

# CompTIA® A+®: A Comprehensive Approach (Exams 220-901 and 220-902)

# CompTIA® A+®: A Comprehensive Approach (Exams 220-901 and 220-902)

Part Number: 093013

Course Edition: 1.1

## Acknowledgements

### PROJECT TEAM

<i>Authors</i>	<i>Media Designer</i>	<i>Content Editor</i>
Pamela J. Taylor	Brian Sullivan	Angie J. French
Gail Sandler		Peter Bauer

Logical Operations wishes to thank the members of the Logical Operations Instructor Community, and in particular Andrew Karaganis, for contributing their technical and instructional expertise during the creation of this course.

## Notices

### DISCLAIMER

While Logical Operations, Inc. takes care to ensure the accuracy and quality of these materials, we cannot guarantee their accuracy, and all materials are provided without any warranty whatsoever, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. The name used in the data files for this course is that of a fictitious company. Any resemblance to current or future companies is purely coincidental. We do not believe we have used anyone's name in creating this course, but if we have, please notify us and we will change the name in the next revision of the course. Logical Operations is an independent provider of integrated training solutions for individuals, businesses, educational institutions, and government agencies. The use of screenshots, photographs of another entity's products, or another entity's product name or service in this book is for editorial purposes only. No such use should be construed to imply sponsorship or endorsement of the book by nor any affiliation of such entity with Logical Operations. This courseware may contain links to sites on the Internet that are owned and operated by third parties (the "External Sites"). Logical Operations is not responsible for the availability of, or the content located on or through, any External Site. Please contact Logical Operations if you have any concerns regarding such links or External Sites.

### TRADEMARK NOTICES

Logical Operations and the Logical Operations logo are trademarks of Logical Operations, Inc. and its affiliates.

CompTIA® A+® is a registered trademark of CompTIA, Inc., in the U.S. and other countries. All other product and service names used may be common law or registered trademarks of their respective proprietors.

Copyright © 2016 Logical Operations, Inc. All rights reserved. Screenshots used for illustrative purposes are the property of the software proprietor. This publication, or any part thereof, may not be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, storage in an information retrieval system, or otherwise, without express written permission of Logical Operations, 3535 Winton Place, Rochester, NY 14623, 1-800-456-4677 in the United States and Canada, 1-585-350-7000 in all other countries. Logical Operations' World Wide Web site is located at [www.logicaloperations.com](http://www.logicaloperations.com).

This book conveys no rights in the software or other products about which it was written; all use or licensing of such software or other products is the responsibility of the user according to terms and conditions of the owner. Do not make illegal copies of books or software. If you believe that this book, related materials, or any other Logical Operations materials are being reproduced or transmitted without permission, please call 1-800-456-4677 in the United States and Canada, 1-585-350-7000 in all other countries.

# **CompTIA® A+®: A Comprehensive Approach (Exams 220-901 and 220-902)**

<b>Lesson 1: Hardware Fundamentals.....</b>	<b>1</b>
Topic A: Personal Computer Components.....	2
Topic B: Storage Devices.....	14
Topic C: Mobile Digital Devices.....	25
Topic D: Connection Interfaces.....	31
<b>Lesson 2: Operating System Fundamentals.....</b>	<b>53</b>
Topic A: PC and Mobile Operating Systems.....	54
Topic B: PC Operating System Tools and Utilities.....	68
<b>Lesson 3: Networking and Security Fundamentals.....</b>	<b>83</b>
Topic A: Network Types.....	84
Topic B: Network Components.....	90
Topic C: Common Network Services.....	96
Topic D: Cloud Concepts.....	99
Topic E: Security Fundamentals.....	103

<b>Lesson 4: Safety and Operational Procedures.....</b>	<b>111</b>
Topic A: Basic Maintenance Tools and Techniques.....	112
Topic B: Personal and Electrical Safety.....	120
Topic C: Environmental Safety and Materials Handling.....	128
Topic D: Professionalism and Communication.....	138
Topic E: Organizational Policies and Procedures.....	140
Topic F: Troubleshooting Theory.....	146
<b>Lesson 5: Supporting Display Devices.....</b>	<b>151</b>
Topic A: Install Display Devices.....	152
Topic B: Configure Display Devices.....	162
Topic C: Troubleshoot Video and Display Devices.....	166
<b>Lesson 6: Installing and Configuring Peripheral Components.....</b>	<b>171</b>
Topic A: Install and Configure Input Devices.....	172
Topic B: Install and Configure Output Devices.....	188
Topic C: Install and Configure Input/Output Devices.....	192
Topic D: Install and Configure Expansion Cards.....	197
<b>Lesson 7: Managing System Components.....</b>	<b>201</b>
Topic A: Identify Motherboard Components and Features.....	202
Topic B: Install and Configure CPUs and Cooling Systems.....	223
Topic C: Install Power Supplies.....	231
Topic D: Troubleshoot System Components.....	239
<b>Lesson 8: Managing Data Storage.....</b>	<b>251</b>
Topic A: Identify RAM Types and Features.....	252
Topic B: Troubleshoot RAM Issues.....	258
Topic C: Install and Configure Storage Devices.....	260

Topic D: Configure the System Firmware.....	268
Topic E: Troubleshoot Hard Drives and RAID Arrays.....	276
<b>Lesson 9: Installing and Configuring Microsoft Windows.....</b>	<b>285</b>
Topic A: Implement Client-Side Virtualization.....	286
Topic B: Install Microsoft Windows.....	293
Topic C: Use Microsoft Windows .....	308
Topic D: Configure Microsoft Windows.....	318
Topic E: Upgrade Microsoft Windows.....	334
<b>Lesson 10: Optimizing and Maintaining Microsoft Windows</b>	<b>341</b>
Topic A: Optimize Microsoft Windows.....	342
Topic B: Back Up and Restore System Data.....	349
Topic C: Perform Disk Maintenance.....	352
Topic D: Update Software.....	355
<b>Lesson 11: Working With Other Operating Systems.....</b>	<b>361</b>
Topic A: The OS X Operating System.....	362
Topic B: The Linux Operating System.....	373
<b>Lesson 12: Customized Client Environments.....</b>	<b>407</b>
Topic A: Types of Common Business Clients.....	408
Topic B: Custom Client Environments.....	411
<b>Lesson 13: Networking Technologies.....</b>	<b>419</b>
Topic A: TCP/IP Properties and Characteristics.....	420
Topic B: TCP/IP.....	435
Topic C: Internet Connections.....	445
Topic D: Ports and Protocols.....	449
Topic E: Networking Tools.....	456

<b>Lesson 14: Installing and Configuring Networking Capabilities.....</b>	<b>465</b>
Topic A: Configure Basic Windows Networking.....	466
Topic B: Configure Network Perimeters.....	474
Topic C: Using Windows Networking Features.....	479
Topic D: Install and Configure SOHO Networks.....	484
<b>Lesson 15: Supporting Mobile Digital Devices.....</b>	<b>495</b>
Topic A: Install and Configure Exterior Laptop Components.....	496
Topic B: Install and Configure Interior Laptop Components.....	505
Topic C: Other Mobile Devices.....	511
Topic D: Mobile Device Accessories and Ports.....	516
Topic E: Mobile Device Connectivity.....	519
Topic F: Mobile Device Synchronization.....	526
Topic G: Troubleshoot Mobile Device Hardware.....	529
<b>Lesson 16: Supporting Printers and Multifunction Devices..</b>	<b>539</b>
Topic A: Printer and Multifunction Technologies.....	540
Topic B: Install and Configure Printers.....	555
Topic C: Maintain Printers.....	561
Topic D: Troubleshoot Printers.....	564
<b>Lesson 17: Security Threats, Vulnerabilities, and Controls..</b>	<b>575</b>
Topic A: Common Security Threats and Vulnerabilities.....	576
Topic B: General Security Controls.....	586
Topic C: Mobile Security Controls.....	598
Topic D: Data Destruction and Disposal Methods.....	602
<b>Lesson 18: Implementing Security Controls.....</b>	<b>607</b>
Topic A: Secure Operating Systems.....	608

Topic B: Secure Workstations.....	621
Topic C: Secure SOHO Networks.....	627
Topic D: Secure Mobile Devices.....	634
<b>Lesson 19: Troubleshooting System-Wide Issues.....</b>	<b>641</b>
Topic A: Troubleshoot PC Operating Systems.....	642
Topic B: Troubleshoot Mobile Device Operating Systems and Applications.....	661
Topic C: Troubleshoot Wired and Wireless Networks.....	665
Topic D: Troubleshoot Common Security Issues.....	671
<b>Appendix A: Mapping Course Content to CompTIA A+ Certification Exam 220-901.....</b>	<b>685</b>
<b>Appendix B: Mapping Course Content to CompTIA A+ Certification Exam 220-902.....</b>	<b>705</b>
<b>Appendix C: A+ Command Reference.....</b>	<b>725</b>
<b>Appendix D: A Brief History of Personal Computers.....</b>	<b>741</b>
Solutions.....	749
Glossary.....	771
Index.....	805



# About This Course

If you are getting ready for a career as an entry-level information technology (IT) professional or computer service technician, the CompTIA® A+® course is the first step in your preparation. The course will build on your existing user-level knowledge and experience with personal computer (PC) software and hardware to present fundamental skills and concepts that you will use on the job. In this course, you will acquire the essential skills and information you will need to install, configure, optimize, troubleshoot, repair, upgrade, and perform preventive maintenance on PCs, digital devices, and operating systems.

