then continue!

Chapter 55

Troubleshooting Mobile Operating Systems' Security Issues

This chapter covers the following A+ 220-1202 exam objective:

- **3.3** – Given a scenario, troubleshoot common mobile OS and application security issues.

Okay, here's the last chapter on mobile device troubleshooting. This one continues on with mobile devices but concentrates more on security issues related to those devices. This is a short one, so take a seat. Ready? Learn!

ExamAlert

Objective 3.3 concentrates on security concerns; application source/unofficial application stores, developer mode, root access/jailbreaking, unauthorized/malicious application, and common symptoms; high network traffic, degraded response time, data-usage limit notifications, limited Internet connectivity, no Internet connectivity, high number of ads, fake security warnings, unexpected application behavior, and leaked personal files/data.

Mobile Device Security Concerns and Symptoms

Some of the most important security concerns are unauthorized access, loss of *authorized* access, and compromised or lost data. You need to protect against these things. In other words, you need to keep the bad guys out and the employees in—while preserving the data.

You can implement a variety of security measures, but you need to be careful not to *oversecure*. Too many hurdles for users can cause an unacceptable number of system lockouts. In addition, when users start to feel that they are being locked out due to overzealous security measures, they start to bypass the security measures themselves. Remember the old meme about people writing down their passwords on the bottom of their keyboards? That really does happen. Lockouts translate to a loss of productivity for users and increased tech support calls to have accounts and/or devices unlocked. Over time, this costs the organization money and slows down projects.

That's why the "three strikes and you're out" rule is a good middle ground. It allows enough attempts for users to make some typos during the login process, but it provides a lockout for an attacker who tries to guess a user's password. This rule can be set up as a policy within a mobile device management program (MDM) and affect all mobile devices within the group. With a typical standalone mobile device, the lockout might last 15 minutes, and subsequent lockouts can be longer. However, when you're configuring this setting within an MDM, the lockout should be more severe, such as locking the account until an administrator confirms the user's identity and perhaps runs a quick interview. Even that might not be enough, however. Just because an account was locked out today doesn't necessarily mean it wasn't compromised previously. The simple fact that the lockout occurred should be a red flag. Many organizations will then launch an investigation at some level or at least do a basic analysis of the account. Logs should be checked for anomalous activity, resource usage should be reviewed, and the admin should double-check for any unauthorized usage of the device, apps, or data.

ExamAlert

Mobile device management (MDM) and mobile application management (MAM) systems can be used to help enterprises

manage and secure the use of those mobile devices in the workplace and to interact with privileged company information and applications.

Speaking of logs, be sure to view log files to ascertain whether any security issues have occurred within a mobile device's operating system or applications. Some applications have their own logs that you can view. Many MDMs have log files that you *definitely* should review periodically. Finally, you can go deep into an individual mobile device programmatically. For example, with Android, you can use the Android software developer kit (SDK) and use the Android Debug Bridge (ADB) from a PC or another system—with USB debugging enabled on the mobile device. Look for errors and anomalous activity that might indicate a security breach.

ExamAlert

Periodically view log files to ascertain if any security issues have occurred within a mobile device's OS or applications.

Apps can be a real target. Remember we mentioned that every program installed on a computer increases the attack surface? One reason so many mobile devices get hacked is that a lot of apps are available out there, each of which poses a security risk to some extent. When you have the power to do so, limit the number of apps that users have access to. An attacker might attempt to gain information from a company's employee by initiating unauthorized location tracking. This can be done with an app or through a backdoor of the OS or with malware, often a Trojan. If you suspect that this is happening, then disable location services until the problem is resolved.

Attackers might also attempt to take control of the camera/webcam and microphone of a mobile device to spy on a user. One way to tell if this is happening is by listening for shutter noises occurring when the user is not taking pictures. Temporary solutions include disabling (or unplugging) the camera/webcam, or covering the camera/webcam with masking tape, and

force stopping any unknown applications. Another basic preventive action is to have the webcam indicate when it is in use, either with a light, tone, or message. Along those lines, you can also check application permissions. For instance, the Camera app will allow certain programs to make use of the camera. If any programs on that list are not expected, are not desirable, or are potentially malicious, then disable them. For example, in Android, a typical navigation path would be **General > Apps & Notifications > App permissions**. From there, you will see the Camera app. Tap it to find out which applications are using it and disable them as necessary.

As a security person, you need to look for high resource utilization or power drain on a mobile device. These issues can indicate that a Trojan has been installed and has taken control of the webcam or is working in a remote desktop manner. Another indicator is high data usage. When the data transmission for a device goes over the limit set by the cellular provider—or over a wireless transmission quota that your organization has set—it is possible that the mobile device has been compromised and is working as a bot. At the very least, this will cause the user to lose productivity.

If you suspect that unauthorized usage is occurring on a mobile device, that device should be taken offline, isolated, scanned, and otherwise analyzed. In many cases, the device will have to be wiped (as per company policy) and re-imaged. If the device is used in a BYOD environment, re-imaging the company partition might be enough, but with some organizations, the device might be banned until the personal side is also re-imaged.

There are some additional concerns for Android and iOS specifically. The first is root access and jailbreaking. We discussed these issues in Chapter 49, "Mobile Device Security," but we have a few more thoughts on the subject. In a nutshell, Android rooting and iOS jailbreaking can be prevented through protection and detection. For example, an organization should use mobile devices that are "business-oriented"—that is, devices that use hardware protection that makes booting in a rooted fashion difficult. This hardware/firmware protection will analyze the OS as it boots and make sure it hasn't been tampered with. This makes it nearly impossible to boot to any untrusted code. A sysadmin should use MDM software to scan for rooted devices. Many business-oriented mobile devices

come with some type of attestation, which means they can reply to an MDM to reveal their true status and whether or not they are rooted. There are also third-party apps that can block rooting and/or jailbreaking.

Note

The trustworthiness of a platform is based on *attestation*. The purpose of attestation is to give you confidence in the identity and trustworthiness of a target device before you interact with the device.

Users should also be careful about where they get software. When Android users obtain apps from Google Play and iOS users obtain apps from the Apple Store, these apps are usually scanned and are typically safe to use (while it's not 100 percent true, it is mostly true). However, Android users can also download application packages from other sources. The problem is that these other sources may or may not check the level of secure coding for an app. These Android packages (APKs) should be downloaded from trusted sources (such as APKMirror). An APK installer can be used instead. Regardless of source, be sure to check the app thoroughly to avoid installing malicious code.

ExamAlert

Remember that gaining administrative Apple iOS privileges is called *jailbreaking* and doing the same on Android-based devices is called *rooting*. Know how to prevent jailbreaking and rooting. By avoiding jailbreaking and rooting, you can ensure that user device security features are working as intended, protecting them from potential threats.

You must take the precautions described here when dealing with Android and iOS apps so that you can avoid rooting and jailbreaking and also to avoid malicious applications (and bootleg apps), as well as application spoofing. An app might look quite normal and legitimate, but if it is

downloaded from an untrusted source, it could actually be something else entirely.

Malicious apps can cause a variety of symptoms, some of which can have the same symptoms as malware—because, essentially, a malicious app *is* malware. Here are some symptoms that you might see:

- **Communications issues:** A device might have no or limited Internet connectivity, experience high network traffic volume, and get data-usage limit notifications.
- **Worrying messages:** A user might see a large number of advertisements and fake security warnings, which are often found when browsing to less-than-reputable websites but which might also pop up when browsing legitimate websites.
- **Performance issues:** A user may experience sluggish response time of the OS in general or of specific apps, as well as unexpected application behavior.
- **Leaked personal files/data:** If this happens, the mobile device should be quarantined and isolated right away because this is a symptom of a larger and potentially devastating problem.

To summarize, you should try to *prevent* the problems mentioned in this chapter from happening. Remember the old saying: "An ounce of prevention is worth a pound of cure." When it comes to mobile devices, prevention means updating and implementing antimalware and firewalls, requiring strong passwords, disallowing public and open Wi-Fi hot spot connections, obtaining software from trusted sources, using data loss prevention (DLP) to prevent leaked data, and, in general, locking down devices at the MDM workstation. These are some of the preventive measures you can take to protect the integrity of the data and keep it confidential while maintaining the productivity of authorized users.

Note

Data loss prevention (DLP) is a system designed to detect and respond to potential breaches. Deploying a DLP solution is meant to

prevent sensitive information from being sent outside of the organization.

Cram Quiz

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

1. A user downloaded an APK from an untrusted source and installed it. Now the mobile device is suffering from slow performance. The user also shows proof that the device is leaking data. What happened to the device?

   - ○ **A.** Jailbreaking
   - ○ **B.** Application spoofing
   - ○ **C.** Developer mode
   - ○ **D.** Rooting

2. Which of the following could result from downloading something from an untrusted source? (Select all that apply.)

   - ○ **A.** Attestation
   - ○ **B.** Malicious apps
   - ○ **C.** Dead battery
   - ○ **D.** App spoofing

3. You suspect that a mobile device has been compromised and is now part of a botnet. What are some of the indicators that this has happened? (Select the two best answers.)

   - ○ **A.** High resource usage
   - ○ **B.** Notification of camera/webcam usage

- ○ **C.** Apps force stopped
- ○ **D.** Power drain
- ○ **E.** Log files unavailable
- ○ **F.** Locked user account

4. You get a notice from your Internet service provider (ISP) that your device is using a lot more data than usual. What could be the cause?
   - ○ **A.** You have been uploading more video than usual.
   - ○ **B.** Your device is usually on Wi-Fi and is instead on cellular broadband.
   - ○ **C.** A malicious app has been using bandwidth in the background.
   - ○ **D.** You have been traveling and using more bandwidth than usual.
5. Ads appear where you do not expect them. What could be a cause?
   - ○ **A.** A malicious app may be feeding ads to your device.
   - ○ **B.** You might have clicked on a website that is feeding ads to your device.
   - ○ **C.** You have an ad behind you that is mirroring off your screen.
   - ○ **D.** You downloaded a free app that uses ads to pay for the development.

Cram Quiz Answers

1. **D.** Of the listed answers, the device has most likely been rooted, and someone else (or the application) has control of the system. The device should be taken offline, quarantined, and isolated immediately. The real issue is that the user downloaded a malicious application from an untrusted source. This application

then took control of the system. A jailbreak occurs on iOS-based devices. We know that this is an Android-based device because the application downloaded was an Android package (APK). The user might have been fooled into thinking that the application was legitimate, but this isn't something that happened to the device per se. Developer mode is used to take control of certain aspects of a mobile device, such as to enable USB debugging mode. While developer mode can be used maliciously, it is more likely that the primary issue here is that the phone was rooted. Similar issues with iOS devices could occur if the device were jailbroken.

2. **B and D.** Always download from trusted sources to avoid rooting and jailbreaking and also to avoid malicious/bootleg applications, as well as application spoofing. An app might look legitimate, but if it is downloaded from an untrusted source, it could actually be something devious. Many business-oriented mobile devices come with some type of attestation, which means they can reply to an MDM to reveal their true status and whether or not they are rooted.

3. **A and D.** If a mobile device has been compromised and added to a botnet, the user might know it but might experience high resource usage, power drain on the battery, and, less commonly, high data usage. You should check all of these things as well as any available logs. (If the logs are not available, then that could also indicate foul play.) Take the device off the network, isolate it, and run a scan of the device; you are on the hunt for Trojans especially. A notification of camera/webcam usage either means that the device is being used properly by the user or an attacker is attempting to spy on the user, but it doesn't mean that the mobile device has joined a botnet; it is possible but unrelated. If apps were force stopped, they might have been stopped by the user, or by a rogue app, or by an attacker who has taken control of the mobile device, but this is also a separate problem. If the user account was locked out, it could simply be that the user forgot the password and had too many failed attempts. Or, it could be that a hacker was attempting to guess the password, either directly or through covert means. Again, that's a separate problem. In all of these cases, the image should be preserved for later analysis, and the device should

most likely be re-imaged to be sure that any bad apps, malware, and so on have been removed.

4. **A, B, and D.** Video takes a lot of bandwidth. If you suddenly are uploading a lot more video than usual, that would increase your bandwidth usage. If you usually connect your mobile device to the Wi-Fi network and it drops that connection, it will fall back onto the cellular network; that will use your cellular data plan. Sometimes, though, the cause is innocent. If you are traveling, you will often use more data than usual, and you might receive a notice of unusual use. Sometimes these notices are innocent. Pay attention to behavior when troubleshooting.

5. **A, B, and D.** You might have downloaded a malicious app. This is especially true if you have jailbroken or rooted your device and installed from an untrusted software source. Those apps may deliver ads to your device. Some websites will deliver ads to your device in the background, even when you are not on the web browser screen. And many "free" apps use advertising to pay the bills. You should actually expect the ads on these apps, but some people forget that the ads are part of the cost of a free app.

That does it for the mobile troubleshooting section of this book. Well done. Review your notes for this chapter and head on to the PC troubleshooting chapter!

Chapter 56

Troubleshooting PC Security Issues

This chapter covers the following A+ 220-1202 exam objectives:

- **3.4** – Given a scenario, troubleshoot common personal computer (PC) security issues.

In Chapter 46, "Wireless Security and Malware," we discussed the types of malicious software you should know for the exam. Now that we've covered a lot more security information, as well as some Windows troubleshooting methods, let's get into how to resolve some common PC security issues.

As we discuss antivirus and malware, keep in mind that some organizations don't want to troubleshoot malware *at all*. They simply wipe a problematic system, re-image it, and restore the data afterward (you are making regular backups, aren't you?). If you do need to remove malware, refer to the steps in the "Removing SOHO Malware" section in Chapter 51.

Be ready to troubleshoot with an open mind (as always) and look for alternative causes for the problems you face.

ExamAlert

Objective 3.4 focuses on common PC security issues and browser-related symptoms of malware.

Symptoms of Viruses

If a computer is infected by a virus, you want to know what to look for so that you can “cure” the computer. Here are some typical symptoms of viruses:

- Internet access or network access is blocked or is redirected.
- You receive unusual error messages or security alerts, which are most likely false (for example, false alerts regarding antivirus protection).
- System files or personal files are altered. Perhaps they are missing or have been renamed. Maybe they have been corrupted, and perhaps folders are created automatically.
- Unwanted notifications occur within the operating system or when browsing the Internet.
- Windows Update fails.
- The computer runs more slowly than usual.
- The computer/PC operating system locks up frequently or stops responding altogether.
- The computer restarts on its own or crashes frequently.
- Storage drives and applications are not accessible or don’t work properly.
- Applications crash more frequently (without another obvious cause, such as a recent update). This could also be a sign of a Trojan that has exhausted the resources needed to run the application.
- Permission to specific files and folders is denied, and “access denied” errors appear.
- Strange sounds occur. Although unusual, this does happen occasionally.
- Display or print distortion occurs.
- New icons appear or old icons (and applications) disappear. Sometimes the icons change in subtle ways.

- There is a “double extension” on a file attached to an email that was opened (for example, .txt.vbs or .txt.exe). These are designed to trick a user into thinking the file attachment is a text file, when in reality it is a potentially dangerous script or executable file.
- Antivirus programs do not run, can’t be installed, or can’t be updated.

Symptoms of Spyware

Spyware is designed to spy on the user and attempt to gain confidential information. Be on the lookout for it. Here are some common symptoms of spyware:

- The web browser’s default home page has been modified. This is a type of browser redirection, and it is a very common browser-related symptom. If this happens, the system might have been hijacked.
- A particular website comes up every time you perform a search.
- Your search engine has been changed without your deliberately changing it.
- Excessive pop-up windows appear. Rogue antivirus applications and security alerts seem to appear out of nowhere, supposedly scanning the system.
- The network adapter’s activity LED blinks frequently when the computer shouldn’t be transmitting data.
- The firewall and antivirus programs turn off automatically.
- New programs, icons, and favorites appear.
- Odd problems occur in Windows. For example, the system might be slow, applications might behave strangely, and so on.

More Symptoms of PC Security Issues and Potential Solutions

There are some more symptoms that we have not covered yet. Table 56.1 lists those symptoms and some potential solutions.

TABLE 56.1 **PC Security Symptoms and Solutions**

Symptom	Potential Solutions
Unable to access the network	▶ Check for common symptoms (Wi-Fi access point in range, connection errors, etc.) discussed in Chapter 27, "Troubleshooting Wired and Wireless Network Problems." ▶ If still unable to connect to the network, follow the steps in the section, "Preventing Malicious Software" in Chapter 46 to help eliminate malware. ▶ Shutting off your Wi-Fi or wired access card on your device and then running an antimalware scan can sometimes help find the issue as well.
Desktop alerts/Unwanted notifications within the OS	▶ If you are getting random desktop alerts and/or pop-ups, run an antimalware scan, as discussed in Chapter 27. Check the notification settings in **Settings > Notifications > Set priority notifications** and **Settings > Notifications** to see what apps can send you notifications. See https://support.microsoft.com/en-us/windows/notifications-and-do-not-disturb-in-windows-feeca47f-0baf-5680-16f0-8801db1a8466 for more information about notifications and alerts.

Symptom	Potential Solutions
False alerts regarding antivirus protection	▶ False alerts can be annoying. If the solutions in the desktop alerts don't work, and you are getting the alerts in your browser, check out the solutions suggested in the article at https://support.microsoft.com/en-us/microsoft-edge/manage-website-notifications-in-microsoft-edge-0c555609-5bf2-479d-a59d-fb30a0b80b2b. Among these solutions is resetting your website notifications, since many of the malicious websites have hidden notification screens that might have tricked users into accidentally allowing the pop-ups.

Symptom	Potential Solutions
Altered system or personal files	▶ The best solution is to restore from a personal backup of your files. ▶ If that isn't possible, and you have sanitized your system according to the instructions in the section "Detecting, Removing, and Preventing Malware Using the Appropriate Tools and Methods" in Chapter 46 (because you don't want the problem to come back), you can sometimes fix corrupted files. ▶ Scan and repair your system disk. To do this, open an elevated Command Prompt (see Chapter 35, "Microsoft Command-Line Tools, Part II," if you don't remember how to do this) and run the command **chkdsk /f [*drive letter*]**. This will scan and repair any problems with the drive. ▶ After you have fixed the physical drive, you need to fix the files. For this, run the System File Checker (SFC). From your elevated Command Prompt, type **sfc /scannow**, which will scan all of your system files and repair them if necessary. Note that you may need to run this in Safe Mode if it can't fix all of the errors. ▶ If your drive is really messed up, you might need to run Deployment Image Servicing and Management (DISM). From that elevated Command Prompt, type **Dism /Online /Cleanup-Image /CheckHealth** to check the health of the drive and files. Then type **Dism /Online /Cleanup-Image /ScanHealth** to see if there are additional errors it can repair. Finally, run **Dism /Online /Cleanup-Image /RestoreHealth** to restore your drive to health again. ▶ Note that you might need to run **sfc /scannow** again after running DISM to correct additional issues.

Symptom	Potential Solutions
Missing or renamed files/Unable to access files	▶ The instructions on altered files should fix any missing or renamed files. ▶ If not, and if the instructions in Chapter 27 do not fix the issue, look for hidden files. To do this, go to **Settings > System > For developers**, select **File Explorer** to activate the drop-down, and toggle on **Show hidden and system files** and **Show file extensions**. ▶ Toggle **Show full path in title bar** to see the actual path to your files, to ensure that you aren't just being redirected to the wrong location. ▶ You might want to click **Show empty drives** because you might have a hidden partition where all your files reside. ▶ Finally, check your Recycle Bin. Some malware puts files into the Recycle Bin but doesn't empty it, so you may find a welcome surprise when you open it. Select all the files, right-click, and select **Restore** to move the files back to their correct location.
OS update failures	▶ The OS can fail to update for several reasons: You might be low on disk space (this issue is less common with modern large hard disk drives, but it happens). Free up space on your drive. You need at least twice the space of the update itself. An easy way to free up space is to empty your Recycle Bin, the Downloads folder, and your Pictures > Screenshots folder. ▶ **Corrupted files:** If your drive has corruption, your updates will not run properly. See the section on altered system or personal files earlier for instructions on how to repair corrupt drives.

Symptom	Potential Solutions
	▶ **Internet connectivity issues:** If your Internet access is not stable, you will have issues downloading updates. Fix the issues with your Internet connection, and that will fix the issues with your updates. ▶ **Incompatible drivers or other software:** If your software is too out of date, it may cause issues when you go to update. That sounds counterintuitive, since you should be updating to the latest version. If this happens, uninstall the driver or software and reinstall the newer version manually. ▶ **Power issues:** If you have a power outage or other interruption, that could corrupt the update, which will then not work. Like the Internet connectivity issue, fix the power issue and your update issue should be fixed as well. ▶ **Hardware issues:** If you have a physical component going bad, your update may not function. Replace or repair the damaged component. ▶ **Software glitches:** Sometimes things just happen. Try the update again. If the update continues to fail, look up the particular error code; that should provide you with a method to troubleshoot. ▶ If your automatic updates don’t work, search for updates manually.

Symptom	Potential Solutions
Browser has random/frequent pop-ups	▶ False alerts can be annoying. If the solutions in the desktop alerts don't work, and you are getting the alerts in your browser, check out the solutions suggested in the article at https://support.microsoft.com/en-us/microsoft-edge/manage-website-notifications-in-microsoft-edge-0c555609-5bf2-479d-a59d-fb30a0b80b2b. Among these solutions is resetting your website notifications, since many of the malicious websites have hidden notification screens that might have tricked users into accidentally allowing the pop-ups. ▶ If you continue having random pop-ups, you might need to adjust your browser's pop-up blocker settings. For Google Chrome, see https://support.google.com/chrome/answer/95472. For Microsoft Edge, see https://support.microsoft.com/en-us/microsoft-edge/block-pop-ups-in-microsoft-edge-1d8ba4f8-f385-9a0b-e944-aa47339b6bb5.
Browser certificate warnings	▶ Analyze and verify installed certificates in the trusted root of the **Certificate Manager (Run > certmgr.msc) > Trusted Root Certification Authorities**. (If you don't recognize an authority, a quick online search will tell you who it is and if it is legitimate.) ▶ Analyze the Security log file in the Event Viewer for information on individual events concerning invalid certificates. ▶ Delete, export, revoke, and otherwise modify the certificates that are invalid and import new trusted certificates from a trusted certificate authority.

Symptom	Potential Solutions
Browser redirection	If there is no malicious activity: ▶ Import new certificates for all parties concerned. For example, in Outlook, go to **File > Options > Trust Center > Trust Center Settings > Email Security**. Then import a new digital ID (certificate). (Be sure to select the **Add digital signature to outgoing messages** checkbox.) ▶ Publish the certificate appropriately if the certificate server being used is not properly integrated with other platforms on the network (for example, Microsoft Exchange Server). If there is potential malicious activity: ▶ Analyze the Event Viewer System, Application, and Security logs. ▶ If needed, revoke the current certificate, create a new one, and import it to all parties concerned. ▶ Scan the system and change account passwords.
Degraded browser performance	There are lots of causes of slow browser performance: ▶ Close unnecessary tabs (especially tabs playing media). ▶ Close any background processes that are using CPU and memory. ▶ Update your browser on a regular basis. Recent updates have substantially improved performance. ▶ Remove any unnecessary browser extensions. ▶ Periodically empty the browser cache and delete the cookies.

ExamAlert

Know the common symptoms of malware and how to troubleshoot and resolve them.

Cram Quiz

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

1. A technician coworker is using certmgr.msc to analyze a problem with a computer. Which of the following issues is the technician most likely troubleshooting?

   - ○ **A.** Trusted root CA
   - ○ **B.** Hijacked email
   - ○ **C.** Spyware
   - ○ **D.** Browser redirection

2. Why might a user be unable to access a network from a Windows computer?

   - ○ **A.** The computer's Wi-Fi access point is out of range.
   - ○ **B.** The network cable is securely connected.
   - ○ **C.** The computer is infected with malware.
   - ○ **D.** The user does not have the correct access point configured.

3. Why might a Windows update fail to install?

   - ○ **A.** The computer's firewall is turned off.
   - ○ **B.** The update was installed successfully but needs a restart.
   - ○ **C.** There is insufficient free space on the hard drive.

- ○ **D.** The computer is connected to a VPN.

4. Why might a user be experiencing excessive browser pop-ups?
   - ○ **A.** The browser's pop-up blocker is turned off.
   - ○ **B.** The browser is in Incognito mode.
   - ○ **C.** The website is listed in the browser's trusted sites.
   - ○ **D.** The computer is infected with malware or adware.
5. Which of these is a common cause of unexpected redirection to malicious websites?
   - ○ **A.** The browser is configured to allow third-party cookies.
   - ○ **B.** The user has bookmarked the website incorrectly.
   - ○ **C.** The computer is infected with malware or a malicious browser extension.
   - ○ **D.** The browser's JavaScript is disabled.

Cram Quiz Answers

1. **A.** The technician is most likely investigating a certificate issue, which is why the tech is using the Certificate Manager (certmgr.msc). The Trusted Root CA (Certificate Authority) section in the Certificate Manager contains all the certificates that were issued to the computer by third-party companies, as well as certificates that were created on the computer itself. When double-clicked, each certificate will display the issuer and the validation dates. Make sure certificates are still valid! Delete any that are not valid and notify the appropriate companies or personnel.
2. **A, D, and possibly C.** The computer's Wi-Fi access point is out of range, and the user does not have the correct access point configured. The access point needs to be in range, and the device must have the correct credentials to access the network. Malware can sometimes interfere as well.

3. **C.** You need enough space available on your system drive to install the update successfully; otherwise, it will fail. Free up more space and try your update again.

4. **D and A.** The browser is likely infected with malware. In that case, use the instructions in the section "Detecting, Removing, and Preventing Malware Using the Appropriate Tools and Methods" in Chapter 46 to help clean the system. However, the browser's pop-up blocker might have been turned off. Sometimes this is by accident, sometimes on purpose. Watch for this possibility.

5. **C.** Malicious browser extensions, either as part of other malware or by themselves, often will redirect your browsing to unexpected websites. Sometimes these sites appear innocuous: a change to your search engine, for instance. Sometimes they are pages full of ads. Still other times the pages are malicious and attempt to steal data. They are always problematic.

Now you're really cooking! Great work! Review, take a short break, and then continue.

Core 2 (220-1202)

Domain 4.0: Operational Procedures

CHAPTER 57 Documentation

CHAPTER 58 Change Management and Backup Methods

CHAPTER 59 Safety Procedures

CHAPTER 60 Environmental Controls

CHAPTER 61 Incident Response, Communication, and Professionalism

CHAPTER 62 Basic Scripting, Part I

CHAPTER 63 Basic Scripting, Part II

CHAPTER 64 Remote Access Technologies

CHAPTER 65 Appropriate Use of Artificial Intelligence

CHAPTER 66 Getting Ready for the Exams, and Farewell

A+ Core 2 (220-1202) Practice Exam

Chapter 57

Documentation

This chapter covers the following A+ 220-1202 exam objective:

- **4.1** – Given a scenario, implement best practices associated with documentation and support systems information management.

Welcome to the first chapter of Domain 4.0: Operational Procedures. This domain is tied with Domain 3.0: Software Troubleshooting for the smallest percentage of the exam, but it's still packed with key information. So, as with all of the other domains, it is important that you understand the content.

We're shifting gears to the organizational, operational, and facilities side of things, so prepare for a bit of a different mindset. Because the goal is to prepare you for the A+ exam, we won't be going very deep into operational procedures, but you need to know the basics.

Proper documentation is a key element of any organization. Without it, you have chaos. With it, you can at least bring some semblance of order to your networks, policies, and decisions. For you as a technician, the most important reason to have solid documentation is that it helps you troubleshoot problems. If each person on the team documents properly, that makes troubleshooting much easier for anyone else who encounters the same or similar problems. This leads to increased productivity for the entire team. And one other thing: *Remember to leave documentation better than you found it*. If something is not accurate, make it so. Others will thank you, and you never know, you might thank yourself one day. (We all know that we technicians talk to ourselves sometimes!)

ExamAlert

Objective 4.1 concentrates on ticketing systems, asset management, types of documents, and knowledge base/articles.

Types of Documents

In the IT field, you will work with all kinds of documents. In fact, in some organizations, the volume of documents is staggering. Here's one tip we need to give you right off the bat: Make use of your human resources department. Unless you are a compliance officer, chances are that you will not understand some of the documentation that your organization uses. Work with your HR department to navigate the sea of paper and e-paper that should be created, modified, and signed off on. Let them guide you to the personnel you will have to deal with on a day-to-day basis.

Note

Keep detailed notes. That's right: You need a document database to help you traverse the plethora of organizational documentation. It could be a simple paper notebook or an application such as OneNote, Evernote, or open-source services such as Joplin.

Let's discuss some of the documents you will most commonly see and work with in the field, including incident report documentation, standard operating procedures, regulatory compliance requirements, and user checklists.

Incident Report Documentation

An *incident report* is a document that you maintain during the incident response process. It should be initiated at the onset of an event and continued through to the event's conclusion. If you know or even suspect that an incident is occurring, start recording all facts and information that

you encounter. Use some type of logbook (hard copy or digital, though we prefer hard copy for the initial logging of this type of procedure), plus a mobile device with a webcam, another digital camera, an audio recorder, or a combination of these to record all the data you can.

Incident documentation is just a piece of incident response. We'll discuss that process in more depth in Chapter 61, "Incident Response, Communication, and Professionalism."

Standard Operating Procedures

A *standard operating procedure (SOP)* is a document that shows, step by step, how to perform a routine operation, such as an installation of software, an upgrade, or an operating system installation. Generally, in an effort to be software-independent, an SOP should focus on the process at hand rather than on the tools to be used. The document should be written plainly so that just about anyone can understand it. Acronyms and technical jargon should be avoided.

For example, you, as a technician, may be called on to do custom software installations several times per week. The process can only be automated so much because the software installation process is customized for each system where the software is installed. Here's a basic SOP example for the installation of an application called *custom package #23*:

1. Log in to the target computer as a user with administrator privileges.
2. Verify that the target computer's operating system is up to date.
3. Download custom package #23 from the trusted intranet source.
4. Verify that the package has not been tampered with.
5. Begin the installation process.
    a. Answer the scripted questions based on the group that the particular computer is a member of. For example, computers with hostnames that start with *eng* are part of the engineering group. Note: Only users within that same group or organizational unit should be able to use this package.

b. Once the files begin copying, start filling out Form #568 Rev B. Submit this to your manager when complete. Take note of any messages that appear on the screen and enter them into Form #568.

6. When the installation has completed, restart the computer.
7. Test package #23. Make sure it can connect to the main database.
8. Check for any errors or warning messages in the system's log.
9. Log off the target computer.

This is just a brief example, but you get the idea. An SOP is not technical, but it requires technical know-how and some specific technology—such as using PGP or SHA to "verify that the package has not been tampered with." The procedure outlined in this SOP might seem simple, but when technicians are running many tasks at the same time, little things can be missed. That's one of the concepts of the SOP—to guide a tech step by step so that those "little things" are carried out properly. Remember that one little mistake can botch an installation, especially a custom installation of software.

Besides written SOPs, some software programs also can help you devise SOPs and store them in an organized fashion. Having access to these tools makes it easier when dealing with software installation policies that might include the purpose, scope of work, records, privacy information, and specific policies for software to be installed, for example. These policies might focus on more generic things that a tech needs to consider, such as installation options, upgrade considerations, data conversions, automated installations, terminal applications, and what to do if the software won't install properly.

Custom Installation Procedure for Software

As a technician, you will be asked to install software on your firm's devices. Although you could just use the default installation each time, by building a custom install, you ensure that your systems remain secure, that you know exactly what will be installed, and that any customization is done properly at the time of installation.

Your documentation for the installation should include what software is to be installed, including version number, whether it is 32-bit or 64-bit, and any licensing information; the users who are authorized to install the software or have it installed; the devices upon which the software may be installed; and whether the users may install the software themselves or whether they must wait for a technician to install it for them, either in person or remotely. The documentation should also include conditions under which the software should be updated, upgraded, or removed.

Note

It is not uncommon for organizations to have a "standard" software load that the bulk of users (or the bulk of a particular department's users) get installed on their devices. Your custom software documentation could include that entire set of software installation for a team or department.

User Checklists (Onboarding and Offboarding)

Most organizations have checklists for the setup of new users and for what to do when users are terminated. For example, new users need a user account in the domain, need some type of system or device to work on, need access to certain areas of the building, and so on. Users who are terminated need to have their computer accounts disabled (not deleted) and their security clearances revoked. These checklists might be incorporated within onboarding and offboarding processes.

Onboarding is the process of adding an employee to an organization and to its identity and access management system. This process includes training, formal meetings, lectures, and human resources employee handbooks and videos. It also applies when a person changes roles in an organization, ensuring that the person has the access and equipment they need to perform their work successfully. Onboarding is also a socialization technique used to ultimately provide better job performance and higher job satisfaction.

Offboarding is the process of removing an employee from an organization's systems, restricting rights and permissions, and possibly debriefing the person or conducting an exit interview. This happens when a person changes roles within an organization or departs the organization altogether. It is possible, therefore, for onboarding and offboarding to be happening simultaneously for the same person as they are changing roles within an organization.

Service-Level Agreements

At its heart, a service-level agreement (SLA) defines the relationship between a service provider and a company. An SLA includes the quality, availability, and performance standards that the service provider commits to, providing a clear understanding of expectations and promoting accountability to both sides and providing a framework for managing the service delivery.

Key components of an SLA include

- **Service description:** The service being provided is clearly defined.
- **Performance metrics:** These are measurable criteria for evaluating service performance. They usually include uptime, response time from the time an incident begins, and resolution time.
- **Responsibilities:** The SLA outlines the duties and obligations of both the service provider and the customer. It is important that both sides are represented here.
- **Remedies and penalties:** These are the actions and/or consequences if the service provider fails to meet the agreed-upon standards. They could include monetary penalties for poor performance as well as bonuses for meeting deadlines ahead of time.
- **Monitoring and reporting:** The SLA specifies how the service performance will be monitored and reported, and it includes who is responsible for reporting any issues.

There are three typical types of SLAs:

- **Customer-based SLAs:** In this type, a service provider and a single customer contract for services. These SLAs can also exist between multiple divisions of a company and multiple divisions of another company.
- **Service-based SLAs:** In this type, the SLAs are identical between a service provider and each of its customers. Cellular service providers are a good example of this; the SLA does not vary between their many clients.
- **Multilevel SLAs:** These SLAs allow one company to have different categories of customers but only one SLA document that incorporates all the different types of customers into that single document.

SLAs can also exist internally to a company, where different internal groups will make agreements outlining their service levels, responsibilities, and expectations to one another. Internal SLAs between sales and marketing teams might specify the number of leads that marketing provides to the sales team each month, for instance, in order for sales to meet their targets.

The goal of all SLAs is to improve communication and collaboration, enhance accountability, streamline processes, improve customer experience, reduce ambiguity and misunderstandings, facilitate performance measurement, and overall produce a better end product.

ExamAlert

Be sure you are familiar with the types of documents listed in Objective 4.1, including incident reports, standard operating procedures (SOPs), software package custom installation procedures, new user/onboarding setup checklists, user off-boarding checklists, and service-level agreements (SLAs).

Knowledge Base/Articles

We've been referencing knowledge base articles throughout the book, especially Microsoft-related articles. But a knowledge base (KB) is more

than articles written by a company; the information is also spread among community support, forums, and blogs. It's important to know *where* and *how* to find the information you seek.

The "where" we can answer with this: Go to the source! We say it often: Use the websites created by manufacturers of hardware and developers of software. For example, if you are supporting Windows clients, use the Microsoft support sites. If you are using Western Digital storage drives, use the Western Digital support site. Remember this when using an Internet search engine. Often, you will get third-party results, which may or may not contain accurate data. Always start by going to the source. Doing so can help prevent information overload.

The "how" might differ depending on which vendor's site you visit, but for the most part, vendors' sites are usually internally searchable by phrase or by KB number. Once you get the knack for searching, you can learn how to do almost everything with a product by using the support website—from installation and configuration to security and troubleshooting. Let's look at a couple of examples now, starting with Microsoft because it is so prevalent on the A+ exams.

The Microsoft Knowledge Base is spread across multiple websites and has hundreds of thousands of articles and posts from Microsoft employees and from the Microsoft "community." To search the Microsoft Knowledge Base, simply go to one of the following sites and type in the search term or KB article number that you wish to learn more about:

- **Microsoft Support (https://support.microsoft.com):** This is the main support site that Microsoft offers for end users and for IT professionals. Over the years, a lot of content from other Microsoft sites has been redirected here. Also, Microsoft has moved away from the term *Knowledge Base* to a certain degree and often uses terms such as *help* or *support* instead. For example, the page at https://support.microsoft.com/en-us/help/322756 demonstrates how to back up and restore the registry in Windows. (It actually redirects to a more name-based web page.) In the past, this article would have been called KB #322756, and it is still searchable that way, but Microsoft has moved toward using more easily searchable URLs, as you will see if

you follow the previous link. (Once you access the link, it will be appended with the post name, which makes it more search engine–friendly.) Microsoft has merged its technical documentation into this site as well.

- **Microsoft Learn:** What used to be the Microsoft Technical Documentation site (https://docs.microsoft.com) now redirects to Microsoft Learn, where you can access self-paced training modules for many Microsoft products. You can also explore technical documentation, but the main focus of the site now is to give access to courseware. Some knowledge base documentation and technical forums may still redirect here.

Here are a few other examples:

- **Apple (https://support.apple.com):** Here, you can find support articles and community support for Apple products, including macOS-based systems and iOS-based mobile devices.
- **Android (https://support.google.com/android/):** Here, you can learn about the Android OS and also get redirected to the major manufacturers that use it on their mobile devices.
- **Intel (https://www.intel.com/content/www/us/en/support.html):** This KB contains articles, posts, and discussions about all of Intel's products. Intel has a separate developer KB as well.
- **Western Digital (https://www.westerndigital.com/support):** This site supplies written articles for the various storage drives and other products that WD manufactures, along with community support. Some WD drives will be supported by Sandisk, including the WD_Black line and Sandisk SSD drives; see https://shop.sandisk.com/support for that support.

> **Note**
>
> Western Digital has separated into two independent companies, so the support process for your Western Digital and Sandisk brand HDD and flash products may have changed. As of Spring

2025, the two sites are redirecting to one another, but if you can't find support for your product at one, check the other site.

- **Ubuntu Community Support: (https://ubuntu.com/support/community-support):** This site offers support for Ubuntu Linux. One of the fabulous things about Linux is the quality of the support communities for distros such as Ubuntu and Arch—and these are just a couple of examples!

For security purposes, we suggest keeping an eye on knowledge bases that describe common vulnerabilities and exposures (CVEs). CVEs are lists of publicly available security flaws that you should be familiar with. For example:

- **Common Vulnerabilities and Exposures registry:** https://www.cve.org/
- **NIST National Vulnerability Database:** https://nvd.nist.gov/vuln

Try accessing some of these links and spend some time searching around the knowledge bases to get a feel for how they work. Think about some of the products and software you use at home or at work and locate support sites and knowledge bases for those products and software. You will find that some companies have better support and KBs than others. Some have superior technical documentation specialists and more efficiently structured community platforms. Over time, this kind of high-quality product documentation often leads to a higher level of customer satisfaction as well as trusted name recognition. This is the model to follow if your organization currently makes or decides to create its own knowledge base.

ExamAlert

Know how to research knowledge bases! If you can research within them, you can research pretty much anywhere.

Ticketing Systems

A *ticketing system* is software that manages issues from end users and customers. An organization might also refer to it as an *issue tracking system*, *trouble ticket system*, *incident ticket system*, or *support ticket system*. Examples of ticketing systems include Zendesk, Freshdesk, and ITSM. Or an organization might design its own or customize an existing open-source solution.

Ticketing systems are commonly used in an organization's call center for support purposes. Often, they are used to support hardware or software issues that arise. Issues are classified with different priority, or urgency, levels. A person working at a help desk is in charge of opening a ticket (unless it was opened by the system and customer already) and then works to fix the issue or escalates the issue to another person or department.

The Help Desk

Typically, ticketing systems are used by help desk support personnel and other types of IT technicians. We haven't talked much about the *help desk* in this book. A typical help desk station has a multiple-monitor setup plus a separate laptop and a (possibly stressed-out) person wearing a headset who is quickly working to solve problems for customers and end users. Multiply that by a couple of dozen—or more or less, depending on the size of the organization. Employees use softphone applications so that they never have to take their hands off the keyboard. In many organizations, help desk personnel are expected to meet a quota and help out a specified number of customers per hour or resolve a certain number of tickets per hour. A help desk position can be an awesome experience (at the right organization), and—if you prove yourself—it can be a stepping stone to other IT positions.

Although ticketing systems can be used in various ways, we'll focus on the help desk as an example. An employee working at a help desk who opens a ticket might communicate with the customer by way of chat, email, or phone. The employee is responsible for collecting details about the user and information about the device or software that the end user or customer is using. All of this information is entered into the ticket. Most importantly, the employee must obtain a detailed description of the problem. (The solution is usually in the details!)

The help desk employee is also responsible for categorizing the issue and determining the severity of the issue. For example, a customer might state that a device won't charge. This would be a power-related issue, and the severity/urgency will probably be somewhat low. Or perhaps a coworker's email client was affected by malware and is now spamming the entire company. That would be an in-house software/security issue, and the severity would be high.

While working to solve the problem, the employee should use clear, concise communication—written and verbal—so that other people will be able to quickly understand the status of the problem. That means making a detailed description of the problem, any progress so far, and the resolution.

In the event that the employee cannot resolve the problem, the problem needs to be escalated or perhaps moved laterally. It could be that the problem requires a help desk level 2 or level 3 technician, or perhaps it needs to be transferred to another department. The employee should track exactly who was brought in to work on the ticket before relinquishing control of the situation. In some cases, the original help desk employee may be required to follow up on the status of those opened tickets. One way or another, the goal is to close tickets (solve the problems) so that the end users or customers walk away happy!

ExamAlert

When working on a ticket, gather detailed information on the problem, use clear and concise verbal and written communications, and track the status of the problem from beginning to end.

A ticket system could be part of a larger set of software, such as help desk software, asset management (more on that in a bit), or IT service management. But for the exam, you should focus on the ticket portion of that software and how to properly create, manage, and resolve tickets. Consider checking out a trial version of a help desk ticketing system to get a feel for how one of these programs works. Figure 57.1 shows a sample help desk ticket.

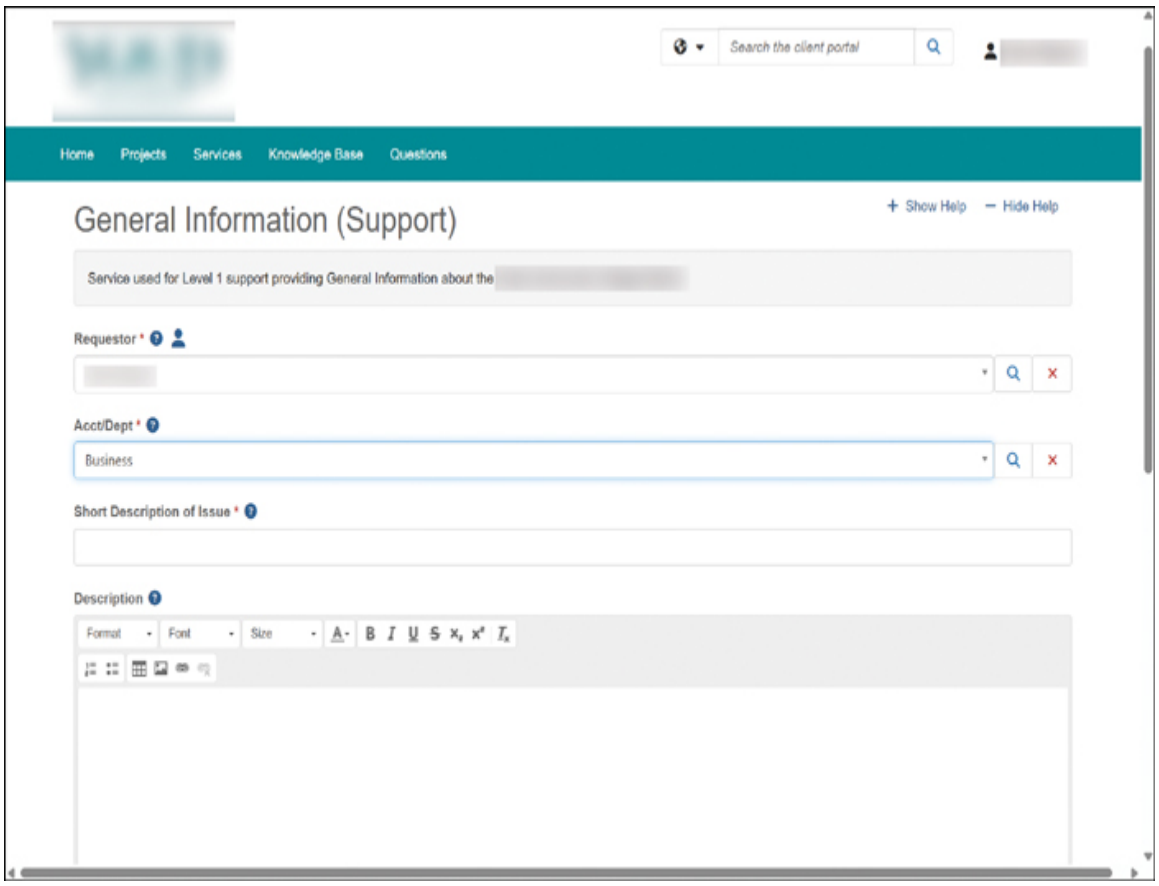


FIGURE 57.1 **A Help Desk Ticket**

Elements of a Help Desk Ticket

The first (and one of the most important) entries in the help desk ticket is the user's name. This information helps the help desk technician identify the user, their department, and their permissions. Sometimes the organization will also include authentication information; for instance, some organizations will ask the user to include some login or other identity information, all to verify which user the technician is helping.

Device information is critical as well. Identifying which device is having trouble saves the technician time figuring out what is going on. After all, many users use multiple devices, including laptops, desktops, monitors, and printers, so it is not unusual for a user to have multiples of each type. By asking for device information up front, the help desk technician can easily track down the device that is having issues.

A description of the issues is all about having the user describe what has gone wrong. Sometimes, the issue is as simple as a burned-out bulb in a projector; other times, the user needs software installed. Still, other times, a website needs to be unblocked from a content filter. Whatever the issue is, the description field tells the technician what needs to be solved.

The help desk ticket often includes a drop-down menu that is used to help the user categorize the problem. Sample categories could include Account management, Password reset, Software installation/update, Hardware problems, and Network problems. It is also not uncommon to subdivide the drop-down; for example, Network problems generates an additional drop-down listing Wi-Fi, Wired, Firewall, Internet, and more as possible responses.

Severity is an important option for users to be able to select. They need to be able to indicate to the help desk how much the problem impacts their job. Sometimes, issues are annoying, like a gnat that buzzes your ear in the middle of the night but is otherwise harmless, or they could prevent the user from doing their job at all. Only the user can tell you that severity.

After the information from the ticket is input into the system, there are several levels to which the particular item can be escalated. Issues begin at the lowest level, which is where most technicians begin. More complex issues will be escalated to upper-level technicians on the help desk. As you become more experienced, you will be able to handle more complex issues and may receive those tasks as well. Generally, tasks are separated into three severity levels and are handled at the lowest possible level.

After the issue is resolved, and at each level (if not resolved at that level), the issue description, notes about the progress, and any resolution—in whole or in part—need to be clearly and concisely written in the notes. The help desk ticketing system generally has a method for recording these notes and can serve as a repository for future problems as well, allowing future technicians to look back on resolved problems to resolve similar issues in the future. As a result, it is critical that your notes are clear, with the issue described fully at each stage of progress all the way through to resolution.

Asset Management

Asset management—in particular, *IT asset inventory management*—is the process of supervising, tracking, and auditing IT equipment within an organization's infrastructure.

All companies are at risk of technology sprawl—meaning the disorganization of IT equipment and software that can occur over time. To reduce this risk, an organization should use written and software-based documentation to track all assets.

Start with inventory lists. Even if they are out of date, this is the place to start. These lists will give you a baseline of what assets the organization believes that it has. From there, you can track physical inventory in the main office at remote facilities and enter this information into an asset management software system. Asset tags and IDs (described shortly) will help with this process.

For software, you will want to track devices on a configuration management database (CMDB). This system inventories the software installed on the company's systems, helps ensure that you don't violate software procurement licenses, and ensures that you know exactly what is installed on each device. If properly configured and filled out, your CMDB can identify the interrelationship between all of your assets, both hardware and software, allowing a deep dive into your entire asset inventory.

Asset tags and IDs are written or printed tags, barcode stickers, or RFID tags that can be attached to devices. They are used for inventory but can also be used for branding purposes; it is not uncommon for an organization's logo to be on the asset tag. If a device is lost, stolen, or otherwise removed from where it is expected to be, the asset tag can be used to help track it. Because a barcode or QR code is easily read by a handheld scanner, maintaining inventory, including check-in and check-out of devices, is made easier. This information is then input (either directly or indirectly) into the asset management software.

ExamAlert

Asset tags and barcodes are used by inventory management systems and software to identify and keep records of company assets.

The procurement life cycle defines the way in which hardware and software can be purchased. There are various models, but it can be summarized into the following general steps: you start by identifying the need, move on to select a vendor or supplier to meet that need, negotiate and award a contract with the vendor, order the product, and finish with any performance monitoring and relationship management after the purchase is made. Larger organizations will have more formalized procurement life-cycle processes (in general, the larger the organization, the more formal the processes).

As a general rule, any product or software that is purchased will come with a guarantee that it is free from defects and that you have permission to use the product. For software, you will generally not have permission to redistribute it outside your organization but will have a license to use it on a certain number of devices within your organization. While a product is under warranty, the promise is that it will function as described for a particular period of time. For software, the licensing could be perpetual (no end) or a particular time period.

Some software licenses can be assigned to specific users; others, certain devices; still others, a specific period of time for all users at an organization. If you are assigning a license to specific users, this generally means that they can use it on any of their devices at any time, provided that they use it on only one device at a time. Some software has a blanket or site or organizational license that is much more unlimited in scope, allowing many more devices to install it at the same time, often at a substantially greater cost.

Keeping track of all of this information is critical. Doing so isn't easy, but the tracking software will help you keep tabs on all of it. Just don't fall behind and you'll be okay.

Documentation Is Key

The bottom line is this: Document everything that you possibly can—within reason. Know how to access all the written and digital documentation. If the process for finding the information is not written, ask your manager or human resources department to help you and ask to put the process in writing. And remember: Leave the documentation better than you found it!

Cram Quiz

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

1. What do inventory management systems and software use to keep track of assets? (Select the two best answers.)

   - ○ **A.** Regulatory policies
   - ○ **B.** User interviews
   - ○ **C.** Asset tags
   - ○ **D.** Barcodes

2. You are working at a help desk and encounter an issue that has not been identified or worked on previously. You go through your troubleshooting methodology, research, and, finally, solve the problem. Which of the following should you do so that the issue can be addressed properly if it is encountered again?

   - ○ **A.** Add your findings to the knowledge base.
   - ○ **B.** Enter the resolution into the ticket and close it.
   - ○ **C.** Escalate the issue to your immediate supervisor.
   - ○ **D.** Email the rest of the technicians on the team, explaining the problem.

3. Why is it important for the IT support ticket to ask for the error message?

   - ○ **A.** To ensure the user feels satisfied with the response time
   - ○ **B.** To charge for additional consulting hours
   - ○ **C.** To speed up the process of identifying and resolving the problem

- ○ **D.** To close the ticket faster without needing more information

4. Why is a configuration management database (CMDB) important for managing IT assets?
   - ○ **A.** It helps track the physical location of each asset.
   - ○ **B.** It stores information about assets and their relationships, helping with problem solving and changes.
   - ○ **C.** It limits the number of assets in the organization.
   - ○ **D.** It ensures assets are used only by authorized users.
5. Why are service-level agreements (SLAs) important in IT service management?
   - ○ **A.** They define the maximum amount of time a service can be down without affecting the business.
   - ○ **B.** They set clear expectations between the service provider and the customer about response times and service delivery.
   - ○ **C.** They restrict the number of incidents that can be reported by users.
   - ○ **D.** They ensure that all IT staff are available 24/7 for support.

Cram Quiz Answers

1. **C and D.** Asset tags and barcodes are used in inventory management systems and software to identify and keep records of company assets. Regulatory policies of an organization attempt to achieve compliance with a government's objectives through laws and regulations. While you might interview users as part of your work, that would be to get information to help with troubleshooting, not for inventory management.
2. **A.** You should add your findings to the knowledge base. Be sure to enter detailed information about the solution so that other techs

can efficiently address the issue if they come across it in the future. You should also enter the resolution into the ticketing system and close that particular ticket so that you have proof of how you solved the problem. However, the issue tracking sytem might not be easily searchable. The knowledge base, on the other hand, is designed for anyone to easily search by issue or by solution. There is no need to escalate the problem because it's been solved! Emailing the rest of the technicians is not necessary; if everyone did this for every problem, the whole team would be swimming in email! Besides, that would defeat the purpose of the knowledge base—to store concise solutions to problems for easy reference later.

3. **C and D.** Speeding up the process of identifying and resolving the problem is best. Closing the ticket faster without needing more information is also true to an extent but is not a guarantee; the more information you can get up front, the less time you will take resolving the problem and the less time to resolution. In a large organization, some technicians specialize in certain problems, so it can also mean getting the right technician right away.

4. **B.** Information about assets and their relationships is stored in a configuration management database (CMDB). This helps with problem solving any issues when any changes are proposed. Although it can help with tracking down physical location, that isn't the main goal of the CMDB. It will not limit the number of assets or their authorized users.

5. **B.** A service-level agreement (SLA) is a formal contract between any service provider (internal or external) and a customer (organization or individual). It defines the expected level of services, outlining the specifics of how services will be delivered. It includes key performance indicators, response times, and other metrics. By setting clear expectations and measurable goals, it improves customer satisfaction.

You are doing *fantastic*! This chapter contains a lot of information. Be sure to review, take a break, sip your favorite beverage, and then continue on to the next chapter of this supertome.

Chapter 58

Change Management and Backup Methods

This chapter covers the following A+ 220-1202 exam objectives:

- **4.2** – Given a scenario, apply change management procedures.
- **4.3** – Given a scenario, implement workstation backup and recovery methods.

In this chapter, we will cover the fundamentals of change management and disaster recovery. As you progress to other certifications, and especially if you ascend into management, these concepts become more crucial.

Understanding Basic Change Management Best Practices

ExamAlert

Objective 4.2 focuses on documented business processes and change management concepts.

Change management is a structured way of changing the state of a computer system, network, policy, procedure, or process. The idea behind this is that change is necessary, but an organization should adapt with that change and be knowledgeable of it throughout its life cycle. Any change that a person wants to make should be introduced to each of the leaders of the various departments that it might affect. Those personnel must approve the change before it goes into effect. Before this happens, department managers will most likely make recommendations and/or give stipulations. There might even be a committee involved; the larger the organization, the more formal the change management procedures will tend to be. Once the necessary people have signed off on a change, it should be tested and then implemented. During implementation, it should be monitored and documented carefully.

In a larger organization that complies with various certifications such as ISO 9001:2015 (https://www.iso.org/standard/62085.html), this whole process can be a complex task. IT people should have charts of personnel, project managers, and department heads. There should also be current procedures in place that show who needs to be contacted about a proposed change.

The typical A+ technician doesn't need to know everything about change management but should understand the basics, including the basic plan for change, how to work within a change management system, and how to implement basic change management best practices. Above all, you need to know who will be approving any change before attempting to make any change yourself. Making an unauthorized change, especially in a tightly structured environment, can lead to bad things (and in the worst-case scenario, can lead to what is euphemistically termed a *résumé-generating event*). Table 58.1 gives definitions for business process terms that you should know for the exam, and Table 58.2 gives definitions for change management terms that you will need for the exam.

TABLE 58.1 **Business Process Terms**

Term	Description

Term	Description
Documented business processes	Most likely, there will be forms involved that require you, as the technician, to state the reason for a proposed change. These are known as *change control forms* or *change request forms*. You should fill out the forms as accurately as possible, in plain English, with little or no jargon.
These processes could possibly include the following:	
Rollback plan	To deal with the possibility that an installation, an upgrade, or a modification fails to perform as expected, a rollback plan is a set of procedures that will bring the application, system, or infrastructure back to the original state before the change was made.
Backup plan	To guard against the failure of equipment, either in whole or in part, or natural disasters, a backup plan is a set of procedures that back up all of the data of an organization on a regular basis. In the case of an equipment failure, these backups can be used to restore the data, thus allowing the organization to continue operating with minimal data loss. In the case of a natural disaster impacting a data center, the backups should be physically stored remotely to ensure that they do not suffer from the same natural disaster that impacted the data center. *Backup* is the process of making copies of the data. *Recovery* is the plan and the processes for using the copies, to get the organization up and running again.
Sandbox testing	Detailed procedures explain how applications and systems will be tested in an isolated environment.
Responsible staff member(s)	It is important to list the person or people who will oversee the business process in question.