The CompTIA A+ course can benefit you in two ways. Whether you work or plan to work in a mobile or corporate environment where you have a high level of face-to-face customer interaction, where client communication and client training are important, or in an environment with limited customer interaction and an emphasis on hardware activities, this course provides the background knowledge and skills you will require to be a successful A+ technician. It can also assist you if you are preparing to take the CompTIA A+ certification examinations, 2016 objectives (exam numbers 220-901 and 220-902), in order to become a CompTIA A+ Certified Professional.

## Course Description

### Target Student

This course is designed for individuals who have basic computer user skills and who are interested in obtaining a job as an entry-level IT technician. This course is also designed for students who are seeking the CompTIA A+ certification and who want to prepare for the CompTIA A+ 220-901 Certification Exam and the CompTIA 220-902 Certification Exam.

### Course Prerequisites

To ensure your success in this course, you should have basic computer user skills, be able to complete tasks in a Microsoft® Windows® environment, be able to search for, browse, and access information on the Internet, and have basic knowledge of computing concepts. You can obtain this level of skills and knowledge by taking any introductory computing course from Logical Operations, such as:

- *Using Microsoft® Windows® 10*



**Caution:** The prerequisites for this course differ significantly from the prerequisites for the CompTIA certification exams. For the most up-to-date information about the exam prerequisites, complete the form on this page: <http://certification.comptia.org/Training/testingcenters/examobjectives.aspx>

## Course Objectives

In this course, you will install, configure, optimize, troubleshoot, repair, upgrade, and perform preventive maintenance on personal computers, digital devices, and operating systems.

You will:

- Identify the hardware components of personal computers and mobile digital devices.
- Identify the basic components and functions of operating systems.
- Identify networking and security fundamentals.
- Identify the operational procedures that should be followed by professional PC technicians.
- Install, configure, and troubleshoot display devices.
- Install and configure peripheral components.
- Manage system components.
- Manage data storage.
- Install and configure Microsoft Windows.
- Optimize and maintain Microsoft Windows.
- Work with other operating systems.
- Identify the hardware and software requirements for client environment configurations.
- Identify network technologies.
- Install and configure networking capabilities.
- Support mobile digital devices.
- Support printers and multifunction devices.
- Identify security threats, vulnerabilities, and controls.
- Implement security controls.
- Troubleshoot system-wide issues.

## The CHOICE Home Screen

Logon and access information for your CHOICE environment will be provided with your class experience. The CHOICE platform is your entry point to the CHOICE learning experience, of which this course manual is only one part.

On the CHOICE Home screen, you can access the CHOICE Course screens for your specific courses. Visit the CHOICE Course screen both during and after class to make use of the world of support and instructional resources that make up the CHOICE experience.

Each CHOICE Course screen will give you access to the following resources:

- **Classroom:** A link to your training provider's classroom environment.
- **eBook:** An interactive electronic version of the printed book for your course.
- **Files:** Any course files available to download.
- **Checklists:** Step-by-step procedures and general guidelines you can use as a reference during and after class.
- **LearnTOs:** Brief animated videos that enhance and extend the classroom learning experience.
- **Assessment:** A course assessment for your self-assessment of the course content.
- Social media resources that enable you to collaborate with others in the learning community using professional communications sites such as LinkedIn or microblogging tools such as Twitter.

Depending on the nature of your course and the components chosen by your learning provider, the CHOICE Course screen may also include access to elements such as:

- LogicalLABS, a virtual technical environment for your course.
- Various partner resources related to the courseware.
- Related certifications or credentials.
- A link to your training provider's website.
- Notices from the CHOICE administrator.

- Newsletters and other communications from your learning provider.
- Mentoring services.

Visit your CHOICE Home screen often to connect, communicate, and extend your learning experience!

## How to Use This Book

### As You Learn

This book is divided into lessons and topics, covering a subject or a set of related subjects. In most cases, lessons are arranged in order of increasing proficiency.

The results-oriented topics include relevant and supporting information you need to master the content. Each topic has various types of activities designed to enable you to solidify your understanding of the informational material presented in the course. Information is provided for reference and reflection to facilitate understanding and practice.

Data files for various activities as well as other supporting files for the course are available by download from the CHOICE Course screen. In addition to sample data for the course exercises, the course files may contain media components to enhance your learning and additional reference materials for use both during and after the course.

Checklists of procedures and guidelines can be used during class and as after-class references when you're back on the job and need to refresh your understanding.

At the back of the book, you will find a glossary of the definitions of the terms and concepts used throughout the course. You will also find an index to assist in locating information within the instructional components of the book.

### As You Review

Any method of instruction is only as effective as the time and effort you, the student, are willing to invest in it. In addition, some of the information that you learn in class may not be important to you immediately, but it may become important later. For this reason, we encourage you to spend some time reviewing the content of the course after your time in the classroom.

### As a Reference

The organization and layout of this book make it an easy-to-use resource for future reference. Taking advantage of the glossary, index, and table of contents, you can use this book as a first source of definitions, background information, and summaries.

### Course Icons

Watch throughout the material for the following visual cues.

Icon	Description
	A <b>Note</b> provides additional information, guidance, or hints about a topic or task.
	A <b>Caution</b> note makes you aware of places where you need to be particularly careful with your actions, settings, or decisions so that you can be sure to get the desired results of an activity or task.
	<b>LearnTO</b> notes show you where an associated LearnTO is particularly relevant to the content. Access LearnTOs from your CHOICE Course screen.
	<b>Checklists</b> provide job aids you can use after class as a reference to perform skills back on the job. Access checklists from your CHOICE Course screen.
	<b>Social</b> notes remind you to check your CHOICE Course screen for opportunities to interact with the CHOICE community using social media.



# 1

# Hardware Fundamentals

**Lesson Time:** 2 hours

## Lesson Objectives

In this lesson, you will identify the hardware components of personal computers and mobile digital devices. You will:

- Identify personal computer components.
- Identify storage devices.
- Identify mobile digital devices.
- Compare PC and device connection interfaces and their characteristics.

## Lesson Introduction

A very large percentage of the work that most IT technicians do entails working with hardware, including installing, upgrading, repairing, configuring, maintaining, optimizing, and troubleshooting computer components. To install and configure computer hardware, you need to recognize the basic components that constitute most personal computers, along with the functionality that each component provides to the computing experience. In this lesson, you will identify hardware components and how they function.

Preparing for a career in computer support and maintenance can be a daunting task. A good place to start is with the basics: the essential hardware components that you find in most computers. Identifying hardware components and their roles give you a solid base on which to build the knowledge and skills you need to install, configure, and troubleshoot computer hardware.

# TOPIC A

## Personal Computer Components

In this lesson, you will identify the hardware components of a computer. The first step is to identify the hardware that you will find in virtually all computer systems. In this topic, you will identify computer system components.

If you are not familiar with the various components that a computer is made up of, it can seem like a jigsaw puzzle. Like most puzzles, each part of a computer connects to other parts in a specific place, but generally, you will find that the pieces fit together almost exactly the same way from one system to another. To help you put the puzzle together, you need to understand what these pieces look like and what they do.

### Common Computer Components

Computing components are the physical devices that are required for a computer to operate properly. There are four main categories of components in a typical computer.

<b>Component</b>	<b>Description</b>
The <i>system unit</i>	The system unit, also commonly referred to as the CPU, or the tower, is the main component of a computer, which houses most of the other devices that are necessary for the computer to function. Traditionally, it comprises a chassis and internal components, such as the system board, the microprocessor, memory modules, disk drives, adapter cards, the power supply, fans and other cooling systems, and ports for connecting external components such as monitors, keyboards, mice, and other devices.  System units are also often referred to as boxes, main units, or base units.