TABLE 58.2 **Change Management Terms**

Term	Description

Term	Description
Request form	This is a form used to request, approve, and track project-related changes. There are many reasons for changes; the form documents the change being requested and the approvals for the change.
Purpose of the change	As the technician, you should give a basic description of the change and why the change should come about (although these might be separated on some forms). For example: “It is my contention that computers 251 through 299 are vulnerable to a certain type of attack that could be prevented by updating their firewalls.”
Scope of the change	In describing the scope of a change, you go into detail about what systems will be updated and the procedure that will take place, including who it will affect and when. For example: “Expanding or reducing the functionality of a networking technology might impact hundreds of systems; therefore, it is wise to perform these changes off-hours.”
Change type	The three main types of changes that can be made to an IT project are standard, normal, and emergency. See the following terms.
Standard changes	Also called routine changes, these changes tend to be preauthorized, consistent changes with little risk associated. They are fairly common and have specific guidelines to follow. Automation is often implemented for standard changes, with minimal planning.
Normal changes	Generally, these are any changes that are not standard and are not emergency changes. They go through the normal change advisory process for approval, with complete oversight on changes. Changes that occur with enough frequency might be converted into standard changes. Unlike standard changes, however, they do require some modification each time they are used, so they are not as easy to automate.

Term	Description
Emergency changes	These are the opposite of standard changes. They must be introduced as quickly as possible, such as a security patch to a zero-day exploit or a response to a DDoS attack. These changes are often not thoroughly tested before deployment due to the urgency of the situation. It is important to have a rollback or backup plan (see Table 58.1) in case things go wrong.
Change management timing	Changes should be done at certain times. You need to set the date and time of any change, whether it is standard, normal, or emergency (though emergency might be "Now!").
Change freeze	This is a time when no changes can be made to a system. A change freeze will allow a system in flux to stabilize or to prevent additional changes from being made that could cause problems. Often change freezes are put out in times of transition or when other change management is happening, such as organizational restructuring. Sometimes change freezes are implemented during times of heavy usage by the business users you support; their crunch times represent times when a change freeze might be a good idea. Be sure to document the change freeze period and spread that information widely. While there will be exceptions (see "Emergency changes" earlier in the table), things that can wait will do so, and you won't overload the rest of the IT staff. Make sure you document what exceptions are okay and what are not.

Term	Description
Maintenance windows	These are periods of time during which preventive maintenance on the IT systems will be performed and may cause disruption of service. These maintenance windows should be scheduled outside of business hours (hopefully at a very slow time) and be widely organized. Because some organizations are 24/7, finding this low-usage time can be difficult; look at the usage metrics to find the least-used times and do your best. The worst possible time is mid-morning on a workday when most of the employees are working (we've seen that happen). Unless it's an emergency change, avoid that time slot. Otherwise, find a time when the least number of folks are going to be impacted. Advertise this maintenance window widely.
Affected systems	It is important to identify the systems that will be impacted by any change you make. Sometimes only one or a handful of devices will be impacted; other times the entire organization will be impacted. Regardless, identifying the affected system or systems is important for knowing how to proceed and how to mitigate any impacts.
Risk analysis	Also called risk assessment, this is an attempt to determine threats that could occur with computers and networks. It's a big topic, but as a technician, you need to simplify based only on the change that is proposed. You should state any vulnerabilities that can be mitigated as part of the change and any that could potentially occur due to that change. For example: "The firewall update could possibly interfere with other installed applications, and it should therefore be tested in an isolated environment first before being deployed." By making a risk analysis, you (and the team) can define the risk level (see the following term).

Term	Description
Risk level	This is the amount of potential risk from a decision. As a rule, high risk issues have a high occurrence and/or a high potential impact, requiring immediate attention and robust mitigation strategies. Medium risks have moderate likelihood and/or impact, requiring timely attention and targeted controls but not immediate repair, and low risks have low likelihood and/or low impact, and can be monitored or addressed with low priority as time permits.
Change board	Also known as a change control board or change advisory board, this group includes department heads, subject matter experts (SMEs), and project managers who will decide whether a proposed change should be approved. In some cases, this group's approval is not necessary; for example, a technician might only need a manager signature to update a single computer's antimalware platform. But in the scenario, multiple computers and users will be affected, so the change request will probably go to a committee to review the change request form and all supporting documentation.
Implementation	After it is approved by the change board, the plan can be carried out, or implemented. You must follow the plan as proposed. Document everything. If you run into issues, be sure to ask for help right away so that little problems now don't become big problems later.
Peer review	Change is hard, whether you are proposing the change, implementing the change, or being impacted by the change. Peer review is the process by which someone else with the same role and similar knowledge base will review the work and assess the change, either before or after the change is implemented. Peer review is important, so you know how the change impacted others and how your role in the change was perceived. Be open to this feedback so you can perform your role more efficiently in the future and continually improve your own processes.

ExamAlert

Know the business procedures and change management terms and definitions in Tables 58.1 and 58.2 for the exam.

Note

Here's a Microsoft-related example of a strategy for change management: https://docs.microsoft.com/en-us/microsoftteams/change-management-strategy.

Note

The Cram Quiz at the end of the chapter covers the material for both Objectives 4.2 and 4.3.

Implementing Workstation Backup and Recovery Methods

ExamAlert

Objective 4.3 concentrates on backup and recovery, backup testing, and backup rotation schemes.

There's no need to go looking for disasters; they will come looking for you—that is, if you don't plan well and if you don't incorporate fault tolerance and redundancy whenever possible. The more you secure and provide redundancy, the more you reduce the risk of disaster. However, a disaster can happen. In the *unlikely* event that it does, you need to be ready. Be prepared with a disaster recovery plan (DRP).

The objective of a DRP is to ensure that an organization can respond quickly to an emergency and minimize the effects of the disaster on the organization, its employees, and its technology. A DRP could be a simple one-page document (for small offices) or an entire set of documentation including profiles, processes, and procedures (and more likely the latter).

> **Note**
>
> The following link leads to NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, which provides plenty of information about security in general, including DRPs: https://www.nist.gov/privacy-framework/nist-sp-800-34.

For the A+ exam, you need to be most concerned with one concept in the realm of disaster prevention and disaster recovery: backup and recovery.

Know this: Your data IS NOT SAFE! (Yes, we were screaming that.) So, backing up data is critical for organizations—as well as individuals! It is not enough to rely on a fault-tolerant array of storage drives or other redundancy methods. You need to back up your own data, either as an entire system drive or as individual files. If you have a portable drive, you can use that. Many people back up their files to the cloud as well. For businesses, there are good options in both network-attached drive storage and cloud storage; with prices of cloud-based storage coming down in recent years, that has become a real game changer for file backups, so it is worth exploring.

Using Windows Backup

Windows Backup is a utility that will back up your files and folders to an external disk or to your OneDrive. (Details are at https://support.microsoft.com/en-us/windows/back-up-and-restore-with-windows-backup-87a81f8a-78fa-456e-b521-ac0560e32338.) Windows Backup allows you to back up your files and folders as well as your Windows settings automatically either one time or on an incremental basis.

To access Windows Backup from Windows 11, go to **Settings > Accounts > Windows Backup**. Figure 58.1 shows the Windows backup screen in Windows 11, where you will set up syncing. Note that you must be logged in to a Microsoft account to set up and use Windows backup, even if you are backing up to a local drive.

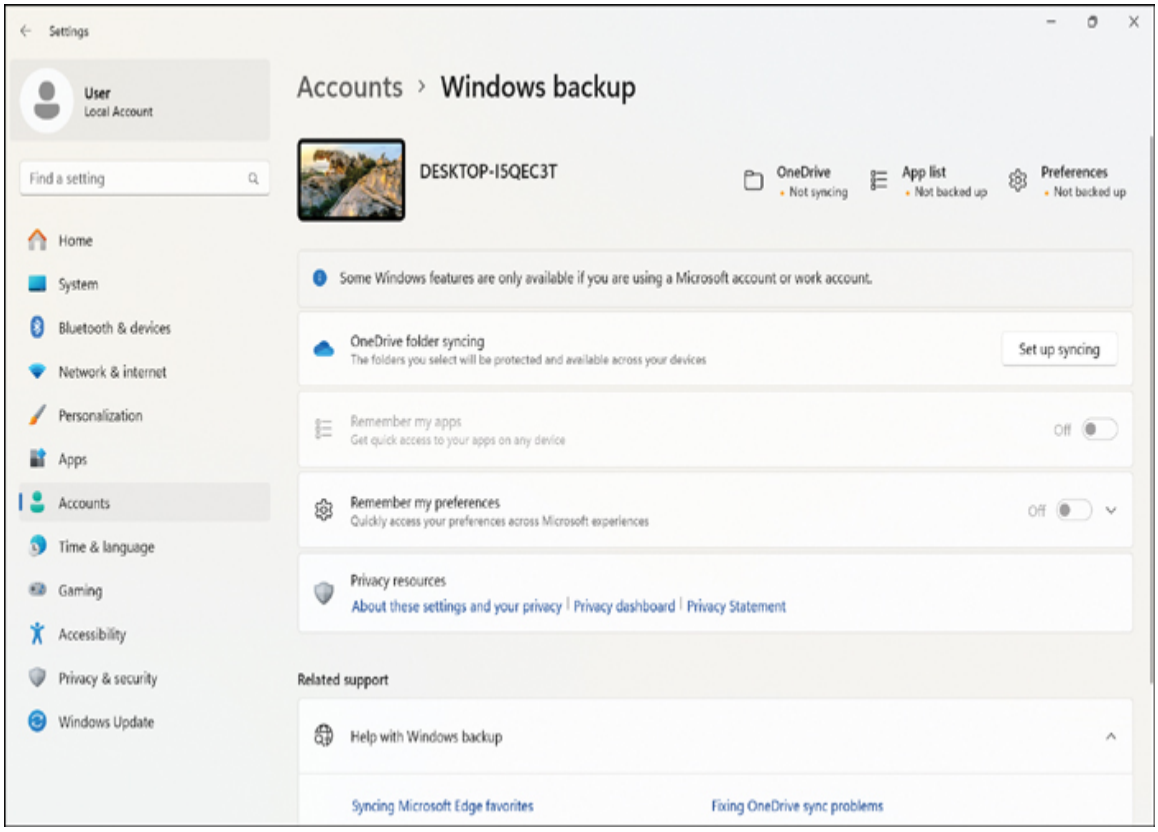


FIGURE 58.1 **Windows Backup Enables You to Configure Backup Settings**

ExamAlert

Know how to use Windows Backup, located at **Settings > Accounts > Windows Backup**.

Larger companies will direct users to save their files to the shared drives instead of the local drives and will back up these shared drives centrally. Sometimes users will not have an option to save files locally. These

centrally managed drive locations come with their own programs that allow you to select various types of backups and verify those backups in several ways. Often these drives are either hosted in an online cloud environment (a corporate version of OneDrive or similar) or will otherwise use specialized hardware and software to create and maintain the backups themselves. Ask at your organization for details of how this is done.

Backup Methods

There are several backup types you should be aware of for the exam, including full, incremental, differential, and synthetic. Most operating systems and third-party backup utilities support some or all of these types. Keep in mind that this list is not the end-all of backup types, but it gives a basic idea of the main types of data backups used in the field. When performing any of these types of backups, you must select what to back up. It could be a folder or an entire volume.

Full Backup

A *full backup* backs up the entire contents of a folder or volume, whichever is selected. A full backup can be stored on one or more tapes. If more than one is used, the restoration process would require starting with the oldest tape and moving through the tapes chronologically, one by one. Full backups can use a *lot* of space, causing a backup operator to use a lot of backup tapes, which can be expensive. Full backups can also be time-consuming if there is a lot of data. So, often, incremental (or differential) backups are used with full backups as part of a backup plan.

Incremental Backup

An *incremental backup* backs up only the contents of a folder that have changed since the last full backup or the last incremental backup. An incremental backup must be preceded by a full backup. Restoring the contents of a folder or volume requires starting with the full backup tape and then moving on to each of the incremental backup tapes chronologically, ending with the latest incremental backup tape.

Note

Some operating systems and backup systems associate an archive bit (or archive flag) with any file that has been modified; this indicates to the backup program that it should be backed up during the next backup phase. The incremental backup resets the bit after backup is complete.

Table 58.3 shows an example of a basic one-week backup schedule using the full and incremental backup types. A full backup is done on Sunday, and incremental backups are done Monday through Friday.

TABLE 58.3 **Sample Incremental Backup Schedule**

Day	Backup Type	Time
Sunday	Full backup	6 p.m.
Monday	Incremental backup	6 p.m.
Tuesday	Incremental backup	6 p.m.
Wednesday	Incremental backup	6 p.m.
Thursday	Incremental backup	6 p.m.
Friday	Incremental backup	6 p.m.

In this schedule, six backup tapes are required, one for each day, and the backups are done at 6 p.m. daily. Tapes might be reused when the cycle is complete, or the organization might opt to archive certain tapes each week —such as the full backup tapes—and use new tapes every Sunday.

Let's say that this backup procedure is used to back up a server. Now, imagine that the server crashes on Wednesday at 9 p.m., and the storage drive data is lost. A backup operator arriving on the scene Thursday morning (or earlier) would need to review any logs available to find out when the server crashed. Then, the admin would need to fix the server, and the backup operator would need to restore the data. This would require

starting with the Sunday full backup tape and continuing on to the Monday, Tuesday, and Wednesday incremental backup tapes. In this case, four tapes in total would be needed to complete the restoration.

Windows Server has a built-in program called Windows Server Backup (wbadmin.msc). After adding it as a feature in Windows Server, you can then back up data as you wish, optimize the backup performance, and select either full or incremental backups for individual volumes, as shown in Figure 58.2.

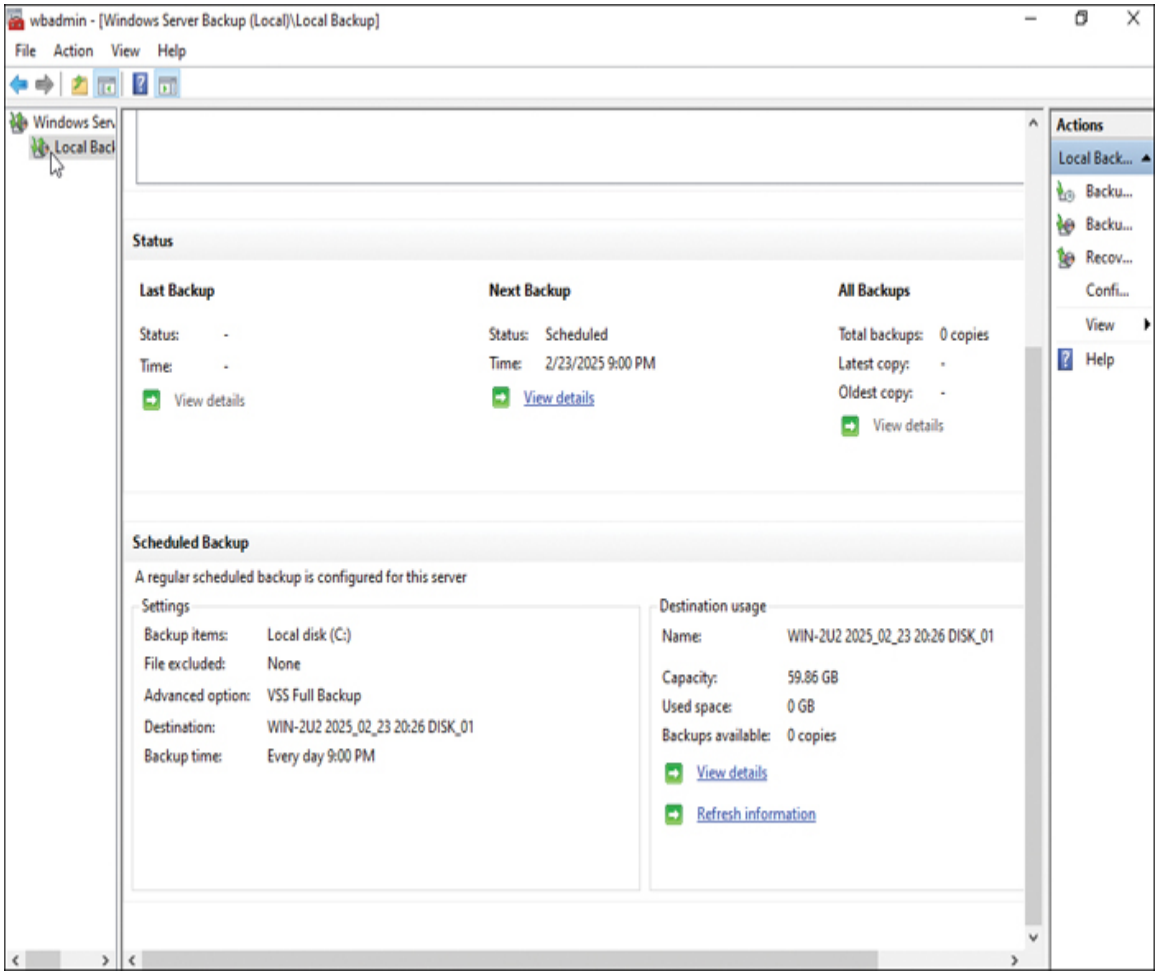


FIGURE 58.2 **Windows Server Backup Screen Set to Full Backup of the C: Drive**

Differential Backup

A *differential backup* backs up only the contents of a folder that have changed since the last full backup. A differential backup must be preceded by a full backup. To restore data, you would start with the full backup tape and then move on to the latest differential tape.

> **Note**
>
> Differential backups do not reset the archive bit when backing up. This means that incremental backups will not see or know that a differential backup has occurred. That also means that differential backups get progressively larger as more time progresses from the last full backup.

Synthetic Backup

Synthetic backups, also called *synthetic full backups*, are full backups that can simplify the restoration process. They are created by taking the full backup and combining them with all of the following incremental backups to create a new full, synthesized backup. They can be incorporated into a full/incremental backup scheme like the one shown in Table 58.3. Let's say you run a full backup on Sunday and incremental backups on Monday through Friday. Now imagine that there is a problem on Friday evening. Without a synthetic backup, you would restore by using all the backup tapes as mentioned previously—first the full backup and then each of the five incremental backups, individually. But with a synthetic backup, you can simplify the process!

One way to use a synthetic backup would be to allow it to create another incremental backup on Friday and then, immediately after, generate a full synthetic backup, based on the original full backup and all incremental backups. Now, if there is a failure on Saturday, the entire backup can be restored from one tape—the synthetic full backup—instead of requiring six tapes of backup.

Recovery

Once you have backed up your data, you need to be able to recover it when needed. After all, the best backup is useless if it can never be recovered when a problem occurs.

There are two different types of recoveries, and you should know about both:

- **In-place or overwrite recovery:** This refers to the restoration of data to its original location. It is called *overwrite* because you are writing over (overwriting) the data on that original device (usually a server) with the backed-up data. This method tends to be faster because you don't have to completely rebuild the server hardware itself. Instead, you are just reloading the data from the backup drive. This approach is most efficient if you have very frequent backups, because otherwise you can lose a tremendous amount of data. It is frequently used when restoring drives for virtual machines.
- **Alternative location recovery:** In this type of recovery, the data is recovered to a different machine, perhaps in an alternate location. The primary location may be unavailable entirely. It can be used as part of the recovery program for natural disasters and can also be used as part of the move to virtualization and the move to cloud-based computing. Because the drives are recovered to an alternate location, the original location is either offline (if some sort of disaster) or potentially still available (if it was a planned recovery).

Backup Testing

After a backup is complete, it should be verified or validated in some way. Manufacturers of backup software and hardware solutions usually include some kind of verification mechanism that you can select during the backup process. This mechanism will verify that the backup was written properly to the backup media.

However, a verification mechanism isn't enough to satisfy a DRP. A backup operator needs to periodically test backups by actually restoring hand-picked backup jobs to test systems. This might seem like a shot in the dark, but you can logically select what to test by being included in the change

management loop. Any substantial change proposals might need to notify the backup group so that those changes can be tested by way of a new backup/restoration.

When you're initially backing up a system, such as a Windows server, that backup should be *thoroughly* tested via a restoration and in-depth comparison of the original data to the restored data. But it goes further than that; restorations should be tested on simulated systems with simulated *failures*. So, for example, if you are concerned that the server's system drive (or array) could fail, then you could test that by setting up a test server with the same configuration and storage drive array and restore the system data or image to that test system. Or, if the IT budget doesn't allow for this, you could at least test it virtually. Quality virtualization software is a must in this case because it needs to emulate hardware appropriately.

Finally, consider the frequency of backup testing. For example, once a year is not enough. Some organizations require that backup testing be done monthly or even weekly.

ExamAlert

Perform backup testing to ensure that backups are actually being performed and that data can actually be restored!

Backup Rotation Schemes

There are a variety of schemes that you can implement when planning your backup schedule. Let's look more closely at a few schemes and some best practices.

Grandfather-Father-Son (GFS)

The GFS backup rotation scheme is a common backup method. When you use this scheme, three sets of backups must be defined; usually, they are daily, weekly, and monthly, corresponding to son, father, and grandfather. Backups are rotated on a daily basis; normally, the last one of the week is

graduated to father status. Weekly (father) backups are rotated on a weekly basis, with the last full backup of the month being graduated to grandfather status. Often, monthly (grandfather) backups, or a copy of them, are archived offsite.

10-Tape Rotation

The 10-tape rotation method is simple and provides easy access to data that has been backed up. It can be accomplished during a two-week backup period, and each tape is used once per day for two weeks. Then the entire set is recycled. Generally, this is similar to the one-week schedule discussed previously; however, the second Monday might be a differential backup instead of a full backup. And the second Friday might be a full backup, which is archived. There are several options; you would need to run some backups and see which is best for you, given the number of tapes required and time spent running the backups.

Onsite vs. Offsite Backups

Most of what we have discussed so far has been based on the backup of data to local storage. The beauty of local storage is that you own it (or your organization does). This means you can access it when you wish, it is physically available to you, and it can most likely be secured relatively easily. In addition, if a failure occurs, the time to repair might be less than if you back up data to the cloud. Plus, simulations and testing can be run faster (in some cases). So being local has advantages. However, it can be costly: Servers, racks, drive arrays, tape drives, *electricity*, and so on can quickly break the bank. And don't forget about disasters such as theft, fire, floods, or natural disasters. If one occurs and it encompasses your building, then your data is gone, and you just might be out of a job. It can make an IT person wonder if backing up to the cloud is a better solution—and sometimes it can be.

The big platforms such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud, and so on have various cloud services plus storage, syncing, and backup solutions. These tend to be more secure than services such as Dropbox, Microsoft OneDrive, and Google Drive because they are designed

for business use, especially enterprise-level business, where security is paramount. There are two keys to this: speed and resilience. You need to have a fast backup solution (and, more importantly, a rapid restoration process), regardless of the location of the backup. And whichever providers are used, the data needs to be redundant and accessible. How would you go about ensuring all this? Think about this situation for a moment. Solutions exist; it just needs to be worked out.

Regardless of the solution you use, the backups should be well documented, and the backup accounts should have strong passwords/passphrases. This is all part of a data backup strategy where you are concerned with having onsite backups (for easy restoration), offsite backups (for disastrous situations), backup testing, and an organized storage system that is properly documented.

Note

Last thought on this: Smart companies "hedge." This means they will use onsite and offsite solutions together to reduce their risk as much as possible.

3-2-1 Backup Rule

The 3-2-1 backup rule is just about as old as the backup tape. Simply stated, it requires *three* copies of data. The first is the actual production data—the data in use. The second and third are backup copies. Those *two* should be stored on two types of storage to minimize the chance of failure (such as disk, tape, or cloud storage), and *one* of them should be stored offsite.

While this rule was used for years by many backup operators, it has limitations. For example, one backup stored offsite is not enough today, especially if you are storing it on the cloud.

Warning

The basic rule of cloud is this: DO NOT RELY SOLELY ON ONE CLOUD PROVIDER! There, we said it.

Another option is to scale the 3-2-1 rule. For example, make it the 3-2-2 rule, where you use two separate geographic regions to store your offsite backups. You might opt to store one backup with a cloud provider such as Microsoft, Google, or Amazon and store another backup at a colocation, or you might use two different cloud providers, as long as the data is stored in two different geographic areas. There are lots of possibilities when it comes to storage locations, and you could further scale the 3-2-1 rule as needed.

Note

The following cram quiz combines this section and the previous section related to Objectives 4.2 and 4.3.

Cram Quiz

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

1. In a change management board meeting, you are discussing any vulnerabilities that can be mitigated as part of a recommended change and anything that could potentially occur due to that change. What best describes what you are discussing?

   - ○ **A.** Purpose of the change
   - ○ **B.** Scope of the change
   - ○ **C.** Backout plan
   - ○ **D.** Document changes
   - ○ **E.** Risk analysis

2. You have been tasked with backing up new user profiles in an enterprise environment. You propose to back up these user accounts to a new tape backup device. Which of the following procedures should you follow? (Select the two best answers.)

- ○ **A.** Change management
- ○ **B.** End-user acceptance
- ○ **C.** Windows Backup
- ○ **D.** Incremental backup
- ○ **E.** Backup testing

3. You work with servers and network infrastructure in an IT department. You are proposing a major operating system upgrade to a Linux server. You have completed the documentation for this, and it shows that the upgrade will impact your organization's web services. You finish the required risk analysis and document the processes that will be required. Which of the following should you complete next?

- ○ **A.** Rollback plan
- ○ **B.** Change request
- ○ **C.** Purpose of the change
- ○ **D.** Scope of the change

4. Which type of backup scheme uses two types of media, with one being stored offsite?

- ○ **A.** GFS
- ○ **B.** 10-tape rotation
- ○ **C.** 3-2-1
- ○ **D.** Cloud storage

5. You have implemented a backup solution that combines a full backup on Monday at 6 p.m. and incremental backups on Tuesday

through Friday at 6 p.m. If there was a storage drive failure on Saturday morning, how many backup tapes would be required to restore the entire backup?

- **A.** 1
- **B.** 2
- **C.** 4
- **D.** 5

6. Which of the following will bring a system back to its original state before a change was made? (Select the two best answers.)

- **A.** A responsible staff member
- **B.** Sandbox testing
- **C.** Undocumented business process
- **D.** Rollback plan

Cram Quiz Answers

1. **E.** You are discussing risk analysis, which is the attempt to determine what threats could occur with computers and networks. The purpose of a change is a basic description of the change and why the change should come about. The scope of a change is to detail what systems will be updated. The backout plan is a set of procedures that will reverse any failed changes made quickly and efficiently. Documenting changes happens once approval is made; you should carefully document any changes that are made and when.

2. **A and E.** Because this is a change (backing up to a new tape device), a change management document will probably be needed, listing procedures for usage of the new backup device and the backup of the new accounts. Backup testing should be done often, or at least periodically, and definitely when it comes to new data, as is the case in this scenario with new user profiles. You are not

concerned with the end-user acceptance aspect of change management because the users should not be affected by this—it should be transparent to them—but if you were, that would be part of change management. Windows Backup is a Windows tool; in enterprise environments, you would use Windows Server Backup or a comparable third-party tool. Because these are new user profiles, you would want to do a full backup, not an incremental backup.

3. **B.** The technical assessments are finished, and you know how you would proceed with the process of upgrading the Linux server. Now it's time to actually fill out the paperwork required by your organization. This would most likely be a change request form. This and any supporting documentation and assessments will be presented to a change control board or committee. This document needs to be approached from a business standpoint and written in a way that your team *and management* can read easily. It will hopefully include many things, such as the purpose of the change, the scope of the change, a rollback plan (or backout plan), systems affected, and so on. As you see, by using the process of elimination, you reject the other potential answers in the question; remember this technique. It's awesome that you are using a Linux server to run web services—perhaps Apache web server or NGINX—and as a technician, you have the know-how to make the upgrade work. However, your proposal needs to "sell" the idea to the organization. The change request document needs to show that the process will not disrupt business operations (at least not too much) and that the organization's risk will be reduced as much as possible. It needs to show that everything is planned out step by step and that you have a contingency plan (backout plan) if something goes awry. Remember, even if you make no mistakes, issues can still occur.

4. **C.** The 3-2-1 rule is a backup scheme that specifies *three* copies of data: one in use and *two* others that are stored on different media types, with *one* of those being stored offsite. The grandfather-father-son (GFS) backup scheme uses three sets of backup tapes: daily, weekly, and monthly. The 10-tape rotation uses two weeks'

worth of daily tapes, which are reused after a two-week period. Cloud storage is a possible backup scheme for your data, and although it is offsite, it does not deal with different types of media.

5. **D.** You would need all five backup tapes to restore the entire backup. That would include the full backup from Monday, and the four incremental backup tapes from Tuesday through Friday. If you had also set up a synthetic backup on Saturday, then you would need only that one tape. If you had a different setup with a full backup on Monday and a differential backup on Friday (with incrementals between Tuesday and Thursday), only two tapes would suffice for the recovery: the full backup and the differential backup (and the incremental backups would not be necessary). If perhaps the failure occurred on Friday morning instead of Saturday, then you would need only four tapes: the full backup and the three incremental tapes from Tuesday through Thursday.

6. **A and D.** A responsible staff member is the person (likely you) who will oversee the business process in question. The business process in question here is a rollback plan that will bring the system back to the original state before the change was made. Sandbox testing is a detailed procedure that explains how applications and systems will be tested in an isolated environment, which is often a virtual machine (VM). An undocumented business process is just that: a business process that has yet to be documented.

Great work! You've completed yet another chapter. Before you know it, we'll be wrapping up this book. There is a lot of detail in this chapter, and the discussion moved away from the computer tech side of things. So, review carefully, take a break, and then forge ahead!

Chapter 59

Safety Procedures

This chapter covers the following A+ 220-1202 exam objective:

- **4.4** – Given a scenario, use common safety procedures.

Safety first! Remember to put safety on the top of your priority list when dealing with computers, power, networking, and people. Protect yourself, protect others, and protect your computer. Proper grounding, electrical safety, physical safety, and fire prevention are the keys to a happy and healthy career.

ExamAlert

Objective 4.4 concentrates on the following: electrostatic discharge (ESD) straps, ESD mats, electrical safety, equipment grounding, cable management, proper component handling and storage, antistatic bags, compliance with government regulations, and personal safety.

ESD Prevention and Equipment Grounding

We'll start this discussion of safety procedures with electrostatic discharge (ESD) prevention. Guard those components! By using antistatic methods, you protect your computer's parts and keep *it* safe.

ESD occurs when two objects of different voltages come into contact with each other. The human body is always gathering static electricity—more than enough to damage a computer component (for example, that $500 video card you just purchased). ESD is a silent killer. When you touch a component without proper protection, the static electricity could discharge from you to the component, most likely damaging it without showing discernible signs of damage. Worse yet, it is possible to discharge a small amount of voltage to a device and damage it enough that it works intermittently, making it tough to troubleshoot. It takes only 30 volts or so to damage a component. On a dry winter's day, you could gather as much as 20,000 volts when walking across a carpeted area! However, you can protect components from ESD by equalizing the electrical potentials in several ways:

- **Use an antistatic wrist strap:** This type of strap, which is inexpensive and takes only a moment to put on and connect, can protect a computer from accidental voltage spikes. In addition, almost all antistatic wrist straps come equipped with a resistor (often 1 megaohm) that protects the user from shock/electrocution hazards. Use one whenever working on PCs or laptops.
- **Use an antistatic mat:** Place the computer on top of the mat. Connect the mat via the antistatic cable the same way you do an antistatic wrist strap. You can also stand on a mat and connect it in the same manner. Ground the mat to earth ground (your building ground is almost always good enough).
- **Self-ground:** To further discharge yourself, touch the chassis of the computer before handling any components. Especially do this when an antistatic strap is not available. This equalizes the electrical potential between you and the equipment.
- **Use antistatic bags:** Adapter cards, motherboards, and the like are normally shipped in antistatic bags. Hold on to them! When installing or removing components, keep them inside an antistatic bag until you are ready to work with them. Keep the bag on top of the antistatic mat.
- **Handle components properly:** If you are sitting at your desk without any ESD protection, there is no reason to be handling components, so

don’t. Handle components only when you are fully protected. When you do handle components, try to hold them at the edge. For example, when installing RAM, hold the module at the sides. This will inhibit any direct handling of the chips, contacts, and other circuitry. Hold adapter cards by the metal plate (bracket) or by the edge of the fiberglass board but never by the contacts. Never touch a CPU’s lands/pins or the CPU cap if at all possible.

Some other ways to prevent ESD include using antistatic wipes, sprays, and gloves; keeping your feet stationary (to reduce friction); working in an uncarpeted area; and raising the humidity. However, while somewhat helpful, each of these approaches is less effective than the preceding list.

Note

Take a look at the various standards for static control at the following site: https://www.esda.org/standards/.

ExamAlert

Remember the main ways to avoid ESD: wearing an antistatic strap, using an antistatic mat, self-grounding (touching the computer case), and using antistatic bags.

Caution

Be Careful with Electricity!

Remember, the whole idea here is to equalize the electric potential between the person and the equipment to reduce the risk of a discharge. But you have to be careful with electrical circuits. If you are not sure what you are doing, *hire a qualified and certified electrician* to help you. In the lab, for example, you can take off the alligator clips of the antistatic wrist strap and mats and connect them

to a common point ground connector, which then plugs into a dedicated grounding outlet (although any properly wired AC outlet will do). In a bench or lab environment, it goes much further: There will be dedicated grounding outlet strips, the entire bench may be grounded, and all kinds of other techniques will be used, such as antistatic gloves, lab coats, special flooring, and so on. Be sure to follow whatever procedures your organization has set forth.

If you are worried about shocking yourself, simply take the electricity out of the mix. Connect the alligator clips of the antistatic strap and mat to the chassis of the computer and then touch an unpainted portion of the case before handling components. This method is not as good as a properly grounded setup, but it does help to equalize the potential.

It is also possible to equalize the potential with the computer plugged in, but we do not recommend it–for a variety of reasons. For example, you might not know whether the AC outlet (or circuit) is wired properly (if an electrical circuit is wired backward, the circuit might still be live even if it is switched off). So, remember to keep the computer unplugged–by disconnecting the power or hitting the kill switch on the back of the computer (if there is one)–before working on the system. You can also connect the device to a power strip and shut that off; the ground will remain active. This way, you reduce the chance of an electrical shock.

It's also important to ground network racks in a server room or data center. You can do this by installing grounding bars to the racks/equipment and by using a thick, low-gauge grounding wire (for example, 6 AWG) and connecting it from the grounding bars to a grounded location, which might be the building's main ground wire, an I-beam, and so on. The key is to provide a path for electricity in the event of a power-related issue. Check your municipality's code to find out what is acceptable, and if you are not sure, get an electrician or the facilities department involved.

Electrical Safety

Electricity is a great energy that should be treated with respect. *Always practice proper power handling*. Before working on any computer component, turn off the power and disconnect the device from the AC outlet. If a device such as a power supply or video monitor has a label that reads "No Serviceable Components Inside," take the manufacturer's word for it and send the component to the proper repair facility or simply replace the component. The message on the device is intended to keep a person out, usually because the internal components might hold electrical charge.

Be sure to use your power supply tester, receptacle tester, and other power testing equipment properly. If you do not know how to use these tools, escalate the issue to the facilities department or another person in your company. If you find issues with AC outlets or other types of AC equipment, refer the issue to your manager or building supervisor. Do not try to fix such issues. If you find an issue like this in a customer's home, tell the customer about the problem and recommend that the AC outlet be repaired by an electrician before going any further.

Do not open power supplies. As far as the A+ exam is concerned, if a power supply goes bad, you should replace it, even if you think it is just the fan and would be an easy repair. A power supply is known as a *field replaceable unit (FRU)* for a reason. Although it is possible to repair power supplies, that type of repair should be done only by trained technicians. Remember that a power supply always holds a charge; this alone should be enough to keep you away from the internals of the power supply. In addition, the amount of time it would take a person to repair a power supply would cost more to a company than just buying a new one and installing it. Be sure to recycle the old one according to municipal guidelines.

LCD (and other flat screen technologies, here generically listed as LCD) monitors can also be dangerous. We can't actually tell you *not* to work on them, especially because laptops integrate them. Regardless, it is again recommended that a failed monitor (or laptop) be sent to the proper repair organization or to the manufacturer if the device is within warranty. However, if you do decide to work on an LCD, one thing to be careful of is capacitors, which are normally near the LCD power supply and hold a charge. Also, make sure that the device is turned off and unplugged; if it is a laptop, make sure the battery has been removed. One of the items that can

fail on an LCD monitor is the backlight inverter. The inverter is usually mounted on a circuit board, and if it fails, either a fuse needs to be replaced or the entire inverter board needs to be replaced. The inverter is a high-voltage device. Try not to touch it, and be especially sure not to touch it when the LCD device is on. (Keep in mind that LED-based LCD monitors don't have inverters, and these monitors are much more common as of the writing of this book in 2025.) A lot of this information is common sense, but it is worthwhile to always be sure—like measuring twice before you cut.

Note

In the uncommon scenario that you come across a CRT monitor, don't open it because it carries a lethal charge. Instead, refer such a monitor to a company that specializes in monitor repair. If you need to dispose of CRTs, find a monitor repair company that will buy them or simply accept them without charge. Otherwise, they need to be recycled in compliance with local government regulations and/or municipal ordinances. For instance, in our community, the local landfill takes them every day for free as part of their e-waste recycling initiative. Yours might too!

ExamAlert

Remember to always recycle in compliance with company policy and local government regulations and/or municipal ordinances.

Another device that you need to make sure you turn off and unplug is a laser printer. A laser printer contains extremely dangerous high voltages. On a related note, if a printer was recently used, watch out for the fuser; the fuser runs hot!

Finally, it is important to match the power requirement of your computer equipment with the surge protector or uninterruptible power supply (UPS)

that it connects to. Verify that the number of watts your computer's power supply requires is not greater than the amount of power your surge protector can provide; the same goes for the watts (or volt-amps) that the UPS can provide. In addition, be sure that you do not overload the circuit that you connect to. For additional information about electrical safety, see the electrical safety and health topics at the Occupational Safety and Health Administration (OSHA) website: https://www.osha.gov/electrical.

Electrical Fire Safety

Let's talk a little about 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. For example, CO_2-based BC fire extinguishers are common and relatively safe to humans, but they can cause damage to computers. If equipment needs to be protected by more than a CO_2-based BC fire extinguisher, an ABC Halotron extinguisher should be used. Server rooms and data centers are often protected by larger special hazard protection systems such as FM-200, which is based on the gaseous suppression agent heptafluoropropane. This clean agent won't cause damage to servers and other expensive equipment.

If you see an electrical fire, first call 911. If the fire is very small, use the proper extinguisher to attempt to put it out. If the fire is too big for you to handle, evacuate the building. Afterward, you can notify building management, your supervisor, or other facilities people.

Hopefully, you will never come near a live electrical wire. But if you do, you want to attempt to shut off the source. Contact your building maintenance right away if you are at work. Never attempt to do this with your bare hands. Make sure that your feet are dry and that you are not standing in any water. Use a wooden stick, board, or rope.

If you find an apparently unconscious person underneath a live wire, do not touch the person! Call 911 right away! If instructed by 911, you might be able to 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 you are clear of the electrical line, attempt to administer first aid to the person.

Note

For more information about fire extinguisher types and their operation and fire protection and fire prevention in general, see https://www.osha.gov/sites/default/files/2019-03/fireprotection.pdf.

Remember: Call 911 right away if there is a fire. Don't wait to call; fires spread quickly. Getting yourself and other people out safely is more important than any equipment that may be damaged. In the case of someone hurt by an electrical problem, 911 will be able to assist you, and the dispatchers are trained to help with these situations. Remember: Don't give them additional victims they need to rescue!

Physical Safety

Physical safety considerations include the following:

- Securing cables
- Using caution with heavy items
- Avoiding touching hot components
- Using safety equipment
- Considering workplace ergonomics

Cables can be a trip hazard. Employ proper cable management by routing cables away from high-traffic areas and keeping computer cables stowed away and tie-wrapped. Network cables should have been installed permanently within the walls and ceiling, but sometimes you might find a rogue cable. If you discover a cable on the floor or hanging from the ceiling, alert your network administrator or your manager. Do not attempt to reroute the network cable. You don't know what data is transferred on the

cable. Because network cabling is monitored by municipalities in the same way other electrical work is monitored, only qualified, trained technicians should take care of network wiring.

Lifting heavy items incorrectly 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. When lifting something, stand close to the item, squat down to the item by bending your knees, grasp the item firmly, keep your back straight, and slowly lift with your legs, not your back. Be sure not to twist your body; keep the item close to your body. This technique helps to prevent back injuries. When you're moving items, it is best to have them stored at waist level so that minimal lifting is necessary. OSHA has plenty of guidelines and recommendations for physical safety at the workplace. Its website is https://www.osha.gov.

Be careful when handling components that might be hot. The best method when dealing with hot items (such as a laser printer's fuser, a burned-out power supply, or a CPU or storage drive that needs to be replaced) is to wait until they have cooled. To be safe, before replacing items, wait 15 minutes for them to cool. Servers and networking equipment can get quite hot as well, even when they are stored in a climate-controlled room. Take great care when working with these devices. Also, be careful with items that hold a charge. For the A+ certification, know that if a device has the possibility of holding a charge, you should not open it. This includes power supplies and CRT monitors. These types of electronics can be recycled in most municipalities. Programs might include curbside pickup, drop-off centers, or recycling events. Usually, these are free. There are also many donation programs for equipment that still functions.

Use safety equipment whenever necessary, including safety goggles, hard hats, air filtration masks, fluorescent clothing, and so on. Whenever you enter a work area, lab, construction site, or any other non-office environments in the field, be sure to follow safety instructions.

ExamAlert

On the exam, remember that personal safety includes disconnecting power before repairing PCs, using proper lifting techniques,

following fire safety principles, and wearing safety goggles and an air filter mask.

You probably won't get any questions on the exam about this, but ergonomics is important when operating a computer. Ergonomics can affect the long-term health of a computer operator. It is important to keep the wrists and hands in line with the forearms and to use proper typing technique. Keep the elbows close to the body and supported if possible. The lower back should be supported, the head and neck should be straight and in line with your back, and the shoulders should be relaxed. Keep the top of the monitor at or just below eye level. Take breaks at least every two hours to avoid muscle cramps and eyestrain. To further reduce eyestrain, increase the refresh rate of the monitor, if possible.

Note

For more information on ergonomics, see OSHA's information on computer workstations at https://www.osha.gov/etools/computer-workstations.

Cram Quiz

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

1. If a power supply fails, what should you do?

- ○ **A.** Replace it.
- ○ **B.** Repair it.
- ○ **C.** Use a different computer.
- ○ **D.** Switch it to a different voltage setting.

2. Which of the following are ways to avoid ESD? (Select all that apply.)

   - ○ **A.** Use an antistatic wrist strap.
   - ○ **B.** Use a vacuum cleaner.
   - ○ **C.** Use an antistatic mat.
   - ○ **D.** Touch the chassis of the computer.

3. You walk into the server room and see a person lying on the floor with a live electrical wire draped over. Which two of the following should you do and in which order?

   - ○ **A.** Run out and call 911.
   - ○ **B.** Grab the wire and fling it off the person.
   - ○ **C.** Grab and drag the person out from under the wire.
   - ○ **D.** Grab a piece of wood and use it to move the wire off the person.

4. A customer is "cleaning house" and asks you what to do with several older CRT monitors. What should you tell this customer?

   - ○ **A.** Throw them in the dumpster out back.
   - ○ **B.** Try to repair them.
   - ○ **C.** Donate them to a thrift store.
   - ○ **D.** Recycle them in compliance with local government regulations and/or municipal ordinances.

Cram Quiz Answers

1. **A.** Replace the power supply. Trying to repair it can be dangerous and is not cost-effective to the company.

2. **A, C, and D.** Using antistatic wrist straps and mats and touching the chassis (self-grounding) of the computer are all ways to stop ESD. Vacuum cleaners can cause damage to components.

3. **A, then D.** The first thing to do is call 911 and get emergency help on the way. After that, if emergency dispatchers approve, you should get a wooden stick, rope, or something similar (every server room should have one) and use it to CAREFULLY move the wire off of the person. In reality, the first thing you should do is breathe and not make any rash decisions in the heat of the moment. After the wire is removed, attempt to offer first aid to the victim. DO NOT ever touch a live wire or anything that the live wire is coming into contact with.

4. **D.** Electronic equipment and devices should be recycled in compliance with local government regulations and/or municipal ordinances. Throwing them in the dumpster out back, trying to repair them, or donating them are all wrong answers and very bad ideas. First, electronic equipment and devices should never just be thrown away in public trash. They are considered e-waste—which is bad for the environment, and your customer could get fined or fired for not following company policy or local government regulations. Second, you should never work inside CRT monitors. Due to the high voltage they carry, the potential for electrical shock if handled improperly, the heavy lead content in their construction, and the risk of glass shards if the screen is broken, proper handling and disposal are crucial.

This was a shorter chapter, but it is very important for your livelihood and for the well-being of the computers you work on. Make it a point to always practice good safety procedures!

Chapter 60

Environmental Controls

This chapter covers the following A+ 220-1202 exam objective:

- **4.5** – Summarize environmental impacts and local environmental controls.

Environmental factors vary from one organization to the next. For the exam, you need to know how to control temperature and humidity, and why, what an MSDS is and how to use it, and how to deal with dust and debris when it comes to computers. You should also have a basic understanding of some of the procedures that a typical organization puts into practice to meet government-based guidelines and regulations.

ExamAlert

Objective 4.5 focuses on material safety data sheet (MSDS) documentation for handling and disposal; temperature, humidity-level awareness, and proper ventilation; and power surges, brownouts (under-voltage events), and blackouts (power failures).

Temperature, Humidity, and Air

You should be aware of the temperature and humidity measurements in your building. You should also think about airborne particles and proper

ventilation. Collectively, the Occupational Safety and Health Administration (OSHA) refers to the removal of air contaminants and/or the control of room temperature and humidity as “air treatment.” Although there is no specific government policy regarding air treatment, there are recommendations, including a temperature range of 68 to 76 degrees Fahrenheit (20 to 24 degrees Celsius) and a humidity range of between 20 and 60 percent. Remember, the higher the humidity, the less chance of electrostatic discharge, but it might get a bit uncomfortable for your coworkers; they might not want to work in a rainforest, so a compromise will have to be sought. If your organization uses air handlers to heat, cool, and move the air, it will be somewhat difficult to keep the humidity any higher than 25 to 30 percent. That brings us to ventilation. An organization should implement 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.

Note

Remember to always keep up with air quality recommendations from Occupational Safety and Health Administration (OSHA) and the Environmental Protection Agency (EPA).

OSHA air quality recommendations: https://www.osha.gov/sites/default/files/publications/3430indoor-air-quality-sm.pdf

EPA air quality recommendations: https://www.epa.gov/indoor-air-quality-iaq

For air treatment, organizations should make use of filtration devices, electronic cleaners, and possibly chemical treatments activated with charcoal or other sorbents (materials used to absorb unwanted gases). Most filtration systems make use of charcoal and high-efficiency particulate air (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. For environments that still have a

considerable number of airborne particles, you can purchase portable air filtration enclosures that also use charcoal and HEPA filters; you can also utilize ultraviolet light to eliminate germs. These solutions are commonly found in PC repair facilities due to the amount of dust, debris, and dirt sitting in PCs that are waiting for repair. Some organizations even foot the bill for masks or respirators for their employees. Many PC workbenches are equipped with compressed air systems and vacuum systems (incorporating HEPA filters) that PC techs can use to blow out the dust and dirt from a computer and vacuum it up at the same time. Otherwise, it is usually best to take a computer outside to work on it, especially when first opening it (except in windy conditions).

ExamAlert

Protect yourself from airborne particles with air filtration masks and goggles!

MSDS and Disposal

Products that use chemicals require a material safety data sheet (MSDS), which is a document that gives information about particular substances (for example, the ink in inkjet cartridges). Information in an MSDS includes

- Proper treatment if the substance is ingested or comes into contact with the skin
- How to deal with spills and other hazards
- How to dispose of the substance
- How to store the substance

It’s easy to find MSDSs; most companies have them online. You can search for them at a manufacturer’s website or by using a search engine. An MSDS identifies a chemical substance and its possible hazards, firefighting measures, handling and storage, and so on. Most MSDSs are available in PDF format.

It's important to know what to do if someone is adversely affected by a product that contains chemicals. A person might have skin irritation due to coming into contact with toner particles or with a cleaner that was used on a keyboard or mouse. As a technician, you are responsible for finding out how to help the person. If you do not have direct access to the MSDS, you should contact your 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. It's better to review all MSDS documents and be proactive, but in cases where you don't have access to the document, you need to collaborate with the facilities department to get the person who was affected the proper first aid and, if necessary, take the person to the emergency room. Finally, remove the affected device (such as a keyboard or mouse). Replace it with a similar device until you can get the original device cleaned properly.

ExamAlert

Know that an MSDS contains warnings and safety information about chemical substances and hazards.

Generally, substances that contain chemicals should be stored in a cool, dry place, away from sunlight. *Cool* means the lower end of the OSHA guideline, approximately 68 degrees F (20 degrees C). Often, this will be in a storage closet away from the general work area and outside the air filtration system. Following this guideline also allows the items to be stored in a less humid area.

Recycling and proper disposal are also important. Batteries should not be thrown away with normal trash because they contain chemicals. First, you should check your local municipal or EPA guidelines for proper disposal of batteries; in some cases, you will find that there are drop-off areas for them —either at the town municipal center or sometimes at office and computer supply stores. This guidance applies to alkaline, lithium (for example, CR2032), lithium-ion, and other types of batteries.

ExamAlert

Check your local municipal and EPA guidelines for information on disposal of batteries, printer toner, and other assets/equipment.

Ink and toner cartridges can usually be sent back to the manufacturer, or office supply stores and printer repair outfits often take them for recycling. Some municipalities have a method for recycling electrical devices in general.

ExamAlert

Toner cartridges should be recycled. Recycling centers will take old toner cartridges and properly dispose of them. The toner itself is a carcinogen, and the cartridges can contain heavy metals that are really bad for the environment. Remember that toner cartridges should be disposed of properly by recycling or returning them to the manufacturer. It's not recommended to throw toner cartridges in the trash.

With regard to recycling and disposal, cell phones, smartphones, and tablets also should be disposed of properly. However, unlike the other devices we have described so far, these devices contain data. Internal memory, SD cards, and SIMs should be wiped and, if necessary, destroyed (as described in Chapter 50, "Data Destruction and Disposal"). If a device is destroyed, the remains need to be recycled by the vendor that provided the destruction services or by the organization, in accordance with municipal guidelines. Phones and tablets that have been wiped properly—but not destroyed—might also be donated to various charities or given to electronics recycling companies or recycled at a community-wide recycling event.

Note

Some companies have policies that require that you get a certificate of destruction (CoD) when having company assets recycled by a professional shredding or recycling company. A CoD confirms that data on paper, hard drives, or other media has been destroyed. It's required by many businesses and organizations to comply with privacy laws.

Power Devices

Many of the issues that you see concerning power are due to lack of protection and improper planning, and you will see several questions on the A+ exam regarding this subject.

Utilizing proper power devices is part of a good preventive maintenance plan and helps protect a computer. You need to protect against several things:

- Surges
- Spikes
- Sags
- Under-voltage events
- Power outages

A *surge* in electrical power means that there is an unexpected increase in the amount of voltage provided. This can be a small increase or a larger, sudden increase, known as a spike. A *spike* is a short transient in voltage that can be due to a short circuit, tripped circuit breaker, power outage, or lightning strike.

A *sag* is an unexpected decrease in the amount of voltage provided. Typically, sags are limited in time and in the decrease in voltage. However, when voltage reduces further, an under-voltage event could ensue. During an *under-voltage event*, the voltage drops to such an extent that it typically causes the lights to dim and causes computers to shut off. This reduction in

power can be damaging to devices that aren't properly protected. This is typically termed a *brownout*.

A *power failure* (blackout) is a total loss of power for a prolonged period. A problem associated with power failures is the spike that can occur when power is restored. In some areas, it is common to have an increased number of tech support calls during July related to lightning storms! Quite often the issues are due to improper protection.

ExamAlert

A power surge is an unexpected increase in voltage. A brownout (an under-voltage event) is a drop in voltage that can cause computers to shut off. A blackout (power failure) is a total loss of power for a prolonged time.

Some power devices have specific purposes, and others can protect against more than one of these electrical issues. Let's examine a few of these devices.

Surge Protectors

A *surge protector*, or *surge suppressor*, is a power strip that also incorporates a metal-oxide varistor (MOV) to protect against surges and spikes. Most power strips that you find in office supply stores or home improvement stores have surge protection capability. The word *varistor* is a blend of the terms *variable* and *resistor*.

ExamAlert

To protect against surges and spikes, use a surge protector!

Surge protectors are usually rated in joules, which measure energy; essentially, the more joules, the better. For computer systems, 1000 joules

or more are recommended. This joule rating gives you a sense of how long the device can protect against surges and spikes. Surges happen more often than you might think, and every time a surge happens, part of the varistor is burned out. The higher the joule rating, the longer the varistor (and therefore the device) should last. Most of today's surge protectors have an indicator light that informs you if the varistor has failed.

Because surges can occur over telephone lines, RG-6 cable lines, and network lines, it is common to see input and output ports for any or all of these on a decent surge protector. Higher-quality surge protectors have multiple MOVs not only for the different connections (such as AC and phones) but for the individual wires in an AC connection.

Uninterruptible Power Supplies

An *uninterruptible power supply (UPS)* combines the functionality of a surge suppressor with a *battery backup*. A UPS protects a computer not only from surges and spikes but also from sags, brownouts (under-voltage events), and blackouts (power failures).

ExamAlert

Remember to use a UPS/battery backup to protect your computer from power outages! It can keep your computer running long enough to save your work and properly shut down the computer, if necessary. Know the difference between a UPS and a surge protector/suppressor for the exam!

But a battery backup can't last indefinitely! It is considered emergency power and typically keeps your computer system running for 5 to 30 minutes, depending on the model you purchase and the load being placed on the UPS. Workstation UPSs often have two types of outlets on the device: one group that is marked for battery backup and surge protection and one that is marked for surge protection only. Server room rack-mountable UPSs often only have battery backup outlets.

Most UPS devices also act as line conditioners, protecting from over- and under-voltage; they condition (or regulate) the voltage sent to the computer. If you happen to see a customer's lights flickering, this could indicate dirty power, and you should consider recommending a UPS for the customer's computers and networking equipment. If there is an alternating current (AC) failure, and the UPS stops receiving power from the AC outlet, the UPS monitoring program identifies the problem, either by beeping or with an LED visual indicator. Most UPS devices today have a USB-based connection so that your computer can communicate with the UPS. When a power outage occurs, the UPS sends a signal to the computer, telling it to shut down, suspend, or stand by before the battery discharges completely. Most UPSs come with software that you can install that enables you to configure the computer with these options.

The output power capacity of UPS devices is rated in volt-amps (VA) and watts. Although you might have heard that volt-amps and watts are essentially the same, they are somewhat different. The volt-amp rating is slightly higher due to the difference between apparent power (when in battery backup mode) and real power (when pulling regular power from the AC outlet). For example, a typical UPS device might have a volt-amp rating of 350 VA but a wattage rating of 200 watts. Generally, this is enough for a computer, a monitor, and a few other devices, but a second computer might be pushing it with this wattage rating. The more devices that connect to a UPS, the shorter the battery lasts if a power outage occurs; if too many devices are connected, there might be inconsistencies when the battery needs to take over. Thus, many manufacturers limit the number of battery backup-protected receptacles on a UPS. Connecting a laser printer to a UPS is not recommended due to the high current draw of the laser printer; also, to protect a UPS from being overloaded, never connect a surge protector or power strip to one of the receptacles in a UPS.

ExamAlert

Do *not* connect laser printers to UPS devices. Most UPS units are not designed to handle the high peak power surges of a laser printer during its fuser warm-up phase.

A UPS has a battery (often lead-acid) that, when discharged, requires several hours to recharge. This battery is usually shipped in a disconnected state. Before charging the device for use, you must first either flip over the battery or otherwise make sure that the battery leads connect to the UPS. If the battery ever needs to be replaced, a red light usually appears and is accompanied by a beeping sound. Beeping can also occur if power is no longer supplied to the UPS by the AC outlet.

The "power" of a UPS can't be denied. It is a required component in server rooms and is very useful at users' computers as well, especially custom workstations. It's interesting to note that most power outages last for 15 minutes or less; often they are short blips. To continue using a desktop computer during a power outage of any length, the user needs to have not only the computer but also the monitor and some peripherals connected to the battery backup outlets of the UPS.

ExamAlert

For custom workstations, make sure that computers, monitors, and powered USB hubs are all plugged into the UPS.

Cram Quiz

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

1. What document can aid you if a chemical spill occurs?

- ○ **A.** HEPA
- ○ **B.** MSDS
- ○ **C.** OSHA
- ○ **D.** EPA

2. A coworker complains that after the cleaning crew has come through, the keyboard irritates his hands and leaves some green residue. What should you do?

- ○ **A.** Call the fire department.
- ○ **B.** Contact the facilities department.
- ○ **C.** Contact the manufacturer of the keyboard.
- ○ **D.** Call OSHA and complain.

3. You are concerned with power outages that occur infrequently and for short periods of time. You don't want your users' computers to suffer from potentially harmful restarts. What device should you install for the users' computers?