In some newer computer models, the system unit is incorporated with the display screen and referred to as an all-in-one computer. Similar to laptops, the system unit is integrated into a smaller configuration, which may make it harder to manage or replace the system unit components.

<b>Component</b>	<b>Description</b>
<i>Display devices</i>	<p>A display device is a personal computer component that enables users to view the text and graphical data output from a computer. Display devices commonly connect to the system unit via a cable, and they have controls to adjust the settings for the device. They vary in size and shape, as well as the technologies used.</p> <p>Common terms for various types of display devices include display, monitor, screen, <i>liquid crystal display (LCD)</i>, and flat-panel monitors.</p>
	
<i>Input devices</i>	<p>An input device is a personal computer component that enables users to enter data or instructions into a computer. Common input devices include keyboards and computer mice. An input device can connect to the system unit via a cable or a wireless connection.</p>
	
<i>Peripheral devices</i>	<p>You can enhance the functionality of practically any personal computer by connecting different types of peripheral devices to the system unit. Also called <i>external devices</i>, peripheral devices can provide alternative input or output methods or additional data storage. You connect peripheral devices to the system unit via cable or a wireless connection. Some devices have their own power source, while others draw power from the system. Common examples of peripheral devices include microphones, cameras, speakers, scanners, printers, and external drives. Of these devices, speakers and printers are output devices; microphones, cameras, and scanners are input devices; external drives are input/output devices.</p>
	

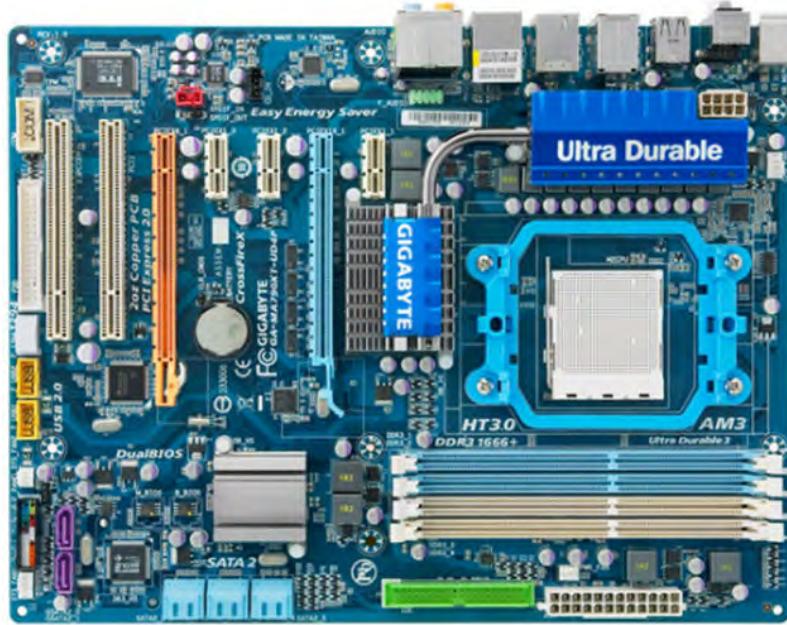
## Computer Cases

The *computer case* is the enclosure that holds all of the components of your computer. Computer cases come in several sizes and arrangements. Some are designed to hold many internal components and have a lot of room to work around those components. These are usually tower or desktop cases and take up a good deal of room. Other cases are designed to use a minimum amount of space. The trade-off is that the interior of the case is often cramped, with little room for adding additional components. Because the tower proved to be popular, there are now several versions of the tower model. These include:

- Full tower, which is usually used for servers or when you will be installing many drives and other components.
- Mid tower, which is a slightly smaller version of the full-size tower.
- Micro, or mini tower, which is the size that replaces the original desktop case in most modern systems.
- Slim line, which is a tower case that can be turned on its side to save room.

## The Motherboard

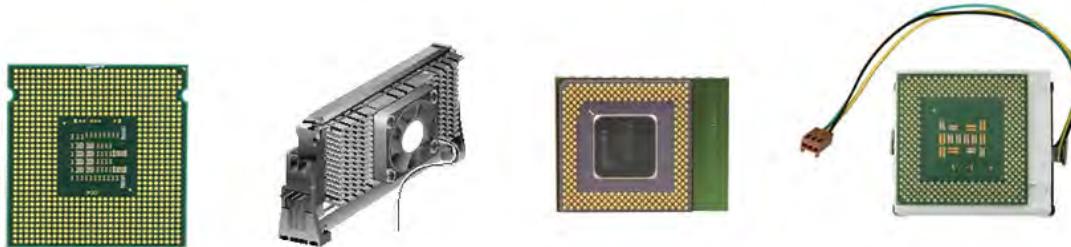
The *motherboard* is the personal computer component that acts as the backbone for the entire computer system. Sometimes called the *system board*, it consists of a large, flat circuit board with chips and other electrical components on it, with various connectors. Some components are *soldered* directly to the board, and some components connect to the board by using slots or sockets.



*Figure 1-1: A motherboard.*

## The CPU

The *central processing unit (CPU)* is a computer chip where most of the computing calculations take place. On most computers, the CPU is housed in a single microprocessor module that is installed on the system board in a slot or a socket.



**Figure 1-2: CPUs.**

## Memory

*Memory* is the computer system component that provides a temporary workspace for the processor. Memory refers to modules of computer chips that store data in a digital electronic format, which is faster to read from and write to than tape or hard drives. Memory chips each contain millions of transistors etched on one sliver of a semiconductor. *Transistors* are nothing more than switches that can be opened or closed. When a transistor is closed, it conducts electricity, representing the binary number 1. When it is opened, it does not, representing the binary number 0.



**Figure 1-3: Sample memory modules.**

There are two types of memory used in computer systems: *Random Access Memory (RAM)* and *Read-Only Memory (ROM)*. RAM is a computer storage method that functions as a computer's main memory. This type requires a constant power source to access the data stored within the RAM. However, data stored on ROM is saved and stored without a constant power source. Once data is written to ROM, it cannot be modified easily.

### Volatile and Non-volatile Memory

Memory is considered to be either volatile or non-volatile:

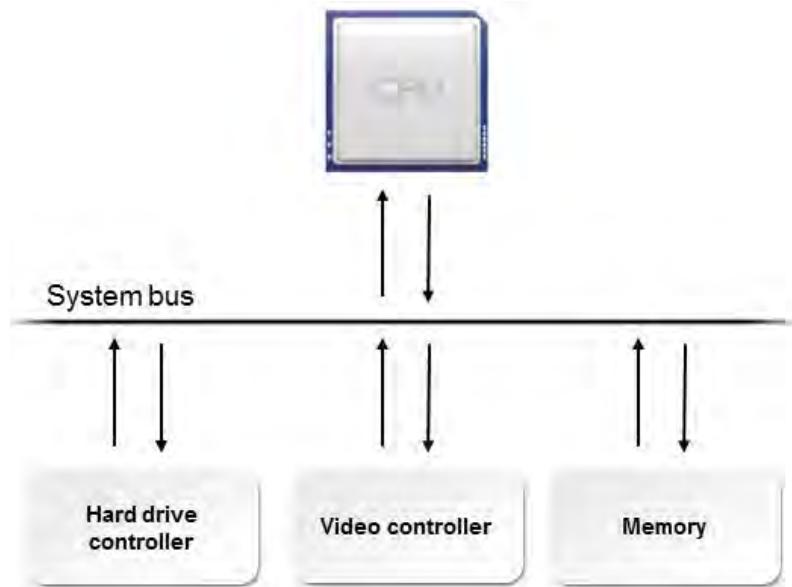
- Volatile memory stores data temporarily and requires a constant source of electricity to keep track of the data stored in it. When the power is no longer available, the data stored in volatile

memory is lost. The computer's main RAM is an example of volatile memory. The computer can both read the data stored in RAM and write different data into the same RAM. Any byte of data can be accessed without disturbing other data, so the computer has random access to the data in RAM.

- Non-volatile memory retains the information stored on it whether or not electrical current is available. ROM is an example of non-volatile memory.

## The System Bus

In computer communications, a *bus* is a group of wires or electronic pathways that connect components. The *system bus* is the wires, or *traces*, on the motherboard that provide the main communication path between the CPU and memory. The system bus enables data transfer between the CPU, memory, and the other buses in the computer, which connect other system components such as hard drives and adapter cards. It is sometimes referred to as the frontside bus or local bus.



**Figure 1–4: A system bus.**

## Storage Devices

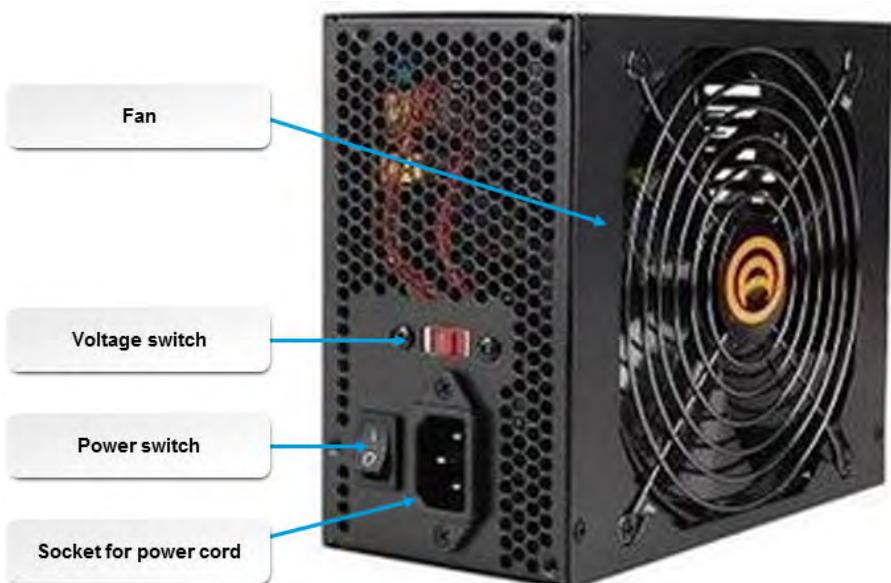
A *storage device* is a computer system component, such as a hard drive, that enables users to save data for reuse at a later time, even after the personal computer is shut down and restarted. Storage devices can save data magnetically, optically, or electronically, depending on their design.



**Figure 1–5:** Examples of storage devices.

## Power Supplies

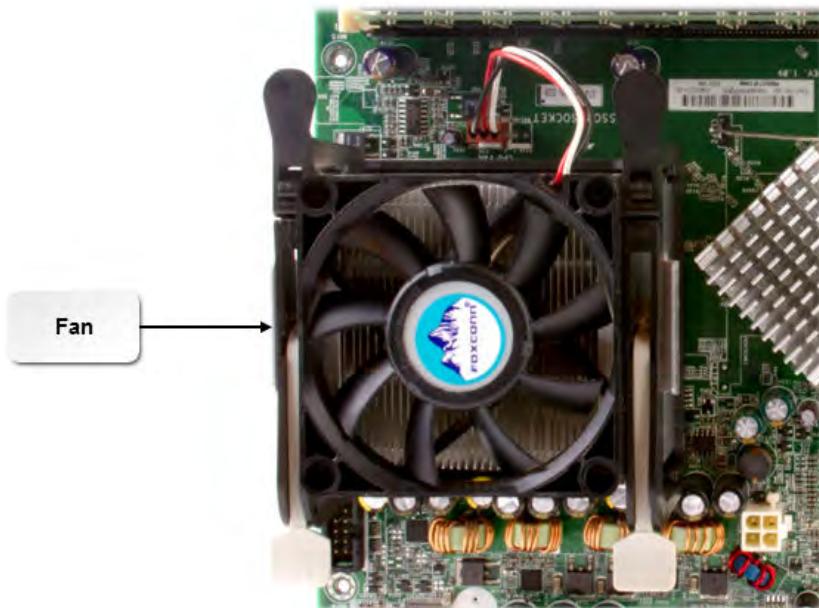
A *power supply* is a computer system component that converts line-voltage alternating current (AC) power from an electrical outlet to the low-voltage direct current (DC) power needed by other system components. The power supply is often referred to as the power supply unit (PSU). The power supply is typically a metal box in the rear of the system that is attached to the computer chassis and to the system board. While the power supply is not itself a component of the system board, it is required in order for system components to receive power. The power supply contains the power cord plug and a fan for cooling, because it generates a lot of heat. Some power supplies have a voltage selector switch that enables you to set them to the voltage configurations that are used in different countries. AC adapters are generally built in to the power supply for desktop systems and are external for laptops and other mobile systems.



**Figure 1–6:** A power supply.

## Cooling Systems

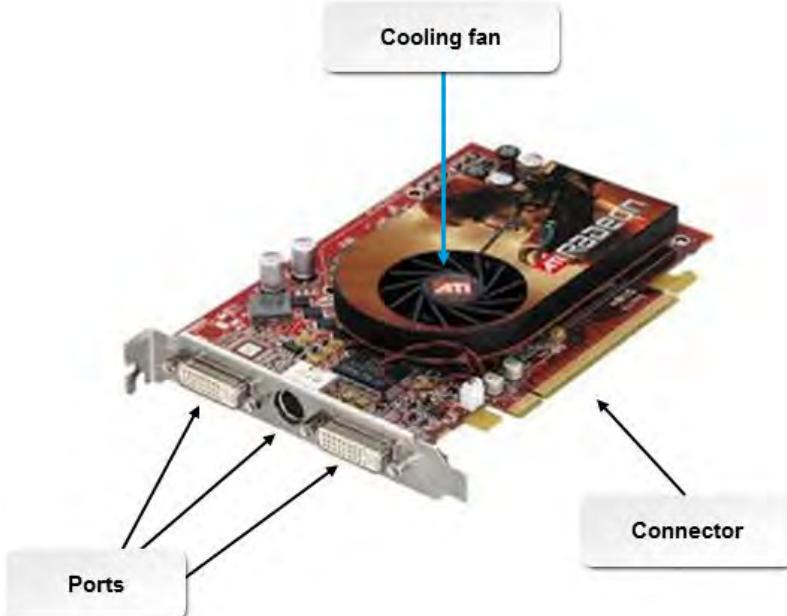
A *cooling system* is a computer system component that prevents damage to other computer parts by dissipating the heat generated inside a computer chassis. The cooling system can consist of one or more fans and other components such as *heat sinks* or liquid cooling systems that service the entire computer as well as individual components, such as the power supply and CPU.



*Figure 1–7: A typical cooling system for a CPU.*

## Expansion Cards

An *expansion card* is a printed circuit board that you install into an expansion slot on the computer's system board to expand the functionality of the computer. In standard desktop systems, cards have connectors that fit into an expansion slot on a system board and circuitry to connect a specific device to the computer. Laptops, on the other hand, typically have slots located on the outside of the case for inserting expansion cards. These cards are often referred to as laptop expansion cards.



*Figure 1–8: An expansion card.*



**Note:** An expansion card is also known as an adapter card, I/O card, add-in, add-on, or simply as a board.

## Riser Cards

A *riser card* is a board that plugs into the motherboard and provides additional expansion slots for adapter cards. Because it rises above the motherboard, it enables you to connect additional adapters to the system in an orientation that is parallel to the motherboard and thus saves space within the system case. Riser cards are commonly found within rackmount server implementations to provide additional slots for expanding the features of a server and in low rise smaller cases to fit larger expansion cards.



**Figure 1–9:** A riser card.



**Note:** A riser card expands motherboard capabilities the way a power strip increases the capabilities of electrical outlets.

## Daughter Boards

*Daughter board* is a general computing and electronics term for any circuit board that plugs into another circuit board. In personal computing, a daughter board can be used as a more general term for adapter cards. Sometimes, in casual usage, the term “daughter board” is used interchangeably with the term “riser card,” but technically they are not the same.

## Firmware

*Firmware* is specialized software stored in memory chips that stores OS-specific information whether or not power to the computer is on. It is most often written on an electronically reprogrammable chip so that it can be updated with a special program to fix any errors that might be discovered after a computer is purchased, or to support updated hardware components.



**Note:** Updating firmware electronically is called *flashing*.

## The System BIOS

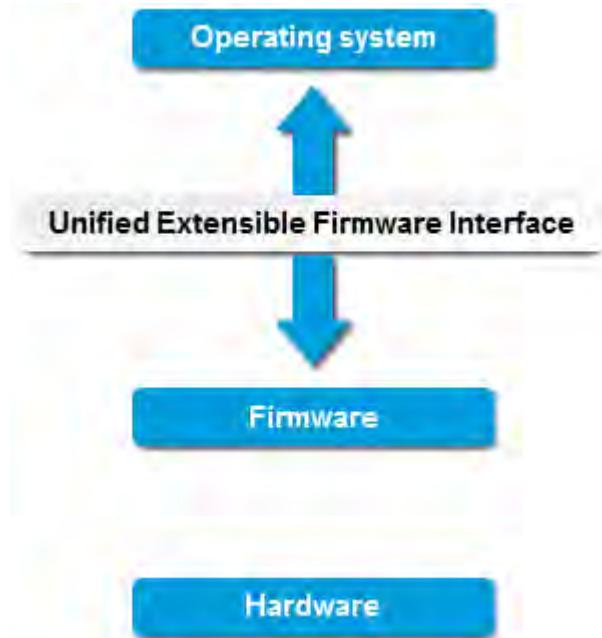
A *Basic Input/Output System (BIOS)* is a set of instructions that is stored in ROM and that is used to start the most basic services of a computer system. Every computer has a *system BIOS*, which sets the computer's configuration and environment when the system is powered on. It is located in ROM chips on the system board. Computers may also include other devices that have their own BIOS to control their functions.