- ○ **A.** Surge protector
- ○ **B.** Line conditioner
- ○ **C.** MSDS
- ○ **D.** UPS

4. What is the term for a total loss of power that lasts for a prolonged period?

- ○ **A.** Power failure (blackout)
- ○ **B.** Surge
- ○ **C.** Spike
- ○ **D.** Under-voltage event (brownout)

5. You want a *cost-effective* solution to the common surges that can affect your computer. Which device offers the best solution?

- ○ **A.** UPS
- ○ **B.** Surge suppressor
- ○ **C.** Power strip
- ○ **D.** Rack grounding

Cram Quiz Answers

1. **B.** A material safety data sheet (MSDS) defines exactly what a particular chemical substance is, what its potential hazards are, and how to deal with those hazards. HEPA stands for high-efficiency particulate air, as in a HEPA filter. OSHA stands for Occupational Safety and Health Administration. EPA stands for Environmental Protection Agency.

2. **B.** Contact the facilities department to see if it has the MSDS for the cleaner. You and/or the facilities department should then treat the irritation according to the MSDS. If this does not work and the problem gets worse, take the coworker to the emergency room. Remove the keyboard from the work environment.

3. **D.** Use an uninterruptible power supply (UPS) to protect a computer from ungraceful shutdowns and restarts that can occur as a result of under-voltage events (brownouts), power failures (blackouts), and other AC failures—which the UPS will monitor for. A surge protector (suppressor) is a power strip that also incorporates a metal-oxide varistor (MOV) to protect against surges and spikes. A line conditioner can level out dirty power but won't protect against a power outage. An MSDS defines what a particular chemical substance is and how to deal with related hazards.

4. **A.** A power failure (blackout) is a total loss of power for a prolonged period. The best protection against power failures is either a UPS (battery backup) or a generator. A surge in electrical power means that there is an unexpected increase in the amount of voltage provided. This can be a small increase or a larger increase, known as a spike—which is a *short* transient in voltage. An under-voltage event (brownout) is a drop in voltage (but not to zero) that can cause computers to shut off. It could be prolonged but is not a complete loss of power.

5. **B.** A surge suppressor (or surge protector) is the right solution at the right price. A UPS is a possible solution but costs more than a

surge protector and is not necessary in this scenario. A power strip doesn't necessarily have surge protection functionality; it is simply a strip of outlets for additional connectivity. Rack grounding is done to protect networking equipment and servers that are installed into racks in a data center or server room.

This chapter and the preceding one were all about health, safety, recycling, and the environment—in essence, protection. You need to protect yourself, your coworkers, the organization's data and systems, and the environment. Do this, and you will have made the world a better place. Continue!

Chapter 61

Incident Response, Communication, and Professionalism

This chapter covers the following A+ 220-1202 exam objectives:

- **4.6** – Explain the importance of prohibited content/activity and privacy, licensing, and policy concepts.
- **4.7** – Given a scenario, use proper communication techniques and professionalism.

How will you respond to incidents? How will you communicate with customers? How will you deal with the best practices, regulations, and laws that your organization complies with? We'll answer these questions and more as we progress through this chapter.

A good technician not only knows how to work with technology but also how to deal with customers, tough problems, and imminent threats. It's the well-rounded technician who enjoys the most job security.

Understanding the Importance of Prohibited Content/Activity and Privacy, Licensing, and Policy Concepts

ExamAlert

Objective 4.6 concentrates on the following: incident response, licensing/DRM/EULA, NDA/MNDA, regulated data, AUP, and regulatory and business compliance requirements.

One of the goals of policies and procedures, best practices, and regulations is to prevent incidents from occurring. However, it is inevitable that incidents will happen. People are imperfect and we create imperfect technologies. When the right criteria are met, small imperfections can pave the way for incidents to transpire. How we respond to these incidents and how we limit the damage are both important.

Incident Response

We need to differentiate between an event and an incident. An *event* is simply something that happens within a computer or on a network. It could be good or bad. For example, an event could be an administrator connecting a system to another system through a mapped network drive according to the organization's procedures. This is an occurrence that is positive. But there are adverse events as well, where negative consequences result—for example, unauthorized privilege escalation or execution of malware. Rev it up further to the computer security *incident*, which is an imminent threat or an outright violation of security policies and a security breach. An example of an incident is an attacker initiating a DDoS attack against a server, perhaps causing that server to crash. Another example is an attacker locking files on a computer with ransomware. A technician or a team of technicians is expected to respond to incidents quickly and efficiently.

How you follow up on an incident is a good measure of your value to an organization. Incident response is a set of procedures that an investigator follows when examining a technology incident. How you first respond, how you document the situation, and your ability to establish a chain of custody are all important to your investigation skills.

First Response

When you first respond to an incident, your first task is to identify exactly what happened. You must recognize whether the incident is a simple problem that requires troubleshooting or whether it needs to be escalated. For example, if you encounter a person who has prohibited content on a computer, this would be considered an incident, and you will be expected to escalate the issue to your supervisor (and law enforcement, if necessary) and report on exactly what you have found. Copyrighted information, malware, inappropriate content, and stolen information could all be considered prohibited. So, before you do anything else, you should report your findings to the proper channels and then make sure the data and affected devices are preserved. Your involvement could mean making a backup of the computer's image/storage drive and making sure the integrity of the data is preserved for future reference or as proof. Exactly what you do at this stage will depend on your organization's policies. Depending on the scenario, you might be told to leave everything as is and wait for a computer forensics expert or a security analyst. The idea here is that the scene will be preserved so that the expert can collect evidence.

Pay attention to the order of volatility, which defines which evidence is the most and least stable. For instance, RAM is the least stable evidence because it would be erased if the device were powered off; data on archived media is much less volatile because it is already in a stable, offline format. The Internet Engineering Task Force (IETF) has guidelines in its document "Guidelines for Evidence Collection and Archiving" at https://www.ietf.org/rfc/rfc3227.txt.

ExamAlert

As a first responder, you identify an incident, report through the proper channels and escalate if necessary, ensure data/device preservation, and document everything!

Remember: Documentation Is Key

The bottom line is this: When an incident occurs, you need to document everything that you find and anything that happens after that. If your organization doesn't have any other methodology, write it down! When you leave the scene, you will be required to divulge all information to your supervisor. If you fixed the problem and no other specialists were required, the documentation process will continue through to the completion of the task and beyond when you monitor the system. You should also document any processes, procedures, and user training that might be necessary in the future.

Incident Response Life Cycle

Let's take this discussion a bit further and examine the computer security incident response. Different organizations have different views on how incident response should be handled. One common method is to incorporate a four-phase life cycle:

1. **Preparation:** An organization with a well-planned incident response procedure, a strong security posture, and a knowledgeable chief information security officer (CISO) will be able to limit damage caused during an incident. Good communication is required, and you, the technician, should have access to secure storage facilities, digital forensic workstations, forensic software, and plenty of documentation.
2. **Detection and analysis:** This stage includes the identification of exactly what is happening during the incident. Because there are literally thousands of attack vectors (and perhaps many more), you can't create step-by-step procedures for every type of incident. However, you can categorize incidents to a certain extent and then take the appropriate steps based on the type of incident you have detected. For example, categories could include DDoS/brute-force attacks, web-based attacks, spoofing/on-path (aka MITM) attacks, and theft. Once you know what an attack is, you can analyze it using the right tools and methods. Of course, you will need to do a certain amount of thinking on your feet; as a technician, you should be ready to adjust your mindset and methodologies in real time. However, the process has to be quick so that you can contain the problem rapidly.
3. **Containment, eradication, and recovery:** Next, isolate the problem: Quarantine systems, isolate networks, place attackers' processes in padded cells or other holding areas (if at all possible), remove devices,

and so on. Then you need to remove the threat by using other mitigation techniques. After that, you can retrieve data, re-enable systems, and recover images and backups. Some organizations break this stage into multiple phases.

4. **Post-incident activity:** During this stage, you review what happened and why, finalize documentation, get signatures, and contemplate, with your team, the lessons learned.

> **Note**
>
> This life cycle is documented in great detail in NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final.
>
> The CompTIA A+ exam won't go far into the depths of this document, but if you are interested in a career that involves incident response, consider reading this document and have it on hand.

Remember that an organization might use phases or break them up differently. In addition, an organization will describe its incident response process in much greater detail than what is shown here. Be ready to study your organization's documentation carefully!

Chain of Custody

If you are required to preserve evidence, one way to do it is to set up a *chain of custody*—a chronological documentation or paper trail of evidence. In accordance with company policy, the chain of custody should be initiated at the start of any investigation. It documents who had custody of the evidence all the way up to litigation (if necessary) and logs the transfer of evidence from person to person. It also verifies that the evidence has not been modified or tampered with. The log should include identifying information for systems such as serial numbers, IP addresses, MAC addresses, and so on; the names, titles, and phone numbers of everyone who collects, analyzes, and handles evidence; the time and date (traditionally in

coordinated universal time, but if not, be sure to list the time zone); and where and how evidence is stored.

ExamAlert

The chain of custody is a chronological, verifiable paper trail documenting who has possessed evidence.

As an A+ tech, you will probably not get too involved with incident investigations, but you should know the basic concepts of first response, documentation, and chain of custody for the exam—and in case you find yourself in a real-life situation where you have found prohibited content or illegal activities. The bottom line is that many times your job will be to escalate the issue to the appropriate personnel.

ExamAlert

For the exam, remember that incident response includes maintaining the chain of custody, informing management/law enforcement as necessary, making a copy of the drive (data integrity and preservation), keeping incident documentation, and paying attention to the order of volatility.

Licensing/DRM/EULA

There are various types of licensing for software, hardware, support, and services. Let's focus on software licensing here. Licensing could be free or might need to be paid for. For example, we mentioned Microsoft Windows client licenses previously in the book. A license is considered to be valid (nonexpired) as long as its expiration date has not passed; many Windows licenses that come with devices are perpetual and do not need to be renewed (and thus do not have expiration dates at all) but are instead tied to the original device (nontransferrable). It's important to have licensing information well organized and accessible. Most proof of licensing today is

digital, and it should be stored in a safe place (possibly encrypted), backed up, and digitally validated.

ExamAlert

A valid license is any software license that is current and not counterfeit. A perpetual (or nonexpiring) license is one that can be purchased for a software product. Many video games often use this license model. You purchase the software and have the right to use the software for life. Software vendors that use perpetual licensing will also offer software upgrades or patches for the first year, and any upgrades after the first year are generally covered under a support or maintenance fee.

Licensing is important during incident response. Depending on the situation, you might need to locate valid licenses (or lack thereof) for software, client connections, and hardware. For example, you might need to be able to locate the client access licenses (CALs) being used to access a Windows server. License compliance violation can have legal ramifications, as well as availability and integrity repercussions.

There are two terms related to licensing that you should know for the exam:

- **EULA:** An end-user licensing agreement (EULA) is a contract or an agreement between a proprietary software vendor and an end user. In most cases, the end user is required to agree to the EULA before using the product. The EULA defines the ways that the software can be used and asserts that the vendor has limited liability for issues and damages that occur through the use of the product. EULAs are usually lengthy documents, but if a company plans to use software products that require a EULA, the appropriate personnel should have a working legal understanding of these agreements.
- **DRM:** Digital rights management (DRM) is a group of security controls designed to restrict the usage or proliferation of copyrighted software and products. For example, various DRM controls can prevent illegal copying of software.

ExamAlert

EULA is a licensing agreement between a software vendor and an end user. DRM restricts usage or proliferation of copyrighted software and products.

Essentially, if you, as a technician, find that a user or company is illegally copying, circumventing, or modifying software; is using software without the appropriate licensing; or is otherwise breaching the EULA or DRM agreement, you should report that finding to the appropriate personnel or authorities and log and document the situation in accordance with incident response procedures.

Software licenses can be commercial—for example, licenses for Microsoft or Apple software—or open source, as is the case with the GNU General Public License (GPL) for Linux software. In the case of commercial or closed-source licensing, the user or organization using the software is usually not allowed to share or modify the software. Some software is covered under a Creative Commons license, which allows for some open sharing and redistribution with certain restrictions, often surrounding commercial use. If you are using a piece of software or an image with a Creative Commons license, be sure to check which type of license it is released under to ensure that you are not violating the terms.

There are also personal and enterprise-level licenses. For example, a home user might have a computer with a paid personal license to use Microsoft Windows 11 Home Edition, but a midsized to large organization will have corporate-use licenses (such as for Windows 11 Enterprise Edition) that are usually bought in bulk.

Software with open-source licensing is usually free to use. With open-source licensing, the user is allowed to study, modify, and share the software or even create new distributions of it and sell it for a profit. Table 61.1 summarizes the common license types.

TABLE 61.1 **Common License Types**

License	Use
Perpetual	Provides permission to use a piece of software (or other intellectual property) for the life of the product. These licenses do not need to be renewed.
Personal-use	Licenses software to a person for their personal use but not for business purposes.
Corporate-use	Licenses software for businesses. Even small businesses need to get this type of license for their software. Often they come with additional support and can be purchased in bulk.
Open-source	Provides permission to download software for free, and the user is allowed to modify and share the software as needed, with restrictions on making money from any modifications (those restrictions vary depending on the open-source license).

ExamAlert

Know what a valid license is. Know what a perpetual license agreement is. Know the difference between open-source and commercial licenses. And know the difference between personal licenses and corporate-use licenses.

Be sure to organize and store licensing information properly, according to organizational policy, and know how to find licenses for your own organization or for a customer if you are contracted to perform work for a customer. Software should be managed and organized with a configuration management database, as discussed in Chapter 57, "Documentation."

Note

In addition to Chapter 57, you can also check out the following:

Microsoft's Software Asset Management (SAM) guide: www.microsoft.com/en-us/download/details.aspx?id=31382

License Manager by License Dashboard:
www.licensedashboard.com

FlexNet Manager by Flexera Software:
https://www.flexera.com/products/flexnet-manager

NDA/MNDA

Nondisclosure agreements (NDAs) bind individuals from sharing sensitive information with others. They protect sensitive information, obligating the recipient to keep the information confidential and not disclose it to others. Sometimes known as confidentiality agreements, these are common in business and government and are important tools enabling businesses, consultants, and contractors to do their jobs without worrying about corporate espionage and leaks of trade secrets and other sensitive information.

Generally, there are two parties to an NDA: the disclosing party, who owns the data, and the receiving party, who will receive the information. The NDA will clearly define which information is confidential and any exclusions, as well as the obligations of the receiving party to keep the information secret and use it only for the intended purpose. It also defines the duration during which the information will remain in effect and any consequences of breach of confidentiality.

ExamAlert

A nondisclosure agreement (NDA) is a legally binding document that organizations might require of both their own employees and anyone else who comes into contact with confidential information. This can include vendors, consultants, and contractors. The purpose of an NDA is to protect an organization's intellectual property and trade secrets.

A *mutual nondisclosure agreement (MNDA)* is a form of NDA where both parties share data and commit to mutual nondisclosure. Whereas an NDA will protect one entity, an MNDA protects both sides, with both sides having their intellectual property protected from the other. These tools often include dispute resolution procedures and remedies for breaches, safeguarding interests for both parties as they build trust, cooperation, and fairness for all sides. They are often used when developing long-term partnerships.

ExamAlert

A mutual nondisclosure agreement (MNDA) is a legal agreement in which both parties agree to protect each other's confidential information. Whereas an NDA imposes confidentiality obligations on just one party, an MNDA imposes these obligations equally on both parties. The main difference between these two types of NDAs lies in the reciprocity of the MNDA.

Regulated Data

Several types of data regulations are covered on the A+ exam. These regulations are designed to protect personal information and people. Here we'll briefly discuss PII, PHI, PCI-DSS, and GDPR.

Note

It is not uncommon for screens containing regulated data, and sometimes entire systems that are connected to networks containing regulated data, to use splash screens—the initial screens that appear upon login or upon access to devices and services. These splash screens serve as a reminder that the information is privileged and should be used only with permission and under the rules set by the owners.

PII

Personally identifiable information (PII) is something that every organization and technician should be concerned with because it affects us all. PII is information used to uniquely identify, contact, or locate a person. This type of information could be a name, birthday, Social Security number, biometric information, and so on. Many laws, regulations, and guidelines exist that are designed to protect PII in a standardized way. However, organizations often have their own privacy policies (which may be based on these best practices) that go further to define how users' identities will be protected in a procedural manner.

An example of PII is personal government-issued information/identification. In the United States, this includes birth certificates, Social Security cards, driver's licenses, non-driver ID cards, passports, permanent resident cards, municipal ID cards, and individual taxpayer ID numbers. There are a lot of ways that a person can be identified, and therefore, there is a lot of information that needs to be protected and secured.

ExamAlert

Remember that personally identifiable information (PII) is information about a person that contains some unique identifier from which the identity of the person can be determined.

PHI

Protected health information (PHI) is information that is protected under the HIPAA Privacy Rule. The Health Insurance Portability and Accountability Act (HIPAA) is a wide-ranging act, passed in 1996, that governs the protection of all kinds of health information. Any organization in the United States that requests, stores, or accesses health information must abide by the rules within HIPAA.

Best practices for PII and PHI are quite similar, so let's discuss a couple of them as they relate to digital records:

- Appoint a security admin (with compliance experience) to oversee the access and storage techniques used for PII and PHI records.
- Physically secure computers, servers, server rooms, data centers, and network connections where records are being stored.
- Store records in an encrypted format and transmit records from one system to another or from a system to or from the cloud using end-to-end encrypted sessions. This way, data at rest, data in transit, and data in use can be protected.

In addition, make use of the many security best practices that we have documented within this book's security chapters and keep in mind that PII and PHI records are at the top of the list when it comes to logging, auditing, and monitoring.

ExamAlert

Remember that protected health information (PHI) is any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service such as treatment or diagnosis. It is protected under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.

PCI-DSS

The payment card industry (PCI) encompasses anything that concerns credit cards, debit cards, ATMs, point-of-sale (POS) machines, and so on, that organizations use or transact with when dealing with user cardholder data. The PCI Security Standards Council (PCI-SSC) developed a compliance program known as the *Payment Card Industry Data Security Standards (PCI-DSS)*. These standards, and the varying levels of compliance, define how credit card data is to be transacted and stored. These data retention

requirements change over time, so organizations should pay close attention to any changes. As a general rule, destroy all sensitive and credit card data as soon as it is no longer required legally. See the links and references in the note that follows to keep up to date on the latest PCI-DSS changes.

The best practices for PCI-DSS include a lot of the security methods we have discussed previously in this book, but from a more high-level viewpoint, the PCI-SSC is looking for a sustainable security program; compliant policies and procedures; performance metrics (such as those defined in NIST SP 800-55 Rev. 1, Performance Measurement Guide for Information Security); specific assignments to qualified personnel (perhaps who certify to PCI-DSS); proper risk assessment and management techniques; monitoring of security controls (which is a big part of the compliance); maintaining of evidence; incident response procedures; and general maintenance of security awareness.

PCI-DSS is important whether your organization is a five-employee office or an enterprise-level corporation.

Note

You can view the entire best practices document (updated to version 2.0 in 2019) as set forth by the PCI-SSC at https://www.pcisecuritystandards.org/documents/PCI_DSS_V2.0_Best_Practices_for_Maintaining_PCI_DSS_Compliance.pdf. The PCI DSS compliance standards, updated frequently, can be found at https://www.pcisecuritystandards.org/standards/pci-dss/; as of this writing (spring 2025), the latest version was released in March 2025.

ExamAlert

Remember that the Payment Card Industry Data Security Standard (PCI-DSS) is designed to reduce fraud and protect customer credit card information.

GDPR

The General Data Protection Regulation (GDPR) is a European Union (EU) regulation that deals with data protection and privacy for people who live in the EU. However, it has wide-ranging implications for companies around the world (especially in the United States) that have transactions with EU citizens, requiring them to adopt policies and best practices that support the regulation. One common example of an industry that was "turned upside down" by GDPR is the email/mailing list industry. These lists contain personal data—meaning information related to an identified or identifiable natural person—and in many cases the way that data was handled was not compliant with the GDPR. The GDPR defines how transparency should function, the proper securing of data, the awareness of what data is being collected, and citizen rights such as the right to access and request erasure of personal data. This regulation was enforceable as of May 25, 2018, and at the time, it seemed that technical changes, written policies, and proper opt-in/opt-out lists became realities almost overnight for many companies. The GDPR affects every single company that we deal with.

Note

The General Data Protection Regulation (GDPR) defines the *data controller* as "a natural or legal person, which alone or jointly with others, determines the purposes and means of personal data processing." This role is essentially the manager of personal data. The GDPR states that those who process personal data on behalf of the data controller are known as the *data processors*. *Data owners* determine the level of classification for their data, and the *data custodian/steward* implements the classification and security controls for the data. Knowing that, you may fall into one of these categories at some point in your career without realizing it, so understanding GPDR is important.

ExamAlert

Know the types of regulated data and related concepts, including PII, PHI, PCI-DSS, and GDPR.

GDPR best practices are similar to what we have mentioned already in this chapter, and the security methods include much of what we have discussed in the security sections of this book. These best practices focus on auditing the data; securely managing data; assessing the risk of data that is stored; assigning a data protection officer (for companies with 250 employees or more); training employees about GDPR best practices; and having in place a data breach and incident response plan.

Note

For more information on the GDPR, see https://ec.europa.eu/info/law/law-topic/data-protection_en.

Don't Be Too Alarmed by Data Regulations!

As an A+ technician, you should know what data regulations and best practices are and should be ready to abide by them when employed by an organization. However, the simple truth is that most A+ technicians will have very little to do with the creation, modification, or enforcement of these regulations. The bottom line is that you should concentrate on identifying the threat model for your organization's data and implement strong security measures that hopefully will prevent data breaches, while monitoring the data carefully for any changes, anomalies, or attacks. If you are ever confused by a regulation, best practice, or written organizational policy, see the appropriate compliance or human resources personnel to get the record straight.

AUP

An *acceptable use policy (AUP)* is a set of rules or guidelines that define what is and is not acceptable when using an organization's technology resources, including their computers, network, and other systems. Some organizations have very formal policies that employees must sign as part of their onboarding (hiring) process and periodically thereafter. Oftentimes

these are also provided, in whole or in part, on splash screens when logging in to systems. Other organizations have less formal AUP processes. Either way, these policies govern what is acceptable and what is not acceptable on the equipment and data networks of the organization.

Generally, the following items are included in an AUP:

- **Network usage:** How employees can access and use the company network and Internet
- **Device usage:** How employees use company-provided or personal devices
- **Software and intellectual property:** Guidelines for installing, using, and protecting software and intellectual property
- **Email and communications:** Rules for using email and other communication platforms such as Microsoft Teams, Zoom, and Google Meet
- **Data security and privacy:** How to protect sensitive information and help ensure compliance with data privacy regulations

AUPs help ensure security, compliance, and legal protection for an organization and its employees while also providing clarity, ensuring productivity, and offering a fair allocation of resources.

Read through the AUP at your organization. Pay attention to how it protects the organization, the employee, and the electronic assets that everyone uses.

ExamAlert

An organization's acceptable use policy (AUP) provides details that specify what users may do with their network access. Such rules help protect the organization's data and guard against legal liability. An AUP provides specific detail about what users may do with their network access, including email and instant messaging usage for personal purposes, limitations on access times, and the storage space available to each user. New employees to an organization are often required to sign an AUP during the onboarding (hiring) process.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading the first part of this chapter again.

1. You find illegal materials on a customer's computer. Your boss commands you to preserve computer evidence until arriving on the scene. What is your boss asking you to begin?

   - ○ **A.** Documentation
   - ○ **B.** Chain of custody
   - ○ **C.** First response
   - ○ **D.** GDPR compliance

2. Which of the following is not one of the steps of the incident response process?

   - ○ **A.** Eradication
   - ○ **B.** Recovery
   - ○ **C.** Containment
   - ○ **D.** Nonrepudiation

3. Which of these is a group of security controls designed to restrict the usage or proliferation of copyrighted software and products?

   - ○ **A.** EULA
   - ○ **B.** Personal use license
   - ○ **C.** DRM
   - ○ **D.** Corporate use license

4. You are the security administrator for your organization. You have just identified a malware incident. Of the following, what should be your first response?

- ○ **A.** Containment
- ○ **B.** Removal
- ○ **C.** Recovery
- ○ **D.** Monitoring

5. Which type of regulated data is specifically protected under the HIPAA Privacy Rule?

- ○ **A.** PII
- ○ **B.** PCI
- ○ **C.** GDPR
- ○ **D.** PHI

6. A company asks you to sign an NDA before showing you company information. Why is the company asking you to sign the document?

- ○ **A.** The company is going to show you illegal information.
- ○ **B.** The company is going to show you confidential information it wants to keep secret.
- ○ **C.** The company wants to collect your Social Security number.
- ○ **D.** The company wants to hire you.

7. Which of the following would typically be included in an acceptable use policy (AUP) for an organization?

- ○ **A.** Permission to share company data with external parties at will
- ○ **B.** Guidelines for ethical and responsible use of the organization's IT resources

- ○ **C.** Prohibition of personal use of the network
- ○ **D.** Requirement to use the organization's network for personal financial transactions

Cram Quiz Answers

1. **B.** Your boss is asking you to begin the process of a chain of custody, which is a chronological paper trail of evidence. It is a specific form of documentation. You were the first responder. These cases will be rare, but you should understand the terminology and what to do if you find illegal materials.

2. **D.** Nonrepudiation, although an important part of security, is not part of the incident response process. Nonrepudiation means that you have irrefutable proof that a person did something; it might include logs, audit trails, and so on. Eradication, containment, and recovery are all parts of the incident response process.

3. **C.** Digital rights management (DRM) is a group of security controls that restrict usage or proliferation of copyrighted software and products. An end-user licensing agreement (EULA) is a contract or an agreement between a proprietary software vendor and an end user. A personal use license is meant for one user. For example, a home user might have a computer with a paid personal use license to use Microsoft Windows 11 Home Edition. A midsized to large organization might have enterprise-level or corporate use licenses (such as for Windows 11 Enterprise Edition) that are usually bought in bulk.

4. **A.** Of the listed answers, most organizations' incident response procedures specify that containment of the malware incident should be first. Next would be the removal of the malware, then recovery of any damaged systems, and finally monitoring (which should actually be going on at all times). But before all of this is the preparation phase; in the scenario, identification was already performed.

5. **D.** Protected health information (PHI) is information that is protected under the HIPAA Privacy Rule. The Health Insurance Portability and Accountability Act (HIPAA) is a wide-ranging act that governs the protection of all kinds of health information. Personally identifiable information (PII) is information used to uniquely identify, contact, or locate a person. The payment card industry (PCI) encompasses anything that concerns credit cards, debit cards, ATMs, or point-of-sale (POS) machines. The General Data Protection Regulation (GDPR) is a European Union regulation that deals with data protection and privacy.

6. **B.** The purpose of a nondisclosure agreement (NDA) is to protect confidential information. The company is going to show you information, and it doesn't want you to share this information with others. It isn't illegal to do this, and the information is not illegal.

7. **B.** Acceptable use policies (AUPs) are all about what should and what should not be done on and with the company's electronic resources. Ethics and responsible use are paramount. If you read the other answers, they just don't make any sense at all.

Using Proper Communication Techniques and Professionalism

ExamAlert

Objective 4.7 focuses on the following: professional appearance and attire; using proper language and avoiding jargon, acronyms, and slang, when applicable; maintaining a positive attitude/projecting confidence; actively listening; taking notes; avoiding interrupting the customer; being culturally sensitive; being on time (and, if late, contacting the customer); avoiding distractions; dealing with difficult customers or situations; setting and meeting expectations/time lines and communicating status with the customer;

and dealing appropriately with customers' confidential and private materials.

Mind your customer service skills. You might be a super technician, but if you don't have people skills, your job market will be limited. By being professional and utilizing good communication skills, you increase the chances of receiving a good customer reaction. Also, these skills help you get to the heart of an issue and can help make you more efficient, saving time as you repair computer problems. Throughout the rest of the book, you have learned how to repair computers. If you put those abilities together with a professional demeanor and good communication skills, there should be no lack of new customers in your future.

Communication Techniques and Professionalism

For the CompTIA A+ 220-1202 exam, communication and professionalism consist of 11 categories:

- **Present a professional appearance and wear appropriate attire:** As they say, "dress for success!" The exact type of dress should be appropriate for the environment and situation. For example, formal dress might be required for a job interview. Formal dress in the workplace usually means a suit and tie for men and a business suit with pants or long skirt and jacket for women. The conventional colors for formal wear are black and navy blue. But this kind of ensemble isn't appropriate for other situations, such as day-to-day work at the office or fixing an end-user's cable Internet connection. In those scenarios (and many others), business casual is recommended. While there is no standard definition for business casual, we can cite some examples: for women, skirt or dress slacks, blouse, sweater, twinset, jacket, and closed-toe shoes; for men, shirt and tie with dress slacks or sweater with chinos, and dark socks and shoes. In many modern offices, business casual has become even more casual; men can forgo the tie and sweater and women the sweater, and both genders can often wear polo shirts. Keep in mind that a company might have its own dress code, which might specify uniforms or other specific requirements. If you aren't

sure, ask! Many HR departments and managers will gladly share what is considered appropriate for the company and might even list this information on a website or in the company portal.

- **Use proper language and avoid jargon, acronyms, and slang, when applicable:** Speak slowly, clearly, and professionally so the customer can fully understand what you are saying. Refrain from slang and profanity. Avoid computer jargon and acronyms (for example, WPA3 or TCP/IP) when working with nontechnical customers. If you use computer jargon, the customer might think that you are insecure and cannot clearly explain things. Stay away from techno-babble. The customer expects you to know these things technically but to explain them in a simple manner. That's the essence of a good teacher!

> **Note**
>
> Even if the customer hits you with something like this: "Hey, my VPN with static IP is using PPTP, but isn't that deprecated? And I really need DynDNS and a RADIUS right away!" you should still respond with as little technical jargon as possible. (This exchange really occurred, but you'll note that the customer didn't actually need DynDNS because they had a static IP address already.)

- **Maintain a positive attitude/project confidence:** Even if the customer thinks the situation is hopeless or the customer is frustrated, be positive. Sometimes problems that appear to be the worst have the easiest solutions! And there is always a solution. It's just a matter of finding that solution. Also, as part of being positive, try to project confidence. Be calm and assure your customer that the problem will be solved.
- **Actively listen (taking notes) and avoid interrupting the customer:** The more you listen, the better you will understand the problem. Write down key points related to the problem the customer is having. Don't interrupt the customer, even if you think you know what the problem is before the customer has fully explained the situation. Be respectful and allow the customer to completely explain the problem. The customer's

tale just might give you clues as to what the real problem is. Listen carefully and be assertive when eliciting answers.

- **Be culturally sensitive:** Understand that customers come from all walks of life. Be aware that cultural differences and similarities exist. Be respectful and kind. Use appropriate professional titles when applicable and when possible. Make an effort to ensure that you and the customer understand each other and work toward a common goal. If you don't at first understand the customer or if there is a language barrier, kindly ask the customer to repeat themselves.
- **Be on time (and, if late, contact the customer):** Be punctual! Be on time! If a customer has to wait, the situation might become difficult before you even begin. If you are running late, contact the customer, say you will be late, and apologize.
- **Avoid distractions:** While you are with a customer, phone calls should be screened and left to go to voicemail except in emergencies. The same goes for emails and text messages that arrive on your smartphone. If other customers call, explain to them that you are with a customer and will call them back shortly (or have your manager or coworker take care of them, if they are available). Avoid talking to coworkers when dealing with customers. The customer wants to feel valued and wants to get the problem fixed in a timely manner. Try to avoid personal interruptions in general. And avoid using social media sites while working with customers or to communicate about customers.
- **Appropriately deal with difficult customers or situations:** By being patient, understanding, and respectful, you show customers that you are a professional and are serious about fixing their computer problems. Never argue with customers or take a defensive or offensive stance. This is one of those times in which you might think of Mr. Spock. Approach customers' computer problems and complaints from a scientific point of view. Try not to make light of a customer's computer issues, no matter how simple they might seem, and avoid being judgmental about any possible user error. Try not to ask things such as "What did you do?" or "Who was working on this?" because these questions can come across as accusations. Ask computer-oriented, open-ended questions when eliciting answers from the customers (for

example, ask “What is wrong with the computer?” or “What can you tell me about this computer?”). Stick with the senses; questions such as “What type of strange behavior did you see from the computer?” keep customers more relaxed and can help you narrow down the cause of the problem. Again, if a customer doesn’t come across clearly, restate what you believe to be the issue or repeat your question so that you can verify your understanding and be on the same page as the customer. Clarify the customer’s statements. Ask concise questions of the customer to further identify what the issue is and narrow the scope of the problem. When you think you understand what the problem is, you should clarify by repeating the problem back to the customer. Restate the issue to verify that everyone understands the problem. Again, do not disclose experiences via social media. Lack of discretion is a no-no and will cause issues, perhaps including termination.

- **Set and meet expectations/timelines and communicate status with the customer:** When you have a clear idea of what the customer’s trouble is, set a timeline; offer a reasonable assessment of how long it will take to fix the issue and what will be involved. Stay in contact with the customer, giving updates at certain intervals—every half hour for smaller jobs and perhaps two or three times a day for larger jobs. If applicable, offer different repair or replacement options as the job progresses. At first, you might inform a customer that it appears a power supply needs to be changed. Later, you might find that an optical drive also needs to be replaced. Keep the customer up to date and offer options. Whatever the service, be clear as to the policies of your company and provide the proper documentation about the services you will be performing. After you finish the job, follow up to verify that the computer runs smoothly and that the customer is satisfied.
- **Deal appropriately with customers’ confidential and private materials:** Do not look at or touch confidential information. Ask the customer to move confidential items to another area where you cannot see them. Do not look at or touch confidential materials located on a computer, desktop, printer, and so on. This could include bank statements, accounting information, legal documents, and other top-secret company information. Going beyond this, don’t disclose any work experiences you had with an organization on social media.

- **Keep information confidential:** You might be asked to sign a nondisclosure agreement (NDA) or mutual nondisclosure agreement (MDNA). This is a contract that legally binds parties to keep certain information confidential. NDAs protect trade secrets and other confidential information secret, and are common in business relationships.

Always remember to do the right thing. If a customer asks you to do something that you think is inappropriate, be sure to verify exactly what it is the customer wants you to do. Then take appropriate action. For example, if a customer asks you to install company software on a personal laptop, you should verify that the installation is allowed under the company's licensing agreements. If so, no harm is done. If not, you will have to politely refuse the customer. This type of customer behavior, while rare, should be reported to your manager.

ExamAlert

Be professional, punctual, and positive and practice all the other skills mentioned in this section. They are important for the exam—and crucial in the computer field.

Cram Quiz

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

1. How will speaking with a lot of jargon make a technician sound?

   - ○ **A.** Competent
   - ○ **B.** Insecure
   - ○ **C.** Smart
   - ○ **D.** Powerful

2. A customer experiences a server crash. When you arrive, the manager is upset about this problem. What do you need to remember in this scenario?

- ○ **A.** Stay calm and do the job as efficiently as possible.
- ○ **B.** Immediately start troubleshooting without acknowledging the manager's concerns.
- ○ **C.** Avoid the customer and get the job done quickly.
- ○ **D.** Refer the customer to your supervisor.

3. Which of the following are good ideas when dealing with customers? (Select two.)

- ○ **A.** Speak clearly.
- ○ **B.** Ignore them.
- ○ **C.** Avoid distractions.
- ○ **D.** Explain to them what they did wrong.

4. You are a field technician working at a customer's site. One of the workers asks you to load a copy of an organization's purchased software on a personal laptop. What should you do first?

- ○ **A.** Verify that the installation is allowed under the company's licensing agreement.
- ○ **B.** Act as though you are distracted and ignore the user.
- ○ **C.** Leave the premises and inform the police.
- ○ **D.** Tell the worker that installing unlicensed software is illegal.
- ○ **E.** Notify the worker's manager of a security breach.

5. You have been asked by a customer at a hospital to perform routine maintenance on a laser printer. Before you begin, you notice that PHI has printed out. What should you do first?

- ○ **A.** Ensure the paper tray is full so that everything can print.

- **B.** Place the printed output in a secure recycle bin and begin maintenance.
- **C.** Kindly warn the customer that printing PHI at work is a HIPAA violation.
- **D.** Ask the customer to move the printed output to another area.

Cram Quiz Answers

1. **B.** Using too much computer jargon can make an end user think that you do not have the qualifications needed and are masking it with techno-babble.

2. **A.** There isn't much you can do when a customer is upset except stay calm and fix the problem! Remember, it's a job; it's not personal.

3. **A and C.** Speak clearly so that customers understand you and avoid distractions so that the customers know they have your complete attention.

4. **A.** You should check whether the company allows installation of paid software on personal computers or laptops. If it is allowed, go ahead and do the installation. If not, you should refuse and notify your manager of the occurrence. Refusal can be tough at times, so be strong and think about the consequences of your actions. They could directly affect you in a negative way.

5. **D.** Ask the customer to move the confidential information. Protected health information (PHI) is information that is protected under the HIPAA Privacy Rule. Before ensuring that the paper tray is full, you should first ask the customer to remove the private information. You should never throw away or recycle customer-printed output unless a customer asks you to. Printing PHI at a hospital is routine and not a HIPAA violation. Remember to always behave professionally and protect people's privacy. If you

make this a regular practice, you will often receive a customer's gratitude, and as time goes on, you will increase your job security.

Nice work! That was a bit of a longer chapter, so review your notes and then take a break because we will be getting back into the more technical side of things in the next chapter. You are doing great!

Chapter 62

Basic Scripting, Part I

This chapter covers a portion of the following A+ 220-1202 exam objective:

▶ **4.8** – Explain the basics of scripting.

The goal of this chapter is to cover the basics of scripting construction. This chapter is not designed to make you a programmer; however, it should enable you to break down the components of some basic scripts. One of the goals of scripting is to make things faster and more efficient by automating processes, ultimately making your job as a technician easier. If you have any doubts about programming computers, let us just say: You can do this! Let's go!

ExamAlert

Objective 4.8 concentrates on the following: script file types, use cases for scripting, and other considerations when using scripts. This chapter focuses on use cases and other scripting considerations. Chapter 63, Basic Scripting, Part II," focuses on the script file types covered in Objective 4.8.

Programming 101

Before we can get into specific scripting types, we need to cover some foundational programming concepts, including data types, script constructs, variables, and comments. This chapter provides a crash course on the basics of programming. We will cover specific scripting types (such as PowerShell and Bash) in the following chapter. Begin.

Basic Data Types

There are two basic data types that you should know: integers and strings. In computer programming and scripting, an integer is essentially the same as in mathematics. An *integer* is a whole number (no fractions or decimal places) that can be positive, negative, or zero.

Integer types can have different sizes, and you have no doubt heard of some of them—for example, the byte of information. Typically, a byte can be between 0 and 255. Computers think in binary, which is made up of zeros and ones (think off and on); in binary, a byte would be 00000000 through 11111111. So, it can have 2^8 (that is, 256) values. But there are more integral data types, like the nibble (which is 4 bits) or a word (which is 16 bits), or the doubleword (which is 32 bits). This concept isn't as complicated as it looks, and you really don't need more than this basic understanding for most things you will do.

All programming languages from C++ and Java to Python and JavaScript use integers because all programming languages are based in basic mathematics.

Note

By the way, if you need fractions or decimal places (real numbers), then you need floating-point numbers rather than integers. The floating-point data types are used to store positive and negative numbers with a decimal point, like 35.5, 2.32, or 0.0036.

A *string* is a sequence of characters used as a constant (such as a "word" like *cat*) or as a variable (such as *x*). A *constant* is something that remains the same. A *variable*, on the other hand, is something that can change over time, but we reference it with something that does not change (for example, *x* or *y*). Simply put, a variable is a symbolic word or combination of letters that can be used to hold a value. The value can be defined as a text, number, Boolean, or array.

As opposed to an integer, a string is designed to represent text instead of numbers. You'll also hear strings referred to as *alphanumeric strings*, which can include letters in the alphabet, digits, blank space, and special characters and punctuation.

Collectively, these data types are the building blocks for data within programming languages. Let's now focus on using these data types in scripting.

Basic Script Constructs

Scripting construct methods are essentially the same from one scripting language to the next. We'll use PowerShell as an example as we discuss some basic scripting constructs.

if Statement

One basic construct to use in scripting is the **if** statement. Here's an example of the general syntax:

```
if (conditional_expression) {
  statement_list
}
```

We use parentheses around the conditional expression, which can include things such as basic math—for example, (1 + 1)—or can point to code blocks, which would be contained in angle brackets (< >)—for example, **<test1>**. If the conditional expression is true, then the ***statement_list*** runs. For example, you might have a script write something to the screen or perform some kind of function within the operating system, using a module from within PowerShell such as Write-Host or PSWindowsUpdate. Whatever it is, it should be confined within the curly braces { }.

This example is a form of an **if-then** statement. While many programming languages use **if-then** statements, PowerShell doesn't actually incorporate the term **then**. Instead, if a condition is true, the code runs. If not, you use the **else** option to specify that other code runs.

Other constructs in PowerShell include **switch**, **for**, **break**, **continue**, **while**, and **do**.

Let's say that you want to repeat a task 10 times. To avoid typing the code 10 times, you can instead incorporate a loop. Two of the most common constructs used for looping in PowerShell are **for** and **while**. Let's look at the **for** loop next.

> **Note**
>
> Microsoft Learn is a great resource for those wanting to know more. For a quick introduction to scripting in PowerShell, see https://learn.microsoft.com/en-us/training/modules/script-with-powershell/. You will use PowerShell a lot, and scripting will save you a lot of time. It's a win-win!

for Loops

A **for** loop is used to repeat a block of code as needed. These repetitions are also known as *iterations*. A **for** loop has two parts: a header specifying the iteration and a body that is executed once per iteration. Look at the following general syntax:

```
for (init; condition; repeat)
    {command_block}
```

In this syntax, ***init*** is the command that is run before the loop begins. Generally, it is used to initialize a variable. ***condition*** is whether the expression is true or false. If it is true, the command will continue to repeat until the loop is exhausted and the condition is changed to false. This is based on the number of iterations, which is also included. ***repeat*** reads the value of the variable and increments it…one at a time. ***command_block*** is the command or group of commands that will repeat. Here's an example of a **for** loop in PowerShell that will count to 10:

```
for ($i=1; $i -le 10; $i++)
    {Write-Host $i}
```

PowerShell always places a **$** before a variable—for example, **$i**. In this case, ***init*** is **$i=1**, so the variable **i** has been set to 1. This is where the counting starts. This loop will repeat 10 times, as set in the condition **-le 10**.

Try this last script and the following one in PowerShell:

```
for ($i=1; $i -le 10; $i++) {$i,"'n"}
```

Both of these scripts will count from 1 to 10, but there is a slight difference between them. Can you spot the difference?

For information on how to open and use PowerShell in Windows, see Chapter 34, "Microsoft Command-Line Tools, Part I."

Remember, we are using the **for** construct to create the loop and the **$i** variable for the integers to be displayed.

As you progress, you will combine **if-then** statements with **for** loops and other programming constructs.

Note

Basic loops let a program execute the same statement multiple times. Each time a loop executes a block of statements, it is called an *iteration*. For a good summary of loops, see https://learn.microsoft.com/en-us/dotnet/visual-basic/programming-guide/language-features/control-flow/loop-structures.

Environment Variables

We have mentioned environment variables previously in the book; for example, %systemroot% (which is usually C:\Windows) and %username% (which is whatever user or users you are referring to). If you are working in the GUI or the Registry Editor, or if scripting in the Command Prompt, you use the *%variablename%* syntax. However, PowerShell has its own variables that start with **$** (which is similar to many other scripting languages)—for example, **$Env:*variablename***, where an actual value might be **$Env:Path**.

Path is a variable in Windows. It allows you to run programs from various locations in Windows without having to type the entire folder path to the executable. For example, a default path in Windows is C:\Windows\System32. You can run programs that reside within System32 in the Run prompt, the Command Prompt, or PowerShell just by typing the executable name. You can find all of these path locations by executing the following in PowerShell:

```
Get-Item Env:Path
```

This command displays any paths that have been added to the **Path** variable. However, it isn't functional only within the shell; **Path**, as well as other variables, can be added programmatically to scripts as well, which has a wide range of implications, from administration to development. Be ready to work with environment variables in Windows and in Linux.

Note

Want to learn more? Check out https://learn.microsoft.com/en-us/azure/devops/pipelines/process/set-variables-scripts?view=azure-devops&tabs=bash to see other ways in which you can use variables within scripts. Note that in this page, you can switch between Bash and PowerShell scripts; you may end up using both types, so it's important to know the similarities and differences.

Comment Syntax

Sometimes you will want to add descriptions, warnings, links, or other information to your scripts that do not actually *do* anything other than give information to the person reading the script. These things can be accomplished by adding comment syntax to the code. You can also *comment out* certain lines of code if you want them to stop functioning temporarily for testing purposes.

Using comment syntax in PowerShell and Bash is as easy as adding a number sign (#) before each line. For example:

```
# this script will count to 100.
for ($i=1; $i -le 100; $i++) {$i,"'n"}
```

Other types of scripts, such as JavaScript, use the double slash (//) before each line, which we'll demonstrate in the JavaScript section in the next chapter.

Note

You should understand how to comment out code with # (in PowerShell and Bash) or // (in other commonly used scripting languages).

When to Use Scripts

We have discussed how to create scripts, but it's also important to know when to use scripts. Scripts can be used to automate lots of basic functions of your device. Experienced script users can automate complex tasks using scripts, saving a lot of time on their daily work. Table 62.1 summarizes some typical scripting use cases.

TABLE 62.1 **Typical Scripting Use Cases**

Use Case	Description	Shell	Sample Commands
Basic automation	Automate basic tasks such as reading large data sets, scraping the Web for news, renaming files, extracting content, and performing other repetitive tasks. Microsoft Learn has a great beginner's class on it at https://learn.microsoft.com/en-us/training/paths/powershell/.	PowerShell	Once it is written, you can fit in this table). The Microsoft Learn example for reading l us/training/modules/s
	For basic Bash shell scripting, check out https://www.freecodecamp.org/news/bash-scripting-tutorial-linux-shell-script-and-command-line-for-beginners/.	Bash	Once it is written, you can fit in this table). Check out https://ww science.html for some
Restart a machine	Use the script to restart a device. This capability is useful when you are installing software that requires a restart.	PowerShell	**Restart-Computer** Note: This command within a PowerShell s

Use Case	Description	Shell	Sample Commands
		Bash	**reboot** Note: In Linux you w **sudo reboot**
Restart multiple machines	Sometimes you need to restart a group of machines (usually servers). Create a text file with all of the hostnames or IP addresses of the devices you want to restart, one per line. Save as inputfile.txt (in the example on the right). Run your script; it will use the **ssh** command to access each host remotely and reboot.	PowerShell	**Restart-Computer -**
		Bash	**for *host* in $(< *inputf*** do **ssh $*host* reboot n** done
Map network drive Note: The same commands work to remap drives if the mapping has been lost.	Mapping network drives to drive letters can be automated. This way, each of your users has the same drive letters for each of your network drives.	PowerShell	**New-PSDrive -Name $networkPath -Pers**
		Command Prompt/Batch file (.bat)	**net use X:*server\sh***
Install new applications	Installing new applications takes time and effort. Save yourself the time and effort by automating the process.	PowerShell	**Install-Package -Na <credentials>** To call PowerShell, y
		Bash	**apt install <*program*** or **dpkg -i <*packagena*** or **dnf install <*program*** or **apt install <*package*** Note: You might neec
Automate backups	Backups are important; after all, it is just a matter of time before your hard drive fails (every drive will eventually). PowerShell and Bash can automate the backup process.	PowerShell Note: You can also program this script to run on a schedule, ensuring your backups are done regularly.	**$source = "C:\path** **$destination = "D:\p** **Copy-Item -Path $s Force**
		Bash This script creates a tar (compressed) backup and saves it to the location of your choosing. Schedule with **cron** if you want it to run on a regular schedule.	**BACKUP_DIR="/p** **SOURCE_DIRS="/** **mkdir -p "$BACKU** **TIMESTAMP=$(da** **BACKUP_FILE="$** **tar -czvf "$BACKU**

Use Case	Description	Shell	Sample Commands
Gather information/data	You can retrieve system information using the **Get** command in PowerShell.	PowerShell	**Get-ComputerInfo** This command gives See https://learn.micr us/powershell/modul computerinfo?view=p use the command.
		Bash See https://github.com/trinib/Linux-Bash-Commands for a list of Bash commands, including an index where you can search by type of command you are looking for.	Bash uses the same c shell. **ifconfig** This command gives **uname -n** This command gives name. **system_profiles and** This command gives
Initiate updates	It is important to keep your devices up to date. Use the Command Prompt or scripts to automate this process.	PowerShell	**Install-module PSW** Then **Install-WindowsUp**
		Bash	**apt update && apt**

Note

Install-Package for PowerShell automates installation from a package repository, ensuring consistency in deployment of packages. It is similar to the InstallerPath tool, which is used for applications that are not in package repositories. Check out https://learn.microsoft.com/en-us/powershell/gallery/how-to/working-with-local-psrepositories?view=powershellget-3.x for more information.

Other Considerations When Using Scripts

Scripts are very powerful, but as the saying goes, with great power comes great responsibility. Scripts are no different. Let's look at some things you need to watch for.

Unintentionally Introducing Malware

Scripts automate what you are working on, which saves time and effort. Unfortunately, humans make mistakes, and these mistakes sometimes can create havoc if you are not careful. While it is extremely unlikely that you will yourself create malware, you might accidentally introduce it into your system. For instance, if you mistype the URL in an installer script, you could download a malware-laden version of an installer instead of the correct version you intended to download and install (copy-and-paste is your friend—and enemy). Perhaps you run a script that accidentally replicates itself (see Von Neuman machines, https://en.wikipedia.org/wiki/Von_Neumann_machine, for what can happen if those go wrong); those can inadvertently cause havoc on networks that don't have proper precautions in place (and if you are in IT support, you may have permissions that override even those precautions). So be careful.

Inadvertently Changing System Settings

Sometimes you will run a script on the wrong system or with incorrect parameters set. Doing so could change the system settings to something you didn't expect or that is incorrect for the user of the system. Best-case scenario: A

user loses access to files they need for their job for a few minutes in the middle of the night. Worst-case scenario: Critical files are lost right before an important deadline. Be careful whenever running scripts that impact system and permissions settings.

Browser or System Crashes Due to Mishandling of Resources

If system resources are mishandled, that could lead to the system locking up for a short period of time or locking up entirely, requiring a hard reset. Users could lose work in progress. If this is a server machine, dozens of users or more could be impacted. Be careful when working with system resources and ensure that you have adequate resources to accomplish the tasks your script is asking the device to complete.

Cram Quiz

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

1. Which of the following is an integer? (Select the two best answers.)

   - ❍ **A.** 16
   - ❍ **B.** cat
   - ❍ **C.** string
   - ❍ **D.** 00000001

2. You want to list a variable number 16 times but don't want to type 16 lines of code. Which of the following techniques should you use?

   - ❍ **A. if-then**
   - ❍ **B.** Looping
   - ❍ **C.** Environment variables
   - ❍ **D.** Comment syntax

3. What should you type to comment out syntax in PowerShell?

   - ❍ **A.** $
   - ❍ **B.** #
   - ❍ **C.** //
   - ❍ **D.** ( )

4. How can PowerShell be used to automate the process of restarting multiple computers in a network?

   - ❍ **A.** By manually running the **Restart-Computer** command on each machine individually
   - ❍ **B.** By using third-party software to remotely restart the computers
   - ❍ **C.** By using only the **Stop-Computer** cmdlet to shut down machines and then manually restarting them
   - ❍ **D.** By creating a PowerShell script that loops through a list of computer names and runs the **Restart-Computer** command

5. Which of the following is a way to automate the installation of applications on multiple computers using PowerShell?

   - ❍ **A.** By manually installing each application on each computer one at a time
   - ❍ **B.** By installing the application only on the local computer and then copying it manually to others

- ❍ **C.** By creating a PowerShell script that remotely installs the application on each computer, using **Invoke-Command** to call a script
- ❍ **D.** By using a third-party installer that requires no installation

6. What is a potential risk when using scripting to automate tasks, especially when running scripts on multiple computers?
   - ❍ **A.** It might automatically create backups of all system files before any changes are made.
   - ❍ **B.** It works only on local machines and cannot affect remote systems.
   - ❍ **C.** It might inadvertently modify or reset system settings, causing unintended system behavior or instability.
   - ❍ **D.** It ensures all changes are tracked and can be undone automatically if needed.

Cram Quiz Answers

1. **A and D.** The number 16 is an integer (any whole number is), and the binary number 00000001 is an integer that is equal to one 8-bit byte of information. The word *Cat* is an example of a string, and the word *string* is also an example of a string, which is a sequence of characters.
2. **B.** Make use of looping, which allows you to write one line of code based on math that will output the 16 lines of code required. In this example, it would be a *conditional loop*, where the operation is repeated until a specific requirement is met. **if-then** statements are used as conditional expressions. Environment variables are variables that define items within the system such as the environment path. Comment syntax is used to temporarily disable lines of code.
3. **B.** Use the number sign (**#**) to add comments or comment out lines of code in PowerShell and Bash. (The # symbol on the keyboard is also known as the pound sign or hash.) The **$** is used to denote a variable in many languages and scripting tools, including PowerShell and Bash. The double-slash (//) is used to add comments or to comment out individual lines of code in JavaScript (and several other types of languages). Parentheses **( )** contain pieces of code, such as a conditional expression within an **if-then** statement.
4. **D.** Create the PowerShell script, which will loop through each of the computers by name and run the **Restart-Computer** command.
5. **C.** The PowerShell script you create will install the software either with the **Install-Package** or the **InstallerPath** command, depending on whether the software is in a repository. Either will work. Pay attention to where your software resides. You can do this!
6. **C.** Be sure to review and test your scripts before deploying them in the field. You don't want to accidentally make changes to systems that cause instability.

All right! Our Programming 101 crash course is now complete. Take a deep breath! If these topics are new to you, then we recommend that you review what you have learned so far before continuing. And for those of you feeling a strange sensation right now, it could be that you are starting to realize the power of programming and scripting. With tools such as PowerShell, Bash, and others, you get complete control over a system and can automate processes, which will save you time and make you a more efficient tech. We mentioned this idea previously in the book: The command line is where real technicians live. And scripting takes the command line to the next level. Embrace the power.

Chapter 63

Basic Scripting, Part II

This chapter covers a portion of the following A+ 220-1202 exam objective:

- **4.8** – Explain the basics of scripting.

Now let's move into scripting types that you will undoubtedly see in the IT field and on the A+ exam. Six scripting types are listed in the A+ objectives. Probably the most important ones for the exam are Windows-based PowerShell scripts (.ps1) and Linux-based Bash scripts (.sh). Let's start with them.

ExamAlert

Once again, **Objective 4.8** concentrates on the following: script file types, use cases for scripting, and other considerations when using scripts.

PowerShell and .ps1

PowerShell is Microsoft's main command-line and scripting environment for Windows. It is a much more powerful shell than the Command Prompt and is the preferred method for administration, scripting, and developing. Go ahead and open PowerShell in elevated mode now in your version of Windows.

Note

> If you plan to use PowerShell often, we recommend creating a shortcut on the desktop (with an associated keyboard shortcut) or have it start automatically when you log on by adding it to the Windows Startup folder or the Task Scheduler.

To begin, you need to make sure that you are running a current version of PowerShell. To find out the version, type the following in the shell:

```
$PSVersionTable
```

For our version of Windows 11 (24H2), the PowerShell version (PSVersion) is 7.5.0. As this book ages, that version will become dated. You will want to upgrade to the current version of PowerShell. To find out more about the current version and to upgrade, see https://docs.microsoft.com/en-us/powershell/.

You will note additional information when running the **$psversiontable** command, such as the OS version (from a programmatic standpoint); at the writing of this book, ours is Microsoft Windows 10.0.26100. Even though we're running Windows 11, it still shows up as Windows 10 here. Tack that up to the underlying mysteries of Microsoft's numbering system (in reality, it does make sense to them, and it doesn't really matter to on-the-ground technicians).

One of the main reasons to use PowerShell is to automate processes or at least make them faster. For example, if you wanted to create a user in Windows, you would have to go through a lengthy process in Settings or in Local Users and Groups, using both the keyboard and the mouse. However, you can also create users in PowerShell. Take a look at the following command:

```
New-LocalUser "user1" -FullName "Test User" -Description "Test use
account."
```

New-LocalUser is a *cmdlet*—that is, a lightweight command that is used in the PowerShell environment. This cmdlet (and ensuing parameters) would result in a new user being created, called *user1*, with the name *Test User*. PowerShell would then ask you to type a password for the account, and the account would be created and placed in the Users folder. You can easily test it by typing **net user**, which will display the users on the computer (though you also get verification from PowerShell after the command is run).

Boom, done, and you didn't have to go through the GUI—so already you can see that PowerShell is a boon for sysadmins.

Now, running commands in PowerShell is super fun, but what if you want to create a script? A *script* is used to run multiple commands in rapid succession and to initiate **for** loops and other programmatical constructs. You could write and run a PowerShell script directly in PowerShell, but it is usually wiser to build a script by using a tool. You could use a basic text editor, such as Notepad (**Run > notepad**), or you could use an integrated development environment (IDE) such as Visual Studio Code (VSC), which you can download free from https://code.visualstudio.com.

When you are done writing a script, you save it as a .ps1 file. The .ps1 extension identifies a file as a PowerShell script. .ps1 is not the only extension you can use, but it's the one we will focus on for the A+ exam.