*Figure 1–10: The system BIOS resides on ROM chips, and sets the computer's configuration and environment at startup.*

## UEFI

The *Unified Extensible Firmware Interface (UEFI)* is a standard firmware interface for PCs that was designed to improve software interoperability and address the limitations in BIOSs. Providing legacy support for BIOS services, UEFI can support remote diagnostics and repair of computers, even without an operating system being installed.



*Figure 1–11: UEFI.*

UEFI firmware provides several technical advantages over a traditional BIOS system:

- Ability to boot from large disks (over 2 TB) with a GUID Partition Table (GPT).
- CPU-independent architecture and drivers.
- Flexible pre-OS environment, including networking capabilities.
- Modular design.



**Note:** Some systems allow users to select options from BIOS or UEFI in order to support legacy technologies.

## The POST

The *Power-On Self Test (POST)* is a built-in diagnostic program that runs every time a personal computer starts up. The POST checks your hardware to ensure that everything is present and functioning properly, before the system BIOS begins the operating system boot process. If there is an error, then an audible beep will alert you that something is wrong.

The POST process contains several steps to ensure that the system meets the necessary requirements to operate properly.



**Note:** The POST process can vary a great deal from manufacturer to manufacturer.

<b>Hardware Component</b>	<b>POST Test Criteria</b>
Power supply	Must be turned on, and must supply its power good signal.
CPU	Must exit Reset status mode, and must be able to execute instructions.
System firmware	Must be readable.
System firmware memory	Must be readable.
Memory	Must be able to be read by the CPU, and the first 64 KB of memory must be able to hold the POST code.
Input/output (I/O) bus or I/O controller	Must be accessible, and must be able to communicate with the video subsystem.

# ACTIVITY 1–1

## Identifying PC Components

### Scenario

In this activity, you will identify personal computer components.

1. Your instructor might provide you with examples of computer components and ask you or other participants to identify them.
2. In this graphic, identify the (A) system unit(s), (B) display device(s), (C) input device(s), and (D) output device(s).



3. What are the minimum requirements for a functioning PC?

- Input devices
- Speakers
- System unit
- Webcam
- Display device

4. Which computer components are part of the system unit?

- Chassis
- Internal hard drive
- Monitor
- Portable USB drive
- Memory

5. In this graphic, identify the components listed by placing the corresponding letters into the boxes. A. Motherboard, B. Power supply, C. Expansion card, D. Storage device, E. Memory, F. CPU.



6. Where is the system BIOS stored?

- On the primary hard drive
- In BIOS memory
- On ROM chips
- In RAM

7. True or False? The GPT is what enables the UEFI to support booting from very large hard disks.

- True
- False

8. Which hardware components are checked during the POST?

- Power supply
- CPU
- Display
- RAM

9. Which system unit components are connected by the system bus?

- CPU
- Memory
- Power supply
- System board
- Cooling system

# TOPIC B

## Storage Devices

In the previous topic, you identified the main components of a personal computer. One of the primary reasons for using a computer is to electronically store data. In this topic, you will identify the types of storage devices used in personal computers.

As a computer technician, your responsibilities are likely to include installing and maintaining many different types of computer components, including storage devices. By identifying the various types of storage devices that can be found in most personal computers, you will be better prepared to select, install, and maintain storage devices in personal computers.

### Hard Drives

A *hard disk drive (HDD)* is a storage device that reads data from, and writes data to, a hard disk. A hard disk consists of several metal or hard plastic platters with a magnetic surface coating. Data is stored magnetically and can be accessed directly. Although the HDD and the hard disk are not the same thing, they are packaged together and are often referred to interchangeably. HDDs are also referred to as hard drives, and they can be internal or external devices. Internal hard drives are mounted inside the chassis and connect directly to the system board through at least one cable for data and one for power, while external hard drives generally connect to the system by means of an expansion card or a port.



*Figure 1-12: An HDD.*

### Disk Controllers

Hard drives require circuitry to communicate with the CPU. This circuitry is known as the *disk controller*. Disk controllers can be built into the drive itself, or they can be contained on an expansion card. In most modern hard drives, the controller is built into the drive.

### Hard Drive Speeds

The speed of a hard drive is based on how fast the disk is spun to retrieve the requested data. This is referred to as revolutions per minute (rpm). Common speeds include:

- 5,400 rpm
- 7,200 rpm
- 10,000 rpm

## Hot Swappable Devices

Hot swapping is a type of hardware replacement procedure where a component can be replaced while the main power is still on. Also called hot plug or hot insertion, hot swap is a feature of USB and FireWire devices, enabling you to install an internal or external drive, network adapter, or other peripheral without having to power down the computer. It is good practice to use the safe removal option from the System Tray before removing a hot-swappable device or peripheral from the computer. Hot swapping can also refer to the computer's ability to detect when hardware is added or removed.

Non-hot-swappable devices require the computer to be shut down and restarted before any device installation updates or removals are recognized by the operating system.

## Types of Hard Drives

Although you might occasionally encounter legacy hard drive technology, the most prevalent types of hard drives that you are likely to be asked to install or troubleshoot are in the SATA family. *Serial Advanced Technology Attachment (SATA)* drives have the following characteristics:

- SATA supports one device per channel.
- SATA supports hot swapping of drives, which means that you can replace a SATA drive without powering down the system.
- Many PCs include external SATA jacks.



**Note:** You might hear SATA pronounced “Serial ay-tee-ay,” “ESS-ay-tee-ay,” “SAY-tuh,” or “SAT-uh.”

## Solid State Storage

*Solid state drives (SSDs)* use flash technology to retain data in special types of memory instead of on disks or tape. Solid state storage uses non-volatile memory to emulate mechanical storage devices, but solid state storage is much faster and more reliable than mechanical storage because there are no moving parts.

## Types of Solid State Storage

Solid state storage comes in several formats, many of which are used in external devices such as digital cameras or mobile devices.

<b>Solid State Storage Device</b>	<b>Specifications</b>
-----------------------------------	-----------------------

USB flash drives USB flash drives come in several form factors, including thumb drives and pen drives. Thumb drives can be small, from 50 to 70 mm long, 17 to 20 mm wide, and 10 to 12 mm thick. Data storage capacities vary, from 128 MB up to 128 GB. Data transfer rates also vary, from 700 KBps to 28 MBps for read operations, and from 350 KBps to 15 MBps for write operations.



SSDs Flash-memory-based disks do not need batteries, allowing makers to replicate standard disk-drive form factors (2.5-inch and 3.5-inch). Flash SSDs are extremely fast since these devices have no moving parts, eliminating seek time, latency, and other electromechanical delays inherent in conventional disk drives. The use of SSDs has been increasing over time due to their speed and quick data access times.  
SSDs can be configured within systems to replace traditional computer hardware such as disk drives, optical drives, and network security appliances that include firewall and routing functions.



<b>Solid State Storage Device</b>	<b>Specifications</b>
-----------------------------------	-----------------------

CF cards CompactFlash (CF) cards are flash memory cards that are 43 mm long by 36 mm wide. Due to their compact size, they are typically used in portable devices. Type I is 3.3 mm thick and Type II is 5 mm thick. They hold 100 GB or more, and have a 50-pin contact. Transfer speeds of up to 66 MBps are possible.

Newer versions of the CF card offer speeds up to 1 Gbps and can store up to 1 terabyte (TB) of data.

CF cards are commonly used for additional storage in:

- Digital cameras
- Music players
- Personal computing devices
- Photo printers
- Digital camera recorders



SM cards SmartMedia (SM) cards are flash memory cards that are similar in size to the CF cards, and are 45 mm long by 37 mm wide by 0.76 mm thick. They can hold up to 128 MB and can transfer data at speeds of up to 8 MBps.