ExamAlert

Know that PowerShell scripts are identified by the .ps1 extension!

Which Tool to Use?

The choice is up to you. Notepad is built into Windows, and it's super easy to use. Feel free to work with that tool or another text editor if you like. However, you need to run Notepad and PowerShell separately, and every time you want to test your code, you have to switch between the two applications. Windows Snap can help somewhat, but you still have to use Alt+Tab or the mouse to switch between apps. That's where an IDE comes in. If you really want to get busy, use VSC. It *integrates* PowerShell (or other shells) right into the program that you code in. Pure genius, right? Downloading and installing it is a breeze. Also, it's cross-platform, so there are downloads for Linux and macOS as well—if you prefer those platforms over Windows. Or, you

might find that you like a different IDE better; we use a couple of different IDEs. There are a lot of options, and which one you choose depends on what kind of work you will be doing. But we *strongly* urge you to check out using VSC as a method for working effectively with PowerShell (and other scripting types).

Now let's take scripting to the next level. Figure 63.1 shows an example of a .ps1 script that adds multiple users at once.

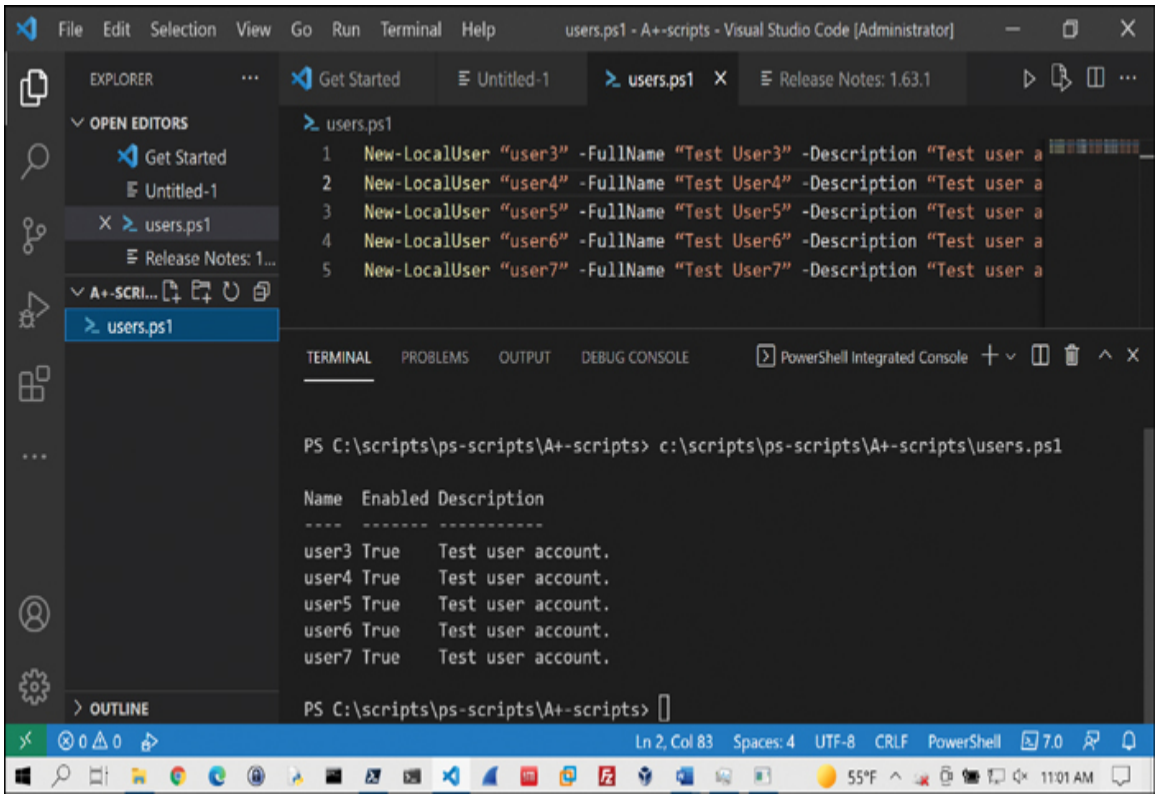


FIGURE 63.1 **users.ps1 Script Example**

We wrote this script in VSC (as an administrator). We created a new .ps1 file called users.ps1, which you can see in the left-hand pane (known as the Explorer). The actual script is the five lines of code you see in the coding area at the top. In VSC, the code can be executed (or run) by clicking the Play button or pressing Ctrl+F5. The results are displayed in the integrated PowerShell console at the bottom. You can see that user3 through user7 were all added at once.

In this example, we added the password during user creation. To create the password first and store it securely, you could use the following code in PowerShell:

```
$Password = Read-Host -AsSecureString
```

Then type the password that you want. Then reference it later during the user creation process in the script with the following:

```
-Password $Password
```

-Password is the parameter, and **$Password** is, wait for it…a *variable*. It will grab the password that you previously stored. In PowerShell, a variable name always begins with a dollar sign (**$**).

The script in Figure 63.1 is *very* basic. It's really just for educational purposes. You could take it further by using more variables, **for** loops, **if-then** statements, and tables (arrays) of information and then adding more and more lines to the script. Then you could save the whole adventure for later use, again as a .ps1 file. This is scripting in a nutshell.

Here's another example of PowerShell usage. Say that you want to test whether a computer is alive on the network. You could run the **ping** command, but PowerShell also offers the **test-connection** cmdlet, which enables you to ping multiple systems and in many ways. Try the following command in PowerShell:

```
test-connection example.com, greencurtaintraining.com
```

If you have a working Internet connection, the results will show the IP address of each website and that each was pinged four times successfully. Because it is a PowerShell-specific command, you could use the **test-connection** command in a .ps1 script as needed. It could be a basic script that simply runs the command with the options you desire—and even that would be a time-saver if it is a test you run often. Or, you could combine it with the programming constructs we described in the preceding chapter to make your tech world even more efficient.

Take it to the next level, and you could run your pings in an *actual* script by using a **for** loop and Microsoft class structures. Instead of using the **ping** or

test-connection command, you could go straight to the source and make use of the Win32_PingStatus class in PowerShell.

> **Note**
>
> For more information about PowerShell, start here: https://docs.microsoft.com/en-us/powershell/scripting/overview.

Challenge: Use PowerShell and VSC!

As mentioned, these challenges are optional, but they are designed to help you grasp the concepts in the A+ objectives as they apply to the real world. So, if you have the time, try the following on a test machine:

1. Update to the latest version of PowerShell.
2. Create a shortcut to PowerShell on the Desktop (as an administrator).
3. Add a user with the **New-LocalUser** command.
4. Ping a domain on the Internet with the **test-connection** command.
5. Download and install VSC and play around with it for a little bit. If you are feeling brave, write a basic script and save it as a .ps1 file.

.bat and Batch Files

For a long time, we DOS/Windows users (aka dinosaurs) would write batch scripts (sometimes complicated and temperamental) to map network drives, add users, perform a series of pings, and so on and then save them as .bat files. Often these files would be written in the Notepad program or something similar and run in the Command Prompt. Here's a basic example:

```
net use Z: \\mach1\superdata
```

This command, when run as a batch process (by executing the .bat file), would map the Z: drive of the local system to the *superdata* share on the *mach1* server. You could then add the batch file to the startup process of the operating system. This approach would be handy if the drive needed to be mapped every time the system booted. But it's not necessary on today's Windows systems.

By the way, to make this command persistent, meaning that the drive would remain after a reboot, you add this option: **/Persistent:Yes**. However, **net use** is the old method. Later in the chapter, we'll look at the newer PowerShell method.

You can still create batch files today within Notepad, and some Windows users still do, but PowerShell makes the process much easier and more configurable. Personally, we left .bat files in the dust many years ago, but they are listed in the A+ objectives, so there you have it!

Bash and .sh

In the Linux world, you can create scripts with a text editor (such as nano, vi, Vim, or gedit) or an IDE like VSC. IDEs in Linux work in the same manner as in Windows, which we showed previously in the PowerShell section. So, for this section, let's focus on using text editors in the Linux Terminal.

In Linux, you can type commands and run text editors directly within Terminal. (Remember: Terminal is the command line for Linux.) This program utilizes one of a variety of shells. (Essentially, the shell is the command-line interpreter.) The default shell in many Linux distributions is called Bash. To find out what shell is being used, type the following command:

```
echo "$SHELL"
```

Bash is also where you can save scripts by default. The path is /bin/bash, though you can save them elsewhere if you wish. Normally, Bash scripts are saved with the .sh extension (short for shell).

Note

You may wonder about the Windows Terminal, because it's referred to by the same term as used in Linux. Windows Terminal is the modern host application for the command-line shells you already use and love, including Command Prompt, PowerShell, and Bash (via the Windows Subsystem for Linux [WSL]). See https://learn.microsoft.com/en-us/windows/terminal/ for more details.

ExamAlert

Know that the .sh file extension represents a Linux/UNIX shell scripting file.

Now let's look at how to build a basic and traditional "Hello, World" script. First, you need to access Terminal. If you are on a Linux desktop, press the super-user key (the Windows key), start typing **terminal**, and Terminal appears. Alternatively, some distros (such as Ubuntu) let you use the keyboard shortcut Ctrl+Alt+T to go straight to Terminal. A Linux server does not usually have a desktop environment, and therefore you are already working in the command line—essentially Terminal.

Once you have opened Terminal, you can open the text editor where you will build your scripts. There are two main options in Linux: nano and Vim.

nano is built into most Linux distros and is the easier tool to use. It is quite similar to Notepad in Windows (but is keyboard only by default). For example, to create and edit a file with nano, you could type **nano testscript.sh**. This command opens the nano program, and you are ready to start typing into your file. You will note several keyboard shortcuts at the bottom of the screen. To save a file and exit out of nano, you press Ctrl+X on the keyboard and then press **y** to save the changes to the file. If you wanted to modify the file later, you could simply repeat the entire process. As you can see, nano is easy to use.

However, many technicians prefer Vim because it is heavily customizable and can provide for excellent workflow. However, it is more cryptic in its usage if you are not used to it.

Vim is based on the original (and ancient) UNIX text editor vi but is a bit easier to use. Vim stands for *vi improved*. vi is included in almost all distributions of Linux, and Vim is included in many as well. However, if Vim is not available in yours, you can install it by using a command like **apt install vim** (in Debian/Ubuntu) or **dnf install vim** (in Fedora/Red Hat). We recommend that you use Vim rather than vi because of its comparative ease of use and because it is very adaptable.

Note

For basic tutorials on Vim, see https://www.linuxfoundation.org/blog/blog/classicsysadmin-vim-101-a-beginners-guide-to-vim and https://opensource.com/article/19/3/getting-started-vim.

To create or modify a file in Vim, type **vim** and then the filename—for example, **vim helloworld.sh**. This opens the Vim editor, and you can get to work. However, to use Vim, you need to know special keystrokes to perform certain actions. For example, to actually enter information, you have to first press a key on the keyboard—most commonly the i key. (Think *i* for insert.) Table 63.1 lists some basic key commands. Most of these will work in Vim or in vi.

TABLE 63.1 **Common Vim Tasks and Keystrokes/Commands**

Task	Keystroke
To enter insert mode for editing (before you can write a script)	Press Esc and type **i**
To go to command mode (for saving, exiting, and so on)	Press Esc
To save a file	Press Esc and type **:w *filename*** (**w** for write)
To quit	Press Esc and type **:q**
To save and quit at the same time	Press Esc and type **:wq** (**w** for write, then **q** for quit)

Keep in mind that you need **sudo** (superuser or equivalent) access to perform some of these actions (unless you are working as root, which you almost never will do). For more information on **sudo** and the root account, see Chapter 40, "Linux."

To try building the "Hello, World" script, follow these steps:

1. In Terminal, type **vim helloworld.sh**.
2. Press Esc and type **i** to enter insert mode (remember that this is the editing mode).
3. Type the following:

```
#!/bin/bash
echo "Hello, World!"
```

4. Press Esc to exit insert mode.
5. To save the file, type **:w** and press Enter.
6. Quit Vim by typing **:q** and pressing Enter. This will bring you back to the standard Bash terminal. Note that you could instead combine steps 5 and 6 by typing **:wq**.
7. Set permissions so that the script will run. For example:

```
chmod +x helloworld.sh
```

8. Run the script by typing **./helloworld.sh**.

You should now see the text that you placed in quotes within the script "Hello, World." Great job! That is an example of the most basic of Linux-based scripts.

Now let's take it up a notch. Here's a script that uses looping and displays the quoted text five times:

```
#!/bin/bash
for i in 1 2 3 4 5
do
  echo "Looping $i"
done
```

If you type this exactly and use **chmod** with it, you should see the looped results. This script also makes use of the variable **$i**, which changes from 1 to 2 to 3 to 4 to 5 on each line.

Now, here's an example of an **if-then** statement as it would work in Bash:

```
if <condition>;
then <commands>
fi
```

This is a little different from the PowerShell-based *if* statement shown in the preceding chapter. It uses an **if-then-fi** statement—also known as **if…fi**—to make decisions and execute statements conditionally. The condition is based on what you type in ***<condition>***, and the ***<commands>*** are what will occur if the condition is met. Here's an example:

```
#!/bin/bash
age=21
if [ $age -gt 18 ]
then
  echo "You can now vote in the United States."
fi
```

In this example, the condition is that the **age** number must be greater than 18 for the command to work. The command is a simple **echo** command that displays the text "You can now vote in the United States." We created a variable where **age=21**, so the condition will be met. It's a bit of a silly script, but it's a quick way of showing how an **if-then** statement works in Bash.

Scripts often run automatically as cron jobs in Linux. Cron jobs can be created by using the **cron** utility, which is a time-based job scheduler. (See Chapter 42, "Cloud-Based Productivity Tools," for other scheduling and automation tools.)

To comment out in Bash, you add the number sign (#) before each line that you want commented out, just as you do in PowerShell. For example, you might type something like this:

```
# test script for voting age - exceptions apply!
```

This would describe what the script is meant to do, but it won't have any impact on how the script functions.

Note

You might have noticed that the Bash scripts started with **#!/bin/bash.** This is known as the shebang, or "bang," line. This is not a comment; rather, it tells Linux to interpret the script using the Bash shell and specifies the absolute directory path to that shell, which is /bin/bash. So, **#!** is different from just #.

ExamAlert

Know how to use Bash, including Terminal and nano, for the exam!

Challenge: Linux, and nano

Linux is a super-important tool for all kinds of techs: sysadmins, developers, and engineers. Practice with it by doing the following on a test system or virtual machine:

1. Create a basic Bash script with nano that will display text on the screen using the **echo** command.
2. Use **chmod** to apply executable permissions to the script and run it!

Note

You will use Linux a lot as you become a more experienced technician. The more you know, the further your career will go!

Use Cases and Other Considerations for PowerShell and Bash

There are a lot of use cases for scripting within PowerShell or Bash. To start, you can create scripts to do basic automation of tasks such as file backups. This way, you don't have to manually run them each time. You can also build scripts to gather data about files, software, users, and so on. If these are the kinds of things that you do on a daily or weekly basis, then automating is the way to go.

There are some other use cases as well. Take a look at Table 62.1 in the prior chapter for some examples. Any of these commands can be placed in a script to run when and how you want.

Mapping a Drive in PowerShell

We discussed mapping in the preceding chapter, but it's important, so we'll cover it again in a bit more depth here. Here's an actual example of mapping a drive in PowerShell using the **New-PSDrive** cmdlet. Type everything here as one line:

```
New-PSDrive -Name "K" -PSProvider FileSystem -Root "\\mach2\megada
-Persist
```

This command would map a K: drive to the *megadata* share on the *mach2* server and make the connection persistent. For more details on the **New-PSDrive** cmdlet, see https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.management/new-psdrive?view=powershell-7.2.

Remapping a Drive

Remapping a drive follows the same steps as mapping a drive. You would do this for the following reasons:

- To re-establish lost connections, usually due to reboots, network reconfiguration, or network connectivity issues
- To access updated network resources, often due to server migration or network drive path changes

- To fix drive letter conflicts or incorrect mappings within the network settings

Remember, you will use the same tools and steps to remap a drive as you used to map the drive in the first place. You will need to remove an existing drive letter first. Remove it with the **net use [*drive letter*] /delete** command, then use the **net use [*drive letter*] [*path*] /persistent:yes** command to place the new drive map in place.

Script Security

Continuing our discussion from the preceding chapter, keep in mind that scripts can be used for productive or malicious purposes, so they should be tightly controlled. For example, when you use the **chmod +x** command on a Bash script, you make it executable. You have to be careful what scripts you allow to execute, and you need to be very aware of the user and group permissions that you set for those scripts.

Here's the thing: A poorly designed script, or a script with weak permissions, can introduce chaos to your systems and networks. You might unintentionally introduce malware because it might be seeking out weak scripts. Another consideration is that you could inadvertently change system settings. Or, if a script is not designed well, it could mishandle the resources of the system (CPU, RAM, and so on), potentially causing web browsers and other applications—or even the entire system—to fail.

One way to avoid these pitfalls when developing scripts and entire applications is to implement *secure coding concepts*—that is, best practices used during software development to increase the security of the script or application being built; secure coding hardens code. An example of secure coding is working within a software development life cycle (SDLC) such as the Agile model. SDLC models have a few core principles, including maintaining confidentiality, preserving integrity, and protecting availability (the CIA triad). There are several things that scripters/programmers can do to incorporate those core principles. The following are some of them, and they apply to all the scripting types in this chapter and to programming in general:

- **Follow the principle of least privilege:** Users should have access only to what they need. Processes and scripts should run with only the bare minimum access needed to complete their functions.
- **Follow the principle of zero trust:** By default, users and devices are not to be trusted, even if they are connected to a privileged network. Every device and every user must be authenticated, even if they were previously verified. This augments the older defense-in-depth strategy. The more security controls, the better.
- **Ensure that applications never trust user input without validation:** Input should be validated carefully.
- **Minimize the attack surface area:** Every additional feature that a person adds to a script or an application increases the attack surface and increases risk. Unnecessary functions should be removed, and necessary functions should require authorization.
- **Establish secure defaults:** Out-of-the-box offerings should be as secure as possible. Permissions should default to "no access" and should be granted only as they are needed.
- **Provide for authenticity and integrity:** For example, when deploying applications and scripts, use code signing in the form of a cryptographic hash with a verifiable checksum for validation.
- **Fail securely:** At times, applications fail. How they fail determines their security.
- **Fix security issues correctly:** Once found, security vulnerabilities should be thoroughly tested, documented, and understood. Patches should be developed to fix the problem but not cause other issues or application regression.

You get the idea. Always be thinking with that CIA triad in the back of your mind when it comes to scripts—or anything else technology-related.

Note

While not completely replaced, the concept of *defense in depth* is increasingly being enhanced and supplemented by *zero trust* security

strategies because zero trust offers a more granular approach to access control that is continuously verifying, moving away from the traditional perimeter-based security model inherent in defense in depth. Essentially, zero trust is considered a more modern and robust way to implement layered security principles.

Python and .py

While PowerShell and Bash are heavily used, they aren't the only scripting tools in town. Case in point: Python.

Python is a high-level object-oriented programming language. While it can be used for scripting, it is a general-purpose programming language that can be used to build in-depth programs, making it more powerful than PowerShell, Bash, JavaScript, and VBScript but slightly less powerful than languages such as C, C++, and Java. The reason is that Python generally requires an interpreter. In general, Python is very flexible and is used in a variety of ways.

To use Python in Windows or Linux, you first have to install it; you can grab it from https://www.python.org. After you install Python, you can access the Python console by simply typing **python** at the command line. You can test your Python commands there or build a Python script in a text editor or an IDE like VSC. When scripting in Python, you save the script as a .py file.

ExamAlert

Python scripting files use the .py file extension.

Python uses statements similar to those in other languages, such as **if**, **for**, and **while**, and it makes use of variables in a similar fashion.

Here's an example of a Python script that displays random six-sided die rolls:

```
import random
number = random.randint(1,6)
print("Your die roll is: " + str(number))
```

Let's say you saved this script as a file called rpg6sider.py. You could then run the script directly from the command line. To do so, you would type **python rpg6sider.py**. The script then runs, and it should randomly select a number between 1 and 6 and display it on the screen. (Gaming night just got geekier!)

Instead of programming everything from scratch, this script imports a module called **random**. This module includes all the math code needed for a pseudo-random generator and saves you a *ton* of time because you don't have to code that yourself. There are many modules and libraries like this. Take advantage of them.

As of the writing of this book, the current version of Python is version 3. (Version 2 is considered deprecated for the most part, and you should not program in it, but you might still see some programs in it hanging around.) For Python documentation, see https://docs.python.org/3/. If you wish to program more in Python and want to use an IDE, consider using PyCharm or VSC.

Note

Interested in learning more? Check out *Intro to Python for Computer Science and Data Science* by Paul Deitel and Harvey M. Deitel. It's good.

Remember that Python is designed for small and large projects, and therefore it can be a great scripting tool in Windows and Linux, regardless of its differences from PowerShell and JavaScript.

JavaScript and .js

If you are going to have a powerful and interactive front end to your website, you will most likely be using JavaScript. Though it can be used in other environments, JavaScript is best known for being used to develop web pages. A good web developer knows to use HTML to define the content of web pages, CSS to work with the layout of web pages, and JavaScript to program how the web pages will behave and to add functionality. For example, if you wanted to have a quiz or a calculator on your website, you could use JavaScript.

You can work with JavaScript in any text editor but will probably have better luck with an IDE such as Eclipse, VSC, or one of the many others that are available. Regardless, when you are finished creating a script with JavaScript, save it as a .js file.

ExamAlert

Remember, JavaScript files use the .js file extension.

To comment out code in JavaScript, use the double-slash method (//), by adding the double-slash before each line to be commented out. // is designed for single lines of code. For multiple lines, use /* at the beginning of the comment and */ at the end. JavaScript will ignore any text between them. This approach is also common in other programming languages, such as C++, as well as markup languages.

Note

Speaking of markup languages, as a technician, you will want to learn a little bit about JavaScript Object Notation (JSON), which was derived from JavaScript. This markup language is used by many programs and systems for configuration files and analysis. Other good markup languages to know include YAML, HCL, and especially Markdown. Trust us on this.

By the way, if you are scripting in JavaScript, you will probably also be working in HTML. If you are working on an HTML web page and you want to leave a comment or comment something out, you use **<!-- -->** with the comment in the middle. A similar programming language that you might encounter is TypeScript (which uses .ts files). It is a superset of JavaScript, which means that all .js files can run within it.

Regardless of what you use, you'll find that all scripting is based on math and common sense—once you get past the syntax and naming conventions, that is!

Visual Basic Script and .vbs

A file with the extension .vbs is a Visual Basic script, or VBScript file. VBScript is an object-based scripting language, and it was historically used in Windows environments (.NET and Office) and in web pages. You can build VBScript scripts within the Windows Notepad program or using any other text editor or IDE. Then simply save the script as a .vbs file. Visual Basic is also heavily used in Microsoft 365 (namely Excel) with the included Visual Basic Editor.

ExamAlert

A file with the .vbs extension is a Visual Basic script, or VBScript file.

Note

In Windows, a lot of what was once done in VBScript is now done with PowerShell. On the Internet, it is more likely that you will use JavaScript or some other tool. However, VBScript still has a place in .NET (though many developers prefer C#) and especially within Microsoft 365. See this site for a tutorial about using the Visual Basic Editor within Microsoft 365, known as Visual Basic for Applications (VBA): https://docs.microsoft.com/en-

us/office/vba/library-reference/concepts/getting-started-with-vba-in-office.

A Final Word on Scripting

You should be able to identify the various types of scripts and file extensions listed in this chapter, but we suggest that you focus primarily on PowerShell and Bash because they are specifically designed for system administration with Windows and Linux, respectively.

Cram Quiz

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

1. A technician just finished scripting a sequence of code and saved the script as a .sh file. What system is the technician working in?

   - **A.** PowerShell
   - **B.** Linux
   - **C.** JavaScript
   - **D.** Python
   - **E.** Batch file

2. You are scripting in PowerShell and need to incorporate a construct that will repeat an operation until a specific requirement is met. What construct should you use, and which extension should you use to save the script?

   - **A.** **if-then** logic and .sh
   - **B.** String variables and .py
   - **C.** Conditional loop and .ps1

- **D.** Integers and .vbs

3. Which of the following can you use to map a network drive in PowerShell?

   - **A. apt install**
   - **B. for** loop
   - **C. restart-computer**
   - **D. Install-WUUpdates**
   - **E. New-PSDrive**

4. Which of the following extensions identify files that can be run as scripts? (Select all that apply.)

   - **A.** .ps1
   - **B.** .exe
   - **C.** .bat
   - **D.** .docx
   - **E.** .vbs
   - **F.** .py
   - **G.** .txt
   - **H.** .sh

Cram Quiz Answers

1. **B.** The technician is working on a Linux system and making use of Bash (perhaps vim). When you work in Bash, it is accepted as a best practice to save the scripts as .sh files. PowerShell uses .ps1 by default. JavaScript is .js. Python is .py. Batch files are used for scripting in Windows and are saved with the .bat extension—but remember that using PowerShell is recommended over using batch files.

2. **C.** The construct required to repeat an operation until a specific requirement is met is a conditional loop (such as a **for** loop). If you are working in PowerShell, then you will most likely save the script as a .ps1 file. **if-then** statements use conditions such as true, false, else, and so on. .sh is used by Bash. Strings are sets of alphanumeric characters, and variables take the place of particular pieces of data. .py is used by Python. Integers are whole numbers, and .vbs is used by Visual Basic Script.

3. **E.** Use the **New-PSDrive** cmdlet to map a network drive in PowerShell. While the **net use** command still works in PowerShell, using **New-PSDrive** is the newer way. **apt install** is used in Linux (Debian/Ubuntu) to install or upgrade packages. A **for** loop is used to repeat a process in programming. The **Restart-Computer** cmdlet in PowerShell will, well, restart the computer. The **Install-WUUpdates** cmdlet in PowerShell will initiate Windows Update.

4. **A, C, E, F, and H.** .ps1 files are PowerShell scripts. .bat files are batch file scripts. .vbs files are Visual Basic scripts. .py files are Python scripts. .sh files are Bash scripts. The incorrect answers are .exe (executable files), .docx (word processor files), and .txt (text files).

This is a monster chapter to be sure, but you did it. There was a lot of content in here that at times might have thrown you for *a loop*! So, review carefully. You might not get a lot of questions on the exam about these concepts (though we can almost guarantee some), but they are super important skills for the IT field. Exceptional work!

Chapter 64

Remote Access Technologies

This chapter covers the following A+ 220-1202 exam objective:

- **4.9** – Given a scenario, use remote access technologies.

Why walk or drive to another computer when you can control it remotely? Unless there is a networking or hardware issue, always try to access a device remotely rather than physically going to the device (a process called "remoting in") to a system to repair it. It will be faster and more efficient than physically going to the device. This is doubly true in the world of remote work and distributed teams; your work team may be distributed across the country or even the world. Tools such as RDP, SSH, and RealVNC are some of a sysadmin's best friends.

ExamAlert

Objective 4.9 focuses on RDP, VPN, VNC, SSH, and other tools, as well as security considerations of each access method.

Remote Desktop

Remote Desktop software, included with Windows, enables a user to see and control the GUI of a remote computer. It enables users to control other computers on the network or over the Internet without leaving their seats. It

aids technicians in their attempts to repair computers because they don't have to go to a system that needs repair.

To have a Remote Desktop session, you need to configure the software. You can configure Remote Desktop within Settings or in the System Properties dialog box:

- **Settings:** Open **Settings > System > Remote Desktop**. From here, you can enable Remote Desktop simply by dragging the slider and selecting users who are allowed to connect to the local system. There are also advanced options, including options for configuring network-level authentication.
- **System Properties dialog box: Run > systempropertiesremote**. This option gives you a little more fine-grained control of Remote Desktop. There are two sections in this window: Remote Assistance and Remote Desktop. Let's examine those two parts now.

Remote Assistance

In the Remote Assistance section, the Allow Remote Assistance Connections To This Computer checkbox is selected by default. This means that connections can be made via Remote Assistance invitations, by email, or via instant messaging. These invitations can ask for help or offer help. This option is often implemented in help desk scenarios in which a user invites a technician to take control of their computer so that it can be repaired. Invitations are made by accessing the Windows Remote Assistance program (simply type it into the Search field). For this to function, in addition to having the checkbox checked, you must enable Remote Control by clicking the **Advanced** button and selecting the **Allow this computer to be controlled remotely** checkbox. When the proper settings are enabled, Remote Assistance calls flow right through Microsoft Defender Firewall. Collectively, this functionality is known as Microsoft Remote Assistance.

Remote Desktop Connection

In the Remote Desktop Connection section, you can select whether other users can connect to, and control, your computer at any time *without* an invitation from you. There are options to disable remote connections, enable connections with any version of Remote Desktop, and enable connections running Remote Desktop with network-level authentication for security. The option to connect is disabled by default, but if it is enabled, remote users can make connections to your system by computer name or by IP address. Finally, you can select the users who are allowed to connect to your computer. If your network is a workgroup, then any local user account you select is just that: local. For a remote user to connect, the remote computer must have an identical account (the same username and password) as the one you selected on your computer, and the remote user must know the username/password. If the network is a domain, this is not an issue due to centralized administration of accounts. Note that not all versions of Windows (like Windows Home) support initiating a Remote Desktop session.

ExamAlert

Be able to explain the difference between Remote Assistance and Remote Desktop and use them both.

How to Connect with Remote Desktop

To make a Remote Desktop connection to a remote computer, you need to make sure the remote computer has Remote Desktop enabled. Next, open the Remote Desktop Connection program. In any version of Windows, simply type **remote** in the Search field and select Remote Desktop Connection. (In Windows 10, you can also go to **Start > Windows Accessories**; this is not available in Windows 11.) Remember, Home editions of Windows only allow the client side of Remote Desktop, so consider using Windows Pro or higher to have full Remote Desktop capabilities.

Click **Show Options** to get the logon settings shown in Figure 64.1. To make a connection, you need to supply the computer name or the IP address

of the remote computer and the username and password for an account on the remote computer.

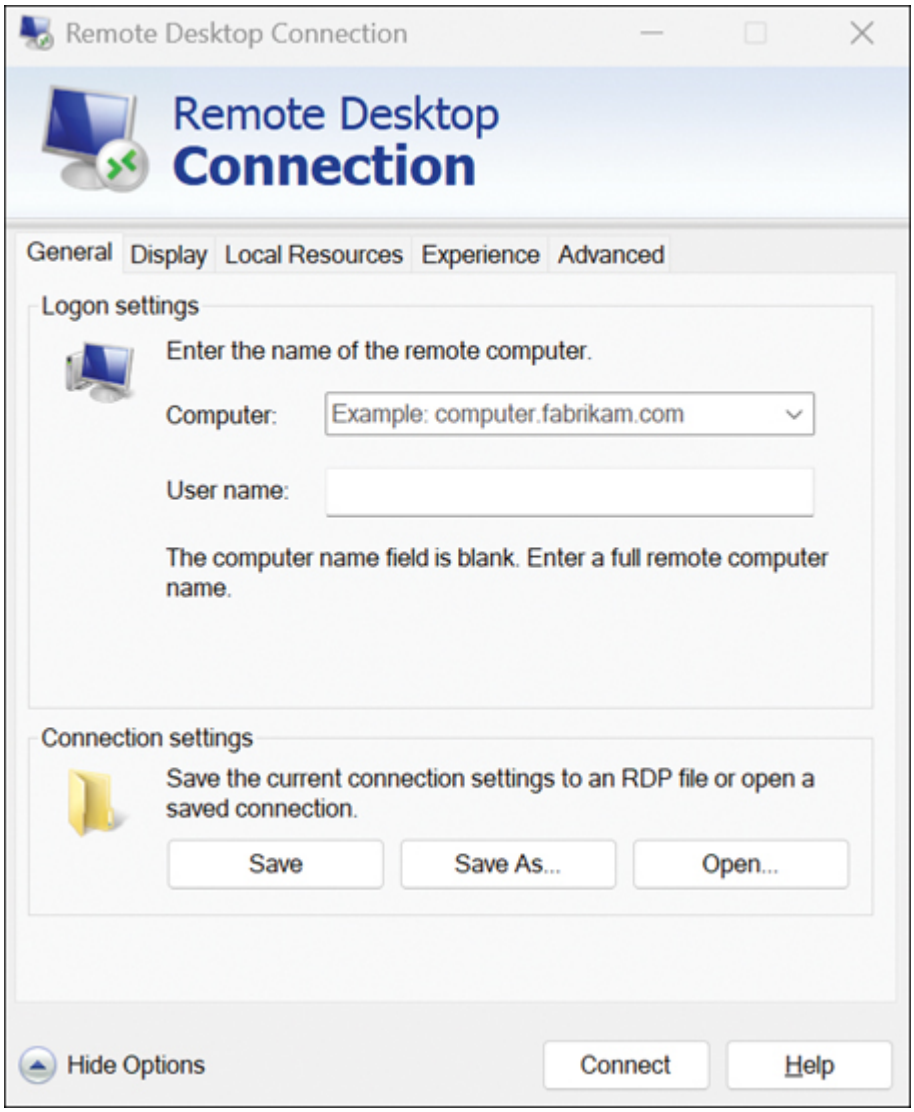


FIGURE 64.1 **The Remote Desktop Connection Window**

Click **Connect**, and the screen of the other computer should show up on your local display. At this point, you can control the remote computer as if you were sitting at it locally. By default, when you connect, the remote computer's physical screen locks; it can be unlocked only with a username/password.

Note

Remote Desktop is based on Remote Desktop Protocol (or RDP, as it is often referred to by techs). When Remote Desktop is enabled, this protocol is allowed through Microsoft Defender Firewall using TCP port 3389 (by default), which is a well-known port. Give *strong consideration* to using network-level authentication when allowing Remote Desktop connections. It is enabled by default for good reason. And, for further security, consider implementing FIPS 140 compliance with TLS and making use of port 443 (configured in Group Policy). Read more about FIPS 140 at https://learn.microsoft.com/en-us/compliance/regulatory/offering-fips-140-2.

ExamAlert

Know how to use Remote Desktop to make connections to remote computers. The RDP port, 3389, is also used by Remote Desktop Services, which is the serverbased companion of Remote Desktop Connection. We can guarantee you will get exam questions on RDP!

You can also use the **mstsc** command. If you use this command by itself, it will simply display the Remote Desktop Connection program, just as before. However, you can use it solely at the command line and add options. For example, you can perform custom Remote Desktop connections, edit existing Remote Desktop configuration files, and migrate old connection files to newer systems. If you want to remotely control another system with the **mstsc** command in full-screen mode, for example, you type the following:

```
mstsc.exe /v:computername /f
```

Note

For more information on the **mstsc** command, visit https://docs.microsoft.com/en-us/windows-

server/administration/windows-commands/mstsc.

Need to control more than one computer remotely at the same time? Consider using the Remote Desktop Connection Manager. Technicians who need to maintain multiple machines—especially servers—remotely use it all the time. It's an extra download for Windows that is available from https://docs.microsoft.com/en-us/sysinternals/downloads/rdcman.

Remote Monitoring and Management (RMM) and Desktop Management Software

Take your work to the next level with *remote monitoring and management (RMM)* solutions. These software tools (often third-party tools) are designed to remotely monitor and manage client endpoints, networks, and computers. These remote IT management solutions go beyond single RDP connections and allow you to have a more wholistic view of systems and networks, all displayed in one window. Examples include LogMeIn Central and NinjaOne.

RMM solutions are similar to *desktop management software* (and the two terms are sometimes used interchangeably). Desktop management software focuses more on client OS management and *security*. In contrast, an RMM might also be used to track customer information, assets, inventory, and so on. Be ready to use RMM tools if you plan to work in an enterprise setting.

ExamAlert

Know that remote monitoring and management (RMM) is a technology that enables users to monitor and manage IT infrastructure and devices remotely. RMM helps technology teams and managed service providers (MSPs) improve efficiency and productivity.

SSH

We can't tell you how many times we've typed **ssh**, and we can't stress enough how important this tool is for your résumé or CV. We briefly

discussed the Secure Shell (SSH) protocol way back in Chapter 4, "TCP and UDP Ports and Protocols." Consider reviewing that information before continuing.

Using SSH is typically considered a secure way to connect to remote systems, network devices, and more (as long as it is configured properly). Once you connect via SSH, you can control the remote system from the command line.

One of the most common SSH clients is PuTTY. Take a look at Figure 64.2, which shows the configuration screen. When you enter the information, you connect directly to the remote device.

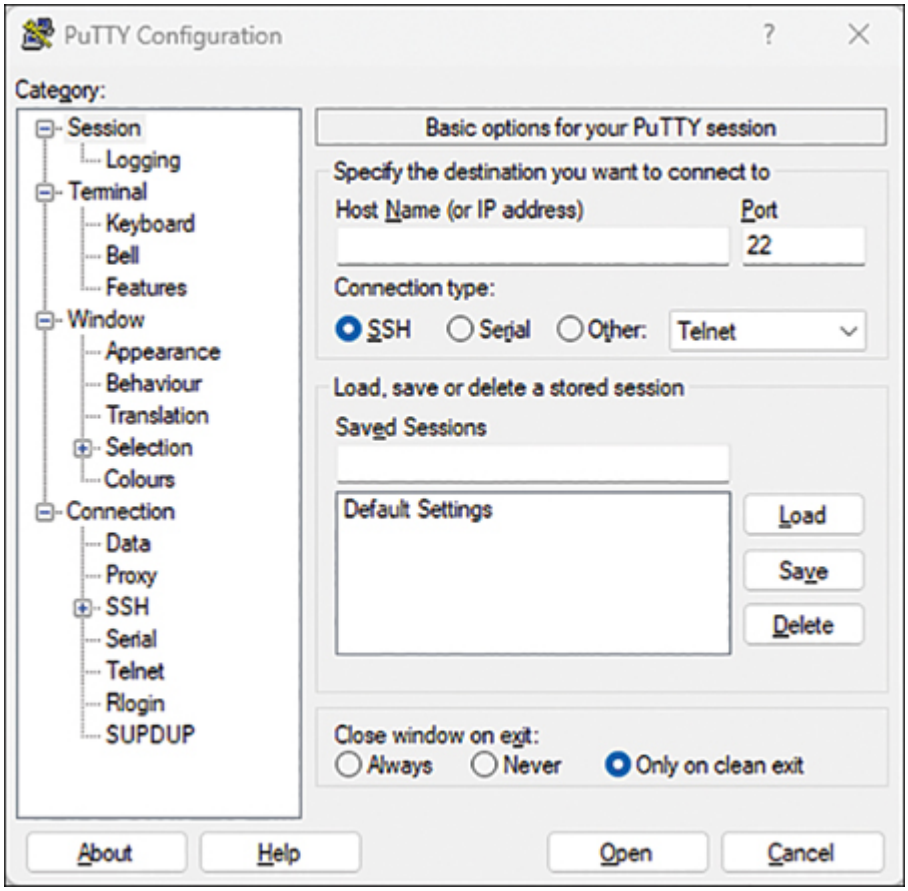


FIGURE 64.2 **SSH Connection Using PuTTY**

However, most of the time, you use SSH directly at the command line, usually by making use of OpenSSH. OpenSSH is a free, open-source tool

that is available on Windows, macOS, and Linux. The following is an example of an SSH connection from a Windows system to a remote system:

```
PS C:\Windows\System32> ssh user@10.42.0.15
user@10.42.0.15's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-91-generic x86_64)
Last login: Tue Nov 30 18:18:14 2021 from 10.42.0.253
user@telemetry:~$ hostnamectl
   Static hostname: telemetry
  Operating System: Ubuntu 20.04.3 LTS
            Kernel: Linux 5.4.0-91-generic
      Architecture: x86-64
user@telemetry:~$
```

Now, we removed *a lot* of content from these results to save space and concentrate on only what you need to know here. We started in the Windows PowerShell and typed the command **ssh user@10.42.0.15**. That means that we are using the SSH protocol to connect, and we are connecting to a computer with the IP address 10.42.0.15. (You could also connect by computer name, of course.) We connected as the user account called, simply, *user*. That is one of the accounts that exists on the remote computer already. SSH then requested the password for the *user* account. We typed that and were granted access to the remote system. (Keep in mind that we will only have access based on the *user* account permissions.) What kind of system did we connect to? If you said Linux, you'd be correct. To be precise, it is an Ubuntu Linux server, version 20.04. You can see that because we typed the Linux command **hostnamectl**, which provides the hostname of the computer, *telemetry*, and a set of additional information, including the OS and Linux kernel used by that OS.

The *user* account is a standard, restricted account, so at this point we can only accomplish basic things on this Linux server. If we wanted full control of the remote Linux system, we would have to log in as root or go the more recommended and secure route of logging in as a user account with **sudo** privileges. For more on **sudo** and the root account, see Chapter 40, "Linux." Also, there are more secure ways of connecting via SSH, such as by using

SSH keys. This discussion gets a bit beyond the A+ certification, but it gives you an idea of the power and depth of SSH. It should be used carefully and secured appropriately.

Note

For an OpenSSH how-to video, see https://greencurtaintraining.com/ssh.php.

Plenty of other SSH clients are available, but note these two important things:

- You must have SSH *installed* on the target device (consider OpenSSH if nothing is already installed).
- The SSH service must be turned on at the computer (or network device) that you want to remote into.

You should also be aware that other protocols and their tools can make use of SSH and port 22—for example, Secure Copy Protocol (SCP), Secure File Transfer Protocol (SFTP), and rsync. For the IT field, we strongly urge you to learn more about these tools and SSH in general.

ExamAlert

You will *definitely* see exam questions on SSH! Understand why you would use SSH, know how to use SSH client software to make connections to remote computers, and remember that SSH uses TCP port 22!

Simple Protocol for Independent Computing Environments (SPICE)

You learned about virtual machines (VMs) in Chapter 21, "Virtualization Concepts." As more and more computing moves to virtualization, both through VMs and their cousin, containers (also in Chapter 21), you will need a way to access these machines remotely. Enter the Simple Protocol for Independent Computing Environments (SPICE).

Originally proprietary, the SPICE protocol is now a widely used open standard for connecting to and managing virtual environments. It allows remote access to the virtual desktop as if you were directly at the host machine. Once it is configured, you can manage VMs just as if you were at the actual device. SPICE uses VDI (also discussed in Chapter 21) to make its connection. For more information about the SPICE project, see https://spice-space.org/.

ExamAlert

SPICE is regularly used to connect to virtual machines, so it is something that you can expect on the test. Know the basics of the protocol and how it connects.

Windows Remote Management (WinRM)

Windows Remote Management (WinRM) is the Microsoft implementation of the WS-Management protocol, a public standard for remotely exchanging management data between computing devices. It uses the Simple Object Access Protocol (SOAP) to allow interoperation between hardware and operating systems from different vendors.

When using WinRM, you can get management data from local and remote computers that have baseboard management controllers (BMCs) using WinRM scripting objects, the WinRM command-line tool, or the Windows Remote Shell (WinRS) command-line tool. If the remote system is running a Windows-based operating system that is also running WinRM, the management data is supplied by Windows Management Instrumentation (WMI). The data is formatted as objects as it is passed to WinRM.

You can also use WinRM to get information about non-Windows devices. The WS-Management protocol is SOAP-based and is formatted in XML.

For more information, see https://learn.microsoft.com/en-us/windows/win32/winrm/about-windows-remote-management, https://learn.microsoft.com/en-us/windows/win32/winrm/using-windows-remote-management, and https://learn.microsoft.com/en-us/windows/win32/winrm/windows-remote-management-reference.

ExamAlert

Passing management data from multiple devices allows you to see the health of your devices quickly and easily. WinRM is the tool you use to see that data. Understanding the basics of WinRM is important for understanding how this works. Check out the links before you take your exam so that you will be ready.

More Third-Party Tools

Plenty of other tools are available for the remote control of systems. We routinely use Virtual Network Computing (VNC) products such as RealVNC to remotely control Linux computers, macOS systems, and Android-based smartphones and tablets. Many other remote control tools are available. Your employer will likely have chosen a tool for you to use; each has its advantages and disadvantages. (We do not endorse any of these tools, and as always, you should use third-party tools with caution.)

You can also share your screen with other systems, which works well for collaboration and education. For example, use Miracast on Windows Surface systems or utilize a web-based webinar system such as Cisco Webex or ON24; these live-stream platforms are great for training and presentations. Or, you might share your screen using videoconference software such as Microsoft Teams, Zoom, or FaceTime. Many of these tools are beginning to converge, so as the market changes, all of them do very similar things. Just make sure that the remote users cannot take control of *your* system (unless you want them to and give them permission to do so).

The key with any of these tools is to make sure that they are secure. If you are connecting over the Internet, you need a secured session. Whether that is done by way of VPN for direct connections or by using an encrypted certificate when connecting via a browser (with TLS, RSA, and AES, for example), you need to make sure that the session is secure and that passwords are lengthy and hard to guess. Also consider using multifactor authentication (MFA) wherever possible.

VPN

We discussed virtual private networks (VPNs) briefly in Chapter 6, "Networked Hosts," and Chapter 38, "Windows Networking." In essence, a VPN provides a way of tunneling through the Internet securely instead of relying on the security (or lack thereof) of your ISP. Microsoft Windows VPN connections can be made with the following protocols: Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), Secure Socket Tunneling Protocol (SSTP), or Internet Key Exchange version 2 (IKEv2). At this writing (early 2025), the preferred methods for Windows clients are SSTP and IKEv2. Certain Windows VPN security features work only with IKEv2; for example, LockDown VPN secures a computer in such a way that traffic can flow only over the VPN connection, and no other network connections or adapters, while the VPN session is active. You can also configure traffic filtering rules based on protocols and using port and IP address ranges.

When signing into a VPN from a Windows client, you need to know the server name or IP address (which is often a public IP address), and you need to configure the VPN type (such as IKEv2). Then you have to specify the sign-in information, which could be the typical username and password or might use a smart card, an OTP, or a certificate.

Windows 11 VPN supports major protocols including IKEv2, L2TP, PPTP, SSTP, and Automatic (which tries each of the built-in tunneling protocols in turn). This allows users to configure and connect to VPNs using the built-in VPN client using any of these protocols. Here are certain things to note about some of these protocols:

- IKEv2 is considered the most widely used and preferred protocol. It is fast and stable, and it works well with mobile devices
- SSTP was developed by Microsoft and is commonly used in Windows environments.
- L2TP and PPTP have fewer security features than the other protocols. If you have a choice, choose one of the other protocols.

ExamAlert

Know that VPNs use secure tunneling protocols to connect secure private networks (or devices) together through public (unsecured) networks such as the Internet. Remember that a VPN provides users with the equivalent of a private network in terms of security. VPNs can also be used as a means of establishing secure remote connectivity between a remote system and another network.

Note

Some organizations use VPN servers or appliances that are not quite compatible with the Windows VPN client. In such cases, always-on VPN services such as OpenVPN can be used, but a separate client has to be downloaded and installed to the Windows computer.

Note

You might opt to run RDP or SSH through a VPN for added security, especially if you are remoting to a computer on the Internet. Some people use OpenSSH with OpenVPN tunneling.

Cram Quiz

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

1. Which program enables users to invite a technician to help repair their computer remotely?

   - **A.** Remote Desktop Connection
   - **B.** Remote Assistance
   - **C.** RDP
   - **D.** Remote connectivity

2. You have been tasked with making a command-line–based remote connection to an Ubuntu Linux computer located on your LAN so that you can run two scripts on it as an administrator. What protocol should you use? (Select the best answer.)

   - **A.** RDP
   - **B. mstsc**
   - **C.** SSH
   - **D.** VPN

3. You are in charge of setting up the administrators' connections to remote Windows computers located at satellite offices using RDP. What are some of the ways to make these connections more secure? (Select the three best answers.)

   - **A.** Use strong passwords.
   - **B.** Use OpenSSH.
   - **C.** Use network-level authentication.
   - **D.** Use PuTTY.
   - **E.** Use L2TP and IKEv2.

4. You are tasked with updating a network switch at a customer location. You need to make sure that data is not sent in plaintext

over untrusted networks. Which of the following protocols should you implement? (Select the two best answers.)

- **A.** RDP
- **B.** SSH
- **C.** FTP
- **D.** SCP
- **E.** Telnet
- **F.** VNC

5. You are a technician working on a help desk. One of your customers installed a program to Windows that requires a license key. After the user contacted you, you accessed the customer's system and entered the license key manually. Which tool did you use to accomplish this?

- **A.** SSH
- **B.** FTP
- **C.** RDP
- **D.** rsync

6. Why might you use SPICE in a virtualized environment?

- **A.** To establish secure remote access to physical servers
- **B.** To enhance remote desktop performance for virtual machines
- **C.** To manage firewall configurations for network security
- **D.** To automate software deployment across multiple endpoints

7. When would you use Windows Remote Management (WinRM) in a networked environment?

- ❍ **A.** To remotely execute commands and manage Windows systems using PowerShell and Windows Management Instrumentation (WMI)
- ❍ **B.** To establish a VPN connection between remote users and corporate networks
- ❍ **C.** To provide graphical remote desktop access to Windows servers
- ❍ **D.** To back up and restore system files on remote machines

8. Before using Windows Remote Management (WinRM) to execute remote commands, what must an IT technician do first?
   - ❍ **A.** Enable and configure WinRM on the target machine
   - ❍ **B.** Install third-party remote desktop software
   - ❍ **C.** Disable the Windows Firewall for unrestricted access
   - ❍ **D.** Assign a static IP address to all remote machines

Cram Quiz Answers

1. **B.** Remote Assistance calls can be made from users to invite other users to help fix problems for them. Remote Desktop connections are the connections that a computer makes to a remote computer to control it.

2. **C.** Use Secure Shell (SSH) to connect to the Ubuntu Linux computer, take control, and run the scripts as required (within Vim or your favorite text editor). You could also incorporate a VPN, but if both systems are on the LAN, a VPN might not be necessary. RDP is the protocol (and commonly used name) behind the Windows Remote Desktop Connection software. **mstsc** is the command-line executable for Remote Desktop Connection.

3. **A, C, and E.** Always use strong passwords (based on length, complexity, or a mixture of the two), as well as network-level authentication, which requires the user's credentials from the client

computer. Also, because the connections in this case are to remote offices, consider using a virtual private network (VPN). Layer 2 Tunneling Protocol (L2TP) is a decent solution for a VPN (if configured properly), but OpenVPN or another always-on VPN service is usually better. Internet Key Exchange version 2 (IKEv2) is the preferred VPN protocol on Windows computers. OpenSSH and PuTTY are used for SSH connections, but they wouldn't be used in this Windows-based scenario because the task requires RDP—meaning the Remote Desktop Connection program.

4. **B and D.** One secure method for moving data over a network is to use Secure Copy Protocol (SCP). This rides on SSH and so, in essence, it means you are using both SCP and SSH. RDP is used to remotely control a Windows system. File Transfer Protocol (FTP) is another method for moving data but is not inherently secure. Using Telnet is an older and deprecated way of connecting to remote systems; SSH should be used instead. VNC is another remote control tool.

5. **C.** You most likely used the Remote Desktop Connection program, which is based on RDP. This program would allow you to remotely control the customer's system and add the license key (which perhaps only your team has access to). SSH is used for controlling remote systems from the command line. It is unlikely that you would use SSH to enter a license key. But it is quite likely that you would use it to connect to a Linux-based system in a data center or in the cloud. FTP and rsync are used to transfer entire files (or groups of files) but not to perform tasks such as entering license keys into an application.

6. **A.** SPICE, the Simple Protocol for Independent Computing Environments, is used to access remote desktop connections to virtual machines. SPICE does not enhance the performance of the virtual machines, nor is it related to firewalls or deployment of virtual machines.

7. **A.** WinRM is designed for remote command execution and system management in Windows environments. It can also be configured

via PowerShell and WMI. WinRM is not a type of VPN, nor does it provide a graphical interface (you use PowerShell and WMI, which are both command-line tools). It is designed to help you manage the machines, which could include backups, but WinRM does not do the backups themselves.

8. **A.** WinRM must be configured on any target machine before it can be used to manage the machines. Once configured on the target machine(s), WinRM can be used to manage all sorts of Windows machines. With WinRM, the technician does not need to install additional third-party remote access software. WinRM is recognized by the firewall; enabling it makes the firewall connections for you. IP addressing is handled via the WinRM service itself so you don't have to do that manually.

Great work! One chapter of content to go! You are well on your way to the A+ exam!

Chapter 65

Appropriate Use of Artificial Intelligence

This chapter covers the following A+ 220-1202 exam objective:

- **4.10** – Explain basic concepts related to artificial intelligence (AI).

Here we have the last of the 220-1202 chapters. It's awesome that you've made it this far. Just a little further to go.

Artificial intelligence (AI) promises to change the workplace in many ways. This is true for IT workers as well. For the person who takes appropriate advantage of it, AI can work alongside you to make your workload more manageable. For the person who is overwhelmed by it or who uses it inappropriately, it can become a burden or, in a worst-case scenario, it might even lead to job loss. Don't let that happen to you! Let's take a look at how you can use AI to your advantage.

ExamAlert

Objective 4.10 focuses on applying AI in applications; appropriate policies regarding AI; AI limitations including bias, hallucinations, and accuracy; and private vs. public data security, data sources, and data privacy while using AI in the IT workforce.

Application Integration

More and more, AI is being integrated into applications themselves. From Cortana being available in Windows, Copilot being available in Microsoft 365, to voice assistants that translate spoken words into text, AI is becoming an integral part of many common applications. With this ready availability of AI comes issues of privacy and security, however, which we will discuss in the next few sections.

Policy and Privacy

Workplace policies surrounding artificial intelligence are evolving and will change rapidly in the upcoming years as AI changes. Let's look at some specific issues that will force those policy changes. Some organizations forbid AI entirely. Others permit it entirely. Neither approach will make sense in the long run because the spread of AI is going to make both approaches difficult (perhaps impossible) to maintain.

Privacy Concerns with Productivity Tools

AI is being integrated into everyday office tools. For instance, as Copilot integrates further and further into Microsoft 365, it will be difficult for most organizations (especially small organizations) to turn it off. And privacy concerns will start to force those organizations that take a laissez-faire approach of allowing anything to start putting restrictions into place. That becomes even more important when we deal with plagiarism, where AI might inadvertently plagiarize documents that others have uploaded while asking for assistance.

Appropriate Use

Plagiarism is troublesome enough for ordinary business users, but it becomes a security issue for IT workers. If, for instance, you ask AI to help you solve an issue with an access control list (ACL), and in doing so you upload your ACL to AI and ask it to find the errors, your code might "leak" later to other users of AI—thus inadvertently opening your network to

others. Similar issues exist if you upload a script for a project to AI asking it for troubleshooting assistance: Your script could make its way to another person when AI is helping them.

A better approach is to ask AI to give you a solution to the problem and then explain it to you. Instead of saying "Here is my code; what is wrong with it?" say "I am working on solving *xyz* problem; can you give me an example solution and explain the steps you used to solve it?" Then compare the sample code to your code, using the steps provided to help you learn how to do it yourself (so you won't run into the issue in the future).

This approach has multiple benefits. First, you aren't giving out your work to the AI, so your privacy—and that of your company and your clients—is maintained. Second, you are learning from the AI and becoming better at your job (always a good thing!). Finally, you are paying attention to the limitations of the AI system. It isn't always right, after all.

Table 65.1 outlines the appropriate, responsible, and ethical uses of AI.

TABLE 65.1 **Appropriate and Ethical Uses of AI**

Appropriate Uses of AI	Responsible and Ethical Uses of AI
Brainstorming: Use AI to help generate ideas, suggest topics, or provide examples.	**Be mindful of privacy:** Be careful with personal information and understand privacy settings.
Research: Use AI to help with research, such as confirming understanding, and checking writing (don't rely on it for sources, though, since it may make those up).	**Be critical:** Use AI to support your own thinking and ideas, rather than relying on it solely.
Scheduling: Use AI tools to manage appointments and deadlines.	**Be transparent:** Disclose your intended use of AI, and be aware of the terms of service.

Appropriate Uses of AI	Responsible and Ethical Uses of AI
Tutoring: Use AI to help with individual tutoring.	**Be aware of limitations:** Don't assume that AI-generated results are accurate or that they are not based on other sources.
Writing: Use AI to help with drafting, but also edit, fact-check, and add your own ideas.	**Acknowledge AI use:** Include an acknowledgment of how you used AI, including your prompts and the generated output.

Limitations of AI

AI might seem like the end all, be all, and the media will tell you that this is true. If you watch sci-fi movies, AI is there to either save the day or destroy the world (or to destroy the world while trying to save the day sometimes too). In reality, it is just a machine doing a job.

Bias

AI has bias. It knows only what it has been taught. Generally, this is due to the human biases that skew the original training data. It is another form of the adage "garbage in, garbage out," but with AI. Due to the nature of AI (and especially with people thinking that AI is somehow infallible—something you need to avoid believing!), this bias becomes even more problematic.

Bias can impact an organization's success and hinder a person's ability to participate in the economy. It reduces the accuracy and usefulness of AI. There was a case at Amazon in 2015 that ended up biased against women engineers. The goal was to make an even playing field in hiring by using AI instead of human reviewers, but in the process, the company ended up accidentally training the AI to discriminate (there is no indication that any of the bias was deliberate). In the end, the entire project had to be scrapped;

none of the work could be saved. The bias in the source material was just too much for it to continue at all.

Hallucinations

When AI does not know the answer, it generally doesn't admit it. AI *hallucinations* are the false or misleading information that AI models produce. They can happen in image recognition, text generation, and other AI systems. Put simply, AI makes up the answer. As a general rule, this is due to gaps or misunderstandings of patterns in the training data. After all, AI is a machine and is not deliberately trying to mislead users. Being aware that AI may make up solutions is important. In the past, we have found links within AI results to be most problematic, but it can happen in other ways as well. In fact, one of the easiest ways to find plagiarism is to look at the citations; it is not uncommon for the citations to be made up or otherwise have errors, and more than one person has been tripped up as a result. Solutions include having high-quality training data, using structured data templates, using refined data sets and prompting techniques, and using human beings to fact-check AI for accuracy. With enough data, AI can stop hallucinating eventually.

Accuracy

AI will sometimes give misleading or incorrect results and sometimes will make up answers (this is especially true of citations, in our experience). Sometimes the reason is that it doesn't have enough data to make predictions about the data as a whole; the data set is incomplete, biased, or otherwise flawed.

Sometimes these inaccuracies are harmless, such as when AI predicts rain when there is none in the forecast. This could result from insufficient historical data about weather patterns. Sometimes the reason is much more problematic, such as when AI flags a transaction as fraudulent when it is not, or vice versa, based on insufficient historical data and patterns. With the use of AI in virus and intrusion detection systems, it becomes critical that the training of the AI systems be top-notch.

Finally, sometimes AI gives the wrong answer. We know a college math instructor who asked AI to solve a calculus question. Not only did the AI get the answer wrong, but it doubled down when questioned, explaining incorrectly why its answer was right. Only after the math instructor explained the how and why of the mistake that the AI had made (it missed a derivative in the middle) did the AI correct itself and admit the mistake. Although the instructor used that scenario as an example to his class to not use AI as a crutch, it is a cautionary tale for us: We need to be wary of the answers we get to important questions we ask of the AI systems we use.

Especially in the IT field, if you accept the answers that AI gives you as gospel, you will find that sometimes the answers aren't correct or, worse, aren't completely correct. That can lead to corrupt data, scripts that don't run properly, and it might even introduce security issues. And this discussion doesn't even begin to address the privacy concerns mentioned previously. As a technician, you need to avoid putting yourself in this position. Be cautious when using any AI. Know its limitations and watch for them. But know that AI is coming and can be a useful tool for helping with your work!

Note

AI will become a more integral part of the modern workforce in the future. Don't be afraid of it, but also don't use it as a crutch. So long as you know the limitations, you'll do fine.

Cram Quiz

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

1. When implementing AI in the IT workflow, which of these do you need to pay close attention to? (Select all that apply.)

   ○ **A.** Data security

- ○ **B.** Bias
- ○ **C.** Accuracy of results
- ○ **D.** Company policies
- ○ **E.** Network ACLs

2. Plagiarism is a problem with AI. Why? (Select all that apply.)

- ○ **A.** AI uses prior queries as answers to future queries.
- ○ **B.** AI will hallucinate correct answers.
- ○ **C.** The data source of your AI is often unknown.
- ○ **D.** You can copy and paste from the AI without being accused of plagiarism.

3. What can you do to assure data security when using AI to help you with a scripting task?

- ○ **A.** Paste your entire script and ask AI to correct it for you.
- ○ **B.** Ask AI how to solve a problem and then paste that code into your script and run it directly.
- ○ **C.** Ask AI how to solve a problem and explain its answer. Once you understand how to do it, write your own script.
- ○ **D.** Avoid asking the AI any questions about scripting. (You should already know this from Chapter 62, "Basic Scripting, Part I," and Chapter 63, "Basic Scripting, Part II."

4. AI gives an answer that turns out to not be correct. What may have happened?

- ○ **A.** AI was right; other people just misunderstood what truth is all about.
- ○ **B.** Citations changed after the AI was trained.
- ○ **C.** AI was programmed with incomplete data, so it made up data to compensate for the lack.

- ○ **D.** AI had partial data and made up citations to justify its position.

Cram Quiz Answers

1. **A, B, C, and D.** Pay close attention to ensure that you are not inadvertently giving out your company's data as you use AI. Pay close attention to any bias that exists in the AI system. Also, be aware that the results may not always be accurate. Follow all company policies regarding the use of AI; some forbid it entirely, and you don't want to get in to trouble for violating that.

2. **A and C.** You don't usually know the data source upon which your AI was trained. Using its answers directly can lead to charges of plagiarism because the AI might have been trained on copywritten sources. Even if not, you should never copy and paste directly. Instead, research any answer to ensure that it is correct (after all, AI can be wrong!) and then rephrase into your own words. AI can be helpful, but it isn't always right.

3. **C.** Ask the AI for its own answer to the problem you are having and ask it to explain how it got to the answer. Once you understand the answer, you will be able to do it yourself.

   You are not expected to know all of this already. Even very experienced technicians use reference books and the advice of other technicians when they run into trouble; that's why collaboration is so important. Keep asking good questions, and soon you will be the expert!

4. **C and D.** When AI has an incomplete data set, it will sometimes make up the answer. This is called hallucinating. Sometimes, it will even make up citations that might look real but are totally fake. Be sure to double-check anything you produce with AI for accuracy.

If you have come this far, we congratulate you! This is the last chapter of the actual CompTIA A+ objective-based content. Completing 65 chapters is quite a lot, even for superheroes. Well done!

Next is the final chapter, where we give some tips for passing the exam and close out the book. Following that you will find the 220-1202 practice exam. Take a break (you deserve it), and then continue on to the practice exam!

If you are planning on taking the actual CompTIA A+ Core 2 (220-1202) exam, be sure to go through the 220-1202 checklist, located in "Introduction to Core 2 (220-1202)," just before Chapter 29.

Chapter 66

Getting Ready for the Exams, and Farewell

This chapter provides some additional tools and information to help you be successful when preparing for and taking the CompTIA A+ Core 1 (220-1201) and Core 2 (220-1202) exams:

- Getting ready for the exams
- Tips for taking the real exams
- Beyond the CompTIA A+ certification

Caution

Don’t skip this chapter! We impart some of the most vital things you need to know about taking the real exams here.

Getting Ready for the Exams

The CompTIA A+ certification exams can be taken by anyone; there are no prerequisites, but CompTIA recommends one year of hands-on experience as an IT support specialist job role. For more information on CompTIA and the A+ certification, visit https://www.comptia.org.

Also visit our A+ page, at https://greencurtaintraining.com, for information, additions, and updated errata.

To acquire your A+ certification, you need to pass two exams: the Core 1 (220-1201) and the Core 2 (220-1202). These exams are administered by Pearson VUE (https://home.pearsonvue.com). You need to register with Pearson VUE to take the exams.

ExamAlert

We strongly suggest that you do not take both exams on the same day. Instead, take them a week or so apart (at least). Trust us on this.

Note

If you haven't already, make use of the step-by-step checklists for each exam, located in the 220-1201 and 220-1202 introductions in this book.

Each exam consists of two types of questions:

- **Multiple-choice:** This type of question asks you to select the correct answer (or answers) from a group of four or more choices. These questions are similar to the questions you've seen throughout this book.
- **Performance-based:** This type of question asks you to answer, complete a configuration, or solve a problem in a hands-on fashion. These questions might ask you to drag and drop information to the correct location or complete a simulation in an emulated or virtual system.

To become proficient at both types of questions, you will need to have a deep understanding of the theory, and you will also need hands-on skills. So, use the companion website materials (described in the Introduction) and practice on actual computers as much as possible. This is, of course,

imperative for the exams, but it is even more important for the real world. The more you install, configure, and troubleshoot real systems, the better you will be prepared for job interviews as well as whatever comes your way once you have acquired a position within an organization.

ExamAlert

You've been warned! Practice as much as possible on the following:

- Real desktop/laptop computer hardware and software
- A SOHO router
- Smartphones and tablets
- Printers, displays, and other peripherals

Be sure to look at the "CompTIA A+ Core 2 (220-1202) Hardware and Software List" section of the CompTIA A+ Certification Exam Objectives for EXAM NUMBER: CORE 2 (220-1202) that you can download from https://partners.comptia.org/docs/default-source/resources/comptia-a-220-1202-exam-objectives-(2-0).

An Important Note Regarding Exam Questions

This book does not offer the exact questions that are on the exam. There are two reasons for this:

- CompTIA reserves the right to change the questions at any time. Any changes, however, will still reflect the content within the current A+ objectives.
- The contents of the CompTIA A+ exams are protected by a nondisclosure agreement (NDA). The NDA states that the questions within the exams are not to be discussed with anyone, and anyone who sits for an exam has to agree to this NDA before beginning a test.

So we cannot tell you exactly what is on the exams, but we do cover all of the exam objectives within this book to give you the best chance of passing the exams.

In addition to using the tear-out Cram Sheet in the beginning of this book (print version), one great way to study is to compile and use a "cheat sheet." We are not saying to cheat (nor do we condone it); we're saying you should create a *key facts* document, containing things that you want to memorize or have a hard time memorizing, such as numbers, acronyms, procedures, minimum requirements, and so on. Include whatever you feel would help you most.

Table 66.1 provides a partial example of a cheat sheet that you can create to aid in your studies. Fill in the appropriate information in the right column. For example, the first step of the six-step troubleshooting methodology is "Identify the problem."

TABLE 66.1 **Example Cheat Sheet**

Concept	**Fill in the Appropriate Information Here**
The six-step troubleshooting methodology	1. 2. 3. 4. 5. 6.
List of commonly used ports	
The laser imaging process	
The malware removal process	
Windows editions and their differences	
Commands and descriptions (For example, **ping** tests to see whether other systems on the network are live.)	
Etc. *	

* Continue Table 66.1 in this fashion on paper. The key is to write down various technologies, processes, step-by-step procedures, and so on to commit them to memory.

Tips for Taking the Real Exams

You might be new to certification exams. This section is for you. If you have taken certification exams before, feel free to skip this section or use it as a review.

Certification exams are conducted on a computer and are composed of multiple-choice and performance-based questions. You have the option to skip questions. If you do so, be sure to mark, or "flag," them for review before moving on. Feel free to mark any other questions that you have answered but are not completely sure about. This approach is especially recommended for the performance-based questions. In fact, you might choose to leave all of the performance-based questions until the end (and some people prefer to do all of the performance-based questions at the beginning). That, of course, is up to you.

When you get to the end, you will see an item review section, which shows you any questions that you did not answer and any that you flagged for review. Be sure to answer any questions that were not completed.

The following lists share tips and tricks that we have developed over the years. We've taken at least 20 certification exams over the past two decades, and the following points have served us well.

General Practices for Taking Exams

- **Pick a good time for the exam:** It appears that the fewest number of people are at test centers on Monday and Friday mornings. Consider scheduling during these times. Otherwise, schedule a time that works well for you, when you don't have to worry about anything else. Keep in mind that Saturdays can be busy. You might also choose to take the test remotely, online from a location of your choice. See the following links for more information about taking a test from home:

  https://www.pearsonvue.com/us/en/comptia.html

https://www.pearsonvue.com/us/en/test-takers/onvue-online-proctoring.html

https://home.pearsonvue.com/comptia/onvue

https://www.comptia.org/testing/testing-options/take-online-exam

Very important: *Don't schedule the exam until you are ready to take it*. We understand that sometimes deadlines have to be set, but in general, don't register for the exam until you feel confident you can pass. Things come up in life that can sometimes get in the way of your study time. Keep in mind that most exams can be canceled as long as you give at least 24 hours' notice. (To be sure, though, double-check that time frame when registering.)

- **Don't overstudy the day before the exam:** Some people like to study hard the day before; some don't. Our recommendations are to study using the Cram Sheet and your own cheat sheet, but in general, don't overdo it. It's not a good idea to go into overload mode the day before the exam. We know the book is called *Exam Cram*, but cramming at the last minute isn't a good idea in the real world.
- **Get a good night's rest:** A good night's sleep (seven to nine hours) before the day of the exam is probably the best way to get your mind ready for an exam.
- **Eat a decent breakfast:** Eating is good! Breakfast is number two when it comes to getting your mind ready for an exam, especially if it is a morning exam. Just watch out for the coffee and tea. Too much caffeine for a person who is not used to it can be detrimental to the thinking process.
- **Show up early:** The testing agency recommends that you show up 30 minutes prior to your scheduled exam time. This is important; give yourself plenty of time and make sure you know where you are going. Know exactly how long it takes to get to a testing center and account for potential traffic and construction. You don't want to have to worry about getting lost or being late.

  Stress and fear are mind killers. Work on reducing any types of stress the day of and the day before the exam. By the way, you do need extra time because when you get to the testing center, you need to show ID,

sign forms, get your personal belongings situated, and be escorted to your seat. Have two forms of ID (signed) ready for the administrator of the test center. Turn off your cell phone or smartphone when you get to the test center; they'll check that, too. Showing up early applies to online testing as well. You will have to go through a similar information check and other things that will require time before the scheduled start time for the exam.

- **Bring ear plugs:** You never know when you will get a loud testing center or, worse yet, a loud test taker next to you. Ear plugs help to block out any unwanted noise in the location where you take the exam. Just be ready to show your ear plugs to the test administrator. While some test centers will offer these, don't rely on someone else to provide them. You should be prepared.
- **Brainstorm before starting the exam:** Write down as much as you can remember from the Cram Sheet and your cheat sheet before starting the exam. The testing center is obligated to give you something to write on; make use of it! Getting all the memorization out of your head clears the brain somewhat so that it can tackle the questions.
- **Take small breaks while taking the exam:** Exams can be brutal. You have to answer a lot of questions (typically anywhere from 65 to 90) while staring at a screen for an hour or more. Sometimes these screens are old and have seen better days, and any monitor can cause strain on your eyes if you stare at it too long. We recommend taking small breaks and using helpful breathing techniques. For example, after going through every 25 questions or so, close your eyes and slowly take a few deep breaths, holding each one for 5 seconds and then releasing each one slowly. Think about nothing while doing so. Remove the test from your mind during these breaks. This type of break takes only about half a minute but can help to get your brain refocused. It's almost a Zen type of thing. When we have applied this technique properly, our scores have improved, and we have even gotten a few perfect scores. It's amazing how the mindset can make or break you. This leads to our last and most important point:
- **Be confident:** You have studied hard, gone through the practice exams, created a cheat sheet. You've done everything you can to prep. These

things alone should build confidence. But actually, you just have to be confident for no reason whatsoever. Think of it this way: You are great. …I am great… (to quote Dr. Daystrom). But truly, there is no disputing this! That's the mentality you must have. You are not being pretentious about this if you think it to yourself. (Acting that way around others, well, that's another matter.) Build that inner confidence, and your mindset should be complete.

Smart Methods for Difficult Questions

- **Use the process of elimination:** If you are not sure about an answer, first eliminate any answers that are definitely incorrect. You might be surprised how often this approach works. This is one of the reasons it is recommended that you not only know the correct answers to the practice exam questions but also know why the wrong answers are wrong. The testing center should give you something to write on; use it to write down the letters of the answers that are incorrect to keep track. Even if you aren't sure about the correct answer, if you can logically eliminate anything that is incorrect, the answer will become apparent. The character Sherlock Holmes summed this up well: "When you have eliminated the impossible, whatever remains, however improbable, must be the truth." There's more to it, of course, but from a scientific standpoint, this method can be invaluable.
- **Be logical in the face of adversity:** The most difficult questions are those where two answers appear to be correct, even though the test question requires you to select only one answer. Real exams should not rely on "trick" questions. Sometimes you need to slow down, think logically, and compare the two possible correct answers. Also, you must imagine the scenario that the question is a part of. Think through step by step what is happening in the scenario. Write out as much as you can. The more you can visualize the scenario, the better able you will be to figure out which of the two answers is the better one.
- **Use your gut instinct:** Sometimes a person taking a test just doesn't know the answer; it happens to everyone. If you have read through a question and all the answers and used the process of elimination, sometimes gut instinct is all you have left. In some scenarios, you might

read a question and instinctively know the answer, even if you can't explain why. Tap into this ability. Some test takers write down their gut instinct answers before delving into the question and then compare their thoughtful answers with their gut instinct answers.

- **Don't let one question beat you!** Don't let yourself get stuck on one question, especially a performance-based question. Skip it and return to it later. When you spend too much time on one question, your brain gets sluggish. The thing with these exams is that you either know the answer, or you don't. But don't worry too much about it; chances are you are not going to get a perfect score. Remember that the goal is only to pass the exams; how many answers you get right beyond that is irrelevant. If you have gone through this book thoroughly, you should be well prepared. You should have plenty of time to go through all the exam questions with time to spare to return to the ones you skipped and marked.
- **If all else fails, guess:** Remember that the exams might not be perfect. A question might seem confusing or appear not to make sense. Leave questions like this until the end. After you have gone through all the other techniques mentioned, make an educated, logical guess. Try to imagine why the test would bring up this topic, as vague or as strange as it might appear. However, remember this: The more you study, the less you will have to guess.

Wrapping Up the Exam

Review all your answers. If you finish early, use the time allotted to you to review the answers. Chances are you will have time left over at the end, so use it wisely! Make sure that everything you have marked has a proper answer that makes sense to you. But try not to overthink! Give it your best shot and be confident in your answers. You don't want to second-guess yourself!

Beyond the CompTIA A+ Certification

CompTIA started a policy on January 1, 2011, which says that a person who passes the A+ exams will be certified for three years. To maintain the

certification beyond that time, you must either pass the new version of the exams (before the three years are up), pass a higher-level CompTIA exam (such as the Network+ or Security+), or enroll in the CompTIA Continuing Education (CE) Program. This program has an annual fee and requires that you obtain Continuing Education Units (CEUs) that count toward the recertification. There are a variety of ways to accumulate CEUs. See CompTIA's website for more information: https://www.comptia.org/continuing-education.

After you pass the exams, consider thinking about your technical future. Not only is it important to keep your current technical skills sharp, but technical growth is important as well; consider expanding your technical horizons by learning different technologies.

Usually, companies wait at least six months before implementing a newly released version of an OS or application on any large scale, but you will have to deal with it sooner or later. Windows, Linux, macOS, Android, and iOS are always coming out with new versions. Consider keeping up with the newest versions and obtaining access to the latest software and operating systems. Practice installing, configuring, testing, securing, maintaining, and troubleshooting them.

To keep on top of the various computer technologies, think about subscribing to technology websites, blogs, RSS feeds, and periodicals—and read them on a regular basis. Check out streaming video tech channels on the Internet. Join computer Internet forums and attend technology conventions. A technician's skills need to be constantly honed and kept up to date.

But the *best* advice we can give is for you to do what you love. From an IT perspective, we usually break it down by technology, as opposed to by the vendor or certification. For example, you might want to learn more about email systems, or securing internetworks, or you might prefer to work on databases, build websites, develop apps—who knows! You are limited only by your desire.

Final note: We wish you the best of luck on your exams and in your IT career endeavors. Please let us know when you pass your exams. We would

love to hear from you! Also, remember that we are available to answer any of your questions about this book via our website:

https://greencurtaintraining.com/

Sincerely,

David Bayne

Mark Smith

John Pickard

A+ Core 2 (220-1202) Practice Exam

The multiple-choice questions provided here help you to determine how prepared you are for the actual exam and which topics you need to review further. Write down your answers on a separate sheet of paper so that you can take this exam again if necessary. Compare your answers against the answer key that follows this exam. Read through the explanations and also the incorrect answers very carefully. If there are any concepts that you don't understand, go back and study them more.

Exam Questions

1. What macOS root level folder holds systemwide settings, resources, and support files used by the applications and the operating system itself?

   - **A.** /Applications
   - **B.** /Users
   - **C.** /Library
   - **D.** /System
   - **E.** /Users/Library

2. You plug a 32 GB flash drive into a Windows laptop. The flash drive has multiple smaller partitions that are not writable. Which of the

following **diskpart** commands can be used to remove the partitions so that you can later format the drive to full capacity?

- **A. repair**
- **B. clean**
- **C. merge**
- **D. extend**

3. Which command is used to list the contents of a directory in the Command Prompt?

- **A. cd**
- **B. dir**
- **C. ping**
- **D. ver**

4. You are a technician working at a help desk in tier 1 support, and you receive a call from a user whose computer is suffering from BSODs. Just as you receive the call, you realize that you are scheduled to take your break. What should you do next?

- **A.** Ask another technician to take the call for you.
- **B.** Ask the user to call back.
- **C.** Send the user to help desk tier 2.
- **D.** Troubleshoot the problem for the user.

5. Your company has multiple users who work with the same commercial software. What is the best type of license to purchase so that your company is in compliance with the EULA?

- **A.** Seat license
- **B.** Commercial license
- **C.** Enterprise license
- **D.** Open source license

6. Which of the following best describes the primary tactic used in a business email compromise (BEC) attack?

- **A.** Exploiting vulnerabilities in third-party software to infiltrate a target's network
- **B.** Inserting malicious scripts into a web page to gain elevated privileges
- **C.** Impersonating trusted individuals via email to deceive employees into transferring funds or divulging information
- **D.** Injecting malicious code into the software build or update process

7. One of your coworkers tells you that whenever they return to their desk, they have to type their username and password to unlock the computer. They say they cannot modify the screensaver. After analyzing the system, you notice that the screensaver and the screen lock options are indeed grayed out. Which of the following is the most likely reason for this?

- **A.** Incorrect local-level user policies
- **B.** Domain-level group policies
- **C.** Antivirus domain-level policies
- **D.** Corrupted Registry

8. Which of the following features in Windows allows the following command to run?

```
$PSVersionTable
```

- **A.** Compatibility mode
- **B.** OneDrive
- **C.** Windows Defender Firewall
- **D.** PowerShell

9. You have been tasked with printing a Group Policy configuration report to an HTML file for offline review. Which of the following commands will enable you to do this?

- **A. gpresult**
- **B. gpupdate**
- **C. gpedit.msc**
- **D. secpol.msc**

10. Which of the following commands should you use to find out what edition of Windows is running?

- **A. pathping**
- **B. winver**
- **C. ls**
- **D. hostname**

11. Which of the following technologies focuses on analyzing endpoint activity to detect unexpected behavior and potential threats, providing context for incident response?

- **A.** Endpoint protection platforms (EPP)
- **B.** Managed detection and response (MDR)
- **C.** Email security gateway
- **D.** Endpoint detection and response (EDR)

12. One of the users in your company frequently leaves their workstation and wants to make sure that their confidential data is not accessed by anyone else. However, the user does not want to turn off the computer when they leave work in the evening. Which of the following is the best solution for securing the workstation?

- **A.** Implement a password and fingerprint lock for after-hours login.
- **B.** Set a strong password that requires a renewal every 30 days.

- **C.** Apply a screen lock after 5 minutes of nonuse and set login time restrictions for after-hours.
- **D.** Run a screensaver after 1 minute of nonuse and a fingerprint lock for after-hours.

13. A manager suspects that a user has obtained movies and other copyright-protected materials through the use of a BitTorrent client. The incident response tech confirms the suspicion; the user is in violation of company policy. What should the incident response technician do next?

- **A.** Immediately delete all unauthorized materials.
- **B.** Secure the workstation in a limited-access storage facility.
- **C.** Reprimand the user and apply a content filter to the user's profile.
- **D.** Document the incident and purge all policy-violating materials.

14. You are required to update a Linux server in a remote data center. Company policy states that you must connect in a secure fashion, using the command line only. Which of the following tools should you use?

- **A.** RDP
- **B.** SFTP
- **C.** VNC
- **D.** SSH

15. You work for an organization that uses various permissions for individual user accounts. One of the managers with a restricted user account receives the following message:

Windows Update cannot currently check for updates because the service is not running.

The manager contacts your organization's help desk to report the error. You connect to the manager's computer and identify the problem. What action should you take next to quickly resolve the problem?

- ○ **A.** Reboot the computer.
- ○ **B.** Roll back the device drivers.
- ○ **C.** Restart the appropriate service(s).
- ○ **D.** Rebuild the Windows profile.

16. Your security team needs to satisfy the following requirements of a disaster recovery plan:

- ▶ The last month of backups should be easily accessible and preferably on-premises.
- ▶ Long-term backups should be stored offsite.
- ▶ There should be minimal use of hardware.

Which of the following answers will best meet the requirements?

- ○ **A.** Store backups with a cloud provider and onsite.
- ○ **B.** Store 30 days' worth of backups onsite and store anything older than that with an offsite cloud provider.
- ○ **C.** Store all backups with a cloud provider.
- ○ **D.** Store backups onsite and use cloud bursting if the backup hardware demands more resources.

17. You have been asked to set up a new networking closet, and you notice that the humidity level in the room is very low. Which of the following tasks should be done before rack-mounting any networking equipment?

- ○ **A.** Install grounding bars.
- ○ **B.** Set up a dehumidifier.

- **C.** Use an ESD strap.
- **D.** Implement a fire suppression system.

18. Which authentication factors are used to verify a person's identity? (Select all that apply.)

- **A.** Knowledge
- **B.** Possession
- **C.** Inherence
- **D.** Context
- **E.** Behavioral
- **F.** Location-based

19. Jenny from accounting reports that when pressing Ctrl+Alt+Del to log on to a Windows workstation, she is asked for a PIN. Which of the following should you tell Jenny?

- **A.** "Enter all the passwords that you have used previously."
- **B.** "Reboot the computer."
- **C.** "Check the network cable."
- **D.** "Please verify that you are using your smart card."

20. A surge suppressor safeguards connected equipment by directing surges to the_____.

- **A.** path of least resistance
- **B.** path of shortest conductance
- **C.** path of lowest inductance
- **D.** path of highest voltage

21. By default, a file or folder receives its NTFS permissions from the parent folder. Which of the following terms is used for this process?

- **A.** Permission propagation

- **B.** Single sign-on (SSO)
- **C.** Client-side virtualization
- **D.** Proxy settings
- **E.** Recovery image
- **F.** Inheritance

22. Which of the following are examples of physical security? (Select the two best answers.)

- **A.** Directory permissions
- **B.** OTP hardware tokens
- **C.** Principle of least privilege
- **D.** Privacy filters

23. You have been given technical documentation from the network administrator that details the switch ports that you need to use for an upcoming network upgrade. Which of the following documents did you receive?

- **A.** Change control form
- **B.** Process diagram
- **C.** Network topology diagram
- **D.** Fiber backbone diagram

24. Which of the following will help protect an organization from further data exposure *after* a list of passwords has already been leaked due to a policy breach? (Select the two best answers.)

- **A.** Require strong passwords.
- **B.** Use multifactor authentication.
- **C.** Educate end users.
- **D.** Enable file encryption.

- **E.** Restrict user permissions.

25. A user is reporting that their web browser is not going to the site they are trying to access. Which of the following statements describes the best way to resolve this issue?

- **A.** Ensure that the user is not using a proxy server.
- **B.** Remove all Internet shortcuts.
- **C.** Delete all Internet cookies.
- **D.** Clear all Internet cache.

26. A customer wants to use FTP to push configurations to a couple of switches that they are updating. The customer can use the FTP program on a laptop and can place the configurations in the proper directories of the switches. But the switches cannot communicate to the PC with FTP. How can you resolve the problem?

- **A.** Change the laptop's IP address to dynamic.
- **B.** Make sure that the laptop's IP address is in the correct VLAN.
- **C.** Generate a static DNS entry on the server for the laptop.
- **D.** Create an exception in the local firewall of the laptop.

27. A customer's mobile device seems to be losing battery life rapidly, and the device is very warm. It is a relatively new mobile device, so the customer believes it must be defective. You inspect the device and find the following:

- Storage: 48 GB used
- Display: Brightness: Auto
- Mail: Pull every 15 minutes
- Privacy: Maps: always enabled

Which of the following should you modify to fix the problem?

- **A.** Storage
- **B.** Display
- **C.** Mail
- **D.** Privacy

28. Which of the following are ways to remove data from a storage drive through destruction? (Select the two best answers.)

- **A.** Disabling ports
- **B.** Shredding
- **C.** Drilling
- **D.** Using low-level formatting

29. Which of the following Internet Options tabs should you access to enable TLS in Internet Explorer?

- **A.** Security
- **B.** Privacy
- **C.** Advanced
- **D.** Connections

30. You are attempting to install a Windows 64-bit OS within a VM, but you keep receiving errors. The specifications for the VM include

- Four 1 GHz CPUs
- 4 GB of RAM
- 15 GB storage drive space
- 720p screen resolution

Which of the following should you do to resolve this issue?

- **A.** Increase the number of CPUs.
- **B.** Increase the amount of memory.

- ○ **C.** Increase the amount of drive space.
- ○ **D.** Increase the screen resolution.

31. Your organization's network consists of 25 computers that are wired to a switch. Your boss is interested in employing a file server with network shares and a print server. Which of the following Windows network setups should you recommend?

- ○ **A.** Workgroup
- ○ **B.** Ad hoc
- ○ **C.** Spoke-hub
- ○ **D.** Domain

32. Which of the following is the best example of the use of chain of custody?

- ○ **A.** The technician notes the date, time, and who was given the computer.
- ○ **B.** The technician remembers when and who they gave the computer to.
- ○ **C.** The technician uses a third party to hand over the computer to the proper authorities.
- ○ **D.** The technician calls the supervisor after the computer has been transferred.

33. You just installed a new updated driver for a network interface card (NIC). Now you want to test its data transfer rate. What tool should you use to run your test?

- ○ **A.** Device Manager
- ○ **B.** Local Security Policy
- ○ **C.** Performance Monitor
- ○ **D.** System Information

34. You just got your first IT job working at a help desk. You get a call from a user about an issue you have never seen before, and you are not sure where to begin troubleshooting. What is the first course of action you should take?

- **A.** Tell the customer that this is the first time you have encountered this problem and to please be patient.
- **B.** Tell the customer that the problem needs to be escalated to a higher-tier technician.
- **C.** Tell the customer to please hold while a senior technician is consulted regarding the problem.
- **D.** Ask the customer if they would mind holding for no more than 2 minutes to check resources.

35. What is the primary purpose of Kerberos?

- **A.** To provide centralized administration for dial-up, VPN, and wireless authentication
- **B.** To act as a three-headed guard dog protecting network servers from illegitimate login attempts
- **C.** To enable computers to securely prove their identity to each other in client/server environments
- **D.** To separate authentication, authorization, and accounting functions for network access

36. Which Windows utility can be used to see which user is currently logged on?

- **A. msconfig**
- **B.** Disk Management
- **C.** Task Manager
- **D.** Windows Tools or Administrative Tools

37. Which of the following tools are commonly used to remove dust from the inside of a computer? (Select the two best answers.)

- **A.** Compressed air
- **B.** Cotton and alcohol
- **C.** Feather duster
- **D.** Antibacterial surface cleaner
- **E.** Vacuum

38. You have been tasked with downloading an operating system image to be installed to a virtual machine. Which of the following file types will you most likely download?

- **A.** EXE
- **B.** appimage
- **C.** ISO
- **D.** VDI

39. Which of the following is a common symptom of a problem that can occur while starting up the Windows operating system?

- **A.** Spontaneous shutdown/restart.
- **B.** Invalid boot disk.
- **C.** WinRE won't start.
- **D.** The BIOS/UEFI's time is not synchronized to a time server.
- **E.** The emergency repair disk doesn't boot.
- **F.** Regsvr32 has failed.

40. Which of the following are possible symptoms of malware? (Select all that apply.)

- **A.** Security alerts
- **B.** Windows Update failures
- **C.** Preinstallation environment
- **D.** Renamed system files

- **E.** Rogue antivirus
- **F.** User error

41. One of your company's users complains that their smartphone is making shutter noises even when they are not taking pictures. What should you do first to determine the cause of the problem?

- **A.** Update all applications on the smartphone.
- **B.** Run OS updates.
- **C.** Uninstall the camera installation.
- **D.** Check the application permissions.
- **E.** Reset the phone to factory settings.

42. You are troubleshooting a Windows system that is suffering from poor performance. The Event Viewer states that the file system is corrupt. What should you do next?

- **A.** Reload the OS using FAT32 instead of NTFS.
- **B.** Run **chkdsk** with the **/R** option and reboot the system.
- **C.** Open the **defrag** utility and run the drive analysis.
- **D.** Change the drive from basic to dynamic.

43. Which type of fire extinguishing technology should be used during an electrical fire?

- **A.** Overhead sprinkler systems
- **B.** Water-based fire extinguishers
- **C.** Class B fire extinguishers
- **D.** Non-water-based fire extinguishers

44. You attempt to install a legacy application on a computer running Windows. You receive an error that says the application cannot be installed because the OS is not supported. Which of the following

describes the first step you should take to continue installing the application?

- **A.** Purchase the latest version of the application.
- **B.** Install the application in Safe Mode.
- **C.** Install the application in compatibility mode.
- **D.** Install the latest security updates.

45. A user's new smartphone is suffering from poor battery life. The user has been using the phone for a short time and has installed several apps lately. Which of the following is the most likely cause of the problem?

- **A.** Unauthorized root access
- **B.** Battery needs to be replaced
- **C.** Defective SD card
- **D.** Signal drop or weak signal
- **E.** Slow data speeds

46. You have been tasked with setting up a SOHO wireless network in a small healthcare office that cannot afford a server. The wireless users require the highest level of security available, and various other levels of desktop authentication for access to cloud-based resources. Which of the following protocols and authentication methods should you implement? (Select the two best answers.)

- **A.** WPA
- **B.** WPA2
- **C.** WPA3
- **D.** TKIP
- **E.** RADIUS
- **F.** TACACS+

- **G.** SSO
- **H.** Multifactor

47. A customer calls to report that when they walk away from their laptop for an extended period of time, they have to reconnect to wireless upon returning. Which of the following will most likely correct this issue?

- **A.** Replace the wireless card.
- **B.** Install a higher-capacity battery.
- **C.** Adjust the power settings.
- **D.** Disable the screensaver.

48. You are an end-user technician working for a computer support company. A typical customer says that they are concerned about the privacy of their home laptop and the security of the network in general when browsing the Internet. Which of the following should you discuss with the customer to educate them while addressing their security concerns? (Select the two best answers.)

- **A.** Antimalware
- **B.** Proxy servers
- **C.** Firewalls
- **D.** VPNs
- **E.** Advanced TCP/IP settings

49. Which of the following commands should be used to search for a specific string in a filename?

- **A. sudo**
- **B. grep**
- **C. chmod**
- **D. wget**

50. You are working on a computer that is displaying a black screen. You restart the computer, but the operating system will not load. After talking with the user, you find out that the operating system was patched the previous evening. Which of the following should you attempt next?

- **A.** Repair the Windows Registry.
- **B.** Configure boot options in the BIOS.
- **C.** Reboot into Safe Mode and roll back the updates.
- **D.** Disable Windows services.

51. You are required to replace a desktop power supply. Which of the following tasks should be performed first?

- **A.** Remove your watch and jewelry.
- **B.** Review local regulations for disposal procedures.
- **C.** Read the MSDS.
- **D.** Check for environmental concerns.

52. When you are integrating AI into your workflow, which of the following should be avoided? (Select all that apply.)

- **A.** Pasting your entire working code into the AI and asking it for comments
- **B.** Asking the AI any question at all
- **C.** Asking the AI general questions
- **D.** Asking the AI to do your work for you

53. You are working at a computer and see the following at the beginning of a script:

```
#!/bin/bash
```

What type of system are you working at?

- **A.** Windows

- **B.** Linux
- **C.** iOS
- **D.** JavaScript

54. Which of the following tools allows you to change the number of CPU cores that Windows uses?

- **A. perfmon**
- **B. dxdiag**
- **C. msconfig**
- **D. taskmgr**

55. Which of the following best describes the primary focus of SAML, in the context of IAM and DLP?

- **A.** Preventing the unauthorized copying or deletion of sensitive data after a user has been granted access
- **B.** Managing and controlling user access to resources and systems based on their identity
- **C.** Securely exchanging authentication and authorization data between an identity provider and a service provider to enable single sign-on
- **D.** Storing and organizing user information like usernames, passwords, and access permissions within a directory service

56. One of your coworkers is attempting to access a file on a share located on a remote computer. The file's share permissions are set to allow the user full control; however, the NTFS permissions allow the user to have read access. Which of the following will be the user's resulting access level for the file?

- **A.** Read
- **B.** Write
- **C.** Modify

- **D.** Full Control

57. You are installing an older 32-bit program on a 64-bit version of Windows. Where does the program get installed to?

- **A.** C:\
- **B.** C:\Program Files
- **C.** C:\Windows
- **D.** C:\Program Files (x86)

58. A home user needs to reinstall Windows on a home computer but cannot find the operating system media that came with the computer. Which of the following would allow the home user to install the operating system?

- **A.** System Restore
- **B.** Recovery partition
- **C.** Linux rescue media
- **D.** Primary partition

59. You have been tasked with running updates on a Windows computer. Some of the updates go through fine, but one of them fails. While troubleshooting, you restart the computer and attempt to install the failed update, but it continues to fail. Which of the following should you do first?

- **A.** Analyze the Event Viewer for more information about the failures.
- **B.** Download the failed update to install it manually.
- **C.** Visit the Microsoft Update website to see if there is an issue with a specific update.
- **D.** Look up the error number associated with the failed update.

60. You are working on a client computer and receive a message that says the trust relationship to the domain has been broken. Which of the

following steps should be taken to resolve this problem from the client computer?

- **A.** Update the BIOS/UEFI using the latest version.
- **B.** Run **chkdsk**.
- **C.** Rejoin the computer to the domain.
- **D.** Reboot the PC as the domain to automatically rebuild the relationship.

61. You are configuring a friend's iPad. This friend needs to access their work email. To provide this access, you require information from the IT department. Which information should you ask for?

- **A.** Server and gateway
- **B.** IP address and domain
- **C.** IP address and DNS
- **D.** Server and domain

62. You need to write a script that checks data one line at a time until the end of the file being searched. Which of the following constructs should you use?

- **A.** Integer
- **B.** Loop
- **C.** String
- **D.** Variable
- **E. if-then**

63. A coworker has asked for a solution that will prevent file corruption by ensuring a graceful shutdown in the event of a power outage. The user would like at least one hour of uptime if the power goes out. Which of the following should you recommend?

- **A.** Surge protector

- **B.** Power strip
- **C.** Uninterruptible power supply
- **D.** Power distribution unit

64. AI is limited by which of the following?

- **A.** Limited inputted information
- **B.** Limited power supply
- **C.** Poorly planned questions
- **D.** Errors in code introduced by programmers working late into the night

65. A customer reports to you that a file shared on their computer for another user is not accessible to that third party. The customer says that the third party was given Allow rights for Read and Write access to the file. Which of the following could be a reason the third party cannot access the file?

- **A.** The parent folder has explicit Allow rights set for the third-party user.
- **B.** The parent folder has explicit Deny rights set for the third-party user.
- **C.** The user forgot to share the parent folder and shared only the specific file.
- **D.** The parent folder likely has the archive attribute enabled.

66. Which of the following tools is used to type recovery commands into a Linux box?

- **A.** Backup/Time Machine
- **B.** Shell/Terminal
- **C.** Restore/Snapshot
- **D.** Command/CMD

67. You are part of a security team that is auditing an organization's server room. You find that a USB drive was previously inserted into three of the servers. There were many login attempts that were successfully performed using common login information. What should you do to prevent the vulnerability from being exploited again? (Select the two best answers.)

- **A.** Remove admin permissions.
- **B.** Modify the AutoRun settings.
- **C.** Install a software-based firewall.
- **D.** Change default credentials.
- **E.** Run operating system security updates.

68. You are tasked with creating a new script in PowerShell. You need to add notes to the script to explain to the engineering group what each portion of the script is meant to do. Which of the following should you make use of?

- **A.** End-user documentation
- **B.** Inline comments
- **C.** Variables and **if-then** statements
- **D.** Change management documentation

69. In a SOHO wireless network, which of the following prevents unauthorized users from accessing confidential data?

- **A.** Enabling MAC filtering
- **B.** Changing the SSID name
- **C.** Setting encryption
- **D.** Reducing broadcast power

70. Which Control Panel utility is best used to remove a Windows application?

- **A.** Disk Cleanup

- **B.** Administrative Tools
- **C.** Folder Options
- **D.** Programs and Features

71. You receive a tech support call from a user on your corporate network about an Internet connection that is not working. You analyze the system and find out that the user's system has a valid IP address, can connect to network shares, and can view local intranet pages in the web browser. However, when you attempt to access a public website, the connection times out. Which of the following should you investigate next?

- **A.** Proxy settings
- **B.** IPv6 settings
- **C.** Hosts file
- **D.** DNS server

72. You have been tasked with setting up an AP in a small office that is in the middle of a crowded building. What should you do to increase the security of the wireless network? (Select the three best answers.)

- **A.** Configure WPA3 encryption.
- **B.** Disable the DHCP server.
- **C.** Reduce the transmit power.
- **D.** Reduce channel availability.
- **E.** Enable QoS management.
- **F.** Disable the SSID broadcast.

73. A computer has been infected with multiple viruses and spyware. Which of the following tasks should be performed before removing this malware?

- **A.** Disable System Restore.
- **B.** Disable network cards.

- **C.** Run Windows Update.
- **D.** Run the **chkdsk /R** command.

74. One of your customers has set up a perimeter firewall and has implemented up-to-date antimalware software. The customer asks you what else they can do to improve security. Which of the following will have the greatest impact on their network security? (Select the two best answers.)

- **A.** Conduct a daily security audit.
- **B.** Use strong passwords.
- **C.** Install additional antivirus software.
- **D.** Assign security rights based on job roles.
- **E.** Disable screensavers.

75. Which of the following statements describe how to demonstrate professionalism when dealing with a customer? (Select the three best answers.)

- **A.** Avoid distractions.
- **B.** Retain a chain of custody.
- **C.** Avoid being judgmental.
- **D.** Leave documentation to the customer.
- **E.** Meet expectations that the customer sets for you.

76. You previously installed a new application for a customer and added three new services. Today, the customer informs you that the application will not start. You find out that one of the three new services has failed to start, and manual attempts to start it fail. Where should you look next for information? (Select the two best answers.)

- **A.** Registry
- **B.** Event Viewer
- **C.** %systemroot%\System32\Drivers

- **D.** Log files for the new application
- **E.** Task Manager

77. Your organization has hired a new IT firm to manage its switches and routers. The IT firm is located in another state and will need to be able to remotely access the devices. Which of the following should be implemented to provide secure access from the IT firm to the switches and routers?

- **A.** RDP
- **B.** Telnet
- **C.** SSH
- **D.** VNC

78. Which of the following is the best way to maintain data security for a mobile device that has been lost or stolen?

- **A.** Passcode lock
- **B.** GPS
- **C.** Remote wipe
- **D.** Login attempt restrictions

79. Look at the following syntax:

```
net use Z: \\servername\sharename
```

Which of the following file types would you expect this syntax to be located in?

- **A.** .vbs
- **B.** .bat
- **C.** .js
- **D.** .py

80. Which of the following networking concepts describes an area that sits between the Internet and a local network, often used to host publicly accessible servers?

- **A.** Network Address Translation (NAT)
- **B.** Port forwarding/mapping
- **C.** Screened subnet (DMZ)
- **D.** Universal Plug and Play (UPnP)

81. Which of the following would most likely cause apps to load slowly or fail to load at all on a mobile device? (Select the best three answers.)

- **A.** Too many apps open
- **B.** GPS is disabled
- **C.** An unintended Bluetooth connection
- **D.** No space left on device

82. Your company is growing to the point where you need a better solution to remotely manage a vast array of client systems, servers, and networks. What monitoring solution would best meet your needs?

- **A.** RMM
- **B.** RDC
- **C.** mstsc
- **D.** Remote Assistance

83. You receive an error message stating “remote desktop can’t connect to remote computer” when trying to assist a remote customer. Which of the following can help you correct this problem? (Select the two best answers.)

- **A.** Have the customer reboot the computer.
- **B.** Run Windows Update to ensure that the system is updated.

- ○ **C.** Change the firewall settings.
- ○ **D.** Change settings to allow remote connections to this computer.

84. Your upgrade attempt from Windows 10 Pro to Windows 11 Pro fails. Your system has the following specs:

- ▶ 64-bit Intel Core i9 3.70 GHz CPU
- ▶ 16 GB RAM
- ▶ 100 GB Storage
- ▶ UEFI Secure Boot enabled
- ▶ TPM subversion 1.**38**
- ▶ Graphics card DirectX 12 with WDDM 2.**0 driver**
- ▶ Display high definition (720p)

Which of the following is preventing you from performing the upgrade to Windows 11 Pro?

- ○ **A.** The processor does not meet the minimum requirements.
- ○ **B.** There is not enough RAM.
- ○ **C.** The graphics card does not meet the minimum requirements.
- ○ **D.** The TPM is incompatible.

85. You go to the store and put your bank card into an ATM and enter your PIN. What examples of multifactor authentication have you exhibited? (Select two.)

- ○ **A.** Something you are
- ○ **B.** Something you have
- ○ **C.** Something you know
- ○ **D.** Somewhere you are

86. You are responsible for setting up a web server and an email server on a secure part of your network, using private IP addresses. Which of the following should you implement?

- **A.** A screened subnet
- **B.** DHCP reservations
- **C.** IP filtering
- **D.** A static WAN IP address

87. One of the users on your network logs on to the Windows domain from a laptop. The user tells you that the computer is taking a long time to log on and that a technician made changes recently. You look at the latest tickets for the user/computer and find out that the user's account was recently switched to a roaming profile. The user says that, previous to that, the laptop started up quickly. What should you check to troubleshoot the issue?

- **A.** The amount of RAM in the laptop
- **B.** The size of the paging file
- **C.** The amount of data in the user's desktop
- **D.** The free space on the network share

88. When you are handling internal computer components, which are best practices to avoid ESD? (Select the two best answers.)

- **A.** Keep the environment dry.
- **B.** Ground yourself before touching the components.
- **C.** Verify that the device is plugged into a grounded outlet.
- **D.** Handle adapter cards by the edge.
- **E.** Wear eye protection.

89. According to the 10 steps to remove malware from a SOHO environment, which of the following actions is recommended after the malware has been removed from a system?

- **A.** Boot into Safe Mode/preinstallation environment to limit malware activity.
- **B.** Reimage/reinstall the operating system.
- **C.** Schedule scans and run updates.
- **D.** Quarantine the infected system.

90. A user wants to protect all of the data at rest on a Windows laptop. You analyze the laptop and find that it has a TPM chip. Which of the following should you use to secure the data while taking advantage of the TPM?

- **A.** BitLocker
- **B.** SFTP
- **C.** ACLs
- **D.** EFS
- **E.** Hardware security module

91. Which of the following are recommended general browser security procedures for an organization to implement? (Select three answers.)

- **A.** Mandate the use of specific web browsers across all departments.
- **B.** Implement policies to manage add-ons and restrict access to malicious websites.
- **C.** Train users on safe browsing habits and how to handle pop-ups.
- **D.** Rely solely on built-in browser security features without additional configurations.
- **E.** Use a proxy and content filter to cache websites and block potentially harmful sites.
- **F.** Disable all JavaScript to prevent malicious code execution.

Answers at a Glance

1. C
2. B
3. B
4. A
5. C
6. C
7. B
8. D
9. A
10. B
11. D
12. C
13. B
14. D
15. C
16. B
17. A
18. A, B, C, E, F
19. D
20. A
21. F

22. B, D

23. C

24. B, C

25. A

26. D

27. D

28. B, C

29. C

30. C

31. D

32. A

33. C

34. D

35. C

36. C

37. A, E

38. C

39. B

40. A, B, D

41. D

42. B

43. D

44. C

45. A

46. C, H

47. C

48. C, D

49. B

50. C

51. A

52. A, D

53. B

54. C

55. C

56. A

57. D

58. B

59. D

60. C

61. D

62. B

63. C

64. A

65. B

66. B

67. B, D

68. B

69. C

70. D

71. A

72. A, C, F

73. A

74. B, D

75. A, C, E

76. B, D

77. C

78. C

79. B

80. C

81. A, D

82. A

83. C, D

84. D

85. B, C

86. A

87. C

88. B, D

89. C

90. A

91. B, C, E

Answer Explanations

1. **Answer: C.** /Library holds systemwide settings.

   Incorrect answers: /System contains core operating system files. Usually, this is not an area to modify! /Applications stores user-installed applications. /Users contains the home directories for users, and /Users/username/Library contains settings, preferences, and support files specific to that user. See Chapter 39, "macOS," for more information.

2. **Answer: B.** The **clean** option in **diskpart** removes all partitions. This way, you can later format the drive to full capacity. As per the docs.microsoft.com **diskpart** page: "clean removes any and all partition or volume formatting from the disk with focus." See Chapter 34, "Microsoft Command-Line Tools, Part I," for more information.

   Incorrect answers: The **repair** option can repair software-based RAID 5 arrays. The **merge** option can be used with virtual drives. The **extend** option extends a volume or partition (along with the file system) into free space on the drive.

3. **Answer: B. dir** is used to list the contents of a directory in the Command Prompt or PowerShell. You might also use the **tree** command to show the tree of directories. See Chapter 34, "Microsoft Command-Line Tools, Part I," for more information.

   Incorrect answers: cd is short for change directory and is used to navigate. **ping** is used to verify whether another computer is available on the network. **ver** shows the version number of the Windows operating system—in the Command Prompt, but not PowerShell. (**winver** gives more information in a graphical format.)

4. **Answer: A.** The best answer listed is to ask another technician to take the call for you. In a typical help desk environment, breaks are scheduled, and you don't want to miss your break because you probably won't be able to take it later! See Chapter 61, "Incident Response, Communication, and Professionalism," for more information.

   Incorrect answers: Asking the user to call back, even if done politely, is not good customer service; if the user does call back, the reason could be to complain to your manager. Sending the user to tier 2 support is not necessary yet because you haven't even attempted to troubleshoot the problem. You never know, multiple BSODs could be a tier 2 problem, but it needs to be analyzed first before you escalate it. Whatever you do, don't put the user on hold or attempt to help the user while taking your break!

5. **Answer: C.** You would want to get an enterprise license (sometimes referred to as a "corporate use" license). This allows multiple users to install the software on their systems, and each can accept the end-user licensing agreement (EULA) individually. See Chapter 61, "Incident Response, Communication, and Professionalism," for more information.

   Incorrect answers: The terms *seat* and *commercial* licensing might be used for other types of licenses, but generally, the term *enterprise* is widely used when there are many end-user licenses required (for example, when you are dealing with Microsoft operating system and Office software). An open-source license (or open license) doesn't require a purchase. It can be downloaded and freely modified, based on the rules of the open-source licensing agreement.

6. **Answer: C.** Impersonating trusted individuals via email to deceive employees into transferring funds or divulging information. Business email compromise (BEC) is a sophisticated scam where attackers impersonate trusted individuals, like executives or vendors, via email to trick employees into transferring funds or divulging sensitive information. See Chapter 47, "Social Engineering, Threats, and Vulnerabilities," for more information.

Incorrect answers: Exploiting vulnerabilities in third-party software to infiltrate a target's network describes a supply chain attack, where attackers target external components to gain access to the main target's network. Inserting malicious scripts into a web page to gain elevated privileges describes cross-site scripting (XSS), a web application vulnerability, not BEC. Injecting malicious code into the software build or update process describes a pipeline attack, which is a specific type of supply chain attack focused on the software delivery process.

7. **Answer: B.** The most likely reason for this is that domain-level group policies have been implemented by the administrator. This is by design so that end users cannot enable screensavers. This policy cannot be changed by the end user. See Chapter 44, "Logical Security," for more information.

   Incorrect answers: As mentioned, these domain-level group policies are by design; they are not incorrect policies, although it is possible to implement a similar security feature with the local computer policy of a system. Antivirus policies that are instituted at the domain level would affect the antivirus software of a group of systems on the network but should not affect Windows settings. A corrupted Registry could cause problems with the logon, but what is happening in the scenario is a specific setting designed to secure the workstations on the domain.

8. **Answer: D.** PowerShell is an advanced command line in Windows that goes beyond the Command Prompt. It is designed for administrators so that they can run scripts, batch commands, and snippets, and save the work as .ps1 files (by default). The command **$PSVersionTable** will tell you the version of PowerShell, the Windows version, and more. The *PS* in the command stands for "PowerShell"! See Chapter 63, "Basic Scripting, Part II," for more information.

   Incorrect answers: Compatibility mode is a mode in Windows that allows you to run older programs within newer versions of Windows. OneDrive is Microsoft's cloud service. Windows Defender Firewall is the built-in software-based firewall that blocks unwanted intrusion.

9. **Answer: A.** Use the **gpresult** command, which allows you to view the results of the Microsoft Group Policy configuration and print it to various file formats if you wish. See Chapter 34, "Microsoft Command-Line Tools, Part I," for more information.

   Incorrect answers: gpupdate takes care of updating settings on a computer regarding the computer policy configuration. **gpedit.msc** opens the Local Group Policy Editor window. **secpol.msc** opens the Local Security Policy window.

10. **Answer: B.** Use the **winver** command to find out the version and edition of Windows that is running. This command opens a window that displays the information graphically. You could also use the **ver** command in the Command Prompt or **$PSVersionTable** in PowerShell. See Chapter 34, "Microsoft Command-Line Tools, Part I," for more information.

    Incorrect answers: The **pathping** command displays the route from the local system to the remote system on another network; it is similar to the **tracert** command. **ls** is a Linux command that displays the contents of the current directory. **hostname** shows the name of the computer.

11. **Answer: D.** Endpoint detection and response (EDR) agents continuously monitor endpoint activity, collecting detailed telemetry like process executions, network connections, and file modifications. This data is analyzed to detect unexpected behavior and potential threats, providing security analysts with context for incident response. See Chapter 46, "Wireless Security and Malware," for more information.

    Incorrect answers: While an endpoint protection platform (EPP) also deals with endpoints, its primary function is preventing known and zero-day malware from executing by blocking malicious files and processes. It doesn't primarily focus on analyzing activity for detection and response in the same way EDR does. Managed detection and response (MDR) augments EDR by providing services like monitoring and incident response, but the core technology responsible for the initial detection through activity analysis is EDR.

MDR relies on the data collected by EDR. An email security gateway focuses on securing email communication by scrutinizing incoming and outgoing emails for threats. It does not analyze endpoint activity in the way described in the question.

12. **Answer: C.** The screen lock and login time restrictions are your best bet. This way, the computer will lock after 5 minutes, even if the user forgets to lock it manually (with a quick Windows+L on the keyboard). Set the login restriction hours within the system or on the domain so that no one can log in after a certain time (such as 5 p.m.). See Chapter 48, "Workstation Best Practices," for more information.

    Incorrect answers: Every system should have a password, and it is required when the computer is first turned on, if the person logs off and logs back on, or if the system is unlocked. To avoid logging off and losing work, use the screen lock option. That will require the password when the user comes back to the computer. A strong password is important but does not meet the requirements when it comes to the person leaving the workstation frequently and the issue of not turning off the computer. A screensaver is not enough because it does not necessarily require a password. The screen lock is a much more secure method in general.

13. **Answer: B.** The incident response technician should secure the workstation in a limited-access storage facility until the matter is sorted out. A company can be liable for what its employees download, so the workstation should be securely stored and not disturbed until the matter has been investigated thoroughly. The incident response technician should also contact the network administrator (or network security administrator) and inform them that the user was able to download a BitTorrent client and figure out a way to block the usage of those. See Chapter 61, "Incident Response, Communication, and Professionalism," for more information.

    Incorrect answers: Because there are legal ramifications (for the user and for the company), the incident response tech should not delete anything and should store the computer securely for the time being. At some point, the tech will probably be called upon to image the drive, and the investigation can then be carried out. Reprimanding

the user is up to the manager, but a content filter would probably be applied for the entire network, not just that individual user's profile. The tech should definitely document the incident—that is of utmost importance—but the tech should not purge the downloaded materials. Instead, quarantine the computer in a safe location until the investigation is complete. If the user was working with a BitTorrent client, there is the chance that the user was performing other illegal acts, so the computer should be thoroughly analyzed, and the drive should be stored indefinitely in a secure place for future reference.

14. **Answer: D.** Use the Secure Shell (SSH) utility. Linux admins use it *all* the time. It allows you to log in to remote systems in a secure way (as long as those systems have an SSH server running). By the way, once you are logged in to the Linux server, use **apt update** or **dnf update** to update the server (depending on the distribution of Linux). See Chapter 40, "Linux," for more information.

    Incorrect answers: Remote Desktop Protocol (RDP) is the commonly used name for the Remote Desktop Connection program in Windows. It is used to connect to remote Windows systems. Secure File Transfer Protocol (SFTP) is a secure tool (that works on SSH), but it is designed to transfer files, not update a Linux server. Virtual Network Computing (VNC) is another way of remotely controlling systems, but it is a *graphical* desktop-sharing system, not a command-line system.

15. **Answer: C.** It is likely that the Windows Update service stopped. You can restart it (along with RPC, which it is dependent on) within the Services console window in Computer Management (or **Run > services.msc**) or within the PowerShell/Command Prompt by typing **net start wuauserv**. However, it might be that Windows Update was disabled on purpose as part of company policy. Always check your organization's policies and procedures first before starting services. See Chapter 33, "Microsoft Operating System Features and Tools, Part II," for more information.

    Incorrect answers: Rebooting the computer will most likely result in the same issue later, when Windows Update needs to update the OS. There are no device drivers that will affect the Windows Update

service. Rebuilding the user profile is also not necessary here; plus, it is a lengthy process and definitely not a quick solution.