SM cards are commonly used for additional storage in:

- Digital cameras
- Digital camera recorders
- Older models of personal digital assistants (PDAs)



<b>Solid State Storage Device</b>	<b>Specifications</b>
xD	xD-Picture Cards (xD) are flash memory cards that are specifically designed for use in digital cameras. They are 20 mm long by 25 mm wide by 1.7 mm thick. They can hold up to 2 GB with plans for up to 8 GB. Data transfer rates range from 4 to 15 MBps for read operations and from 1.3 to 9 MBps for write operations.



MSs Memory sticks (MSs) are flash memory cards that are 50 mm long by 21.5 mm wide by 2.8 mm thick. They can hold up to 16 GB and are used extensively in Sony products such as VAIO® laptops. Data transfer rates are 2.5 MBps for read operations and 1.8 MBps for write operations.



<b>Solid State Storage Device</b>	<b>Specifications</b>
SD cards	<p>The original Secure Digital (SD) Memory Card is 32 mm long, 24 mm wide, and 2.1 mm thick. The miniSD Card measures 21.5 mm by 20 mm by 1.4 mm, and the microSD/TransFlash Card measures 15 mm by 11 mm by 1 mm. SD Memory Cards are currently available in several capacities, up to 2 TB. Data transfer rates range from 10 MBps to 20 MBps.</p> <p>SD cards are used in many different devices, including:</p> <ul style="list-style-type: none"> <li>• Laptops</li> <li>• Digital cameras</li> <li>• Smartphones</li> <li>• Handheld gaming devices</li> <li>• Audio players</li> </ul> 
MMCs	<p>MultiMediaCards (MMCs) are 32 mm long by 24 mm wide by 1.5 mm thick. Reduced Size MMCs (RS-MMCs) and MMCmobile cards are 16 mm by 24 mm by 1.5 mm. MMCmini cards are 21.5 mm by 20 mm by 1.4 mm, and MMCmicro cards are 12 mm by 14 mm by 1.1 mm. These cards can hold up to 8 GB, and data transfer rates can reach 52 MBps. MMC cards are generally also compatible with SD card readers and are used in many of the same devices.</p> 

## Solid State Hybrid Drives

*Solid state hybrid drives (SSHDs)* combine the best features of solid state and magnetic data storage by combining the traditional rotating platters of a magnetic HDD and a small amount of high-speed flash memory on a single drive.

An SSHD monitors the data being read from the hard drive, and then caches the most frequently accessed bits to the high-speed flash memory. The data stored on the flash memory will change over time, but once the most frequently accessed bits of data are stored on the flash memory, they will be read from the flash, resulting in SSD-like performance for the files that are accessed the most.

Some of the advantages of SSHDs include cost, capacity, and manageability.

- Only a relatively small solid-state volume is required to boost performance through the caching functionality, so a large investment in a high-capacity SSD isn't required. Hybrid drives tend to cost slightly more than traditional hard drives, but far less than comparably sized solid-state drives.
- Operating systems perceive an SSHD as a single drive, making it easy to manage.
- Because the cache volume is basically hidden from the operating system, users don't need to select the data that is stored on the SSD. Boot times are also improved.

## Optical Discs

An *optical disc* is a storage device that stores data optically, rather than magnetically. The removable plastic discs have a reflective coating and require an optical drive to be read. In optical storage, data is written by either pressing or burning with a laser to create pits (recessed areas) and lands (raised areas) in the reflective surface of the disc. Common optical discs include compact discs (CDs), digital versatile discs (DVDs), and Blu-ray discs.

Some optical discs, such as DVDs, can be single-sided or double-sided. Double-sided optical discs have one recordable layer on each side of the disc. For writable and rewritable double-sided discs, you burn data to one side, then flip the disc over to burn the other side.

### Types of Optical Discs

There is a wide variety of optical discs available in the marketplace, each with its own requirements and specifications.

<i>Optical Disc Type</i>	<i>Description</i>
CD-ROM	Compact Disc-Read Only Memory. Data is permanently burned onto the disc during its manufacture. The capacity for CD-ROMs ranges from 700 to 860 MB.
CD-RW	CD-Rewritable. Data can be written to the disc multiple times. CD-RW capacities also range from 700 to 860 MB.
DVD-ROM	Digital Versatile Disc-Read Only Memory. Data is permanently burned onto the disc during its manufacture. Single-sided DVD-ROMs have a capacity of 4.7 GB, while double-sided DVD-ROMs can hold 9.4 GB.
Single Layer DVD-R	Single Layer Digital Versatile Disc-Recordable. Data can be written to a DVD-R disc once. Single Layer DVD-R discs hold up to 4.7 GB of data.
Single Layer DVD+R	Single Layer Digital Versatile Disc+Recordable. Data can be written to a DVD+R disc once. Single Layer DVD+R discs hold up to 4.7 GB of data. DVD+R is faster than DVD-R.
Double Sided DVD-R and DVD+R	Double-sided DVDs have one layer on each side of the disc. Discs can store up to 8.75 GB of data.

<b>Optical Disc Type</b>	<b>Description</b>
Dual Layer DVD-R	Dual Layer Digital Versatile Disc-Recordable. A DVD-R disc that has two separate recordable layers on a single-sided disc. Dual Layer DVD-R discs can hold up to 8.5 GB of data.
Dual Layer DVD+R	Dual Layer Digital Versatile Disc+Recordable. A DVD+R disc that has two separate recordable layers on a single-sided disc. Dual Layer DVD +R discs can hold up to 8.5 GB of data. DVD+R is faster than DVD-R.
Single Layer DVD-RW	Single Layer Digital Versatile Disc-Rewritable. Data can be written to the disc multiple times. Single Layer DVD-RW discs hold up to 4.7 GB of data.
Dual Layer DVD-RW	A DVD-RW disc that has two layers of writable space with a maximum capacity of 8.7 GB for single-sided DVD-RWs and 17.08 GB for double-sided DVD-RWs. These discs are not used widely due to the cost and the release of Blu-ray.
DVD-RAM	Digital Versatile Disc-Random Access Memory. A DVD that is rewritable and erasable. You can erase or rewrite specific sections of the disc without affecting other parts of the disc. Often used for backup storage.
BD-ROM	Blu-ray Disc-Read Only Memory. Blu-ray discs (BD) are intended for high-density storage of high-definition video as well as data storage. BD discs have a capacity of up to 128 GB, depending on the number of layers. Each layer on the disc has a capacity of 25 GB. Newer discs have the capability of holding up to four layers of storage.
BD-R	Blu-ray Disc-Recordable (BD-R). Data can be written to BD-R once. BD discs have a capacity of up to 128 GB, depending on the number of layers.
BD-RE	Blu-ray Disc-Recordable Erasable. BD-RE is a disc that can be written to as well as erased. Data can be written to and erased from the disc many times without compromising the integrity of the disc or the data stored on it. BD discs have a capacity of up to 128 GB, depending on the number of layers.

## Optical Drives

An *optical drive* is an internal or external disc drive that reads data to and writes data from an optical disc. Internal optical drives generally have a 5.25-inch form factor.

### Types of Optical Drives and Burners

Optical drives include CD, DVD, and Blu-ray drives. Some optical drives provide only read capabilities, while others enable users to write, or burn, data to optical discs. CD, DVD, and Blu-ray drives have varying characteristics and specifications.

<b>Optical Drive Type</b>	<b>Description</b>
CD	CDs are widely used to store music and data. To meet the audio CD standard, the CD drive on a computer must transfer data at a rate of at least 150 KBps. Most CD drives deliver higher speeds: at least eight times (8x) or sixteen times (16x) the audio transfer rate. There are also drives with much higher transfer rates, up to 52x. CD drives use one of two special file systems: Compact Disc File System (CDFS) or Universal Disc Format (UDF).

<b>Optical Drive Type</b>	<b>Description</b>
DVD	DVD drives access data at speeds from 600 KBps to 1.3 MBps. DVD drives use UDF as the file system. If you plan to take advantage of dual-layer technology, you must use a dual-layer-enabled DVD burner with dual-layer DVD media.
Blu-ray	Named for the blue laser it uses to read and write data, Blu-ray drives read and write data from Blu-ray discs. The wavelength of the blue laser is shorter than that of the red laser used in previous optical drives, so data can be more tightly packed on a Blu-ray disc. Blu-ray uses UDF v2.5.
Combination drives and burners	A combination drive, also referred to as a combo drive, can read and write to a number of different optical disc types. Older combo drives were equipped with the read/write function for CDs only, but could also read DVDs. However, most combo drives today are primarily DVD-RW burners that also have the ability to read/write CDs and Blu-ray discs. Depending on your needs, you may require a combo drive that can also support the use of dual-layer DVD-RW discs. Depending on the manufacturer, some combination Blu-ray drives and players can also read/write to CDs and DVDs. It is a best practice to check the specific manufacturer's drive capabilities to verify which media the device can support.

## Tape Drives

A *tape drive* is a storage device that stores data magnetically on a tape that is enclosed in a removable tape cartridge. Data on the tape must be read sequentially. Sizes for external tape drives vary, but internal drives have a 5.25-inch form factor. Tape drives are most commonly used to store backup copies of archived, offline data in large data centers and are almost never used with desktop computers.



**Figure 1–13:** A tape drive.

The capacity for tape cartridges varies, but high-end tapes can store up to 10 TB of uncompressed digital data.

Relatively recent technological advances made by IBM have allowed for data on tapes to be accessed and read in a file format method similar to other storage media, such as optical discs and flash drives. The specification is called *Linear Tape File Systems (LTFS)*. LTFS is a tape format that determines how data is recorded on tape and how specialized software will read that data. LTFS works in conjunction with Linear Tape-Open (LTO) tape technology, which is an open-standards magnetic tape data storage technology.

## eMMC

An *embedded Multi-Media Controller (eMMC)* is a storage component that contains flash memory and a flash memory controller integrated onto the same silicon die. The eMMC solution consists of at least three components:

- A MMC (multimedia card) interface
- Flash memory
- A flash memory controller

Today's embedded applications such as digital cameras, smartphones, and tablets almost always store their content on flash memory. In the past, a dedicated controller managed the reading and writing of data, driven by the application's CPU. As technology evolved to support increased storage density, it became inefficient for the controller to manage these functions from outside the flash memory die. eMMC was developed as a standardized method for bundling the controller into the flash die. The eMMC standard also supports features such as secure erase and trim and high-priority interrupt to meet the demand for high performance and security.

# ACTIVITY 1–2

## Identifying Storage Devices

### Scenario

In this activity, you will identify storage devices.

- 
1. Your instructor might provide you with examples of storage devices and ask you or other participants to identify them.
  
  2. Which storage device records data magnetically and is most often used for backups?
    - FDD
    - HDD
    - Optical disc drive
    - Tape drive
    - SSD
  
  3. What is the primary benefit of using solid state storage?
  
  
  4. Which two media types allow you to write to an optical disc only once?
    - CD-ROM
    - CD-R
    - CD+RW
    - DVD+R
    - DVD-RW
  
  5. True or False? No optical disc can hold more than 50 GB of data.
    - True
    - False
  
  6. Which features are characteristic of SSHDs?
    - Solid state memory used to cache most-accessed data.
    - Boot speed is diminished.
    - Faster data access than with magnetic disks.
    - Lower cost than pure solid state storage.
-

# TOPIC C

## Mobile Digital Devices

In the last topic, you identified storage devices. Another category of hardware that you will encounter as an IT technician includes portable devices like laptops, tablets, and similar mobile devices. In this topic, you will identify mobile digital devices.

Not only has mobile technology reached a new level of performance and portability, but also the use of these devices is on the rise every day. As a certified A+ technician, you will be expected to understand how these devices work and how they should be deployed within the workplace. A good place to start is to differentiate between the various mobile devices available today.

### Mobile Digital Devices

A *mobile digital device* is an electronic device that provides computing power in a portable format. Common characteristics of mobile digital devices include:

- A small form factor. Some sources restrict the size to being hand-held and less than two pounds in weight, while others include larger, but still portable items such as laptops and notebook computers.
- Wireless network connectivity. Mobile digital devices have at least one wireless network interface, which can use Wi-Fi, cellular networking, or other technologies that connect to the Internet and other data networks.
- Local nonremovable data storage. In many cases, mobile digital devices use solid state storage, eMMC, and other variations of flash memory to store data.

There are many types of mobile digital devices, including:

- Laptops and notebook computers
- Tablet computers
- Smartphones
- Phablets
- Wearable technology
- e-Readers
- Smart cameras
- GPS devices

### Laptops

A *laptop* is a complete computer system that is small, compact, lightweight, and portable. All laptops have specialized hardware designed especially for use in a smaller portable system, use standard operating systems, can run on battery or AC power, and can connect to other devices. Laptops and their components can vary by the following factors:

- Size of the device. Smaller models are referred to as notebooks or sub-notebooks and typically have fewer features.
- Display size, quality, and technology.
- Keyboard size, number of keys, and additional options.
- Pointing device used.
- Power supply type.
- Battery type used.
- Length of battery support time.
- How long it takes to recharge the battery.

- Power cord connection and power source options.
- Docking solutions.
- Connections for external peripherals.
- Location of the power button. The power button can be located inside or outside of the closed case. It is more often located inside so that it is not accidentally turned on when it is in the user's briefcase or being transported in some other bag.
- Bays or connections for additional drives such as optical drives.



**Figure 1-14:** A laptop.

## Tablets

A *tablet* is a mobile device that includes a touch screen display, a virtual keyboard, and flash memory for data storage.

Tablets can range in size from larger tablets that look like a traditional laptop with a touch screen to small notebook-sized mobile devices that operate similarly to a smartphone, but are a bit larger and have more computing power. Just like smartphones, tablets can run different operating systems depending on the manufacturer:

- iOS® runs on both Apple's iPad® and iPod touch®.



**Note:** Because of its size and functionality, iPod touch is not considered a tablet, even though it includes many features that tablets offer.

- The Android™ OS is used in several different tablets, including Amazon™ Kindle Fire™, Samsung™ Galaxy tablets, and Toshiba Excite™.
- Microsoft Windows 7, 8, 8.1, and 8.1 RT are used on various Windows-based tablets.
- BlackBerry® OS is used on the BlackBerry PlayBook™.

For a complete list of tablets and operating systems, visit [www.tabletpccomparison.net](http://www.tabletpccomparison.net).

## Smartphones

A *smartphone* is a mobile digital device that combines the functionality of a portable phone with that of media players, GPS navigation units, personal digital assistants (PDAs), and cameras. Special mobile operating systems enable the use of apps that extend the base functionality of the smartphone even further. New smartphones are emerging almost every day. The market is expanding, and demand for powerful mobile devices has never been higher. While Android and iOS dominate the smartphone marketplace, there are many other technologies and devices available.

As an A+ technician, it can be challenging to keep up with the mobile device market as it is constantly changing and there are so many different smartphones, all with unique features and functions. The following are the most popular devices used in the marketplace.

Type of Smartphone	Description
iPhone	<p>iPhones are a combination of a phone, an Internet gadget, and a widescreen iPod, which runs on the iOS operating system. Apart from the more common features of a telephone, music player, camera, and games, the latest iPhone includes features such as video conferencing and Siri®—a voice-controlled software assistant to perform various tasks and run other applications through a multitouch interface.</p> <p>iPhone apps use innovative iOS technology to facilitate Wi-Fi Internet connectivity with <i>General Packet Radio Service (GPRS)</i>, an intuitive user interface, GPS, the accelerometer, audio, video and graphic capabilities, and other advanced features.</p>
Android smartphones	<p>Android-based smartphones have functions similar to the iPhone, except that the Android OS allows multiple applications to run simultaneously without interruption. Popular Android-based smartphones include:</p> <ul style="list-style-type: none"> <li>• Samsung™ Galaxy S® 6 Edge</li> <li>• MOTOROLA® DROID Turbo</li> <li>• HTC One™ M9</li> </ul>
Windows smartphone	<p>Windows smartphones run on the Windows Phone OS, which is maintained and developed by Microsoft. Features include a suite of Microsoft® Office® applications, Outlook® Mobile, web browsing, Windows Media® Player, and other advanced features.</p>

## Phablets

A *phablet* is a mobile digital device that is typically larger than a smartphone and smaller than a tablet. A phablet's screen generally measures from 5 to 7 inches on the diagonal. This screen size lends itself to viewing multimedia files and intensive web browsing. Some phablets include a stylus for drawing and writing.



*Figure 1–15: Phablets are larger than phones but smaller than tablets.*



**Note:** The term "phablet" is an industry term that was used to describe the Samsung Galaxy Note®. Some experts believe that the term is being phased out in favor of phone or smartphone.

## Wearable Technology

*Wearable technology* includes small mobile computing devices that are designed to be worn under, with, or on top of a person's clothing.

Common examples of wearable technology include:

- *Smart watches*, which are multipurpose devices that run computing applications and are worn on a person's wrist. Smart watches use wireless communication technology to communicate with a smartphone so that they can alert the wearer to missed messages or calls.
- Fitness monitors, which include activity trackers that record data such as the number of steps taken in a day or the heart rate and pulse of the wearer.
- Glasses and headsets, which provide access to hands-free, voice activated computing capabilities.