16. **Answer: B.** Store 30 days (1 month) of backups onsite (on-premises, or "on-prem") and store older backups with a cloud provider that is offsite (and preferably in a different geographic location). This meets all the requirements in the question: The last month of backups is easily accessible; the reason is that it is onsite, long-term backups are stored offsite (cloud provider), and there is minimal use of hardware because you don't have to use as many tapes, disk arrays, and NAS boxes since the cloud is storing all backups older than 30 days. Of course, the cloud provider will use a lot of hardware, and that's part of the point of using the cloud. All that said, it's a good idea to have your 30 days of on-premises backups duplicated and stored offsite as well. Remember the 3-2-1 rule? See Chapter 58, "Change Management and Backup Methods," for more information.

    Incorrect answers: Storing backups with a cloud provider and onsite is not specific enough. Storing all backups with the cloud provider is not a good answer because requirements say that only the long-term backups should be stored offsite. Storing backups onsite and using cloud bursting will probably entail using too much hardware.

17. **Answer: A.** All networking racks should be grounded, either to grounding bars or an I-beam in the ceiling or using some other grounding method. This should be done before installing any equipment to the racks to prevent any damage from electrostatic discharge (ESD). See Chapter 59, "Safety Procedures," for more information.

    Incorrect answers: A dehumidifier would make the problem worse by removing additional humidity from the air. An ESD strap will provide some protection to the devices while you work on them, but it won't help once you disconnect. Fire suppression systems are important but won't protect against ESD.

18. **Answers: A, B, C, E, and F.** Unauthorized access can be prevented through the use of authentication. These authentication factors are something the user knows (knowledge factor), something the user has

(possession factor), something the user does (behavioral factor), and somewhere the user is (location-based factor). See Chapter 44, "Logical Security," for more information.

Incorrect answers: While the context of how the person is logging in is important, it is through the preceding factors that authentication can be measured.

19. **Answer: D.** You should tell Jenny to make sure she is using her smart card. In a multifactor authentication system, you might have a combination of a physical smart card requiring that a personal identification number (PIN) be typed and then the password. So, you want to make sure that users are swiping (or inserting) their smart card before entering the PIN code. Of course, it depends on the type of authentication (or MFA) system that is in place. In this scenario, and with the answers listed, verification of the user's smart card is the best answer. See Chapter 44, "Logical Security," for more information.

    Incorrect answers: The user probably hasn't gotten to the authentication stage where the password needs to be entered, but in any case, it is not a good idea to suggest entering all past passwords. Rebooting the computer can fix many problems, but in situations such as this one, it will simply result in the same issue. The network connection shouldn't play into the PIN requirement. Please note that Windows Hello authentication can also use a PIN; however, that is not given as a choice here, so a smart card is the only answer that makes sense here.

20. **Answer: A.** Surge suppressors (otherwise known as surge protectors) safeguard the equipment that is connected to them by directing surges to the path of least resistance. Electrical resistance is the measure of difficulty in passing an electric current through a conductor and is measured in Ohms (Ω). It usually means redirecting the current to ground. So, the metal-oxide varistor (MOV) within the surge suppressor will normally redirect to the ground wire of the AC circuit because there is no resistance on that wire. See Chapter 59, "Safety Procedures," for more information.

Incorrect answers: Electrical conductance deals with current and how easily it flows; it is the inverse quantity of resistance. Inductance deals with changes in current flowing through a circuit. The path of highest voltage is just that—for example, the hot wire of an AC circuit (120 V). You would not want a surge to be redirected to high-voltage areas, and you should always redirect surges and spikes to the ground.

21. **Answer: F.** Inheritance means that a file or folder receives its NTFS permissions from the parent folder. It is the default setting of the Advanced configuration dialog box within the Security tab of a file or folder. In Windows, it is shown as a button that can enable or disable inheritance (also described as "Include inheritable permissions from this object's parent" in older versions of Windows). See Chapter 45, "Windows Security Settings," for more information.

    Incorrect answers: This is different from permission propagation in that with propagation, a parent folder forces the permissions to the subfolder. It can be initiated by the user, it is a separate configuration, and it is not necessarily configured to work by default. Single sign-on (SSO) is a type of authentication method in which a single username/password combination (or another single authentication scheme) is used to gain access to multiple different resources. With client-side virtualization, a client operating system (such as Windows) is run in a virtual machine. The virtual software applications that house VMs have their own set of requirements, as do the VMs themselves. For example, Windows running within a VM will not require as many resources as Windows running on a physical computer in a standard installation. Proxy settings are Internet connectivity settings that are set up on a computer running an OS such as Windows. The proxy setting is usually an IP address of a special computer on the network that acts as a go-between for the client computer and the Internet. It stores web information so that the client computer can gain access to the information faster while conserving Internet bandwidth. A recovery image is an image file that can recover an operating system. It is created by a manufacturer or by a user as a form of preventive maintenance in the event of a system

crash and can be saved to an optical disc, a USB flash drive, or a special partition on the storage drive.

22. **Answers: B and D.** One-time password (OTP) tokens are usually implemented as hardware-based tokens that a person carries with them. The passcode changes periodically (for instance, every 60 seconds). A privacy filter is one that is placed in front of a monitor to reduce the viewing angle and make it more difficult for shoulder surfers (social engineers) to discern information from the screen. Another example is an RSA token. An RSA token can be a physical device, either located within a smart card or a key fob. This is intelligent technology that communicates with the security system, transferring information such as identification, dynamic passcodes, and more, allowing for a more secure authentication method. See Chapter 44, "Logical Security," for more information.

    Incorrect answers: Directory permissions are the rights granted to users within Windows, allowing or denying them access to files, folders, printers, and other resources. The principle of least privilege states that a person should have access only to what is absolutely necessary; the concept "need to know" is part of this principle.

23. **Answer: C.** A network topology diagram shows network devices, such as switches and their individual ports (among other things.) This documentation is designed to help describe where computers and other networking equipment should connect, on a port-to-port basis. Often, a network topology diagram deals with physical connections, but it can also detail logical connectivity—for example, the IP addresses used by a LAN and what device that group of computers connects to. This might also be referred to as a logical topology diagram. See Chapter 57, "Documentation," for more information.

    Incorrect answers: A change control form is used to document business processes during change management. A process diagram is a diagram that shows a step-by-step procedure or troubleshooting process. A fiber backbone diagram shows high-speed connections, often from one network to another. It wouldn't be required for an upgrade that concerns switch ports, which most likely implies standard 1 or 10 Gbps switches.

24. **Answers: B and C.** You should implement a multifactor authentication system (such as one that uses usernames/passwords and also a smart card). You should also educate end users about company policies regarding the usage and storage of files and databases that can include passwords and personally identifiable information (PII). See Chapter 44, "Logical Security," for more information.

    Incorrect answers: The strength of the password was not the problem here. The organization might have already instituted a policy that requires complex passwords; it's the password file or database that was leaked (most likely by an employee, possibly a malicious insider). But strong passwords are nonetheless important. File encryption is also a good idea, but it won't help with authentication strength. Restricting user permissions is important, too, but if the password list that was leaked includes administrator passwords, game over. You would need to implement an organization-wide password reset (right away).

25. **Answer: A.** Make sure the user is not using a proxy server within the browser before attempting anything else. A proxy address (whether added by malware or by the user) can redirect the browser to unwanted websites (often malicious in nature). See Chapter 38, "Windows Networking," for more information.

    Incorrect answers: Internet shortcuts that were added without the user's knowledge could also be a culprit, so they should be checked, and the browser should also be cleared of cookies and cache, if necessary. But check that proxy setting first!

26. **Answer: D.** You most likely need to create an exception in the local firewall of the laptop. Outbound connections from the laptop are working fine, but that doesn't necessarily mean that inbound connections will work; in fact, most host-based firewalls have an implicit deny on all incoming traffic, while outgoing traffic is allowed. See Chapter 45, "Windows Security Settings," for more information.

Incorrect answers: You shouldn't need to change the IP address of the laptop. If it can push the configurations to the switches via FTP, then you know you have a valid network connection. That means a specific VLAN is not necessary either because connectivity has already been established. (However, a specific management VLAN is a good idea!) No static DNS entry is needed in this scenario, which made no mention of servers or DNS in general. DNS is extremely important in today's networks, but there is no evidence that DNS has failed here. In addition, sometimes technicians and administrators who need to perform technical tasks, such as pushing configurations via FTP, do so via an IP address directly—skipping DNS altogether.

27. **Answer: D.** Disable Maps in the privacy settings. If Maps is always on, then it will drain the battery quickly, which subsequently makes the device considerably hotter. It's not just GPS; any powerful application (games, virtual reality programs, mobile OS update programs, and so on) can cause the battery to drain quickly and cause the device to heat up rapidly. See Chapter 54, "Troubleshooting Mobile Operating Systems and Applications," for more information.

    Incorrect answers: Many mobile devices will come with 32 or 64 GB of storage. Using up 48 GB should not cause the battery to drain quickly, nor should the device heat up in the manner described in the question. Stored data is data at rest; it isn't doing anything with the other resources of the system—*unless* it is opened or used by an application. Having the display brightness set to auto is a good thing; it allows the device to monitor the ambient lighting and reduce or increase the brightness of the screen as necessary; this is actually a power-*saving* feature. Likewise, 15 minutes between mail pulls would not cause a power drain. If, however, it were set to automatic or real time, that could cause a drain on the battery, but it would still not cause as much drain as the GPS program that is always on in the scenario.

28. **Answers: B and C.** A drive shredder or drill can be used to physically tear the drive into multiple pieces or to make holes in the platters of the hard drive, thus making it inoperable. It can then be disposed of according to municipal guidelines. This is one of several

ways to physically destroy a drive and is performed only when the drive has met the end of its life cycle, is not going to be recycled within the organization, and is to be disposed of. However, shredding (or pulverizing) is the best way to destroy a drive; vendors offer services to perform this work and provide a certificate of destruction when complete. See Chapter 50, "Data Destruction and Disposal," for more information.

Incorrect answers: Ports are disabled on a firewall or SOHO router to block access into (or out of) a network. A low-level format is a type of formatting procedure done in the BIOS/UEFI of a system (on older drives), through the use of special removable media, or is done at the manufacturer. It removes more data than a standard operating system format but does not destroy the drive (though it can cause damage to particular sectors if performed too often). Many technicians also refer to data wiping as a method of low-level formatting.

29. **Answer: C.** Use the Advanced tab to enable TLS 1.2/1.3 (and other security protocols) within Internet Explorer. See Chapter 36, "Windows Control Panel Utilities," for more information.

    Incorrect answers: This is a bit of a trick question. At first glance, you would think that TLS is a security feature, and while it is, the Security tab deals with zone *security*, not specific protocol-based security options. The Privacy tab deals with blocking cookies. The Connections tab concerns setting up Internet connections, VPNs, and proxy server connections.

30. **Answer: C.** The storage drive space is not large enough for Windows 11. The 64-bit installations of Windows 11 require 64 GB of storage drive space. This holds true for physical installations and virtual installations. The virtual machine (VM) installation will fail until the VM's drive space is increased. In fact, 15 GB is not even enough for Windows 8, though chances are you won't be seeing much of that since its EOL was January 2023. See Chapter 31, "Basic Features of Windows Editions," for more information.

Incorrect answers: The rest of the listed specifications for the VM are enough for Windows 11, so the rest of those do not need to be modified.

31. **Answer: D.** You should recommend the Microsoft domain setup. This means installing a server that acts as an Active Directory domain controller, where all logon authentication is centralized. This way, all access to network shares and print servers is also centralized. A domain controller is a server that is running a version of the Windows Server operating system and has Active Directory Domain Services (AD DS) running. See Chapter 38, "Windows Networking," for more information.

    Incorrect answers: A workgroup is a good choice for networks with 20 or fewer computers. Once you exceed 20 computers, it is wise to configure a domain. The main reason for this is that a single Windows client computer can handle only 20 connections simultaneously. Storing all your data on one computer for every user to access is fine for networks with 10 to 15 computers. But as you increase your network to 20 computers or more, you are forced to store resources on multiple computers, which can create confusion. Ad hoc means that no single computer is in control; this especially applies to wireless networks and is sufficient for a few systems but definitely not for 25 computers. Spoke-hub (also known as hub-and-spoke, or the older star topology) refers to the network topology or how computers are connected. This isn't covered in the A+ objectives, but it essentially means that the computers are wired in such a way that all of them physically connect to a central connecting device (such as a switch) or wirelessly connect to a wireless access point. This is easily the most common way that computers connect to a wired network. You wouldn't recommend this approach because it already exists! This will be the wired network configuration in the vast majority of scenarios. However, in this 220-1202 practice exam, the question is assessing your understanding of the Windows solution for how the data will be shared.

32. **Answer: A.** Chain of custody is the chronological documentation (written) of evidence pertaining to a computer or other technical

device that has prohibited content or has been confiscated. The technician should write (or type) the date, time, and who took custody of the computer next. It's important for the technician to adhere to the chain-of-custody rules when storing the computer or data. It's also important to verify that the chain of custody remains intact, so as to ensure evidence is admissible in legal proceedings. See Chapter 61, "Incident Response, Communication, and Professionalism," for more information.

Incorrect answers: Committing such important facts to memory is not enough; this will not stand up in court as evidence. A "third party" will break the chain of custody. Calling the supervisor is part of first response; it's not part of chain of custody.

33. Answer: C. Use Performance Monitor (**Run > perfmon.exe**) to analyze a device. In this example, you can find out how many bits per second the NIC can transfer (that is, the data transfer rate). You can also use this tool to monitor all of the other devices (objects) on the system and save and report on those findings in a variety of ways. Another useful tool is Resource Monitor. See Chapter 32, "Microsoft Operating System Features and Tools, Part I," for more information.

Incorrect answers: Device Manager (**Run > devmgmt.msc**) is where you would go to install or uninstall a device or roll back the driver for that device. Local Security Policy (**Run > secpol.msc**) is where you would go to enable or disable rules (policies) on a Windows client computer. System Information (**msinfo32**) gives you the Windows system summary for hardware resources, components, and the software environment, but it cannot perform tests.

34. Answer: D. Most help desks' standard policy is to have their techs research new problems for a couple of minutes before escalating them to higher-level techs. Often this approach proves to be the right course because the technician is often able to find the answer within 2 or 3 minutes. Of course, if you do place the customer on hold, watch the time (I suggest a timer app) and be sure to get back to that person when that time is up. See Chapter 61, "Incident Response, Communication, and Professionalism," for more information.

Incorrect answers: It's better to tell the customer that you are checking resources than to tell the customer that you have never encountered the problem before because it instills more confidence. If you can't find the answer in 2 minutes, then inform the customer that you will have to escalate the problem.

35. **Answer: C.** To enable computers to securely prove their identity to each other in client/server environments, especially with Active Directory, is the primary purpose of Kerberos. See Chapter 46, "Wireless Security and Malware," for more information.

    Incorrect answers: The primary function of RADIUS is to provide centralized administration for dial-up, VPN, and wireless authentication. Yes, Kerberos is named after Cerberus, the Greek three-headed dog of the underworld in mythology, but its actual purpose is authentication not guarding! Terminal Access Controller Access-Control System Plus (TACACS+) separates authentication, authorization, and accounting functions for network access.

36. **Answer: C.** In Windows, the Task Manager Users tab shows any currently logged-on users and their status. The Task Manager shows the percentage of resources that are being used by each user. See Chapter 32, "Microsoft Operating System Features and Tools, Part I," for more information.

    Incorrect answers: msconfig (System Configuration) is used to change boot settings and disable services. Disk Management is used to monitor the status of drives and to work with partitioning/formatting. Windows Tools is a collection of tools used to configure the OS, but it does not offer a quick way to see which users are logged in to the system. In older versions of Windows, the Windows Tools was called Administrative Tools, so you may see it referred to that way also.

    Note that Microsoft has renamed the Administrative tools folder in Start to Windows Tools starting with the Windows 10 build 21343 release to better organize all the admin and system tools. The tools in the folder might vary depending on which edition of Windows you are using.

37. **Answers: A and E.** Compressed air and a vacuum are tools commonly used to remove dust and debris from inside a computer. Of course, when you use compressed air, consider doing this outside because the dust and dirt will fly all over the place. Use a vacuum to clean up after you are done. If you do use a vacuum inside a computer, make sure it is an antistatic, computer-ready vacuum, and, importantly, don't touch any of the components inside the system! See Chapter 60, "Environmental Controls," for more information.

    Incorrect answers: Cotton and alcohol (or a 50/50 mix of alcohol and water) might be used to clean a printer's rubber rollers, the bottom of an ink cartridge (if it is very dirty), or a display. A feather duster would cause electrostatic discharge (ESD) and should be avoided; it is not a good tool for the job. Antibacterial surface cleaner should be used only on the outside of a computer case.

38. **Answer: C.** Using an ISO image (.iso) is a common way to allow for the download of operating systems such as Windows, Linux, and so on. It can be easily read by virtualization programs to install operating systems into virtual machines. An ISO image is designed to take the place of an entire optical disc. See Chapter 30, "Operating System Installations and Upgrades," for more information.

    Incorrect answers: .exe files are executable programs. An appimage is an image of an application that can run without needing to be installed; it is common in Linux. .vdi is the default extension used in VirtualBox for virtual storage drives.

39. **Answer: B.** An invalid boot disk error is a common symptom of a problem loading the Windows operating system. It could be caused by removable media inserted into the computer (an optical disc or USB flash drive) that is not bootable. This could be avoided by setting the storage drive to first in the BIOS/UEFI boot order. Another possible symptom of problems loading the operating system would be if a RAID array was not detected during bootup or during installation of the OS. Either way, the storage drive, or RAID array of drives, should be inspected for faulty connections. See Chapter 53, "Troubleshooting Microsoft Windows," for more information.

Incorrect answers: A spontaneous shutdown and restart indicate either a problem with the power supply or the possibility of malware on the system. Note that the question refers to "starting up" Windows; a shutdown or restart can only happen when the system has already booted. WinRE is the Windows Recovery Environment, which includes System Recovery Options such as Startup Repair and System Restore. WinRE is not accessible during a routine bootup of Windows but can be initiated by booting from a special partition on the storage drive or by booting from a USB flash drive (or, in older versions of Windows, from an optical disc). Whether or not the BIOS/UEFI is synchronized to a time server shouldn't matter. However, it is important to sync Windows time to a time server. An emergency repair disk (or disc) should be booted to only in the event that there is a problem with Windows. A failure to boot to an emergency repair disk is not a common symptom of a problem starting Windows, but you might use a recovery disc to fix the problem. Regsvr32 is a tool used in the Command Prompt to activate or deactivate ActiveX controls, none of which should stop Windows from booting.

40. **Answers: A, B, and D.** Malware can have many symptoms. Viruses are especially prevalent in today's society; there are millions of different kinds. Fake security alerts, failure to update Windows, and renamed system files are all possible symptoms of malware—specifically, viruses. See Chapter 56, "Troubleshooting PC Security Issues," for more information.

    Incorrect answers: Windows has a preinstallation environment known as Windows PE or simply WinPE; this is a lightweight version of Windows that is often used to deploy the operating system. It can be booted from optical disc, USB flash drive, over the network via PXE, or by the storage drive. It is an add-on to Windows available with the Windows Assessment and Deployment Kit (ADK). It can be used to run recovery tools such as Windows RE and for running drive-cloning utilities. Rogue antivirus programs are not symptoms of malware; they *are* malware! A rogue antivirus program can often be something that appears to be legitimate when it is not. Or it could be a part of a rogue security software suite, which deceives the user into

paying for fake malware protection. User error is not a symptom of malware, but it could very well be the cause. If a user surfs to a malicious website or opens an unknown email attachment without verifying the source of the email first, malware could be—and often is—the result. Educate the end user when it comes to screening emails and surfing the Web. Show the user how to be responsible when accessing online information.

41. **Answer: D.** It could be that another program (quite possibly malicious) is using the camera on its own, without user intervention. So, the best first thing to do is to check the application permissions. For example, in Android, a typical navigational path would be **General > Apps & Notifications > App permissions**. From there, you will see the Camera app; tap it to find out which applications are using it. Then, you can deselect whichever apps you need to. You might also find that a malicious or unwanted program is on the list and enabled for camera usage; if so, it should be removed. See Chapter 54, "Troubleshooting Mobile Operating Systems and Applications," for more information.

    Incorrect answers: Updating all applications is a bit premature. You may want to do that at some point, though, as long as company policy allows it. OS updates should be checked as well at some point but not first because that does not get to the root of the problem. Uninstalling the camera application won't change how other apps can use the camera. You will simply be preventing the user from using the camera. Resetting the phone is one of the last options to try, but it could be a reality if the smartphone has been compromised, which is a distinct possibility in this scenario. If resetting is necessary, your company might also require a few overwrites of data first.

42. **Answer: B.** The only option that would help the situation would be to run the **chkdsk** command with the **/R** option. **/R** locates bad sectors and recovers readable information, which is the only option listed that might fix the file system corruption (keyword *might*). **/R** implies **/F** as well, which fixes basic errors on the drive. Though not listed in the A+ objectives, you might also use the **dism** tool to repair a slowly

running Windows system. See Chapter 34, "Microsoft Command-Line Tools, Part I," for more information.

Incorrect answers: Reloading the OS would wipe all data (on the system partition at least), so it is not recommended. In addition, you wouldn't normally go from NTFS to FAT32; it's recommended to use NTFS. Plus, if the file system were corrupt, a reinstall of the OS (using NTFS again) would fix those issues. Opening the **defrag** utility and running a drive analysis doesn't really change the drive; it simply tells you if the drive is fragmented. You change the drive from basic to dynamic so that you can resize partitions.

43. **Answer: D.** Non-water-based fire extinguishers should be used during an electrical fire. This could be a CO_2-based fire extinguisher such as a Class C extinguisher, a Halotron fire extinguisher, or an FM-200 overhead system. See Chapter 59, "Safety Procedures," for more information.

    Incorrect answers: Standard overhead sprinkler systems use water. They should not be present where expensive computer equipment is located (for example, in server rooms). Regular water-based fire extinguishers should not be used. Class B extinguishers are meant for burning gases and liquids, whereas Class C are meant for electrical fire (think "C" for "copper," like the copper inside electrical wiring).

44. **Answer: C.** Attempt to install legacy (older) applications in compatibility mode. Select the older OS that the application was originally written for. See Chapter 36, "Windows Control Panel Utilities," for more information.

    Incorrect answers: Your first step should never include the word *purchase*; besides it is not necessary in a system such as Windows, where compatibility mode exits. Normally, you wouldn't install an application in Safe Mode; you might run the application or troubleshoot the system in that mode. Security updates probably won't have an effect on this scenario either.

45. **Answer: A.** Of the listed answers, the most likely cause in this scenario is that there has been unauthorized root access. Whether this was done by the user on purpose or without the user's knowledge by

one of the newly installed apps is still something you need to discover. Unauthorized root access by an app or by a user could cause the phone to perform unwanted actions, which would most likely drain the battery quickly. See Chapter 54, "Troubleshooting Mobile Operating Systems and Applications," for more information.

Incorrect answers: It is unlikely that the battery needs to be replaced since it is a new phone, but it is something you can investigate after determining whether the phone has been rooted. A defective SD card probably won't affect the battery. Weak signal could cause battery drain (especially if the user is in a basement or other unfavorable wireless location), but short battery life is more likely caused by root access, by powerful apps pulling too much power, or by a bright display that has been configured to not shut off. Slow data speeds are an annoyance, but they're not something that should cause the battery to drain quickly.

46. **Answers: C and H.** For the highest level of wireless security, use WPA3 (and AES). For authentication, select multifactor authentication (MFA). Many healthcare providers are required to log on with a username/password and a smart card (or biometric). See Chapter 46, "Wireless Security and Malware," for more information.

    Incorrect answers: Out of WPA, WPA2, and WPA3, WPA3 is the most secure. Protocols such as WEP, WPA, and TKIP are especially vulnerable; they are outdated examples of encryption protocols. RADIUS and TACACS+ are examples of authentication servers—and the scenario mentioned that the company cannot afford a server. It is unknown what the cloud contains; there is probably an authentication server there (connected to via secure VPN), but it is not something that *you* would implement at the SOHO. SSO stands for single sign-on, and it quite possibly is already set up in the cloud because it is very common in the healthcare industry.

47. **Answer: C.** Try adjusting the power settings so that wireless connections will not time out as quickly. This can be done in Windows in Power Plans and the Power Options dialog box. See Chapter 36, "Windows Control Panel Utilities," for more information.

Incorrect answers: If the wireless card was faulty, the customer would never be able to get onto a wireless network, so there is no reason to replace the wireless card. The capacity of the battery will not affect wireless connections. Disabling the screensaver will also not affect the wireless connection; however, you can get to some of the power options necessary to solve the wireless problem indirectly from the screensaver window.

48. **Answers: C and D.** You should discuss firewalls (for the general security of the network) and a VPN (for security while browsing the Internet). These two concepts can help make the home user's network and laptop more secure and will protect the user's privacy. See Chapter 45, "Windows Security Settings," and Chapter 64, "Remote Access Technologies," for more information.

    Incorrect answers: Antimalware programs help with malicious programs, but not with privacy. A proxy server can be used in multiple ways: by an organization to act as a go-between and a caching device for multiple clients and by an end user who *really* wants to protect their privacy. This is not something you would bring up with a typical customer. Remember your professionalism best practices: It's not a good idea to bring up heavily technical concepts (such as advanced TCP/IP settings) with a customer.

49. **Answer: B. grep** is the Linux command used to search for matching information in a file, files, or filename. See Chapter 40, "Linux," for more information.

    Incorrect answers: Other Linux commands include **sudo**, which is used to allow a user to execute a command as another user (for example, an administrator); **chmod**, which is used to change the permissions of a file or folder; and **wget**, which retrieves content from web servers (as opposed to the **get** command, which is often used to obtain files from an FTP server).

50. **Answer: C.** Chances are that the update caused an issue with the computer; perhaps the video driver or another driver was updated, resulting in the black screen. Booting into Safe Mode can help you figure out the problem. If Safe Mode displays properly, you can be

fairly certain that there is a video driver issue or some other driver issue; the driver can be rolled back. If you aren't sure what was affected, you can roll back the entire update. See Chapter 53, "Troubleshooting Microsoft Windows," for more information.

Incorrect answers: The Registry is rarely the first place to go when troubleshooting problems, and it definitely would not be first in this case. The Registry is where you go to make advanced configuration changes to the OS. Many times, when you take exams, two answers will look plausible; that's the case here with "Configure boot options in the BIOS." Often, if there is a black screen, it might be accompanied by a message such as "invalid boot device" or "No OS found." If that is the case, then it could very well be that the BIOS boot priority needs to be changed. However, in the scenario, there is no mention of a message of any sort, but you did get information that there was an update the night before. (It could be that the video card is simply displaying a black screen.) Disabling Windows services is a possibility, but you would want to boot into Safe Mode first and diagnose the system further before disabling any services.

51. **Answer: A.** Remove watches, jewelry, and any other metals when working on a computer so they are out of the way and do not pose any threats while working on the computer. See Chapter 59, "Safety Procedures," for more information.

Incorrect answers: You should review local regulations and check for environmental concerns when disposing of storage drives, batteries, and toner cartridges. Read the MSDS (material safety data sheet) when you encounter a fluid spill or other unknown chemical.

52. **Answers: A and D.** Be careful what you ask of an AI system. It is okay to ask it *how* to do the work. Questions like "How can I do *xyz*?" are fine. Questions like "Here is my code; please help me troubleshoot" will lead to trouble. Assume that any data that you enter into an AI system will eventually leak out and thus is a security risk. See Chapter 65, "Appropriate Use of Artificial Intelligence," for more information.

Incorrect answers: It is okay to ask questions of an AI, even if those questions are general. After all, it is a tool. Just don't rely on it to do everything; that promise is not fulfilled (and may never be).

Asking the AI any question at all is incorrect because it assumes that AI isn't a useful tool. It can be, so long as you are aware of the limitations of the tool. Pay attention to the limitations and be aware that, while AI seems all-knowing, it is really just regurgitating information and often is just an exceedingly sophisticated search engine (albeit one with much more capability). Don't be afraid of it, but don't toss it out as a tool entirely.

Asking the AI general questions is incorrect because ultimately you, as a user, are responsible for the work. The act of copying and pasting from an AI system is a type of plagiarism, and while the AI system may seem infallible, you will find yourself in situations where you are asked to perform tasks that the AI cannot do or situations where the AI has given an incorrect answer, either of which will lead to trouble for you. Just like a hammer cannot replace a carpenter, an AI system cannot replace a person; your knowledge and creativity are what set you apart, and that is not replaceable.

53. **Answer: B.** This is a Linux, UNIX, or macOS system. When it comes to Linux, UNIX, and similar systems, a lot of technicians simply refer to them as *nix, meaning anything ending in *nix*. Many Linux distributions use the Bash shell by default. This is where scripts are run. This default line tells the system the path and how to interpret the upcoming script. See Chapter 63, "Basic Scripting, Part II," for more information.

    Incorrect answers: Windows uses PowerShell. Saved scripts (such as .ps1 files) don't use this type of line to identify the shell interpreter. iOS doesn't use Bash or Terminal the way that macOS and Linux do (though Windows can install a Bash shell). JavaScript is not a system at all; instead, it is a type of scripting language that is often used with websites.

54. **Answer: C.** The System Configuration utility (msconfig.exe) can be used to change the total number of CPU cores used by Windows. You

can find this by going to the **Boot** tab and clicking the **Advanced options** button. From there, check the **Number of processors** checkbox and select the number of CPU cores (or the actual number of CPUs if you have more than one). This is usually done to troubleshoot the CPU or Windows; in most cases, Windows will use all CPU cores available to it by default. See Chapter 32, "Microsoft Operating System Features and Tools, Part I," for more information.

Incorrect answers: The Performance Monitor (perfmon.exe) is used to analyze system performance and can view each core in real time, as can the Task Manager (taskmgr.exe). The DirectX Diagnostics tool (dxdiag.exe) is used to analyze audio and video DirectX components in the system.

55. Answer: C. The primary focus of SAML, in the context of IAM and DLP, is securely exchanging authentication and authorization data between an identity provider (IdP) and a service provider (SP) to enable single sign-on (SSO). The text explicitly states that Security Assertion Markup Language (SAML) is an open standard used for authentication and authorization data exchange between an IdP and an SP, enabling SSO. See Chapter 44, "Logical Security," for more information.

Incorrect answers: Preventing the unauthorized copying or deletion of sensitive data after a user has been granted access describes the primary function of data loss prevention (DLP), not SAML. While SAML plays a role in granting initial access, it doesn't directly control actions on data post-access. Managing and controlling user access to resources and systems based on their identity are the core function of identity and access management (IAM) as a whole. While SAML is a technology used within IAM for authentication, it's not the overarching system that manages all aspects of user access. Storing and organizing user information like usernames, passwords, and access permissions within a directory service describe the function of directory services, which are a component of IAM. While SAML relies on the information managed by directory services, SAML itself is the protocol for exchanging authentication and authorization data, not the system for storing user information.

56. Answer: A. The user will have only read access to the file. Remember that the more restrictive permissions take precedence, so in this case, the NTFS "Read" permission level takes effect. See Chapter 45, "Windows Security Settings," for more information.

Incorrect answers: It is possible for the user to get write, modify, or full control access—but only if the NTFS permissions are configured to allow the user to do so. As it stands, the user has only read access.

57. Answer: D. The program would be installed to C:\Program Files (x86). This is the default folder for 32-bit programs when installed to a 64-bit version of Windows. See Chapter 41, "Application Installation and Configuration Concepts," for more information.

Incorrect answers: Keep in mind that 64-bit programs are installed to the C:\Program Files folder. The operating system is installed to C:\Windows. Finally, C:\ is the root of the drive. A few system files are placed in the root, but otherwise the OS and applications are installed to folders within the root. x86 is the general term applied to 32-bit computers, whereas x86-64 (or simply x64) is the term applied to 64-bit computers.

58. Answer: B. If the computer has a recovery partition, then Windows can be reinstalled from there. This is often a partition that was placed on the storage drive by the computer manufacturer for just this type of scenario. See Chapter 30, "Operating Systems Installation and Upgrades," and Chapter 53, "Troubleshooting Microsoft Windows," for more information.

Incorrect answers: System Restore is an example of Windows functionality that can bring the system back to an earlier point in time but does not reinstall the entire OS. Linux rescue media (flash drive or boot disc) might work, but only if a Windows image is available somewhere, so the answer is not specific enough. (You might also use a flash drive with a Windows image.) The primary partition is where Windows is installed *to*. It does not normally contain recovery data or a recovery Windows image.

59. Answer: D. The first thing you should do is look up the error number. If an item fails during Windows Update, an error log called

WindowsUpdate.log can be written to C:\Windows\Logs\WindowsUpdate, but only if you have run the **Get-WindowsUpdateLog** cmdlet in PowerShell first. (In previous versions of Windows, it was in the %systemroot%, usually C:\Windows.) An example of an error code is 0x80243FFF, which is a user interface error. (It might show up in the log without the 0x.) You might also need to access the CBS.log file, which is located in %systemroot%\Logs. See Chapter 37, "Windows Settings," for more information.

Incorrect answers: While the Event Viewer can be very handy for analyzing system file, application, and security issues, it is not the first and best place to go when troubleshooting Windows Update errors. The Event Viewer is more generic (problem-wise), whereas the WindowsUpdate log files and CBS.log files are very specific. Downloading the failed update and installing it manually will probably result in the same error. You need to dig deep and find out what the real cause of the problem is. You do want to visit the Microsoft website, but you will most likely be going to https://support.microsoft.com or https://docs.microsoft.com (or both); there is no Microsoft Update website per se (as of the writing of this book).

60. Answer: C. You must rejoin the computer to the domain. You can do this by navigating to the **Computer Name** tab of the System Properties dialog box, which is accessed from the **Advanced settings** link from the System window or by executing **systempropertiescomputername.exe** at the Run prompt. You might also use the **netdom** command in the Command Prompt if you have Remote Server Administration Tools (RSAT) enabled on the Windows client or are working directly on a Windows server. See Chapter 38, "Windows Networking," for more information.

Incorrect answers: Updating the BIOS/UEFI to the latest version will help with any firmware issues but won't have any effect on trust relationships within Windows. Running **chkdsk** will check for errors on the storage drive. Rebooting the PC will not automatically rebuild the relationship; you must manually rejoin the computer to the domain.

61. Answer: D. Your friend might have an address such as thomas_r@example.com. To enable the iPad access to this email account, you'll need the type of server that handles email (be it SMTP, POP3, IMAP, or an Exchange server) and the domain name that the server resides on. Often, this will be the same domain name as the email address, but not always. An example of an SMTP mail server might be mail.example.com. A POP3 server might be pop.example.com. See Chapter 54, "Troubleshooting Mobile Operating Systems and Applications," for more information.

Incorrect answers: IP addresses aren't necessary when configuring an email account on an iPad, an Android device, a PC, or any computer, really. The reason is that the email account software will automatically attempt to resolve the mail server name to the IP address, in the same manner a web browser does when you type in a web address. The gateway address and DNS server are only necessary when attempting to connect a device to the Internet. This most likely won't be an issue with an iPad, but it can be configured in the networking settings, if necessary.

62. Answer: B. You want to use a loop construct, such as a **for** or **while** loop, that will loop through a command block until the condition changes from true to false (the end of the file). See Chapter 62, "Basic Scripting, Part I," for more information.

Incorrect answers: An integer is any whole number. A string is one or more characters. A variable is something that refers to something else and can change over time (for example, $x = 42$). Integers, strings, and variables can be used *within* conditional loops. And a loop might be used within an **if-then** statement, which can be described as a statement that contains a hypothesis followed by a conclusion. In programming, it provides a secondary path of execution when the if portion is evaluated as false.

63. Answer: C. You should recommend an uninterruptible power supply (UPS). This meets both requirements: It enables the system to gracefully shut down in the event of a power outage, which protects files from corruption, and it can provide an hour of uptime (though

that will require a fairly powerful UPS of at least 1500 VA). See Chapter 60, "Environmental Controls," for more information.

Incorrect answers: A surge protector and power strip don't meet either of the two requirements. A power strip simply allows for more outlets, while a surge protector can help protect a computer against surges or spikes. A power distribution unit (PDU) is a device with multiple outlets that can come in many forms, including as a strip; however, it is much more than a power strip in that it can be monitored and controlled. PDUs are often used in data centers and server rooms and are also known as main distribution units (MDUs).

64. **Answer: A.** An artificial intelligence system is only as good as the data upon which it was trained. If it was trained poorly, it will deliver poor (even biased) results. Sometimes the AI will make up the answers (hallucinations), and other times it will give wrong answers; either makes the AI fallible. See Chapter 65, "Appropriate Use of Artificial Intelligence," for more information.

    Incorrect answers: While it is true that poorly planned questions of the AI system do give poor results, that isn't a fault of the AI system. The AI systems are getting better at analyzing poor questions and guessing what the users intended to ask. Power is not an issue (that's for dystopian fiction to discuss). And human-based errors aren't related to the hallucinations that AI may encounter and share with users.

65. **Answer: B.** The best answer listed is that the parent folder has explicit Deny rights set for the third-party user. If this is the case, then by default, that permission will *propagate* to any subfolders and files within the parent. This can also be expressed as the default action for a subfolder (also known as a child folder) to *inherit* its permissions from the parent. Basically, you should remember two things: A folder inherits its permissions from the parent, and Deny rights will always override Allow rights. See Chapter 45, "Windows Security Settings," for more information.

    Incorrect answers: If the folder were set with Allow rights, the third party should be able to access the data. If the user forgot to share the

folder, the third party would not be able access the data. However, it's the second part of that answer that is impossible because you can't share a specific file; you can only share folders. The archive attribute would simply create a backup copy of a file or folder. Permissions questions can be some of the toughest on the A+ exam, but if you remember a few basic rules (such as the ones mentioned here), you should survive them!

66. **Answer: B.** The most common Linux shell program is the Terminal utility, which uses the Bash shell by default on most Linux distros. (This is also available in macOS.) This utility allows the user to enter commands of all types—including recovery commands—to be executed by Linux. See Chapter 40, "Linux," for more information.

    Incorrect answers: Windows Terminal is a modern terminal emulator. In this, you can interact with cmd.exe (the Command Prompt), PowerShell, and even Linux shells running in Windows Subsystem for Linux (WSL). The Command Prompt is often referred to as CMD because it can be opened with the cmd.exe executable. Backup and restoration programs, such as macOS's Time Machine, Windows System Restore, and so on, cannot have recovery commands typed into them. You require some kind of text interface to do so.

67. **Answers: B and D.** Modify the AutoRun settings for USB drives. Modify AutoPlay/AutoRun by disabling it in the Group Policy Editor or in **Settings > Bluetooth & devices > AutoPlay**. (Also, the use of USB drives and other removable media should be disabled in the BIOS/UEFI.) Since the login attempt appears to have used common login information, that could indicate that shared credentials might have been compromised and should be changed as well. See Chapter 48, "Workstation Best Practices," for more information.

    Incorrect answers: Removing admin permissions is somewhat vague. An administrative account has administrative permissions for a reason: so that the admin can access the server. Removing a user from the Administrators group would result in a standard user account, which is great from a principle of least privilege perspective, but that person could no longer log in to the server, making it

pointless. A software-based firewall would not have prevented this exploit because the user was local (behind the firewall) using a USB stick. You could change the default credentials of the Guest account, but it is better to either give it a strong password (if you have to use it) or, better yet, disable the account altogether; Windows 10 and following disable this account by default, and you should double-check to ensure that it has remained disabled. OS security updates should be run on a regular basis, but this is an issue that goes beyond updates.

68. **Answer: B.** Use comments to describe what the script is doing. In PowerShell, Bash, and many other scripting systems, use the number sign (#) to start a comment. Remember, comments don't actually *do* anything other than provide explanation. See Chapter 62, "Basic Scripting, Part I," for more information.

    Incorrect answers: End-user documentation is an important element to include in any software. However, that is better developed as a PDF file or online documentation (readthedocs, mkdocs, and so on). In addition, end users usually won't see your scripts; in the scenario, the comments are designed for the engineers who might actually look at the script. Variables and **if-then** statements are components of a script that actually do something (unlike comments). Change management documentation would be required if you were to make changes to the script.

69. **Answer: C.** Encryption (for example, WPA3 with AES) prevents unauthorized users from accessing confidential data that is transmitted over the wireless network. One of the best ways to protect confidentiality of data in general is through encryption. Use the highest level of encryption possible on a SOHO wireless network to eliminate this threat. See Chapter 51, "SOHO Security," for more information.

    Incorrect answers: Enabling MAC filtering looks like a good answer. However, it is used to stop unauthorized computers from accessing the wireless network. While a good idea, it does nothing to protect the actual data. Plus, a good hacker can get past MAC filtering. If that happens, encryption is going to be the savior anyway.

While anything is hackable, breaking the AES cipher will require a powerful computer and a lot of time. Changing the SSID name only modifies the name of the wireless network. However, by default, the SSID is broadcast from most SOHO routers, which is easily found by various wireless scanning software packages. Reducing the broadcast power is a smart idea as well, but this simply reduces the distance the SOHO router sends its wireless signal. If the hacker is within this range, they will have access to the network. The key here is *confidential*. To protect confidentiality, use encryption.

70. **Answer: D.** Programs and Features is the place to go in the Control Panel (CP) to remove an application in Windows. You can also open this by entering **appwiz.cpl** in the Command Prompt. Or you could access **Settings > Apps > Apps & features**. See Chapter 36, "Windows Control Panel Utilities," and Chapter 37, "Windows Settings," for more information.

    Incorrect answers: Disk Cleanup is used to remove temporary files; it's not used to remove applications. Windows Tools, known as Administrative Tools in older versions of Windows, is a group of tools, such as Event Viewer, Task Scheduler, and Computer Management. Folder Options (or File Explorer Options) is where you can go to change how folders are displayed. Many of these tools are being migrated to the Settings controls as time goes on. See https://learn.microsoft.com/en-us/windows/client-management/client-tools/administrative-tools-in-windows?pivots=windows-11 for additional information.

71. **Answer: A.** Check the proxy server settings in the browser. A large network may use a proxy server to facilitate the caching of web pages —often for external, or *public*, websites only. It could be that the proxy server was not configured properly or wasn't configured at all. See Chapter 38, "Windows Networking," for more information.

    Incorrect answers: You shouldn't have to modify the IPv6 settings because the question says the system has a valid IP address. The hosts file is an older text file used to statically resolve hostnames to IP addresses. Although this file still exists in some versions of Windows, it is rarely used, except for malicious purposes. If it was used for

malicious purposes, the browser probably wouldn't be able to connect to any websites—external or internal. A DNS server performs domain name-to-IP address resolution; if other pages are working on the intranet, then chances are that the DNS server is not the issue.

72. **Answers: A, C, and F.** Of the listed answers, you should make sure WPA3/AES is on if your router supports it—at least WPA2/AES if not. Then reduce the transmitting power of the AP and disable the SSID broadcast. Reducing the power prevents signal bleed to other offices; usually this can be set to "low" or something similar. Disabling the SSID or network name of the AP makes it so that a typical user cannot scan for and locate the wireless network. Other smart ideas are to put a strong password on the admin account, implement MAC filtering, and disable WPS. See Chapter 51, "SOHO Security," for more information.

    Incorrect answers: Disabling the DHCP server won't do much for security, but it will hamper availability because most end users' computers will obtain IP addresses automatically. Most SOHO routers can modify the channel width but can't reduce the channel *availability*. Users can either connect or not. When enabled, quality of service (QoS) can help to prioritize traffic from specific computers or applications.

73. **Answer: A.** For proper quarantining and removal of malware, you usually have to disable System Restore first because it can get in the way of the antimalware scanning and removal processes by possibly reinfecting the computer. See Chapter 51, "SOHO Security," and the 10-step procedure for removing malware for more information.

    Incorrect answers: You might ask, "Well, what about disabling the network cards so that the malware doesn't spread?" While this approach might work, the best way is to physically disconnect the computer from the wired network and turn off any wireless on/off switches if at all possible. Or remove the wireless antenna from the computer. It's just impossible to tell if a virus or other type of malware is playing tricks on the Windows option to disable a networking card. Windows Update should be run after quarantining and removal processes are complete. You can run **chkdsk /R** to locate

bad sectors and recover readable information, if necessary, after the malware removal is complete.

74. **Answers: B and D.** Among other things, you should recommend using strong passwords and assigning security rights based on job roles. Strong passwords are important on routers, wireless devices, switches, computers, and anything else that can be logged in to. Role-based access control means rights and permissions are assigned based on the person's job in a company—accounting, marketing, and so on. See Chapter 48, "Workstation Best Practices," for more information.

    Incorrect answers: Daily security audits might be a good idea, but they do not increase security; they only determine whether there is a threat or vulnerability that needs to be attended to. The customer already said that their antimalware software is up to date, so additional antimalware software should not be necessary. In fact, you shouldn't run any more than one type of antimalware software because they can have conflicting results that can slow down the system. Disabling screensavers doesn't really increase the security of the network, but setting up a password lock within the screensaver can make the individual systems more secure.

75. **Answers: A, C, and E.** Professionalism comes in many forms. When dealing with a customer, you should avoid distractions, avoid being judgmental, and meet expectations that are set. Also, avoid arguing, talking to coworkers, and engaging in personal interruptions. Be positive and listen to the customer. See Chapter 61, "Incident Response, Communication, and Professionalism," for more information.

    Incorrect answers: It is important to retain a chain of custody, but this has more to do with tracking evidence and less to do with professionalism. Documentation is important as well and should be developed by you, as the technician; it should not be left to the customer.

76. **Answers: B and D.** You should look in the Event Viewer (Application log) and look for any other log files that are created by that new application. These might contain clues about why the

service won't start. Perhaps the service is dependent on another service, or perhaps a particular file needs to be replaced. See Chapter 32, "Microsoft Operating System Features and Tools, Part I," for more information.

Incorrect answers: The Registry contains all of the parameters of the operating system, but it won't give you error information. %systemroot%\System32\Drivers contains drivers for hardware. The log file might lead you to believe that a driver needs to be replaced, but it isn't the first place you should look. Task Manager shows the performance of the CPU and RAM and shows what services are running. You might have attempted to start the service from there (or the Services Console) as part of the scenario.

77. **Answer: C.** Secure Shell (SSH) is the best of the listed answers. It allows for secure sessions from a client to a server or to a network device. SSH needs to be installed/enabled on the switches and routers, and then the IT firm employees need to connect with a secure SSH client (such as OpenSSH, PuTTY, or something similar). See Chapter 64, "Remote Access Technologies," for more information.

    Incorrect answers: RDP stands for Remote Desktop Protocol; it is a commonly used term to refer to Microsoft's Remote Desktop Connection program, which can only be used to connect to Windows clients and servers. Telnet is an insecure protocol that was the predecessor to SSH. It is disabled on most client systems, and some switches and routers don't incorporate its functionality at all. Virtual Network Computing (VNC) is used most often to connect to remote client computers such as Windows, macOS, Linux, and Android, but SSH is the preferred method for connecting to network devices such as switches and routers.

78. **Answer: C.** The best answer to maintain data security is to initiate a remote wipe on a device that has been lost or stolen. That will delete the data and make it very difficult to reconstruct. See Chapter 49, "Mobile Device Security," for more information.

    Incorrect answers: Passcode locks and login attempt restrictions will only hamper a hacker who has appropriated the device. GPS (or

location services) can help to find the device; however, if a device has been stolen or lost, time is of the essence, and the data should be remotely wiped right away.

79. **Answer: B.** The syntax shown is one way of mapping a network drive in Windows. **net use** is the command, the drive letter to be used is Z:, and the path to the share is *servername**sharename*. This type of command would historically be found in a batch file in Windows; it uses the .bat extension. However, PowerShell is the newer, and better, tool to work with; it uses the .ps1 file extension by default. And while you can still use the **net use** command, PowerShell uses the newer **Get-PSDrive** cmdlet. See Chapter 63, "Basic Scripting, Part II," for more information.

    Incorrect answers: .vbs indicates Visual Basic script, which can be used in Windows but is not necessary for basic networking procedures such as mapping network drives. .js indicates JavaScript, which is often used in websites. .py indicates Python, which is used for a variety of things, but again, is not necessary for mapping network drives.

80. **Answer: C.** A screened subnet, also known as a demilitarized zone (DMZ), is an area that is not quite on the Internet and not quite part of your LAN. It's a sort of middle ground that is for the most part protected by a firewall, but particular traffic will be let through. A screened subnet is a good place for web servers, email servers, and FTP servers because these are services required by users on the Internet. See Chapter 51, "SOHO Security," for more information.

    Incorrect answers: Network Address Translation (NAT) is the process of transforming IP addresses as data crosses a router, primarily to hide the internal LAN IP address space. It doesn't describe an intermediary network area. Port forwarding maps an external network port to an internal IP address and port, allowing specific traffic to reach internal servers. While related to making servers accessible, it's a mechanism, not the description of the network area itself. Universal Plug and Play (UPnP) is a group of networking protocols that allows devices to discover each other on a

network for easier connectivity. It is not related to creating a buffer zone between the Internet and the LAN for servers.

81. **Answers: A and D.** Apps might also fail to load or might load very slowly. The reason could be that there are too many apps open, or perhaps the web browser has too many tabs open. It could also be a sign that there is no space left on the device. Remove and/or relocate apps to see if that fixes the problem. See Chapter 54, "Troubleshooting Mobile Operating Systems and Applications," for more information.

    Incorrect answers: Disabled GPS or an unintended Bluetooth connection would not likely cause apps to load slowly (or not at all). However, a disabled Wi-Fi connection could be another reason for failing apps.

82. **Answer: A.** Remote monitoring and management (RMM) solutions are software tools that are designed to remotely monitor and manage client endpoints, networks, and computers. These remote IT management solutions go beyond single RDP connections and allow a technician to have a more wholistic view of systems and networks, all displayed in one window. See Chapter 64, "Remote Access Technologies," for more information.

    Incorrect answers: Use Remote Desktop Connection (RDC) in Windows to make a single Remote Desktop connection to a remote computer. Use the **mstsc** command to simply display the Remote Desktop Connection program or to make full connections to remote systems from the command line. Remote Assistance calls can be made from Windows users to invite other users to help fix a problem for them.

83. **Answers: C and D.** Windows Defender Firewall may be blocking the connection to the remote system. (By the way, RDC uses port 3389.) Have the customer ensure that Remote Desktop is allowed through the firewall. Also check that remote connections are allowed by going to the Search field and typing **allow remote connections to this computer**. Look for the option **Change settings to allow**

remote connections to this computer. See Chapter 64, "Remote Access Technologies," for more information.

Incorrect answers: Rebooting the computer or running Windows Update simply won't address the problem at hand. Either the firewall is blocking the connection, or the system isn't configured to accept remote connections. Also, it wasn't specified who would be running Windows Update, but it certainly couldn't be you because you have been blocked by the remote computer.

84. **Answer: D.** Your system does not meet Trusted Platform Module requirements. According to Microsoft's Windows 11 Pro minimum requirements (as of March 2025), TPM version 2.0 is required to upgrade your system to Windows 11 Pro. To fix the problem, you would have to upgrade the TPM firmware and possibly flash the BIOS/UEFI. See Chapter 30, "Operating System Installations and Upgrades," for more information.

    Incorrect answers: As of March 2025, the Windows 11 installation requirements in general are 1 GHz or faster processor with two or more cores on a compatible 64-bit processor or System on a Chip (SoC), 4 GB RAM, 64 GB or larger storage device, UEFI Secure Boot capable, Trusted Platform Module version 2.0, graphics card compatible with DirectX 12 or later with a WDDM 2.0 driver, and high def (720p) display. Your system meets all requirements with the exception of the TPM requirement.

85. **Answers: B and C.** An automated teller machine (ATM) is a common example of a multifactor authentication system. Usually, an ATM requires "something you have" (your ATM card) and "something you know" (personal identification number [PIN]). See Chapter 44, "Logical Security," for more information.

    Incorrect answers: "Something you are" is incorrect because that includes a biometric factor—for example, a fingerprint, retinal pattern, or hand geometry. "*Somewhere* you are" is incorrect because that would include authenticating to a specific network in a specific geographic area or boundary, using geofencing or GPS, for example.

86. Answer: A. Use a screened subnet (also known as a DMZ) to house the servers. This will secure them by isolating them from the LAN. See Chapter 51, "SOHO Security," for more information.

Incorrect answers: In a DHCP scope, DHCP reservations are IP addresses that are reserved for specific devices or computers. While it is possible that you might assign the servers reserved addresses in the scope, it is more likely that the servers will use static IP addresses (as most servers do). IP filtering is a mechanism in which particular types of IP datagrams and packets are discarded. A static WAN IP is a public address (one that faces the Internet), and it does not change. This is something that you would apply to the Internet side of your router or a server that faces the Internet. But the question asked for private IP addresses, so these servers will not face the Internet directly.

87. Answer: C. Check the amount and type of the data stored on the user's desktop. When a user is set up with a roaming profile, some of the local profile information (and desktop data) is *merged* with the roaming profile to the network. This can cause logging on and logging off to take a long time. That time can be reduced by checking for (and possibly moving) data on the user's desktop and elsewhere. Speed can also be increased if you properly configure how roaming profiles work. The idea is to ultimately have small, compact roaming profiles because they follow the user around the network. See Chapter 44, "Logical Security," for more information.

Incorrect answers: While there are other things that can slow down the computer—including limited RAM, limited paging (swap) file, improper time synchronization, DNS issues, and so on—the rest of the answers are less likely to be the problem, especially because the laptop was working quickly until the user's account was changed to roaming. A network share is used to store user data centrally at a server, on a NAS, on a SAN, in the cloud, and so on. That is where you would probably want to move some of the data from the user's laptop.

88. Answers: B and D. First, ground yourself. The best way is to use an antistatic strap and other antistatic measures, including touching the

chassis of the computer. Second, handle adapter cards and other electronics by the edge to avoid making contact with any of the circuitry—but don't touch the slot connectors! See Chapter 59, "Safety Procedures," for more information.

Incorrect answers: A dry environment actually increases the chance of ESD; keep the humidity higher and use a hygrometer to measure it. It is not recommended to plug the device into an outlet when working on it. Wearing eye protection is a good idea when working with hazardous materials and particulate matter, but it is not always necessary when working on electrical components.

89. Answer: C. In step 8, after removing the malware, it is suggested to schedule regular full system scans with your antivirus software. Also, keep your operating system, applications, and browser extensions updated to patch vulnerabilities and prevent future infections. See Chapter 51, "SOHO Security," for more information.

Incorrect answers: Booting into Safe Mode/preinstallation environment to limit malware activity is step 6, which is part of the malware removal process itself, not an action taken after removal. Reimaging/reinstalling the OS is a drastic step to be taken during the removal process if other methods fail, not an action taken after successful removal. Quarantining the infected system is step 2, which is one of the initial steps taken during the malware removal process, not after it.

90. Answer: A. Use BitLocker to encrypt the data on the laptop. As long as the laptop has a Trusted Platform Module (TPM) chip (or uses USB keys), BitLocker can be implemented to encrypt entire volumes/drives (data at rest) using AES. See Chapter 45, "Windows Security Settings," for more information.

Incorrect answers: Secure File Transfer Protocol (SFTP) is used to transfer data from a client to an FTP server—that's data in motion—and one way to protect that is by using SFTP, which makes use of SSH for security. Access control lists (ACLs) are rules that allow or disallow access on a firewall. Encrypting File System (EFS) is also found in Windows; it is used to encrypt individual files or folders and

does not need a TPM. A hardware security module (HSM) can create secure boot keys; it must be enabled properly within the BIOS/UEFI; it is a different technology than TPM in that it is not (usually) included *within* the computer out of the box; instead, it is a standalone device or an add-on adapter card.

91. **Answers: B, C, and E.** Policies can be configured to manage add-ons and disallow access to websites that are known to be malicious. User training is also important when it comes to helping users know which websites to access, how to use search engines, and what to do if pop-ups appear onscreen. In addition, use a proxy and content filter to cache websites and block potentially harmful sites. See Chapter 52, "Browser Security," for more information.

    Incorrect answers: While standardizing browsers could be part of a security strategy in some organizations, mandating specific browsers isn't a "general" browser security procedure. Relying solely on built-in browser security features without additional configurations is not going to cut it usually. While disabling JavaScript could prevent some malicious code, it would also severely limit the functionality of many legitimate websites.

A Final Word About the 220-1202 Exam

After taking this practice exam, if you are unsure or unconfident in any way, then we urge you to step back and continue studying the 220-1202 objectives before attempting the real exam. And don't forget, if you purchased the print version of this book, you have a bonus practice exam waiting for you on the companion website (as well as other bonus materials). See the Introduction of this book for details.

Be ready for anything! We can't tell you *exactly* what will be on the exam because that would violate the CompTIA NDA, and the questions can change at any time! But the bottom line is this: If you know the concepts, you can pass any test. Use the official CompTIA A+ objectives as your guide. Review this book thoroughly. Finally, we challenge you to study in a hands-on manner on real computers and investigate all the concepts to the best of your ability. This will help you not only for the exam but also in the real world!

The CompTIA A+ Cram Sheet

This cram sheet contains the distilled, key facts about the CompTIA A+ Core 1 (220-1201) and Core 2 (220-1202) exams. Review this information as the last step before you enter the testing center, paying special attention to those areas in which you think that you need the most review.

220-1201

1. Laptops are smaller, portable versions of desktop PCs with replaceable items such as keyboards and touchpads. Fn key for implementing secondary key functions, 2.5" or 1.8" hard drives (SSD, HDD, or hybrid), M.2 and Mini PCIe cards, and SODIMM RAM: DDR4 (260-pin), DDR5 (262-pin).
2. Smartphone and tablets are mobile devices that have ARM-based CPUs, internal flash memory, multitouch displays, and Li-ion batteries. Often IP68-compliant (dust and water tight). Android = USB-C; iOS = USB-C or Lightning connector for older iOS devices. Privacy and security components to consider include biometrics, NFC scanner features, Wi-Fi connector/placement, camera/webcam/microphone.
3. GPS and geotracking provide location information about mobile devices.
4. Mobile devices connect to Internet via cellular WWAN (example: 5G, 4G, LTE), and Wi-Fi (WLAN). Bluetooth and NFC are common ways to connect to a personal area network (PAN). Mobile device

accessories can include stylus, headsets, speakers, webcam, docking station, and port replicator.

5. LAN = local area network. WAN = wide area network. MAN = metropolitan area network. PAN = personal area network. SAN = storage area network. WLAN = wireless local area network. WISP = wireless Internet service provider.

6. Switches connect computers together in a LAN. They can be managed (admin controlled) or unmanaged. Routers connect two or more LANs and connect LANs to the Internet. Firewalls protect individual computers and networks from unwanted intrusion. IDS = intrusion detection system. IPS = intrusion prevention system. An access point (or wireless access point) enables Wi-Fi-enabled computers and devices to communicate on the LAN wirelessly.

7. **Networking connectors:** Twisted pair (RJ-45, RJ-11); Fiber optic (SC, ST, and LC); Coaxial (RG-6, F-type connector). Single-mode fiber cable is used for longer-distance runs. Multimode is the more commonly used fiber optic cable in server rooms. Molex is a power connection with four wires. DB9 is a serial connector used with RS-232 connections.

8. **T568B standard:** 1. White/orange, 2. Orange, 3. White/green, 4. Blue, 5. White/blue, 6. Green, 7. White/brown, 8. Brown. T568A reverses the orange and green. (Straight through cable = T568B to T568B; crossover cable = T568B to T568A).

9. IPv4 addresses are 32-bit dotted-decimal numbers (example: 192.168.1.1) and can be statically (manually) inputted or dynamically (automatically) assigned (DHCP).

   127.0.0.1 is the loopback address.

   APIPA is 169.254.x.x (also known as link-local).

   To use the gateway, computers must be on the same network number as the gateway device. The subnet mask defines which portion of the IP address is the network number and which portion is the individual host number. Private IP addresses are internal to your network and do not communicate directly with the Internet. Public IP addresses communicate directly with the Internet. APIPA (Automatic Private IP

Addressing) is a system used on Windows to automatically self-assign an IP address in the 169.254.x.x range in the absence of a DHCP server. The following table provides a snapshot of some key IPv4 and IPv6 address features.

Address Feature	IPv4 Address	IPv6 Address
Loopback address	127.0.0.1	0:0:0:0:0:0:0:1 (::1)
Networkwide addresses	IPv4 public address ranges	Global unicast IPv6 addresses
Private network addresses	10.0.0.0 172.16.0.0 192.168.0.0	Site-local address ranges (FEC0::)
Autoconfigured addresses	IPv4 automatic private IP addressing (169.254.0.0)	Link-local addresses of FE80:: prefix

10. IPv6 addresses are 128-bit hexadecimal numbers (example: 2001:7120:0000:8001:0000:0000:0000:1F10).

::1 is the loopback address.

Link-local addresses begin with FE80::/10 prefix.

11. Common network speeds are 1000 Mbps (gigabit Ethernet) and 10 Gbps (10 Gb Ethernet).

12. Networking protocols include

- FTP (File Transfer Protocol). Ports 20/21. Secure versions: FTPS port 989/990 and SFTP on port 22.
- SSH (Secure Shell). Port 22
- Telnet. Port 23 (*not secure*)
- SMTP (Simple Mail Transfer Protocol). Port 25. Secure version uses SSL/TLS on ports 587 or 465.
- DNS (Domain Name System). Port 53

- DHCP (Dynamic Host Configuration Protocol). Ports 67/68
- HTTP (HyperText Transfer Protocol). Port 80
- NTP (Network Time Protocol). Ports 123 and 1023
- POP3 (Post Office Protocol). Port 110. Secure version uses SSL/TLS on port 995.
- NetBIOS/NetBT (NetBIOS over TCP/IP). Ports 137–139
- IMAP (Internet Message Access Protocol). Port 143. Secure version uses SSL/TLS on port 993.
- SNMP (Simple Network Management Protocol). Ports 161/162
- LDAP (Lightweight Directory Access Protocol). Port 389. Secure version uses SSL/TLS on port 636.
- HTTPS (HTTP Secure). Port 443
- SMB/CIFS (Server Message Block/Common Internet File System). Port 445
- RDP (Remote Desktop Protocol). Port 3389

13. Twisted pair cabling standards (maximum 328 feet/100 meters):

- Category 5: rated for 100 Mbps
- Category 5e: Rated for 100 Mbps and gigabit networks
- Category 6/6a: Rated for gigabit and 10 Gbps networks
- Plenum-rated cable: fire-resistant cable designed for airways, conduits, and areas sprinklers cannot reach.
- Direct burial cable is used outdoors, 8 inches underground, 8 inches away from power lines.

14. Wireless Ethernet:

- 802.11a, 5 GHz speed
- 802.11b, 2.4 GHz speed; up to 11 Mbps
- 802.11g, 2.4 GHz speed; up to 54 Mbps
- 802.11n (Wi-Fi 4), 2.4 and 5 GHz speed; up to 600 Mbps

- 802.11ac (Wi-Fi 5), 5 GHz speed; up to 3.5 Gbps
- 802.11ax (Wi-Fi 6), 2.4 and 5 GHz (6 GHz for Wi-Fi 6E) speed; up to 9.6 Gbps
- 802.11be (Wi-Fi 7), 2.4, 5, and 6 GHz speed; up to 46 Gbps
- 2.4 GHz channels: 1–11
- 5 GHz channels: 36, 40, 44, 48, 149, 153, 157, 161, 165
- Nonoverlapping channels are a set of wireless frequency channels that do not interfere with each other. For example, in the 2.4 GHz band, channels 1, 6, and 11 are commonly considered nonoverlapping channels for Wi-Fi networks.

15. Bluetooth is a short-range technology aimed at simplifying communications and synchronization among network devices.

    Bluetooth classes: Class I maximum transmission range: 100 meters; Class II (most common) range: 10 meters; Class III range: 1 meter. Class 4 range: 0.5 meter.

    Cellular: Cellular Internet connections use mobile networks to provide Internet access. These connections are based on technologies such as 4G LTE and 5G.

16. **NAT (Network Address Translation):** The process of modifying an IP address as it crosses a router. Translates from one network to another.

    Database Servers: Database servers store, manage, and retrieve data for applications and users. Examples of popular database management systems include Microsoft SQL Server, Oracle Database, MySQL, and PostgreSQL.

17. Port forwarding forwards an external network port to an internal IP address and port.

18. **Screened subnet (aka DMZ):** Area of network for servers that must be accessible by sources both outside and inside your network, not within LAN, but between it and the Internet.

19. **QoS (quality of service):** Prioritizes computers or applications. Enables administrators to predict, monitor, and control bandwidth use to ensure that bandwidth is available to applications that need it.
20. **PoE (Power over Ethernet):** 802.3af PoE devices send Ethernet data and power over twisted pair cable to compliant devices (for example, a PoE injector or switch).
21. Video cards typically connect to motherboards by way of x16 PCIe expansion slots. Video connector types include DVI, VGA (not digital but analog), HDMI, Mini-HDMI, DisplayPort, and USB-C.
22. USB (Universal Serial Bus). Type A/Type B connectors are used by desktops/laptops, USB-C connectors are used by tablets/smartphones, etc. USB 2.0 (high-speed) = 480 Mbps. USB 3.0 (SuperSpeed) = 5 Gbps. USB 3.1 (SuperSpeed+) = 10 Gbps. USB 3.2 = 10/20 Gbps (requires USB-C). USB 4.0 = 40 Gbps (requires USB-C).
23. **Thunderbolt:** Ver 1 = 10 Gbps and uses DisplayPort; Ver 2 = 20 Gbps (also DisplayPort); Ver 3 = 40 Gbps and uses USB Type C. Ver 4 = 40 Gbps and uses USB Type C.
24. **Random access memory (RAM):** DIMMs include DDR4 (288-pins) and DDR5 (288-pins); none are backward compatible. Example of DDR transfer rate: DDR5-4800 = 38,400 MBps. While the pin count for DDR5 is the same as DDR4, the keying notch and pinouts are different, making DDR5 desktop modules incompatible with DDR4 sockets. DDR4 SODIMMs (Small Outline DIMMs) for laptops have 260 pins. DDR5 SODIMMs have 262 pins. ECC RAM detects and corrects errors while non-ECC does not.
25. Storage drives are non-volatile devices that store data. Types of drives and interfaces include
    - **HDD:** Hard disk drive (magnetic-based)
    - **SSD:** Solid-state drive (flash-based). Can be SATA or M.2
    - **SATA:** Serial ATA uses a 15-pin power connector and 7-pin data connector. Rev 3 = 6 Gb/s, Rev 3.2 (SATA Express) = 16 Gbps.
26. **RAID:** Redundant array of independent (or inexpensive) disks. RAID 0 = striping (not fault tolerant), RAID 1 = mirroring (minimum 2

disks), RAID 5 = striping with parity (minimum 3 disks), and RAID 6 = striping with double distributed parity (minimum 4 disks). RAID 10 (1+0) is mirrored sets that are striped (minimum 4 disks).

27. ATX 12V 2.x Power Supplies connect to: motherboard (24-pin cable). CPU (4-pin/8-pin). PCIe video (6 or 8-pin) or new 12VHPWR (16 pin). SATA (15-pin). Molex (4-pin).

28. BIOS/UEFI identifies, tests, and initializes components and boots to storage drive, optical disc, USB flash drive, or network via PXE. CR2032 lithium battery provides backup power.

    BIOS/UEFI configurations: time/date, boot device priority (boot order), passwords, power management, WOL, monitoring, clock and bus speeds, virtualization support (Intel VT or AMD-V), enable/disable devices, and intrusion detection. For BIOS/UEFI update, flash it with new firmware.

29. The central processing unit (CPU) or processor takes care of most calculations. Speed measured in GHz. PGA (older AMD/AM4 and previous) = Pin Grid Array. LGA (Intel and newer AMD/AM5) = Land Grid Array. L1/L2 cache in each core. L3 cache is shared among entire CPU. Thermal paste/pads are required whenever heat sink is installed. TDP = thermal design power, example: 140 watts.

30. Case fans are important to keep components cool. CPU fans and liquid cooling can help keep CPU cool. CPU fan failure and power supply failure can cause system to shut down.

31. **Printer configuration settings:** Duplexing = printing on both sides; orientation = portrait or landscape; quality = DPI (600 or 1200), tray settings (such as size = 8 1/2" × 11").

32. **Cloud models:** SaaS (Software as a Service), IaaS (Infrastructure as a Service), PaaS (Platform as a Service).

    - **Public cloud:** Service provider offers applications and storage space to the general public over the Internet.
    - **Private cloud:** Designed with the needs of an individual organization in mind. Administrator has more control over the data and infrastructure than is the case with a public cloud.

- **Community cloud:** Mix of public and private, but multiple organizations can share the public portion.
- **Hybrid cloud:** Somewhere between public and private. Dedicated servers located within the organization and cloud servers from a third party form the collective network.

33. **Cloud concepts:** Metered utilization (service): only the services accessed are paid for. Rapid elasticity: Ability to scale the network quickly. On-demand service means that the cloud service is available at all times. Multitenancy means a single instance of software or infrastructure serves multiple customers (tenants). Tenants share the same resources but maintain separate, secure virtual instances.

34. **Virtualization:** *Type 1* hypervisor is native or bare metal (has direct access to hardware). *Type 2* is hosted; runs on top of OS. Examples: VMware, Hyper-V, VirtualBox. Network connectivity: Bridged (direct access to Internet), NAT (separated access), host-only (private, no Internet), or no networking. A virtual sandbox can be any environment created for development, testing, or training that is isolated from any production servers and isolated from the rest of the operating system that the sandbox is running on. Containers are generally used for running applications, while sandboxes are used for testing and analyzing potentially unsafe code or software. A VM provides an abstracted version of the entire hardware of a physical machine, including the CPU, memory, and storage. Containers are portable instances of software with its dependencies that run on a physical or VM. With a virtual desktop infrastructure (VDI), multiple virtual desktops for multiple users are hosted by a service. It is a technology that hosts desktop environments on a central server.

35. CompTIA 6-step *Troubleshooting Methodology*:

    Always consider corporate policies, procedures, and impacts before implementing changes.

    1. Identify the problem.
    2. Establish a theory of probable cause. (Question the obvious.)
    3. Test the theory to determine cause.

4. Establish a plan of action to resolve the problem and implement the solution.
5. Verify full system functionality and, if applicable, implement preventive measures.
6. Document findings/lessons learned, actions, and outcomes.

36. Time/Date resets to earlier date? Check lithium battery. For OS, synchronize to a time server.

37. Trouble with CPU? Check CPU fan, heat sink and thermal paste/pads, overclocking setting in BIOS/UEFI, and whether CPU is secure.

38. Noisy computer? Check CPU fan, case fan, power supply fan, and use compressed air and vacuum.

39. RAM issue? Reseat modules; clean with compressed air. Overheating? Try RAM heat sinks. BIOS beep codes or displayed errors? Consult motherboard docs and analyze POST beep codes and numbers.

40. Power issues? Test AC outlet with receptacle tester. Test power supply with PSU tester: A power supply tester tests 3.3 V, 5 V, −5 V, 12 V, and −12 V. Do not open power supply; it is an FRU (field replaceable unit).

41. Slow storage drive? Defrag it, use disk cleanup, and scan drive with AV software. Drive isn't recognized? Check connections, check in BIOS/UEFI, initialize, partition, and format in Disk Management.

A missing RAID array could be caused by several issues, such as disconnected drives, a disabled RAID setting in the BIOS/UEFI, a failed RAID controller, or firmware corruption. Begin troubleshooting by verifying physical connections, checking BIOS/UEFI settings for RAID configuration, and ensuring the RAID controller is functioning properly.

42. No second screen on laptop? Check Fn key. Laptop display blank? Check brightness, resolution settings (Safe Mode if necessary), and for older LCDs: inverter and backlight.

Degraded performance on mobile devices is often caused by resource-intensive applications, outdated software, or insufficient available

storage. A common symptom is slower response times when launching apps or navigating menus.

43. Printer paper jam? Power cycle, check paper tray, rollers, paper type, fuser, and entire paper path. Blank paper? Check toner cartridge and transfer corona wire. Lines or smearing? Check drum, primary corona wire, and replace toner cartridge. Toner not staying on paper? Check fusing assembly. Garbled print/Garbage printout? Check driver. Ghosted image? Check drum and toner cartridge. Incorrect paper size? Check the tray and type of paper. No connectivity? Check power, network connection, whether printer is shared, proper IP address, and whether printer is set up as default in Windows.

    A printer failing to recognize a paper tray can prevent users from completing print jobs. This issue is often caused by incorrect tray configuration, physical misalignment, or firmware/software bugs.

44. Test network connections with patch tester, LAN cable tester, tone, and probe kit. Test NIC or RJ-45 jack/switch port with loopback plug.

45. No network connectivity? Check the link light, patch cable, disabled NIC, wireless switch is off, IP configuration, and Windows Network Troubleshooter. Limited connectivity? Ping localhost, then move outward, and use **ipconfig/all**. Poor wireless signal? Check distance, placement, antennas, and update hardware and software. APIPA or IP conflict? **ipconfig/release** and **/renew**; check DHCP server.

46. Authentication failures occur when a user cannot access network resources due to incorrect credentials or issues with the authentication system. These failures may present as error messages indicating incorrect username/password, account lockouts, or expired credentials.

220-1202

1. Windows 11 min. requirements: CPU = 1 GHz; RAM = 4 GB; Free drive space = 64 GB; UEFI (secure boot) capable; TPM 2.0; DirectX 12; 720p resolution.

2. Common system tools include Task Manager, Microsoft Management Console (MMC) snap-in, Event Viewer (eventvwr.msc), Disk Management (diskmgmt.msc), Task Scheduler (taskschd.msc), Device Manager (devmgmt.msc), Certificate Manager (certmgr.msc), Local User 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), Disk Defragment (dfrgui.exe), and Registry Editor (regedit.exe).
3. Many system tools have been migrated to the Settings app. Look there to configure your device.
4. Remote Desktop connection software (known as RDP) enables a user to see and control the GUI of a remote computer.
5. Workgroups are for small networks (20 maximum inbound sessions to a Windows client). Domains are for larger networks and are controlled by a domain controller that has Microsoft Active Directory installed.
6. The %systemroot% is C:\Windows by default.
7. In Windows, **dir** is the directory command. Navigate with the **cd** command, including **cd ..** and **cd **.
8. File management command-line tools include **md** (makes directory), **rmdir** (removes directory, **robocopy** (robust file copy, copies multiple files and directory trees).
9. Disk management tools include **format** (writes new file system), and **diskpart** (does everything Disk Management does, but in PowerShell/Command Prompt).
10. File checking command-line tools that can be used in Windows include **chkdsk** (**/F** fixes errors; **/R** locates bad sectors and recovers info) and **sfc** (System File Checker). **sfc /scannow** is common.
11. Certain command line tools are important to know:

Tool	Run All from a Command Prompt or Power Shell Prompt

Tool	Run All from a Command Prompt or Power Shell Prompt
hostname	Gives you the name of your own device on the network. You can also find this information in the Settings under System.
net user	Enables you to see which user account is logged in to the device you are currently using.
winver	Tells you which Windows you are currently running, including the version and the build.
whoami	Displays the current user, group, and privileges information. By itself it gives the user name as a network name.
[*command name*] **/?**	Help on any command can be found by typing the name of the command followed by **/?**
gpupdate	In an Active Directory environment, **gpupdate** forces a device to check for group policy changes and, if they exist, will apply them. It also processes any client-side extensions as part of the group policy updating. When complete, it will schedule the next update (usually 90 minutes). If sent from the server, **gpupdate** will force an update downstream to a client system.
gpresult	Used to find the resulting set of policies and permissions for an individual user on a specific machine after all group policies have been assigned.
nslookup	Use when you want information directly from the DNS server. It will open a connection; type a URL or IP address and the DNS server will return information directly. You can also type **nslookup [***URL or IP address***]** to get the same information without opening an nslookup window.

Tool	Run All from a Command Prompt or Power Shell Prompt
net use	Connects a device to or disconnects from a shared resource, or displays information about computer connections. Also controls persistent net connections. Without parameters, **net use** retrieves a list of all network connections.

12. A storage drive using GPT (GUID Partition Table) can have 128 partitions and go beyond MBR's 2 TB limit. GPT is stored in multiple locations. Requires UEFI-compliant motherboard. A storage drive using MBR can have four partitions: up to four primary partitions, but only one extended partition. Logical drives are sections of an extended partition. The Active partition is the one that is booted from; it usually contains the OS. Any section of a drive with a letter is called a volume. Volumes in dynamic drives can be resized, but not in basic drives. NTFS is the most common file system in Windows. exFAT is for flash drives.
13. Backups can be accomplished with Windows Backup or third party solutions. Windows File History is being phased out in favor of other backup solutions. It's not fully replaced yet but is expected to be removed in the future. For a comprehensive backup solution, consider third-party imaging software or cloud storage options.
14. System Restore can fix issues caused by defective hardware or software by reverting back to an earlier time with restore points.
15. The Windows Recovery Environment (Windows RE) includes System Recovery Options such as Startup Repair, System Restore, Command Prompt, and Startup Settings.
16. Startup Settings brings up options such as Safe Mode, Enable Low-Resolution Video, and Last Known Good Configuration. Safe Mode boots the system with minimal drivers.
17. The Event Viewer warns about possible issues and displays errors as they occur within three main log files: System, Application, and Security. Security displays auditing information.

18. A stop error (also known as a Blue Screen of Death or BSOD) completely halts the operating system and displays a blue, green, or black screen with various text and code. Can be caused by faulty hardware or bad drivers. macOS's equivalent error is the spinning pinwheel.
19. **gpresult** displays policy information for the user/computer. **gpupdate** updates policies without having to log off and on.
20. Common Windows networking command-line tools include
    - **ipconfig:** Displays current TCP/IP network configuration values; **ipconfig/all** shows additional information such as MAC address.
    - **ping:** Tests whether another host is available over the network (example: ping 192.168.1.1). Ping 127.0.0.1 or ping ::1 to test the local computer. **Ping -t** is continuous, **ping -n** is a set of pings. **ping -l** changes the size of each ping, **ping -a** resolves IP address to hostname.
    - **tracert:** Sends packets to test destinations beyond the local computer's network. **pathping** is similar.
    - **netstat:** Shows the network statistics for the local computer. Displays TCP and UDP sessions by computer name (or IP) and port.
    - **nslookup:** Used to query DNS servers to find out DNS details, including the IP address of hosts.
    - **net:** Used to map network drives (**net use**), view computers (**net view**), view users (**net user**), start/stop services (**net start** and **net stop**), and synchronize time (**net time**).
21. **Troubleshooting Windows:** Use WinRE startup settings, Startup Settings, Msconfig Safe Boot, use the Troubleshooter tool, restart services in services.msc (and with **net start / net stop**), end tasks in Task Manager, remove/repair applications in Programs and Features, enable/disable Windows components (such as Hyper-V) in Windows Features. Analyze and remove certificates in certmgr.msc.
22. macOS quick glance: Common macOS features and tools include the following:

- **Dock:** The icon bar at the edge of the screen providing quick access to frequently used apps, files, and minimized windows.
- **Multiple desktops (Spaces):** Create and manage separate virtual workspaces to organize open application windows and reduce clutter.
- **Gestures:** Multi-touch trackpad or mouse commands for navigating macOS, zooming, switching apps, and accessing features like Mission Control.
- **Finder:** macOS's file manager used for navigating folders, finding files/apps, and managing storage devices.
- **Keychain Access:** Securely stores and manages user passwords, certificates, keys, and sensitive notes.
- **Mission Control:** Offers a bird's-eye view of all open windows, virtual desktops (Spaces), and full-screen apps for easy switching.
- **Spotlight:** A systemwide search utility for rapidly finding files, apps, emails, and other information on your Mac.
- **iCloud:** Apple's cloud service for data storage, syncing information (such as contacts, calendars, photos) across devices, and device backups.
- **iMessage:** Apple's instant messaging service for sending texts, photos, and videos between Apple devices.
- **FaceTime:** Apple's integrated video and audio calling application for communication between Apple devices.
- **Continuity:** Features enabling seamless interaction between Apple devices, such as Handoff, Universal Clipboard, and AirDrop file sharing.
- **Screen Sharing:** A built-in VNC client/server enabling you to view or remotely control another Mac on the network.
- **Time Machine:** The integrated backup software that automatically creates incremental backups of your files and system state.
- **Terminal:** Provides command-line interface access to the underlying Unix operating system for advanced users.

Application Installation and Management:

- **.dmg (Disk Image):** A common file format for distributing apps; usually requires dragging the contained .app file to the Applications folder.
- **.pkg (Package):** An installer file that runs a setup wizard for applications often requiring system-level changes or specific installation steps.
- **.app (Application Bundle):** A self-contained package holding the executable application and its resources, typically stored in /Applications.
- **App Store:** Apple's curated digital marketplace for discovering, purchasing, installing, and updating macOS applications.
- **Uninstallation process:** Usually involves simply dragging the application's .app file from the /Applications folder to the Trash.

System Folders:

- **/Applications:** The default location for storing most user-installed application bundles (.app files).
- **/Users:** Contains individual home directories for each user account, storing their personal files, downloads, and settings.
- **/Library:** Holds systemwide settings, fonts, application support files, and resources shared across all user accounts.
- **/System:** Contains the core macOS operating system files managed by Apple and protected by System Integrity Protection (SIP).
- **/Users/Library (~/Library):** Stores user-specific settings, preferences, caches, and application support files within a user's home directory (often hidden).

Accounts and Security:

- **Apple ID:** Your personal account used to access Apple services like iCloud, the App Store, iTunes, iMessage, and FaceTime.
- **Corporate restrictions (MDM):** Mobile Device Management configurations applied by organizations to enforce security policies

and manage settings/apps on Macs.

Best Practices:

- **Backups (using Time Machine):** Regularly back up your system and personal data using Time Machine or another method to prevent data loss.
- **Antivirus:** Employ reputable antimalware software for an additional layer of protection against threats, complementing macOS's built-in security.
- **Updates/patches:** Consistently install macOS and application updates to ensure you have the latest security fixes, bug resolutions, and features.
- **Rapid Security Response (RSR):** Quickly apply Apple's RSR updates, which deliver targeted, critical security improvements between major OS updates.

System Settings Panes:

- **Displays Settings:** Configure monitor resolution, arrangement, brightness, color profiles, and AirPlay display options.
- **Network Settings:** Manage Wi-Fi, Ethernet, Bluetooth PAN, VPN connections, firewall, and network service order.
- **Printers & Scanners Settings:** Add, remove, configure, and share printers and scanners connected to your Mac.
- **Privacy & Security Settings:** Control app permissions (location, camera, microphone), manage FileVault encryption, firewall, and other security options.
- **Accessibility Settings:** Customize macOS features like VoiceOver, Zoom, captions, and pointer control for users with disabilities.
- **Time Machine Settings:** Select backup disks, exclude items from backup, manage backup frequency, and view backup status.

macOS Utilities:

- **Disk Utility:** Manages storage devices; used for formatting, partitioning, verifying, repairing disks, and creating disk images.

- **FileVault:** Encrypts the entire startup disk to protect your data if your Mac is lost or accessed without authorization.
- **Terminal:** Provides command-line access.
- **Force Quit:** A tool used to immediately terminate applications that have become unresponsive or frozen.

23. Linux typically uses GPT and the ext4 file system, although some use the XFS file system. Paths use slashes, for example: /Downloads/PDFs. Distros include Debian, Ubuntu, Fedora, Red Hat, CentOS Stream, Kali, and Mint. Find the distro version by typing cat /etc/os-release.

Linux Terminal tools:

- **ip a:** Linux equivalent of **ipconfig**.
- **Is:** Lists directory contents; **chmod:** Modifies permissions; **chown:** Changes file ownership; **ps:** Displays process information; **apt & dnf:** Installs packages; **sudo:** Executes commands as admin; **su:** Switch user; **vi/Vim/nano:** Opens text editor; **passwd:** Changes password; **pwd:** Displays full path/filename of working directory; **mv:** Moves or renames files; **cp:** Copies files and directories; **rm:** Removes files and directories; **fsk:** File system check scans and repairs inconsistencies in a file system; **mount:** Enables USB drives, network shares, and storage devices to be mounted to a specific directory; **shutdown:** Brings system down; **kill:** Terminates processes; **cat:** Displays file content; **grep:** Searches for matching information; **df:** Reports disk space usage; **man:** Manual pages (help); **top:** Analyzes running processes, CPU, and RAM; **find:** Locates files; **ping:** Network diagnostic tool to test whether the device is reachable by sending data packets and measuring response time; **dig:** Finds out information related to DNS; **curl:** Allows requesting and transfer of data over a URL using various protocols such as HTTP, HTTPS, FTP, and more; **traceroute:** Network diagnostic tool to trace route taken by packets from source to destination; **du:** Displays disk usage.

Linux common configuration files:

- **/etc/passwd:** Stores essential user account information like username, UID, GID, home directory, and shell, viewable by all users.
- **/etc/shadow:** Securely holds encrypted user passwords and password aging policies; accessible only by root.
- **/etc/hosts:** Provides static hostname-to-IP address mappings used for local name resolution before querying DNS.
- **/etc/fstab:** Lists filesystems, their mount points, types, and options to be automatically mounted during system boot.
- **/etc/resolv.conf:** Configures the system's DNS client by specifying nameserver IPs and default search domains.

Linux OS components:

- **systemd:** Acts as the init system, the very first process started by the kernel, which then initializes the rest of the system by launching and managing other essential services and software.
- **kernel:** The core of the Linux operating system, managing hardware resources, process scheduling, and providing essential system services.
- **bootloader:** Software that initializes the hardware and loads the Linux kernel into memory to start the operating system when the computer powers on.
- **Root account:** The administrative superuser account possessing unrestricted privileges to perform any action on the Linux system.

24. Wireless encryption protocols include

- WPA (Wi-Fi Protected Access), version 2 and 3 are 256-bit.
- AES (Advanced Encryption Standard).
- Best combination is WPA3 with AES (as of writing this book).
- PSK (pre-shared key) is stored on AP. RADIUS server is used (port 1812) for external authentication.
- Deprecated protocols include WEP, WPA, and TKIP.

Wireless authentication methods include

- **RADIUS:** Provides centralized authentication, authorization, and accounting (AAA) for network access, commonly used in WPA2/WPA3-Enterprise Wi-Fi.
- **TACACS+:** A Cisco AAA protocol, often used for device administration, that separates authentication, authorization, and accounting functions.
- **Kerberos:** A network authentication protocol that uses tickets issued by a trusted authority to verify user or host identities securely.
- **Multifactor Authentication (MFA):** Enhances security by requiring users to provide two or more different types of proof of identity for authentication.

25. **Malicious software:** Known as malware. This includes
    - **Virus:** Code that runs on a computer without the user's knowledge.
    - **Trojan horses:** Appear to perform desired functions but actually are performing malicious functions behind the scenes.
    - **Spyware:** Type of malicious software that is either downloaded unwittingly from a website or is installed along with some other third-party software.
    - **Rootkit:** Software designed to gain administrator-level access to the core of a system without being detected.
    - **Keylogger:** Hardware or software that captures the keystrokes of a keyboard.
    - **Ransomware:** Software designed to hold the computer hostage, encrypting files or locking the computer until the user pays the attacker. Often propagated by a Trojan.
    - **Cryptominer:** Software that attempts to calculate hashes for cryptocurrency tokens. Can use up resources on a system, making it perform sluggishly.
    - **Boot sector virus:** Infects the computer's startup code on the hard drive, activating before the operating system loads.

- **Stalkerware:** Secretly monitors and transmits a user's device activity, location, and communications without their consent, often used for interpersonal spying.
- **Fileless:** Operates directly in system memory (RAM) without installing files onto the hard drive, making it harder to detect.
- **Adware:** Automatically displays unwanted advertisements, often bundled with free software or through browser pop-ups.
- **Potentially unwanted program (PUP):** Software that, while not strictly malicious, may be unwanted and often comes bundled with other downloads, potentially causing ads or performance issues.

26. Best practice for malware removal:

1. Investigate and verify malware symptoms
2. Quarantine infected systems
3. Disable System Restore in Windows Home
4. Remediate infected systems by doing steps 5–7
5. Update antimalware software
6. Scan and removal techniques: Boot into Safe Mode/preinstallation environment and scan.
7. Reimage/reinstall: if steps 5–6 fail, reinstall but back up important data.
8. Schedule scans and run updates
9. Enable System Restore and create a restore point in Windows Home
10. Educate the end user

27. Social engineering: The act of manipulating users into revealing confidential information or performing other actions detrimental to the user. Know phishing, vishing, smishing, whaling, impersonation, shoulder surfing, tailgating and dumpster diving!

28. **Network attacks:** Know on-path attack, spoofing, zero-day, dictionary, and brute force. DDoS (distributed denial of service): enabled by a botnet. Evil twin: a rogue and malicious copy of a wireless access point. You should also know what insider threats, business email compromise (BEC), supply chain/pipeline attacks, cross-site scripting (XSS), and SQL injections are.

29. **Authentication:** The verification of a person's identity; helps protect against unauthorized access.

    Broken down into: 1. Something the user knows (password or PIN); 2. Something the user has (a smart card or other security token); 3. Something the user is (biometric reading: fingerprint or retina scan); or 4. Something a user does (signature or voice print).

    MFA = multifactor authentication. Example: A password and a smart card.

    UAC (User Account Control) in Windows requires administrative login to perform higher tasks.

30. **Security techniques:** Access control vestibule or mantrap (quarantine area with two doors and surveillance), one-time password (OTP: card with changing code), RFID badge, biometric reader, smart cards, and ACLs (access control lists).

31. **Encryption:** The act of changing information using an algorithm known as a cipher to make it unreadable to anyone except users who possess the proper "key" to the data.

    - **Encrypting File System (EFS):** Encrypts one or more files or folders directly within the Properties page in Windows.
    - **BitLocker:** Encrypts an entire drive in Windows. Requires TPM (Trusted Platform Module). BitLocker To Go encrypts USB drives and other removable devices.

32. **Storage drive disposal:** Destruction (pulverizing/shredding, drilling holes in platters, incineration, degaussing; acquire certificate of destruction when complete). Know regulatory and environmental requirements like HIPAA, GDPR, and NIST guidelines for secure erasing/physical destruction and disposal.

33. BIOS/UEFI security includes administrator and user passwords, drivelock passwords, disabling removable media, UEFI Secure Boot (helps prevent rootkit access) and setting the boot device priority to storage drive first.
34. **Permissions:** The most restrictive permission takes effect and overrides the less restrictive permission (NTFS vs. share). Inheritance/propagation: If you create a folder, the default action it takes is to inherit permissions from the parent folder (so, the parent propagates to the child). If you move a folder within the same partition, it retains the permissions. If you move or copy a folder to another partition, the (new) folder inherits from the new parent.
35. **Mobile device security:** Screenlocks (pattern, PIN, password), invalid attempts lockout, remote wipe, remote backup, and antivirus. Disallow rooting and jailbreaking—removing limitations to Android and iOS to gain super-user capabilities.
36. **Wireless security:** Change admin password, change/disable SSID, reduce radio power, disable WPS, use WPA3/AES, enable MAC filtering, update firmware, enable firewall, disable ports, enable content filtering.
37. **Safety:** Do not open power supplies or monitors, test AC outlets before use, use Class C CO_2-based, or BC fire extinguisher on electrical fires, and call 911. Employ cable management, material safety datasheets (MSDS), and consult when encountering a product with chemicals (toner cartridges, cleaners).
38. ESD = electro-static discharge. Prevent with antistatic strap, mat, touch chassis, antistatic bags, unplug computer, and increase humidity.
39. UPS has battery backup for protection during electrical outages.
40. Trouble tickets include user/device information, description of problems, severity, and should be clearly written.
41. **Change management:** Includes purpose of change, scope of change, affected systems, risk analysis, end-user acceptance, change board approvals, and should include a rollback plan and sandbox testing.

42. **Incident response:** First response, identify what happened, report through proper channels, preserve data and devices, document, and set up chain of custody (chronological paper trail).
43. **Regulated data:** Includes PII (personally identifiable information), PHI (protected health information), personal government-issued information (Social Security card, etc.), PCI DSS (Payment Card Industry Data Security Standards), and GDPR (General Data Protection Regulation). Store in a secure area with encryption and proper permissions, and lockouts.
44. **Professionalism:** Professional appearance, punctuality, listen to customer, take notes, clarify problems, positive attitude, speak clearly, project confidence, be culturally sensitive, set and meet expectations, avoid distractions (phone calls, texting, social media), and avoid confidential data.
45. Basic loops (such as **for**) tell a program to execute the same statement several times.
46. PowerShell and Bash will always place a **$** before a variable.
47. **Scripting types:** Windows PowerShell (.ps1), batch file (.bat); Linux Bash (.sh); Python (.py); Visual Basic script (.vbs); JavaScript (.js).
48. **Remote access:** RDP (Remote Desktop Protocol, port 3389), SSH (Secure Shell, port 22), Virtual Network Computing (VNC), Windows Remote Management (WinRM), Simple Protocol for Independent Computing Environments (SPICE).
49. AI is making its way into productivity software. Be careful not to accidentally plagiarize the work of others, and be cautious when feeding it data that you don't accidentally give the AI access to your local work also. Instead, ask the AI how it would solve a similar problem.
50. AI can have bias, can hallucinate when it doesn't know the answer, and is not always accurate. Be cautious when using the answer that an AI system gives you.

Index

Numbers

2FA (two-factor authentication), 704
3–2-1 backup rule, 958–959
3G, 54
3.5 mm audio jack, 39
4G, 54
5G, 54
10-tape rotation, 957–958
12VHPWR, 235, 272
30-second trick, 11
64-bit, 691–192
80 Plus certification, 277
802.1X, 769
802.11 wireless, 83–85

A

AAA (authentication, authorization, and accounting), servers, 98–100, 769
AC adapter, laptop, 8–10
access control vestibule, 717, 788
accessibility settings, 623–625

accessing
storage drives, 21
Windows Settings, 609–610
accuracy, AI, 1054
acknowledgment, DHCP, 113
ACLs (access control lists), 730–731, 740, 934
AD (Active Directory), 76, 709
domain controller, 754–755
group policy, 757–758
home folder, 756–757
logon script, 756
Microsoft domain, 753–754
security groups, 758–759
user profiles, 755
adapters, connector, 188
administration tools, Windows 11, 536
administrative shares, 750–751
AES (Advanced Encryption Standard), 766–767
AHCI (Advanced Host Configuration Interface), 364
AI
accuracy, 1054–1055
application integration, 1051–1052
appropriate use, 1052–1053
bias, 1053–1054
hallucinations, 1054
limitations, 1053
policies, 1052
air treatment, 973–974
airplane mode, 28, 47, 54
alarms
building, 719
RAID controller, 364

algorithms, load balancing, 102
alternative location recovery, 956
AMD
CPUs, 256–257
sockets, 258
Android, 479
Force Stop option, 899–900
rooting, 822, 914–915
sideloading, 822
Wi-Fi settings screen, 46–47
antiglare filter, 375–376
antimalware, 776–777
antiphishing campaigns, 779–780
antivirus software, 776
AP (access point)
evil twin, 792–793
MAC filtering/IP filtering, 849
placement, 847
positioning antennas, 847
reducing transmission power, 846–847
APIPA (Automatic Private IP Addressing), 133, 401
App Store, 661
.app files, 661
Apple. *See also* iOS; macOS
Find My services, 819
iCloud, 656–657
Lightning connector, 36, 183
Apple ID, 662–663
apps and applications. *See also* browser
AI integration, 1051–1052
authenticator, 729
cloud-based, 334–335

distribution methods, 695–696
impact, 697–698
installing, 695–696
ISO image, 695–696
licensing, 710
life cycle, 506
Linux, 668
locator, 819
malicious, 915
messaging, 733
mobile device
installing, 389–390
troubleshooting, 899–901, 903
permissions, 629, 698
pinned, 517
security, 698–699
settings, 615–617
suspending, 652
system and OS requirements, 693–694
developer program, 695
video editing program, 694
uninstalling on macOS, 662
updating, 902–903
ARM (Advanced Reduced Instruction Set Computer Machine), 254
asset management, 938
inventory lists, 938–939
procurement life cycle, 939–940
attacks
BEC (business email compromise), 794
brute-force, 791–792
cryptoanalysis, 792

DDoS (distributed denial-of-service), 790–791
dictionary, 791
DoS (denial of service), 790
on-path, 789
spoofing, 789
SQL injection, 795
supply chain/pipeline, 794
USB drop, 245
zero-day, 789–790
attrib command, 749
ATX (Advanced Technology eXtended), 228–229, 272
audio. *See also* sound
captions, 624
mobile device, troubleshooting, 391
settings, 377–378, 624
AUP (acceptable use policy), 995–996
authentication, 723–724
802.1X, 769
biometric, 718
email, 109
DKIM (DomainKeys Identified Mail), 109–110
DMARC (Domain-based Message Authentication, Reporting & Conformance), 110–111
SPF (Sender Policy Framework), 110
Kerberos, 770
multifactor, 27, 704, 718, 724–726
passwordless, 742
passwords, 801–803
RADIUS (Remote Dial-In User Service), 768–769
servers, 99
SSO (single sign-on), 709
TACACS+, 769

troubleshooting, 397–398
two-factor, 704
two-step, 818–819
authenticator applications, 729, 818–819
auto-brightness, mobile device display, 385–386
AutoPlay/AutoRun, disabling, 811

B

backlight, 165, 167
backup, 217–218, 782. *See also* DRP (disaster recovery plan)
3–2-1 rule, 958–959
battery, 343
full, 952
incremental, 952–954
mobile device, 819–820
onsite vs. offsite, 958
versus RAID, 366
rotation schemes
10-tape, 957–958
GFS (Grandfather-Father-Son), 957
synthetic, 955
testing, 956
bandwidth, 174. *See also* latency
baseband, 55
Bash script, 1024–1028
basic drive, 502
batch scripts, 1023–1024
battery
backup, 343
CMOS, 241
disposal, 976

laptop, troubleshooting, 10
mobile device
overheating, 387–388
replacing, 39–40
troubleshooting, 389, 904–905
settings, 621–622
BEC (business email compromise) attack, 794
beep codes, BIOS POST, 246, 343–344
Berg connector, 276
bias, AI, 1053–1054
biometrics, 27, 718
BIOS (Basic Input/Output System), 14, 241–242, 348
boot options, 242
fan settings, 243
flashing the, 241
HSM (hardware security module), 244
passwords, 244, 804–805
POST (power-on self-test), 246, 343–344
RAID, enabling, 365
Secure Boot, 244
temperature monitoring, 244
TPM (Trusted Platform Module), 244
troubleshooting, 342–343
video settings, 373
virtualization support, 245
bit, 174
BitLocker, 628–629, 752–753
Bluetooth, 22, 38
Low Energy Audio, 624
pairing, 49–50
settings, 614–615
troubleshooting on mobile devices, 896–897

Blu-ray, 222–224
bollards, 719–720
Boot Camp, 655
boot methods
internal drive installation, 495
Internet-based installation, 495
local installation from external drive, 494
network boot (PXE) installation, 494–495
boot process, Linux, 683–684
boot sector virus, 774, 778
brightness, mobile device display, 385–386
browser
-based email, 332
-centric OS, 478
download/installation, 855–857
extensions and plug-ins, 858–859
general security procedures, 865–866
password manager, 860–861
patching, 857–858
privacy, 857
Proxy setting, 645
secure connections, TLS (Transport Layer Security), 861–863
secure sites and tracking, 863–864
settings, 858, 864–865
signatures, 857
brute-force attack, 791–792
BSD (Berkeley Software Distribution), 650–651
BSOD (blue screen of death), 348, 363, 881–883
burn-in, 372–373
bus speed, 253
BYOD (bring your own device), 42, 62, 796, 826–827. *See also* MDM (mobile device management)

byte, 174

C

cable/s, 177–178. ***See also*** **connectors**
coaxial, 178–179
crimper, 155
crossover, 177
cutter, 154
data transfer rate, 174
direct burial, 178
HDMI (High-Definition Multimedia Interface), 379
Internet, 147
lock, 27
modem, 126
optical, 179–180
patch panel, 123
plenum, 177–178
serial, 184–185
standards, 175
storage drive, 187
straight-through, 177
stripper, 154
tester, 154–155
twisted pair, 173–174. *See also* STP (shielded twisted pair); UTP (unshielded twisted pair)
Category 5, 174
patch cable, 177
wire termination, 154
cache memory, 256
calibrating
monitor, 375

touchscreen, 168
camera/webcam
disabling, 23
microphone, 23–24
mobile device, securing, 913
replacing, 23
troubleshooting, 24
USB-based, 24
captive portal, 848
capture cards, 239
car, synchronizing with your mobile device, 60–61
case connectors, 274–275
case fans, 262–263, 274
Category 5, 174
CCFL (cold cathode fluorescent lamp), 165
CCTV (closed-circuit television), 719
CD (compact disc), 222–223
cellular technology
3G, 54
airplane mode, 54
cellular location, 57
eSIM, 55–56
geofence, 56
GPS (Global Positioning System), 56–57
GSM (Global System for Mobile Communications), 55
IMEI/IMSI, 57–58
Internet connections, 150
laptop, 22
location services, 56
mobile device, 46
Certificate Manager, 539–540
certification

80 Plus, 277
CompTIA A+, 1066–1067
chain of custody, 986–987
change management, 945–946
business process terms, 946
terms, 947–949
channel/s
bonding, 86
selection, 86
width, 85–86
wireless, 85
checksum, 857
chemical storage, 975–976
chipset, 233, 257
chkdsk, 482–483, 572–573
Chrome OS, 477–478
CIA triad, 737
classful IP address, 138
Classic Mac OS, GUI (graphical user interface), 649. ***See also*** **macOS**
classless IP address, 138
clean install, 497
cleaning, mobile devices, 389
clearing data, 836
clock speed, 251–253
closed source, 649
cloud/cloud computing, 331–332, 489
backup services, 820
-based applications, 334
-based printing, 293
characteristics, 334–336
collaboration tools, 706

instant messaging, 707–708
presentation tools, 708
spreadsheets, 707
videoconferencing, 706–707
word processing tools, 709
file synchronization, 336
hybrid, 334
IaaS (Infrastructure as a Service), 332
iCloud, 656–657
measured services, 335
metered services, 335
mobile device synchronization, 58–59
multitenancy, 336
PaaS (Platform as a Service), 312, 332–333
private, 333
productivity tools
email systems, 703–705
online storage, 705–706
public, 333
rapid elasticity, 336
resource pooling, 336
SaaS (software as a Service), 51, 332, 704
CMDB (configuration management database), 939
cmdlet
New-LocalUser, 1020
New-PSDrive, 1029
coaxial cable, 178–179
code, 667–668. *See also* script/s; source code
collaboration tools, 706
instant messaging, 707–708
presentation tools, 708
spreadsheets, 707

videoconferencing, 706–707
word processing tools, 709
collating, 290
color gamut, 170
color scheme, sound card, 237–238
commands/command line, 563–564
Command Prompt, 564–565
help file, 567
Linux, 668
ip, 677
ip a, 26
lsblk, 484–485
su, 677–678
sudo, 678, 1043
macOS
diskutil list, 485
ifconfig, 652
mstsc, 1040
navigating, 567–570
PowerShell, 565–566, 835, 1020
$psversiontable command, 1019–1020
running, 1019–1020
test-connection, 1022
Windows
attrib, 749
chkdsk, 572–573
chkdsk /r, 482–483
defrag, 358–360
dir, 570
dxdiag, 374
gpresult, 575
gpupdate, 575–576

hostname, 585–586
ipconfig /all, 26, 396–397, 401, 579–581
net, 587–589
netstat, 77, 586–587
netstat -a, 399
nslookup, 587
ping, 135, 398, 400, 581–583
robocopy, 570–571
Run, 558–559
sfc, 573
systeminfo, 315
Terminal, 566–567
tracert, 583–585
whoami, 589
winver, 573–575
wmic logicaldisk get name, 569

compatibility
CPU (central processing unit), 256–257, 258
between operating systems, 488–490
power supply, 273–275
RAM (random-access memory), 17

compliance, data destruction and disposal, 838. ***See also*** **regulations/regulated data**

component failures, troubleshooting on motherboard, 343–344

compromised and damaged devices, 820

CompTIA A+ exam, 1059–1060
Core 1 (220–1201), 1127–1137
cram sheet, 1119–1125
domains, 1
exam preparation checklist, 2–3
registration, 3
Core 2 (220–1202)

cram sheet, 1127–1137
domains, 469
exam preparation checklist, 470–471
smart methods for difficult questions, 1065–1066
tips, 1062–1064
types of questions, 1060–1061
Computer Management tool, 543–544
Computer Name/Domain Name Changes dialog box, 636–637
computers. ***See*** **PCs**
configuration files, Linux, 680–681
configuration profiles, 815–816
configuration window, 518
connectionless session, 70
connection-oriented sessions, 70
connections & connectivity
Internet
cable, 147
cellular, 150
DSL, 147–148
fiber, 148–149
satellite, 149
troubleshooting, 396–398
metered, 644
mobile device, troubleshooting, 894–895
network, 643–645
connectors
12VHPWR, 235
adapters, 188
ATX (Advanced Technology eXtended), 228
Berg, 276
case, 274–275
Lightning, 183

Molex, 276
power, 260
power supply, 272–273, 275–276
RJ-45, 176
SATA (Serial ATA), 240
storage drive, 187
T568A/T568B, 176
USB, 182–183
video card, 185–187
constant, 1006
containers, 323–324
Continuity, 657
continuity tester, 154–155
contrast themes, 624
Control Panel, 519, 593, 631–632. ***See also*** **Windows Settings**
Device Manager, 632–633
Devices and Printers, 596
Ease of Access Center, 605
File Explorer Options, 600–601
Indexing Options, 599
Internet Options, 594–596
Mail, 597
Microsoft Defender Firewall, 597
opening and viewing utilities, 594
Power Management, 602–604
Programs and Features, 596–597
Sound, 597–599
System and Security, 632
User Accounts, 599
cooling, CPU (central processing unit). ***See also*** **overheating**
fans, 262–263
heat sink, 261

liquid, 263–264
thermal paste/pads, 261–262
COPE (corporate-owned personally enabled) devices, 827–828
corporate and ISP email configuration, 51–53
counter
laser printer, 301
performance, 541
CPU (central processing unit), 251
32-bit, 692
64-bit, 691–692
AMD, 256–257
ARM (Advanced Reduced Instruction Set Computer Machine), 254
bus speed, 253
cache memory, 256
clock speed, 251–253
Efficiency/Performance cores, 255
fans, 262–263
GPU (graphics processing unit), 256
heat sink, 261
installing, 264–267
Intel, 256–257
liquid cooling, 263–264
multicore, 255
multithreading, 255
overclocking, 253
replacing, 346
socket, 257–259
thermal paste/pads, 261–262
troubleshooting, 345–346
VM requirements, 318
voltage, 259–260

x64, 692
x86, 253–254, 692
cram sheet
CompTIA A+ Core 1 exam, 1119–1125
CompTIA A+ Core 2 exam, 1127–1137
creating
restore points, 878–879
VM (virtual machine), 315
Credential Manager, 804
crimper, 155
cron jobs, 1027
crossover cable, 177
cross-platform virtualization, 321–322
cryptoanalysis attack, 792
cryptography, 751
cryptominer, 775
cursor drift, 16
custom install, documentation, 931
CVEs (common vulnerabilities and exposures), 935
CYOD (choose your own device), 42, 62, 828

D

DAC (discretionary access control), 748
daisy wheel printer, 304
Dashboard, macOS, 655
database
configuration management, 939
servers, 95–96
SQL injection, 795
data/data security
clearing and purging, 836

controller, 994
custodian/steward, 994
deleting, 834–835
destruction, 837–838
floating-point, 1006
input source, 372
integers, 1006
owners, 994
regulated. *See also* regulations/regulated data
PCI-DSS (Payment Card Industry Data Security Standards), 993–994
PHI (protected health information), 992–993
PII (personally identifiable information), 992
-at-rest, 752, 811
strings, 1006
transfer rate, 828–829
PCIe (PCI Express), 231–232
slow, troubleshooting, 399
twisted pair cable, 174
USB, 181–182
DDoS (distributed denial-of-service) attack, 790–791
DDR3, 194–195
DDR4, 16–17, 195–196
DDR5, 16–17, 196
DDR6, 196–197
default password, changing, 844–845
defense in depth, 779, 825–826
defrag command, 358–359
defragging, 358–359, 551–552
degaussing, 837
deleting data, 834–835
desktop, Windows, 516

desktop distributions, Linux, 668–669
desktop PC. *See* PCs
destroying storage media, 837–838, 976
development server, 325
Device Manager, 537–539
device/s. *See also* mobile device/s
bring your own, 42, 62, 796
COPE (corporate-owned personally enabled), 827
default password, changing, 844–845
EOL (end-of-life), 486–487
network tap, 156–157
power, 977–978
surge suppressor, 978
UPS (uninterruptible power supply), 978–980
routers, 121
assigning static IP address, 849–850
default password, changing, 844–845
IP address, 844
settings, 614–615, 632–633
switches, 119–121
symbols used in Device Manager, 539
DHCP (Dynamic Host Configuration Protocol), 75–76, 113–114, 136–137
acknowledgment, 113
discovery, 112
exclusions, 114
request, 113
reservations, 114–115
servers, 96–97
dialog box
Computer Name/Domain Name Changes, 636–637
Sound, 598

dictionary attack, 791
digital optical port, 238
digitizer, 167–168. *See also* touchscreen
DIMM (dual-inline memory module), 193–194
dir command, 570
direct burial cable, 178
directories
changing, 568–569
commands for working with, 570–571
DirectX, 374
disabling
AutoPlay/AutoRun, 811
SSID, 845–846
unused services, 810–811
WPS (Wi-Fi Protected Setup), 848–849
disassembling, mobile devices
documentation, 391
manufacturer resources, 392
tools, 392
discovery, DHCP (Dynamic Host Configuration Protocol), 112
Disk Cleanup, 550–551
Disk Management utility, 548–550
Disk Utility, 660
diskpart utility, 502, 505–506, 835
diskutil list command, 485
DisplayPort, 186, 377, 655
displays. *See also* projectors
antiglare filter, 375–376
burn-in, 372–373
calibrating, 375
CCFL (cold cathode fluorescent lamp), 165
color gamut, 170

digitizer, 167–168
driver, 374
laptop
backlight, 165
inverter, 165
IPS (in-plane switching), 164
LCD (liquid-crystal display), 163–164
LED (light-emitting diode), 164
mini-LED, 165
OLED (organic light-emitting diode), 164–165
TN (twisted nematic), 164
VA (vertical alignment), 164
mobile devices, troubleshooting, 385–386
native resolution, 170
operator control panel, 410
pixel density, 168–169
refresh rate, 169
resolution, 373, 375
screen magnifier, 623–624
screen resolution, 170
screen sizing, 373
standard dynamic range, 170
troubleshooting, 166–167
disposal
battery, 976
hardware, 976
DKIM (DomainKeys Identified Mail), 109–110
DLP (data loss prevention), 732, 915
DLP (Digital Light Processing), 378
DMARC (Domain-based Message Authentication, Reporting & Conformance), 110–111
.dmg files, 661

DNS (Domain Name System), 76, 107–108
FQDN (fully qualified domain name), 108
records, 108–109
RRs (resource records), 108–109
servers, 97
DNSSEC (Domain Name System Security Extensions), 111
Dock, macOS, 651
Docker, 323
docking station, 40–41
documentation, 927. *See also* policy/ies
custom installation procedure for software, 931
help desk ticket, 938
incident report, 929
incident response, 985
knowledge base/articles, 933–936
licensing, 990
mobile device disassembly, 391
MSDS (material safety data sheet), 975
physical security, 720–721
printer manual, 410
SLA (service-level agreement), 931–933
software license, 940
SOP (standard operating procedure), 929–931
ticketing systems, 936–937
user checklists, 931
domain/s
CompTIA A+ Core 1 exam, 1
CompTIA A+ Core 2 exam, 469
controller, 637, 754–755, 770
network, 635–637
DoS (denial of service), 790
dot-matrix printer, 304–305

drawing pad, 41
drivers
display, 374
printer, 287–288
updating, 537–538
video card, installing, 235–236
drives. *See* storage drives

DRM (digital rights management), 988
DRP (disaster recovery plan), 950–951
DSL (digital subscriber line), 147–148
DSL modem, 126
dual-booting, 501, 655, 684
dual-channel architecture, 201
dumpster diving, 788
duplexing, 290
DVD (digital versatile disc), 222–223
DVI (Digital Visual Interface), 185
dxdiag command, 374
dynamic drive, 502

E

ECC (error correction code), 203
EDR (endpoint detection and response), 776–777
educational campaigns, antiphishing, 779–780
Efficiency cores, 255
egress data, 335
electrical fire safety, 968–969
electrical safety, 966–968
laser printers, 968
LCD monitors, 967

power supplies, 966
email, 72–73
authentication, 109
DKIM (DomainKeys Identified Mail), 109–110
DMARC (Domain-based Message Authentication, Reporting & Conformance), 110–111
SPF (Sender Policy Framework), 110
browser-based, 332
cloud-based, 703–705
IMAP (Internet Message Access Protocol), 73
mail servers, 95
mobile device
corporate and ISP configuration, 51–53
integrated commercial provider configuration, 51
SSL/TLS (Secure Sockets Layer/Transport Layer Security), 53
synchronizing to the cloud, 58–59
POP3 (Post Office Protocol Version 3), 73
protocols, 73
security, 733–734
security gateway, 777
SMTP (Simple Mail Transfer Protocol), 73
embedded systems, 103–104
EMI (electromagnetic interference), 178
emulation, versus virtualization, 313
encryption, 751–752
BitLocker, 628–629, 752–753
data-at-rest, 811
FileVault, 660
mobile device, 823–825
wireless, 766, 767–768
AES (Advanced Encryption Standard), 766–767

TKIP (Temporal Key Integrity Protocol), 766
WPA2 (Wi-Fi Protected Access version 2), 766
WPA2-Enterprise, 768
WPA3 (Wi-Fi Protected Access version 3), 766
endpoint security software, 821–822
energy efficiency, power supply, 277
entry systems, 716–717
environment variables, 1009
EOL (end-of-life), 486–487
EPPs (endpoint protection platforms), 776–777
equipment grounding, 965–966
eSATA (external SATA) ports, 239
ESD (electrostatic discharge), 15, 346
prevention, 963–965
troubleshooting on motherboard, 343
eSIM, 55–56
Ethernet, Power over, 123–125
EULA (end-user licensing agreement), 988
Event Viewer, 534
events, 535–536
log files, 535
panes, 534–535
evil twin, 792–793
exFAT, 482
expansion bus
PCI (Peripheral Component Interconnect), 232
PCIe (PCI Express), 231–232
expansion cards, 233, 239–240
ext4, 484, 670
extended partition, 501
extended warranty, 410
extensions, browser, 858–859

external audio interface, 238
external monitor, troubleshooting, 377–378
eye tracker, 625

F

factory reset, mobile device, 387
fan
case, 274
CPU (central processing unit), 262–263
power supply, troubleshooting, 350–351
settings, BIOS configuration, 243
Fast Startup, 622
FAT32, 220, 481
fault tolerance, 217–218, 278
fencing, 719–720
fiber optic Internet connections, 148–149. *See also* optical cable
file security, 749–750
administrative shares, 750–751
BitLocker, 752–753
encryption, 751–752
file server, 94
file synchronization, 336
file system, 481
exFAT, 482
FAT32, 481
formatting a hard drive, 486
full format, 482–483
Linux, 483–484
ext4, 484, 670
file path, 484
swap partition, 485

XFS (High-Performance Scalable File System), 670
macOS, 485
NTFS, 481
quick format, 482–483
ReFS, 481–482
file types
.app, 661
.dmg, 661
.pkg, 662
.iso, 696
fileless malware, 775
fileshare, 94
FileVault, 660, 804
***Find My Device*, 819**
Finder, 654
firewall, 122, 779
Microsoft Defender, 597
network, 100
settings, 850–851
firmware
BIOS (Basic Input/Output System), 241–243
boot options, 242
fan settings, 243
HSM (hardware security module), 244
passwords, 244
Secure Boot, 244
temperature monitoring, 244
TPM (Trusted Platform Module), 244
virtualization support, 245
printer, 288–289
radio, 55
flapping, 400

flash drives, 218–221
flashing the BIOS, 241
floating-point data types, 1006
flow control, 70
Fn (function) key, 12–14
folders
administrative shares, 750–751
home, 756–757
permissions, 748–749
form factor, motherboard, 228
ATX (Advanced Technology eXtended), 228–229
ITX (Information Technology eXtended), 230
microATX, 229–230
NUC (Next Unit of Computing), 230
format command, 835
formatting a hard drive, 834
FPS (frames per second), 169
FQDN (fully qualified domain name), 108
freeware, 774
FRT (facial recognition technology), 718
FTP (File Transfer Protocol), 74
full backup, 952

G

gaming, settings, 630
gateway address, IPv4, 134
GDPR (General Data Protection Regulation), 994–995
geofence, 56
gestures, 655
GFS (Grandfather-Father-Son) backup rotation scheme, 957
ghost cursor, 16

Gmail, 51, 58–59, 704
GNOME, 668
God Mode, 745
Google, Find My Device, 819
gpresult command, 575
GPS (Global Positioning System), 56–57
GPT (GUID Partition Table), 502–503, 670
GPU (graphics processing unit), 256
gpupdate command, 575–576
group policy, 757–758
Group Policy Editor, 541–542
GSM (Global System for Mobile Communications), 55
guest networks, 848
GUI (graphical user interface)
Classic Mac OS, 649
Linux, 668
macOS, 651
Windows, 515

H

hallucinations, AI, 1054
hard disk drive, 20
hard reset, 11, 901–902
hardware
EOL (end-of-life), 486–487
physical address, 26
procurement life cycle, 939–940
recycling and disposal, 976
tokens, 694, 729–730
hashing, 857
HDD (hard disk drive), 211–213. *See also* storage drives

defragging, 358–359, 551–552
formatting, 486, 834
HDMI (High-Definition Multimedia Interface), 186, 377, 379
headers, motherboard, 240
heat sink, CPU, 261
helloworld.sh, 1024–1028
help desk. *See also* incident response
employee, 936–937
ticket, 938
ticket escalation, 937
Hertz (Hz), 169
hibernation, 603–604
hidden shares, 639
hives, 557
home folder, 756–757
hostname command, 585–586
hot dock, 40
hotspot, 38, 47–48
HSM (hardware security module), 244
HTTP (Hypertext Transfer Protocol), 71
HTTPS (Hypertext Transfer Protocol - Secure), 71–72
hybrid cloud, 334
hybrid drive, 20
Hyper-V
enabling in Windows Features, 314–315
Windows support, 318–319
hypervisor, 313–314

I

IaaS (Infrastructure as a Service), 332
IAM (identity and access management), 732

iCloud, 656–657
icons, Windows, 517
IDE (Integrated Drive Electronics), 187
identity synchronization, 709
IDS (intrusion detection system), 101
IEC cable, 280
if statement, 1007
ifconfig command, 652
if-then-fi statement, 1027
image deployment, 498–499
IMAP (Internet Message Access Protocol), 73
IMEI (International Mobile Equipment Identity), 57–58
impact printers, 304–305
impersonation, 788–789
improper, spontaneous, and frequent shutdowns, troubleshooting, 879–880
IMSI (International Mobile Subscriber Identity), 57–58
IMT-Advanced (International Mobile Telecommunications Advanced) requirements, 54
inbound port, 71
incident report, 929
incident response, 984
chain of custody, 986–987
documentation, 985
first response, 984–985
licensing and, 988–990
life cycle, 985–986
incremental backup, 952–954
indexing, 599, 629
ingress data, 335
inkjet printers, 301–303
insider threat, 793–794

installing. ***See also*** **boot methods**
applications, 389–390, 695–696
CPU (central processing unit), 264–267
M.2 or Mini PCIe card, 25–26
operating system, 503–504
clean install, 497
image deployment, 498–499
from a recovery partition or disc, 500
remote network installation, 499
reset/restore, 499
unattended installation, 498
upgrade, 497–498
zero-touch deployment, 499
power/power supply, 278–281
RAM (random-access memory), 197–201
SODIMM (small outline dual inline memory module), 17–18
video cards, 233–237
web browser, 855–857
Windows updates, 627
Install-Package for PowerShell, 1013
instant messaging, 707–708, 733
integers, 1006
integrated commercial provider email configuration, 51
Intel
ATX 3.0 standard, 272
-based RAID, 364
CPUs, 256–257
Performance/Efficiency cores, 255
internal clock speed, 252
Internet. ***See also*** **IoT (Internet of Things)**
-based resources, 396
connection types

cable, 147
cellular, 150
DSL, 147–148
fiber, 148–149
satellite, 149
options, 610–611
security appliances, 100
load balancers, 102–103
network firewall, 100
spam gateway, 101–102
UTM (unified threat management), 100–101
settings, 611–613
inventory lists, 938–939
inverter, 165, 166
IOPS (input/output operations per second), 361
iOS, 36, 479–480
jailbreaking, 822, 914–915
malicious apps, 915
IoT (Internet of Things), 104–105, 825–826
IP (ingress protection), 40
ip command, 677
IP filtering, 849
IP subnetting, 115–116
iPadOS, 480
ipconfig /all command, 26, 396–397, 401, 579–581
IPS (in-plane switching), 164
IPS (intrusion prevention system), 101
IPv4
APIPA (Automatic Private IP Addressing), 133
classful versus classless IP addresses, 138
configuring with PowerShell, 135
conflict messages, troubleshooting, 401

DNS server address, 134
gateway address, 134
IP address
configuring, 131–133
network and host sections, 133
versus IPv6, 138
private addresses, 135–136
public addresses, 136–137
IPv6, configuring, 138–139
ISO image, 696
ISP (Internet service provider)
email configuration, 51–53
wireless, 149–150
iteration, 1007–1008
ITX (Information Technology eXtended), 230

J

jailbreaking, 822, 914–915
JavaScript, 1032–1033
jitter, 400
just-in-time access, 726–727

K

KDC (key distribution center), 770
Kerberos, 770
kernel, 324, 679
keyboard
laptop, 11–15
onscreen, 625

Keychain Access utility, 655
keylogger, 775
keyring services, 804
kill switch, 279
knowledge base/articles, 933–936

L

LAN (local area network), 115–116, 143–144
language, settings, 625–626
laptops, 8
airplane mode, 28
battery, troubleshooting, 10
Bluetooth, 22
camera/webcam
disabling, 23
microphone, 23–24
replacing, 23
troubleshooting, 24
displays. *See also* displays
backlight, 165
inverter, 165
IPS (in-plane switching), 164
LCD (liquid-crystal display), 163–164
LED (light-emitting diode), 164
mini-LED, 165
OLED (organic light-emitting diode), 164–165
TN (twisted nematic), 164
troubleshooting, 166–167
VA (vertical alignment), 164
docking station, 40–41
external monitor, troubleshooting, 377–378

hard reset, 11
hot dock, 40
keyboard/keys, 11–12
special function, 12–14
troubleshooting, 14–15
multiport adapter dongle, 40
NFC (near-field communication), 27–28
physical security, 26–27
power
AC adapter, 8–10
troubleshooting, 8–11
RAM (random-access memory). *See also* RAM (random-access memory)
compatibility, 17
installing, 17–18
SODIMM (small outline dual inline memory module), 16
troubleshooting, 18–19
screen switching, 377
storage drives, 19
accessing, 21
SATA (Serial ATA), 19–21
tethering, 37
touchpad, 15–16
track point, 41
Wi-Fi
adapter, 26
connecting, 21–23
PCI Express Mini card/M.2 card, 24–26
WLAN button, 21–22
laser printers, 297–300
counter, 301

electrical safety, 968
maintenance, 300–301
latency, 400, 581
satellite Internet, 149
troubleshooting, 399
LCD (liquid-crystal display), 163–164
electrical safety, 967
projectors, 378
LDAP (Lightweight Directory Access Protocol), 76
least connections algorithm, 102
LED (light-emitting diode) display, 164
legacy systems, 104
Lenovo ThinkPad, track point, 41
LGA (Land Grid Array), 258
LibreOffice, 668
licensing, 987–988
DRM (digital rights management), 988
EULA (end-user licensing agreement), 988
software, 940, 989
life cycle
incident response, 985–986
operating system, 506
lighting, 719
Lightning connector, 36, 183
Linux, 477, 667
applications, 668
boot process, 683–684
commands/command line, 668, 670–676
ip, 677
lsblk, 484–485
su, 677–678
sudo, 678, 1043

configuration files, 680–681
cron jobs, 1027
desktop distributions, 668–669
desktop environments, 668
dual-booting, 684
file system
ext4, 484, 670
file path, 484
swap partition, 485
XFS (High-Performance Scalable File System), 670
GNOME, 668
GPT (GUID Partition Table), 670
ip a command, 26
kernel, 679
keyring services, 804
permissions, 685–686
recovery mode, 679–680
root account, 685
scripting, 1024–1028
shebang, 1028
Terminal, 670–671
text editors, 676
Ubuntu, 669
updating, 681–683
liquid cooling, PC, 263–264
liquid damage, on mobile devices, 390
load balancers, 102–103
local accounts, 741–742
local printer, 292
local resources, 396
Local Security Policy, 542
location services, 56

locator application, 819
locks, 716
logical security
ACLs (access control lists), 730–731
authentication, 723–726
authenticator applications, 729
DLP (data loss prevention), 732
hardware and software tokens, 729–730
IAM (identity and access management), 732
just-in-time access, 726–727
MDM policies, 728
principle of least privilege, 727–728
SAML (Security Assertion Markup Language), 731
SMS (Short Message Service), 733
SSO (single sign-on), 731–732
logon script, AD (Active Directory), 756
logs
MDM (mobile device management), 912–913
syslog, 98
long-range fixed wireless, 87–88
for loop, 1007–1008
loopback address, 582
loopback plug, 155–156
lsblk command, 484–485
lumens, 378

M

M.2 drives, 21, 24–26, 213–214
MAC filtering, 849
MAC ID, 26
Macintosh computers, 476

macOS, 476, 649
Boot Camp, 655
close, minimize, and full screen buttons, 652
commands
diskutil list, 485
ifconfig, 652
Continuity, 657
Dashboard, 655
Disk Utility, 660
Dock, 651
file system, 485
FileVault, 660, 804
Finder, 654
gestures, 655
GUI (graphical user interface), 651
Keychain Access utility, 655, 804
Mission Control, 654–655
RSR (Rapid Security Response), 660
Screen Sharing, 655
SPOD (spinning pinwheel of death), 660
Spotlight search tool, 654
system folders, 657–659
System Preferences, 651–653
Terminal, 652, 659
Time Machine, 659–660
uninstalling applications, 662
updating, 660
VNC (Virtual Network Computing), 655
magnetic disk, 20
magnetometers, 719–720
mail servers, 95
maintenance. ***See also*** **preventive maintenance**

impact printer, 305
inkjet printer, 303
laser printer, 300–301
printer, 409–410
thermal printer, 304
malicious apps, 915
malware, 775–776. *See also* preventing malware; social engineering
cryptominer, 775
fileless, 775
keylogger, 775
preventing, 776–780, 915
ransomware, 775
removing, 841–843
rootkit, 774
spyware, 774, 780–781, 920–921
Trojan horse, 774, 780
unintentionally introducing in scripts, 1014
virus, 773
boot sector, 774, 778
symptoms, 919–920
worm, 773
MAM (mobile application management), 62, 823
MAN (metropolitan area network), 144–145
managed/unmanaged switch, 120
mantrap, 717
manufacturer resources, mobile device, 392
mapping a drive, 640–641, 1029
MBR (Master Boot Record), 502–503
MDM (mobile device management), 61–62, 728, 796–797, 827. *See also* mobile devices
BYOD (bring your own device), 62

configuration profiles, 815–816
log files, 912–913
preventing malware, 915
security profiles, 828–829
servers, 823
“three strikes and you’re out” policy, 912
MDNDA (mutual nondisclosure agreement), 991
MDR (managed detection and response), 776–777
measured services, 335
memory. *See also* RAM (random-access memory); storage drives
add-on storage, 39
cache, 256
random-access, 18–19
compatibility, 17
SODIMM (small outline dual inline memory module), 16
SODIMM (small outline dual inline memory module), installing, 17–18
storage drives, 19
accessing, 21
SATA (Serial ATA), 19–21
message server, 95
metered connection, 644
metered VPN, 644
MFA (multifactor authentication), 27, 718, 724–726
microATX, 229–230
microphone, camera/webcam, 23–24
Microsoft accounts, 741
Microsoft Defender Antivirus, 551, 738
Microsoft Defender Firewall, 542–543, 597, 738–740, 779
Microsoft Knowledge Base, 934
Microsoft Outlook, 704

Microsoft Teams, 707–708
MIMO (multiple input, multiple output), 85
mini-ITX, 230
mini-LED, 165
minimum system requirements, 693–694
developer program, 695
video editing program, 694
Windows 10, 496
Windows 11, 496–497
Windows 11 editions, 513–515
Mission Control, 654–655
MMC (Microsoft Management Console), 532
adding snap-ins, 532–533
Certificate Manager, 539–540
Device Manager, 537–539
Group Policy Editor, 541–542
Performance Monitor, 540–541
Services, 542–543
Task Scheduler, 536–537
mobile device/s. *See also* apps and applications; MDM (mobile device management)
3.5 mm audio jack, 39
add-on storage, 39
airplane mode, 47
Android, 479
Force Stop option, 899–900
rootkit, 822
sideloading, 822
Wi-Fi settings screen, 46–47
applications, troubleshooting, 899–901
backup/restore, 819–820
battery

replacing, 39–40
troubleshooting, 904–905
cellular technology, 46
airplane mode, 54
cellular location, 57
eSIM, 55–56
geofence, 56
GPS (Global Positioning System), 56–57
GSM (Global System for Mobile Communications), 55
IMEI/IMSI, 57–58
location services, 56
cleaning, 389
compromised and damaged, 820
disassembling
documentation, 391
manufacturer resources, 392
tools, 392
drawing pad, 41
email
corporate and ISP configuration, 51–53
integrated commercial provider configuration, 51
SSL/TLS (Secure Sockets Layer/Transport Layer Security), 53
encryption, 823–825
endpoint security software, 821–822
factory reset, 387
hard reset, 901–902
iOS, 479–480, 822
IP (ingress protection) compliant, 40
jailbreaking, 822
locator application, 819

NFC (near-field communication), troubleshooting, 898
patch management, 820–821
ports, 36
security
    authenticator applications, 818–819
    profiles, 828–829
    screen locks, 816–818
    unauthorized access, 911–914
serial interfaces, 37
soft reset, 901
stylus, 41
synchronization, 58
    to the car, 60–61
    to the cloud, 58–59
    to the desktop, 59–60
tethering, 37
track point, 41
trackpad, 41
troubleshooting
    application installation, 389–390
    application issues, 903
    battery, 389
    Bluetooth, 896–897
    connectivity, 894–895
    display, 385–386
    liquid damage, 390
    overheating, 386–388
    random reboots, 903–904
    system freezes, 389
    touchscreen, 390–391
updating, 820–821, 902–903
USB debugging, 912

video issues, troubleshooting, 905–907
webcam, securing, 913
wireless connections, 37–38
Bluetooth, 38
hotspot, 38, 47–48
NFC, 38–39
Qi charging, 39–40
mobile digital keys, 717
mobile-ITX, 230
modem, cable/DSL, 126
Molex connector, 276
monitoring, performance, 540–541
monitors, 375–376. *See also* displays
antiglare filter, 375–376
external, troubleshooting, 377–378
temperature, 244
motherboard, 227. *See also* power/power supply
BIOS (Basic Input/Output System), 241–242, 348. *See also* BIOS (Basic Input/Output System); UEFI (Unified Extensible Firmware Interface)
boot options, 242
fan settings, 243
HSM (hardware security module), 244
passwords, 244
Secure Boot, 244
temperature monitoring, 244
TPM (Trusted Platform Module), 244
virtualization support, 245
capture cards, 239
chipset, 233, 257
CPU (central processing unit), 251
AMD, 256–257

ARM (Advanced Reduced Instruction Set Computer Machine), 254
bus speed, 253
cache memory, 256
clock speed, 251–253
Efficiency/Performance cores, 255
fans, 262–263
GPU (graphics processing unit), 256
heat sink, 261
installing, 264–267
Intel, 256–257
liquid cooling, 263–264
multicore, 255
multithreading, 255
overclocking, 253
power consumption, 259
socket, 257–259
thermal paste/pads, 261–262
troubleshooting, 345–346
voltage, 259–260
x86–64, 253–254
expansion bus
PCI (Peripheral Component Interconnect), 232
PCIe (PCI Express), 231–232
expansion cards, 233, 239–240
form factor, 228
ATX (Advanced Technology eXtended), 228–229
ITX (Information Technology eXtended), 230
microATX, 229–230
NUC (Next Unit of Computing), 230
headers, 240
multisocket, 258–259

northbridge/southbridge, 233
ports, 239
power connectors, 260
riser card, 241
SATA connectors, 240
sound card, 237
color scheme, 237–238
S/PDIF (Sony/Phillips Digital Interconnect Format) port, 238
TPM (Trusted Platform Module) chip, 245
troubleshooting
component failures, 343–344
ESD (electrostatic discharge), 343
UEFI/BIOS firmware issues, 342–343
video card
analyzing, 236–237
installing, 233–237
testing, 235, 236
motion sensors, 719
mount points, 548–550
mouse
settings, 623, 625
wheel, scroll rate, 615
mSATA (Mini-SATA), 211
MSConfig, 554–556
MSDS (material safety data sheet), 975
mstsc command, 1040
multibooting, 501
multicore CPU, 255
multifactor authentication, 704
multifunction device, 285–288
multimeter, 342

multimode fiber, 179–180
multipath propagation, 85
multiport adapter dongle, 40
multisocket motherboard, 258–259
multitenancy, 336
multithreading, 255

N

NAND flash memory, 219–220
nano, 676
nano-ITX, 230
Narrator, 624
NAT (Network Address Translation), 137, 850
native resolution, 170
navigating, command line, 567–570
NDA (nondisclosure agreement), 990
net command, 587–589
netstat command, 77, 399, 586–587
network/ing, 69. *See also* IPv4
authentication, troubleshooting, 397–398
-based attacks
DDoS (distributed denial-of-service), 790–791
DoS (denial of service), 790
on-path, 789
spoofing, 789
zero-day, 789–790
zombies, 790
commands
hostname, 585–586
ipconfig, 579–581
net, 587–589

netstat, 586–587
nslookup, 587
tracert, 583–585
whoami, 589
connectivity, troubleshooting, 396–397, 398
DHCP (Dynamic Host Configuration Protocol), 75–76
acknowledgment, 113
discovery, 112
exclusions, 114
offering, 112
request, 113
reservations, 114–115
DNS (Domain Name System), 76, 107–108
FQDN (fully qualified domain name), 108
RRs (resource records), 108–109
domain, 635–637
establishing connections, 643–645
fileshare, 94
firewall, 100, 122
guest, 848
HTTPS (Hypertext Transfer Protocol - Secure), 71–72
IoT (Internet of Things), 104–105
jitter, 400
latency, troubleshooting, 399
local area, 143–144
local resources, 396
location, 645
management, 78
mapping a drive, 640–641
metropolitan area, 144–145
personal area, 146
printers, 292–293, 641–643

remote resources, 396
routers, 121
servers. *See* servers
settings, 611–613
sharing data and resources, 637–641
slow transfer speeds, troubleshooting, 399
storage area, 145, 239
switches, 119–121
tap, 156–157
TCP (Transmission Control Protocol), 70
flow control, 70
socket connection, 70
three-way handshake, 70
UDP (User Datagram Protocol), 70
virtual private, 116–117, 644–1047
VLAN, 115–116
VM requirements, 319–320
VoIP, troubleshooting, 400
wide area, 144
wired, 21–22
wireless. *See* wireless/Wi-Fi
wireless local area, 145
wireless mesh, 145–146
workgroups, 635–637
New-LocalUser cmdlet, 1020
New-PSDrive cmdlet, 1029
Nexcloud, 58
NeXTSTEP, 650
NFC (near-field communication), 27–28, 38–39
troubleshooting on mobile devices, 898
nibble, 174
NIC (network interface card), 122–123

NID (network interface device), 126
NIST, password guidelines, 802–803
NLQ (near letter quality), 307
NMI (non-maskable interrupt), 348
northbridge/southbridge, 233
Notepad, 571, 1021, 1024
notification area, Windows, 517–518
nslookup command, 587
NTFS, 220, 481, 746–747
NTP (Network Time Protocol), 98
NUC (Next Unit of Computing), 230
Num Lock key, 13–14
NVMe (Non-Volatile Memory Express), 213–214

O

offboarding, 931
offering, DHCP (Dynamic Host Configuration Protocol), 112
offsite backup, 958
OLED (organic light-emitting diode), 164–165
OLT (optical line terminal), 127
onboarding, 931
online storage, 705–706
onsite backup, 958
ONT (optical network terminal), 126
open source, 478
    Android, 479
    licensing, 989
operating systems. *See also* Windows
    Android, 479
    boot methods
        internal drive installation, 495

Internet-based installation, 495
local installation from external drive, 494
network boot (PXE) installation, 494–495
Chrome, 477–478
compatibility between, 488–490
dual-booting, 655
installation, 503–504
clean install, 497
image deployment, 498–499
from a recovery partition or disc, 500
remote network installation, 499
reset/restore, 499
unattended, 498
upgrade, 497–498
zero-touch deployment, 499
iOS, 479–480
iPadOS, 480
life cycle, 506
Linux, 477, 667. *See also* Linux
applications, 668
boot process, 683–684
code, 667–668
configuration files, 680–681
desktop distributions, 668–669
desktop environments, 668
dual-booting, 684
ext4, 484, 670
file path, 484
GNOME, 668
GPT (GUID Partition Table), 670
ip a command, 26
ip command, 677

lsblk command, 484–485
permissions, 685–686
recovery mode, 679–680
root account, 685
su command, 677–678
sudo command, 678
swap partition, 485
Terminal, 670–671
Ubuntu, 669
updating, 681–683
XFS (High-Performance Scalable File System), 670
macOS, 476, 649. *See also* macOS
Boot Camp, 655
close, minimize, and full screen buttons, 652
Continuity, 657
Dashboard, 655
Disk Utility, 660
Dock, 651
FileVault, 660
Finder, 654
gestures, 655
Keychain Access utility, 655
Mission Control, 654–655
RSR (Rapid Security Response), 660
Screen Sharing, 655
SPOD (spinning pinwheel of death), 660
Spotlight search tool, 654
system folders, 657–659
System Preferences, 651–653
Terminal, 659
Time Machine, 659–660
uninstalling applications, 662

updating, 660
VNC (Virtual Network Computing), 655
multibooting, 501
NeXTSTEP, 650
vendor life-cycle limitations, 486–488
Windows, 476
workstation, 475
operator control panel, 410
optical cable, 179–180
optical drives, 222–224
Optimize Drives utility, 551–552
OSHA (Occupational Safety and Health Administration), air treatment recommendations, 973–974
overclocking, 253
overheating
mobile device, 386–388
troubleshooting, 352–353
overwriting drives, 834–836
ownership, 748, 994

P

PaaS (Platform as a Service), 312, 332–333
pairing, Bluetooth, 49–50
PAM (privileged access management), 727
PAN (personal area network), 146
paper tray, printer, 409
partitioning, 501
basic drive, 502
dynamic drive, 502
extended partition, 501
GPT (GUID Partition Table), 502–503

MBR (Master Boot Record), 502–503
primary partition, 501
volumes, 501
passwordless authentication, 742
password/s, 744, 801–802
BIOS (Basic Input/Output System), 244
BIOS/UEFI, 804–805
cracking, 791–792
default, changing, 844–845
length, 802–803
lockout, 809
managers, 803–804, 860–861
NIST guidelines, 802–803
policies, 805–806
strong, 802
patch management, 820–821
patch panel, 123
patch tester, 155
on-path attack, 789
PCBs (printed circuit boards), 344
PCI (Peripheral Component Interconnect), 232
PCI-DSS (Payment Card Industry Data Security Standards), 993–994
PCIe (PCI Express), 24–26, 213–214, 231–232
PCs, 516. *See also* laptops
audio output settings, 377–378
symptoms of security issues, 921–924
synchronizing with your mobile device, 59–60
system overheating, troubleshooting, 352–353
tethering, 37
video issues, troubleshooting, 371–376
virtualization, 312

virus, symptoms, 919–920
performance
counters, 541
storage drive, 361
Performance cores, 255
Performance Monitor, 540–541
permissions, 746
application, 629, 698
DAC (discretionary access control), 748
inheritance, 747–748
Linux, 685–686
moving and copying folders, 748–749
NTFS, 746–747
printer, 292
propagation, 748
Search, 629
PGA (Pin Grid Array), 258
PHI (protected health information), 992–993
phishing, 786
physical address, 26
physical safety, 969–970
physical security
alarm systems, 719
bollards, 719–720
for documentation, 720–721
entry systems, 716–717
fencing, 719–720
laptop, 26–27
lighting, 719
locks, 716
magnetometers, 719–720
pico-ITX, 230

piezoelectric inkjet printers, 302
piggybacking, 788
PII (personally identifiable information), 992
ping, 135, 398, 400, 581–583
pinned applications, 517
pixel density, 168–169
.pkg files, 662
PKI (public key infrastructure), 861–862
in-place recovery, 956
plenum, 177–178
plug-in, browser, 858–859
PoE (Power over Ethernet), 123–125
pointer drift, 16
policy/ies, 542
acceptable use, 995–996
AI-related, 1052
BYOD (bring your own device), 826–827
group, 757–758
MDM (mobile device management), 728
password, 805–806
security best practices, 795–797
"three strikes and you're out", 912
POP3 (Post Office Protocol Version 3), 73
port/s. *See also* connectors; USB
eSATA (external SATA), 239
flapping, 400
forwarding, 850
inbound, 71
Lightning, 183
mobile device, 36–37
motherboard, 239
replicator, 40

RJ-45, 239
security, 739
S/PDIF (Sony/Phillips Digital Interconnect Format), 238
Thunderbolt, 183–184
POST (power-on self-test), 235, 246, 343–344
power/power supply
compatibility, 273–275
connectors, 260, 272–273, 275–276
CPU (central processing unit), 259
cycling, 372–373
electrical safety, 966–968
energy efficiency, 277
failure, 977
hibernation, 603–604
IEC cable, 280
installing, 278–281
kill switch, 279
laptops
AC adapter, 8–10
troubleshooting, 8–11
management, 602–604
over Ethernet, 123–125
rails, 228, 273
redundant, 278
selecting, 272
semi-modular, 278
settings, 621–622
standby, 602–603
surge, 977
surge suppressor, 343, 978
testing, 280–281, 349–350
troubleshooting, 349–352

uninterruptible, 343, 968, 978–980
wattage and capacity requirements, 275
PowerShell, 565–566, 1019. *See also* script/s
cmdlet
New-PSDrive, 1029
test-connection, 1022
comment syntax, 1009–1010
format command, 835
Install-Package, 1116
IPv4 configuration, 135
mapping a drive, 1029
New-LocalUser cmdlet, 1020
$psversiontable command, 1019–1020
running commands, 1019–1020
variables, 1008
PPI (pixels per inch), 168–169
presentation tools, 708
pretexting, 788–789
preventing malware, 776–780, 915
rootkit, 781–782
spyware, 780–781
Trojan horse, 780
preventive maintenance
extended warranty, 410
storage drives, 358–359
primary partition, 501
principle of least privilege, 727–728
print servers, 95
printer/s
cloud-based, 293
collating, 290
configuration settings, 289–291

dot-matrix, 304–305
driver, 287–288
duplexing, 290
extended warranty, 410
firmware, 288–289
impact, 304–305
inkjet, 301–303
laser, 297–300
    counter, 301
    maintenance, 300–301
local, 292
maintenance, 409–410
manual, 410
network, 292–293
page orientation, 290
permissions, 292
print quality, 290–291
safety, 286
security, 293–294
setup considerations, 285–288
sharing, 291–292, 641–643
thermal, 303–304
toner, 300
tray settings, 290
troubleshooting
    common issues, 405–409
    operator control panel, 410
    paper tray, 409
Windows environment
    frozen print queue, troubleshooting, 411
    print jobs, 411
    print spooler, 412–414

privacy
browser, 857
BYOD and, 826–827
settings, 628–630
private cloud, 333
private IP addresses, 135–136
probe kit, 155
procurement life cycle, 939–940
production server, 325
productivity tools
email systems, 703–705
online storage, 705–706
projectors
DLP (Digital Light Processing), 378
LCD (liquid-crystal display), 378
lumens, 378
troubleshooting, 378–380
protocols
DHCP (Dynamic Host Configuration Protocol). *See* DHCP (Dynamic Host Configuration Protocol)
DNS (Domain Name System). *See* DNS (Domain Name System)
email, 73
IMAP (Internet Message Access Protocol), 73
POP3 (Post Office Protocol Version 3), 73
SMTP (Simple Mail Transfer Protocol), 73
LDAP (Lightweight Directory Access Protocol), 76
SMB (Server Message Block), 77
SNMP (Simple Network Management Protocol), 78
proxy servers, 96, 645–646
$psversiontable command, 1019–1020
public cloud, 333

public IP addresses, 136–137
punchdown tool, 154
PUP (potentially unwanted program), 774
purging data, 836
PuTTY, 1041–1043
Python, scripting, 1031–1032

Q

Qi charging, 39–40
quad shield, 179
quadruple-channel architecture, 201–203
quick format, 482–483
quishing, 786–787

R

radio firmware, 55
RADIUS (Remote Dial-In User Service), 768–769
RAID (redundant array of inexpensive disks), 215–218
    versus backup, 366
    Intel-based, 364
    troubleshooting, 363–366
rails, 228, 273
RAM (random-access memory), 18–19, 193
    compatibility, 17
    DDR3, 194–195
    DDR4, 195–196
    DDR5, 196
    DDR6, 196–197
    DIMM (dual-inline memory module), 193–194

dual-channel, 201
dynamic, 193
ECC (error correction code), 203
installing, 197–201
quadruple-channel, 201–203
single-channel, 201
SODIMM (small outline dual inline memory module), 16–18, 193–194
static, 256
swap partition, 485
troubleshooting, 347–349
virtual, 203–205
VM requirements, 318
random reboots, troubleshooting on mobile devices, 903–904
ransomware, 775
rapid elasticity, 336
RDP (Remote Desktop Protocol), 77, 1040
recovery, 782. *See also* backup; DRP (disaster recovery plan); WinRE (Windows Recovery Environment)
alternative location, 956
console, 778
mode, Linux, 679–680, 865–866
in-place, 956
Recycle Bin, 358
recycling, 976
redundant power supply, 278
refresh rate, 169
ReFS, 481–482
registration, CompTIA A+exam, 3
Registry, 556–557
hives, 557
rules for making changes, 557

Run commands, 558–559
regulations/regulated data, 995
destruction and disposal, 838
GDPR (General Data Protection Regulation), 994–995
PCI-DSS (Payment Card Industry Data Security Standards), 993–994
PHI (protected health information), 992–993
PII (personally identifiable information), 992
wiring and cable, 154
remapping a drive, 1029–1030
remote access technologies
Remote Desktop, 1037–1041
RMM (remote monitoring and management solutions), 1041
SPICE (Simple Protocol for Independent Computing Environments), 1044
SSH (Secure Shell), 1041–1043
third-party, 1045
VPN (virtual private network), 1046–1047
WinRM (Windows Remote Management), 1044–1045
remote network installation, 499
remote resources, 396
removing malware, 841–843
replacing
camera/webcam, 23
CPU (central processing unit), 346
mobile device battery, 39–40
request, DHCP (Dynamic Host Configuration Protocol), 113
reservations, DHCP, 114–115
reset/restore, 499
resolution, display, 373, 375
Resource Monitor, 553–554
resource/s

local, 396
pooling, 336
remote, 396
sharing, 638–641
system, mishandling, 1014
restore points, creating, 878–879. *See also* backup
revision control, 326
RFID (radio-frequency identification), 56, 88–89
-based entry systems, 716–717
tags, 939
RG-6 cable, 178–179
riser card, 241
RJ-45 connector, 176
RMM (remote monitoring and management solutions), 1041
roaming profile, 755
robocopy command, 570–571
rollback plan, 946
root account, Linux, 685
rooting, 822, 914–915
rootkit, 774, 781–782
round-robin algorithm, 102
routers, 121
assigning static IP address, 849–850
changing default password, 844–845
content filtering/parental controls, 851–852
disabling physical ports, 852
firewall settings, 850–851
IP address, 844
RRs (resource records), DNS (Domain Name System), 108–109
RS-232, 184–185
RSR (Rapid Security Response), 660
Run commands, 558–559

S

SaaS (software as a Service), 51, 332, 704
safety
electrical, 966–968
electrical fire, 968–969
ESD prevention, 15, 963–965
physical, 969–970
printer, 286
SAML (Security Assertion Markup Language), 731
SAN (storage area network), 145, 239
sandboxes, 324–326, 946
sanitizing a drive, 836
SAS (Serial Attached Small Computer System Interface), 214
SATA (Serial ATA), 187, 240, 364
satellite-based Internet, 149
SCADA (supervisory control and data acquisition), 103
screen locks, 816–818
screen magnifier, 623–624
screen resolution, 170
Screen Sharing, 655
screen switching, 377
screened subnet, 850–851
script/s, 1019–1024
batch, 1023–1024
comment syntax, 1009–1010, 1027
constructs
if statement, 1007
for loop, 1007–1008
environment variables, 1009
if-then-fi statement, 1027
inadvertently changing system settings, 1014

logon, 756
security, 1030–1031
system crashes due to mishandling of resources, 1014
tools
Bash, 1024–1028
JavaScript, 1032–1033
PowerShell, 1019–1024
Visual Basic, 1033–1034
unintentionally introducing malware, 1014
when to use, 1010–1064
scroll rate, 615
SCSI (Small Computer System Interface), 187
SD cards, 221–222
Search tool, Windows, 517
Secure Boot, 244
security. ***See also*** **AD (Active Directory); attacks; authentication; encryption; incident response; password/s; social engineering; threats; vulnerabilities**
administrative shares, 750–751
administrator access, 745
application, 698–699
browser
extensions and plug-ins, 858–859
general procedures, 865–866
password managers, 860–861
patching, 857–858
secure sites and tracking, 863–864
settings, 864–865
signatures, 857
CIA triad, 737
defense in depth, 779, 825–826
email, 733–734

file, 749–750
administrative shares, 750–751
BitLocker, 752–753
encryption, 751–752
groups, 758–759
IoT, 825–826
logical
ACLs (access control lists), 730–731
authentication, 723–726
authenticator applications, 729
DLP (data loss prevention), 732
hardware and software tokens, 729–730
IAM (identity and access management), 732
just-in-time access, 726–727
MDM policies, 728
principle of least privilege, 727–728
SAML (Security Assertion Markup Language), 731
SMS (Short Message Service), 733
SSO (single sign-on), 731–732
mobile device
authenticator applications, 818–819
backup/restore, 819
screen locks, 816–818
unauthorized access, 911–914
webcam, 913
PC, symptoms of potential issues, 921–924
permissions, 746
DAC (discretionary access control), 748
inheritance, 747–748
moving and copying folders, 748–749
NTFS, 746–747
propagation, 748

physical
alarm systems, 719
biometrics, 718
bollards, 719–720
for documentation, 720–721
entry systems, 716–717
fencing, 719–720
lighting, 719
magnetometers, 719–720
physical locks, 716
video surveillance, 719
port, 739
printer, 293–294
profiles, 828–829
sandboxes, 324–326
script, 1030–1031
settings, 628–630, 632
user account, 806–810
VM requirements, 320–321
selecting, power supply, 272
semi-modular power supply, 278
serial interfaces, mobile device, 37
servers, 93–94
AAA, 98–100, 769
database, 95–96
development, 325
DHCP, 96–97
DNS, 97
domain controller, 637
file, 94
FTP, 74
mail, 95

MDM (mobile device management), 823
NTP, 98
print, 95
production, 325
proxy, 96, 645–646
syslog, 97–98
web, 94
service/s
Apple, user ID, 662–663
Find My, 819
Infrastructure as a, 332
keyring, 804
-level agreement, 931–933
metered, 335
Platform as a, 312, 332–333
Software as a, 332, 704
unused, disabling, 810–811
Windows, 542–543
Settings, Windows. ***See*** **Windows Settings**
SFC (System File Checker), 573
shares. ***See*** **administrative shares**
sharing
data and resources, 637–641
hidden shares, 639
printers, 291–292, 641–643
remote disks on Mac computers, 659
Screen, 655
shebang, 1028
shoulder surfing, 787
sideloading, 822
signatures, 857
SIM (System Image Manager), 498

single-channel architecture, 201
single-mode fiber, 179
SLA (service-level agreement), 931–933
S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology), 362, 365–366
smart cards, 717
SMB (Server Message Block), 77, 288
smishing, 786
SMS (Short Message Service), 733
SMTP (Simple Mail Transfer Protocol), 73
Snap, 518
SNMP (Simple Network Management Protocol), 78
social engineering, 787
dumpster diving, 788
impersonation, 788–789
phishing, 786
piggybacking, 788
quishing, 786–787
shoulder surfing, 787
smishing, 786
spear phishing, 786
tailgating, 788
vishing, 786
whaling, 786
socket, 257–259
SODIMM (small outline dual inline memory module), 16–18, 193–194
soft reset, 901
software
antivirus, 776
closed source, 649
custom installation procedure, 931

endpoint security, 821–822
EOL (end-of-life), 486–487
jailbreakme, 822
licensing, 940, 989
open source, 478
procurement life cycle, 939–940
revision control, 326
tokens, 730
updating, 777
virtualization
Hyper-V, 314–316
Oracle VirtualBox, 317
VMware Workstation, 316–317
software development
development server, 325
sandboxes, 324–326
SOHO environment. ***See also*** **routers**
removing malware, 841–843
routers, 852
assigning static IP address, 849–850
changing default password, 844–845
content filtering/parental controls, 851–852
disabling physical ports, 852
firewall settings, 850–851
IP address, 844
wireless
AP placement, 846–847
assigning static IP addresses, 849–850
changing and disabling the SSID, 845–846
disabling WPS, 848–849
guest networks, 848
MAC filtering/IP filtering, 849

SOP (standard operating procedure), 929–931
sound
mobile device, troubleshooting, 391
settings, 618–619
sound card, 237
color scheme, 237–238
external audio interface, 238
S/PDIF (Sony/Phillips Digital Interconnect Format) port, 238
Sound dialog box, 598
source code
closed source, 649
open source, 650–663
revision control, 326
spam gateway, 101–102
S/PDIF (Sony/Phillips Digital Interconnect Format), 238
spear phishing, 786
special function keys, laptop keyboard, 12–14
SPF (Sender Policy Framework), 110
SPICE (Simple Protocol for Independent Computing Environments), 1044
SPOD (spinning pinwheel of death), 660
spoofing attack, 789
Spotlight search tool, 654
spreadsheets, 707
spyware, 780–781, 920–921
SSD (solid-state drive), 213–214
SSH (Secure Shell), 74, 1041–1043
SSID (service set identifier), changing and disabling, 845–846
SSL/TLS (Secure Sockets Layer/Transport Layer Security), 53
SSO (single sign-on), 709, 731–732, 742
stalkerware, 774
standard dynamic range, 170

standards
802.11, 83–84
cabling and wiring, 175
media sanitization, 836
payment card industry data security, 993–994
PoE (Power over Ethernet), 125
RS-232, 184–185
standby, 602–603
Start menu, Windows, 517
static IP address, assigning to a router, 849–850
stop errors, 348, 881–883
storage
chemical, 975–976
cloud-based, 705–706
external, 334
VM requirements, 320
storage drives, 19, 569–570
accessing, 21
add-on, 39
cables and connectors, 187
defragging, 358–359, 551–552
deleting, 834–835
flash, 218–221
formatting, 834
HDD (hard disk drive), 211–213
high-level formats, 834
IOPS (input/output operations per second), 361
M.2, 21, 213–214
mapping a drive, 640–641
mounting, 548–550
mSATA (Mini-SATA), 211
optical, 222–224

overwriting, 834–836
partitioning, 501
basic drive, 502
dynamic drive, 502
extended partition, 501
GPT (GUID Partition Table), 502–503
MBR (Master Boot Record), 502–503
primary partition, 501
volumes, 501
physical destruction, 837
preventive maintenance, 358–359
RAID, 215–218
sanitizing, 836
SATA (Serial ATA), 19–21, 209–211
SD cards, 221–222
SSD (solid-state drive), 213–214
troubleshooting
bootable device not found, 360
missing files at startup, 361–362
missing or corrupted files, 362
noisy drive/lockups, 362–363
slow reaction time, 360–361
Windows not seeing a second drive, 360
volumes, 569–570
zeroing out, 834–836
STP (shielded twisted pair), 178
straight-through cable, 177
strings, 1006
strong passwords, 802
stylus, 41, 167, 390
su command, 677–678
sudo command, 1043

Super-IPS, 164
supply chain/pipeline attack, 794
surge suppressor, 343, 978
surveillance, video, 719
suspending applications, 652
swap partition, 485
switches, 119–121
symbols, device, 539
symptoms
of PC security issues, 921–924
spyware, 920–921
virus, 919–920
synchronization
identity, 709
mobile device, 58
to the car, 60–61
to the cloud, 58–59
to the desktop, 59–60
synthetic backup, 955
syslog server, 97–98
system folders, macOS, 657–659
system freezes, mobile device, 389
System Information tool, 553–556
System Preferences, 652–653
System Restore, 878–879
systeminfo command, 315

T

T568A/T568B, 176
TACACS+, 769
tailgating, 788

Task Manager, 527–529
App History tab, 530
Processes tab, 529
Services tab, 530
Startup apps tab, 530
Users tab, 530
verifying RAM, 198–199
Task Scheduler, 536–537
taskbar, 517
TCP (Transmission Control Protocol), 70
flow control, 70
socket connection, 70
three-way handshake, 70
TDP (thermal design power), 259
Telnet, 74–75
temperature monitoring, 244, 374. *See also* overheating
Terminal, 659
Linux, 670–671
macOS, 652
test-connection cmdlet, 1022
test/ing
backup, 956
power supply, 349–350
power-on self-, 235, 246
power/power supply, 280–281
sandbox, 946
video card, 235–236
tethering, 37
text editors
nano, 676
Notepad, 571, 1021
Vim, 571, 676, 1025–1026

VSC, 1021–1022
themes, contrast, 624
thermal inkjet printers, 302
thermal paste/pads, 261–262
thermal printers, 303–304
third-party remote access tools, 1045
threat/s
insider, 793–794
model, 825
“three strikes and you’re out” policy, 912
three-way handshake, 70
throughput, 174
Thunderbolt, 183–184
ticket, help desk, 938
ticketing systems, 936–937
time, settings, 625–626
Time Machine, 659–660
TKIP (Temporal Key Integrity Protocol), 766
TLS (Transport Layer Security), 861–863
TN (twisted nematic) display, 164
tokens, 730
hardware, 729–730
software, 730
tone generator, 155
toner, 300, 976
tool/s. ***See also*** **collaboration tools; productivity tools**
DirectX Diagnostic, 374
diskpart, 502, 505–506
mobile device disassembly, 392
multimeter, 342
scripting
Bash, 1024–1028

JavaScript, 1032–1033
PowerShell, 1019–1024
Python, 1031–1032
Visual Basic, 1033–1034
System Restore, 878–879
Wi-Fi analyzer, 87, 157–158
wiring
cable cutter, 154
cable stripper, 154
cable tester, 154–155
crimper, 155
loopback plug, 155–156
patch tester, 155
punchdown tool, 154
tone generator/probe kit, 155
TOSLINK, 238
touchpad, laptop, 15–16
touchscreen
calibrating, 168
troubleshooting, 390–391
TPM (Trusted Platform Module), 244–245, 742
tracert command, 583–585
track point, 41
trackpad, 41
tray settings, printer, 290
Trojan horse, 774, 780, 913
troubleshooting
authentication, 397–398
BSOD (blue screen of death), 881–883
camera/webcam, 24
CPU (central processing unit), 345–346
improper, spontaneous, and frequent shutdowns, 879–880

laptops
backlight, 166–167
external monitor, 377–378
inverter, 166
keyboard/keys, 14–15
power, 8–11
RAM, 18–19
touchpad, 16
mobile devices
application installation, 389–390
application issues, 903
applications, 899–901
battery, 389, 904–905
Bluetooth, 896–897
connectivity, 894–895
displays, 385–386
liquid damage, 390
NFC (near-field communication), 898
overheating, 386–388
random reboots, 903–904
sound, 391
system freezes, 389
touchscreen, 390–391
video issues, 905–907
motherboard
component failures, 343–344
ESD (electrostatic discharge), 343
UEFI/BIOS firmware issues, 342–343
networks
connectivity, 396–398
IP addressing, 401
jitter, 400

latency, 399
slow transfer speeds, 399
VoIP, 400
power supply, 349–352
printers
common issues, 405–409
operator control panel, 410
paper tray, 409
projectors, 378–380
RAID arrays, 363–366
RAM (random-access memory), 347–349
storage drives
bootable device not found, 360
missing files at startup, 361–362
missing or corrupted files, 362
noisy drive/lockups, 362–363
slow reaction time, 360–361
Windows not seeing a second drive, 360
system overheating, 352–353
Windows, common symptoms and solutions, 883–889
wireless, low RF signal, 399
trusted source, 859
twisted pair, 173–174
Category 5, 174
data transfer rate, 174
patch cable, 177
shielded, 178
unshielded, 173–174, 177
two-step authentication, 818–819
type 1 hypervisor, 314
type 2 hypervisor, 314

U

UAC (User Account Control), 728
Ubuntu, 669
UDP (User Datagram Protocol), 70
UEFI (Unified Extensible Firmware Interface), 14, 241. *See also* BIOS (Basic Input/Output System)
passwords, 804–805
Secure Boot, 245
TPM (Trusted Platform Module), 245
troubleshooting, 342–343
unattended installation, operating system, 498
unauthorized access, on mobile devices, 911–914
uninstalling applications, on macOS, 662
UNIX, 679
untrusted source, 859
unused services, disabling, 810–811
updating
applications, 902–903
drivers, 537–538
Linux, 681–683
macOS, 660
mobile device/s, 820–821
software, 777
Windows, 626–627
upgrade paths, Windows, 520–521
upgrading
operating system, 497–498
SATA magnetic disk, 21
UPnP (Universal Plug and Play), 851
UPS (uninterruptible power supply), 343, 968, 978–980
USB

-based webcam, 24
battery saver, 614–615
biometric reader, 27
connectors, 182–183
data transfer rate, 181–182
drop attacks, 245
flash drives, 218–221
local installation from flash drive, 494
mobile device ports, 36–37
ports, 239
power management, 602
settings, 615
Type-C, 186
user accounts
Apple ID, 662–663
group membership, 744–745
identity synchronization, 709
licensing assignment, 710
local, 741–742
Microsoft, 741
passwords, 744
profiles, 755
securing, 806–810
settings, 630–631
types, 742–744
user checklists, 931
UTM (unified threat management), 100–101
UTP (unshielded twisted pair), 173–174, 177. *See also* twisted pair

V

VA (vertical alignment) display, 164

variables, 1006, 1022
environment, 1009
PowerShell, 1008
VBScript, 1033–1034
VDI (virtual desktop infrastructure), 312
versions, Windows, 487–488
VGA (Video Graphics Array), 186
video card
analyzing, 236–237
connectors, 185–187
installing, 233–237
temperature threshold, 374
testing, 235–236
video issues, troubleshooting
BIOS/UEFI settings, 373
mobile device, 905–907
PC, 371–376
video surveillance, 719
videoconferencing, 706–707
Vim, 571, 676, 1025–1026
virtual RAM, 203–205
virtualization, 311
configuring, 245
containers, 323–324
cross-platform, 321–322
desktop, 312
versus emulation, 313
Hyper-V, enabling in Windows Features, 314–315
hypervisor, 313–314
sandbox, 324–326
VDI (virtual desktop infrastructure), 312
virus, 773

boot sector, 774, 778
symptoms, 919–920
vishing, 786
VLAN (virtual LAN), 115–116
VM (virtual machine), 311
creating, 315
Hyper-V, 314–316
network requirements, 319–320
Oracle VirtualBox, 317
requirements, 318–319
security requirements, 320–321
sprawl, 322
storage requirements, 320
VMware Workstation, 316–317
VMware Workstation, 316–317
VNC (Virtual Network Computing), 655
voice-to-text, 624
VoIP, troubleshooting, 400
voltage
CPU (central processing unit), 259–260
sag, 977
volumes, 501, 569–570
VPN (virtual private network), 116–117, 644–645, 1046–1047
VRT (voice recognition technology), 718
VSC, 1021–1023
vulnerabilities, 795–797. *See also* threats
SQL injection, 795
XSS (cross-site scripting), 794–795

W

WAN (wide area network), 144

wattage, power supply, 275
web browser. *See* browser
web servers, 94
webcam, mobile device, securing, 913
Western Digital, 934–935
whaling, 786
whoami command, 589
Windows, 476
32-bit, 692–693
64-bit, 692–693
ADK (Assessment and Deployment Kit), 498
BSOD, troubleshooting, 881–883
commands/command line
attrib, 749
chkdsk, 572–573
chkdsk /r, 482–483
Command Prompt, 564–565
defrag, 358–360
dir, 570
dxdiag, 374
gpresult, 575
gpupdate, 575–576
help file, 567
hostname, 585–586
ipconfig /all, 26, 396–397, 401, 579–581
navigating, 567–570
net, 587–589
netstat, 77, 586–587
netstat -a, 399
nslookup, 587
ping, 135, 398, 400, 581–583
PowerShell, 565–566

robocopy, 570–571
sfc, 573
systeminfo, 315
tracert, 583–585
whoami, 589
Windows Terminal, 566–567
winver, 573–575
wmic logicaldisk get name, 569
configuration window, 518
Control Panel, 519, 593, 631–632
Device Manager, 632–633
Devices and Printers, 596
Ease of Access Center, 605
File Explorer Options, 600–601
Indexing Options, 599
Internet Options, 594–596
Mail, 597
Microsoft Defender Firewall, 597
opening and viewing utilities, 594
Power Management, 602–604
Programs and Features, 596–597
Sound, 597–599
System and Security, 632
User Accounts, 599
Credential Manager, 804
desktop, 516
Disk Cleanup, 550–551
Disk Management utility, 548–550
Display Settings, 373
Fast Startup, 622
file systems
exFAT, 482

FAT32, 481
NTFS, 481
quick format, 482–483
ReFS, 481–482
God Mode, 745
GUI (graphical user interface), 515
Hello, 742
icons, 517
improper, spontaneous, and frequent shutdowns, troubleshooting, 879–880
MMC (Microsoft Management Console), 532
adding snap-ins, 532–533
Certificate Manager, 539–540
Device Manager, 537–539
Event Viewer, 534–536
Group Policy Editor, 541–542
Performance Monitor, 540–541
Services, 542–543
Task Scheduler, 536–537
notification area, 517–518
Optimize Drives utility, 551–552
pinned applications, 517–518
printers
print jobs, 411
print spooler, 412–414
Registry, 556–557
hives, 557
rules for making changes, 557
Run commands, 558–559
Resource Monitor, 553–554
restore points, creating, 878–879
restoring, 883

Search tool, 517
security. *See* security
Settings, 519, 605
SIM (System Image Manager), 498
Snap, 518
Start menu, 517
System Configuration tool, 554–556
System Information tool, 553
Task Manager
App History tab, 530
Processes tab, 529
Services tab, 530
Startup apps tab, 530
Users tab, 530
verifying RAM, 198–199
taskbar, 517
touchscreen, calibrating, 168
troubleshooting, common symptoms and solutions, 883–889
upgrade paths, 520–521
versions, 487–488
Windows 10
comparison with Windows 11, 521–522
editions, comparing, 511–512
end of support, 523
minimum system requirements, 496
Windows 11
administration tools, 536
comparison with Windows 10, 521–522
editions, comparing, 513–514
Home edition, 513
minimum system requirements, 496–497, 513–515
RAM limits, 514

Windows Sandbox, 326
Windows Backup, 951–952. *See also* backup
Windows Features, enabling Hyper-V, 314–315
Windows N, 522
Windows Settings, 519
Accessibility, 623–625
accessing, 609–610
Accounts, 630–631
Apps, 615–617
Bluetooth & Devices, 614–615
Gaming, 630
Internet Options, 610–611
Network & Internet, 611–613
Personalization, 630
Privacy & Security, 628–630
Storage Sense, 605
System, 617–618
About screen, 618
For Developers, 619–620
Power & Battery, 621–622
Sound, 618–619
Time & Language, 625–626
Windows Update, 627
Windows Update & Security, 626
Windows Tools. *See also* MMC (Microsoft Management Console)
Computer Management, 543–544
Event Viewer, 534
events, 535–536
log files, 535
panes, 534–535
Performance Monitor, 540–541
Task Scheduler, 536–537

WinRE (Windows Recovery Environment), 778–779, 874–875
Advanced Options screen, 875–877
Startup Settings, 877–878
WinRM (Windows Remote Management), 1044–1045
winver command, 573–575
wire termination, 154
wireless/Wi-Fi, 21–22, 37–38. *See also* SOHO environment
802.11 standards, 83–85
adapter, 26
advanced settings, 895–896
analyzer, 87, 157–158
AP (access point)
evil twin, 792–793
placement, 847
positioning antennas, 847
reducing transmission power, 846–847
authentication
802.1X, 769
RADIUS (Remote Dial-In User Service), 768–769
TACACS+, 769
Bluetooth, 38, 49–50
channel/s, 85
bonding, 86
selection, 86
width, 85–86
connecting a laptop, 21–22
encryption protocols, 766–768
AES (Advanced Encryption Standard), 766–767
TKIP (Temporal Key Integrity Protocol), 766
WPA2 (Wi-Fi Protected Access version 2), 766
WPA2-Enterprise, 768
WPA3 (Wi-Fi Protected Access version 3), 766

evil twin, 792–793
hotspot, 38, 47–48
Internet service provider, 149–150
long-range fixed, 87–88
mobile device
airplane mode, 47
Android, 46–47
multipath propagation, 85
NFC (near-field communication), 38–39
Qi charging, 39–40
RFID (radio-frequency identification), 88–89
SSID, changing and disabling, 845–846
troubleshooting
connectivity, 894–895
low RF signal, 399
unlicensed frequencies, 87
WISP (wireless Internet service provider), 87
WLAN (wireless local area network), 145
wmic logicaldisk get name command, 569
WMN (wireless mesh network), 145–146
word processing tools, 709
workgroups, 635–637
workstation operating systems, 475
worm, 773
WPA2 (Wi-Fi Protected Access version 2), 766
WPA2-Enterprise, 768
WPA3 (Wi-Fi Protected Access version 3), 766
WPS (Wi-Fi Protected Setup), disabling, 848–849

X

x64, 692–693

x86, 253–254, 692–693
XDR (extended detection and response), 776–777
XFS (High-Performance Scalable File System), 670
XSS (cross-site scripting), 794–795

Z

zero trust, 1030
zero-day attack, 789–790
zeroing out a drive, 834–836
zero-touch deployment, 499
ZIF (zero insertion force), 258, 265
zombies, 790

To receive your 10% off Exam Voucher, register your product at:

www.pearsonitcertification.com/register

and follow the instructions.

Limited time offer.

See the registration page at the front of the book for details.