## Smart Cameras

A *smart camera* is a digital camera that includes a processor, memory, cellular and Wi-Fi support, and a mobile operating system. Smart cameras often include apps for editing, organizing, and storing photos.



Figure 1-16: A smart camera.

## e-Readers

An *e-reader* is a mobile digital device designed primarily for reading digital publications such as e-books and digital periodicals. Most e-readers are similar in size to tablets, but they might not have the same feature set. They can hold hundreds of digital publications that the reader can access repeatedly. Most e-readers have enhanced readability to support reading in sunlight, as well as a longer battery life.

## GPS Devices

A *global positioning system (GPS) device* is a mobile digital device that provides navigational directions to reach specified destinations. Features commonly included on GPS devices include:

- Destination search capabilities.
- Routing and rerouting instructions.
- Hands-free calling.
- Real-time traffic information.
- Integration with contacts and social media.

## ACTIVITY 1–3

### Identifying Mobile Digital Devices

#### Scenario

In this activity, you will identify mobile digital devices.

---

1. What do you think are the two most popular types of mobile digital devices?
  
  2. What types of wearable technology have you experienced? If possible, share your experience with the other participants.
  
  3. Which other mobile devices do you have experience with?
  
  4. Do you have a preference for which mobile OS you use?
-

# TOPIC D

## Connection Interfaces

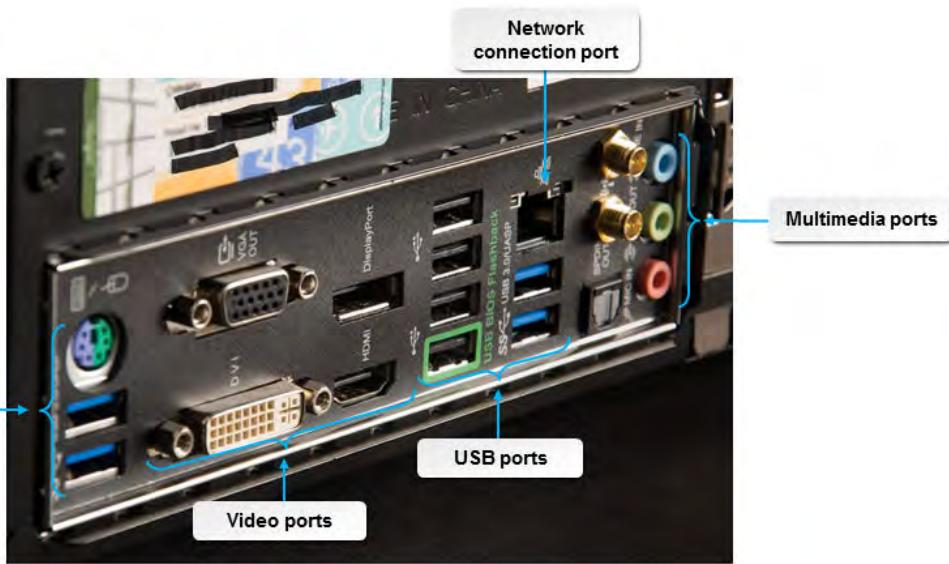
So far in this course, you have identified the common components that make up a personal computer (PC), as well as commonly used mobile digital devices. Next, you need to be able to identify how components are connected together to form a complete computer system. In this topic, you will compare PC and device connection interfaces and their characteristics.

A PC is made up of many different components. All of these components need to be able to communicate with each other so that the computer can function properly. As PCs have evolved over the years, several connection technologies have been implemented to provide communication among computer components. As a computer technician, identifying the methods used to connect devices to a computer will enable you to install, upgrade, and replace PC components quickly and effectively.

### Physical Ports

An *interface* is the point at which two devices connect and communicate with each other. A *port* is a hardware interface that you can use to connect devices to a computer. The port can also be referred to as an endpoint.

The port transfers electronic signals between the device and the system unit. A port is either an electrically wired socket or plug, or it can be a wireless transmission device. Ports can vary by shape, by color, by the number and layout of the pins or connectors contained within the port, by the signals the port carries, and by the port's location. Ports exist for both internal and external devices. External ports often have a graphical representation of the type of device that should be connected to it, such as a small picture of a monitor adjacent to the video port.



**Figure 1-17: Ports.**

### Genders

Most ports and the cables that connect to them have genders. For example, most computer ports are jacks, into which you plug in the matching cable. The computer's jacks are most often the female connectors and the cable's plug is most often the male connector. You can always look directly at

the innermost electrical connections on the connectors to determine the gender. The one with the protruding pins is the male and the one with the holes to accept the pins is the female.

## Computer Connections

*Computer connections* are the physical access points that enable a computer to communicate with internal or external devices. They include the ports on both the computer and the connected devices, plus a transmission medium, which is either a cable with connectors at each end or a wireless technology. Personal computer connections can be categorized by the technology or standard that was used to develop the device.

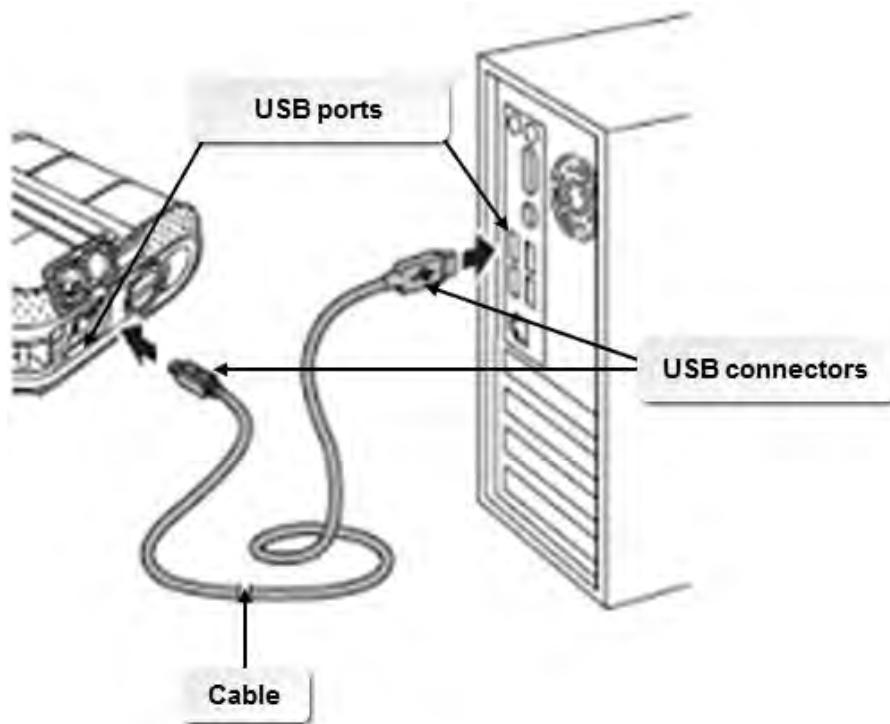


Figure 1–18: A computer connection.

## Characteristics of Connection Interfaces

Device connections are often described and distinguished from one another by the following characteristics:

- Whether they carry analog or digital signals.
  - *Analog transmissions* carry information in the form of a continuous wave. Analog signals are most often generated by electrical current, the intensity of which is measured in volts. An analog signal oscillates over time between maximum and minimum values and can take on any value between those limits. The size, shape, and other characteristics of that *waveform* describe the analog signal and the information it carries.
  - *Digital transmissions*, unlike analog transmissions, which can have many possible values, hold just two values—ones and zeroes. These values represent an on and off state, respectively. Digital data, which is a sequence of ones and zeroes, can be translated into a digital waveform. In computer systems and other digital devices, a waveform switches between two voltage levels representing 0 and 1.
- The distance limitations of the associated media, such as cables.
- Their data transfer speeds.

- Signal quality. This can include the likelihood of dropped connections, garbled transmissions, lag or latency, slow connections, and susceptibility to interference.
- Their support for *digital rights management* (DRM) capabilities. DRM is a way to control access to copyrighted content that is presented in digital format. Used to protect content such as e-books, digital video and music, and even software programs, DRMs establish a copyright for a piece of content, manage the distribution of that copyrighted content, and control what the consumer can do with that content once it has been distributed.
- Their *frequencies*. For analog signals, frequency is the number of complete cycles per second in a wave. For digital signals, frequency is often cited for wireless (radio) communication, as different types of wireless communication operate at distinctly different frequencies.

## USB Connections

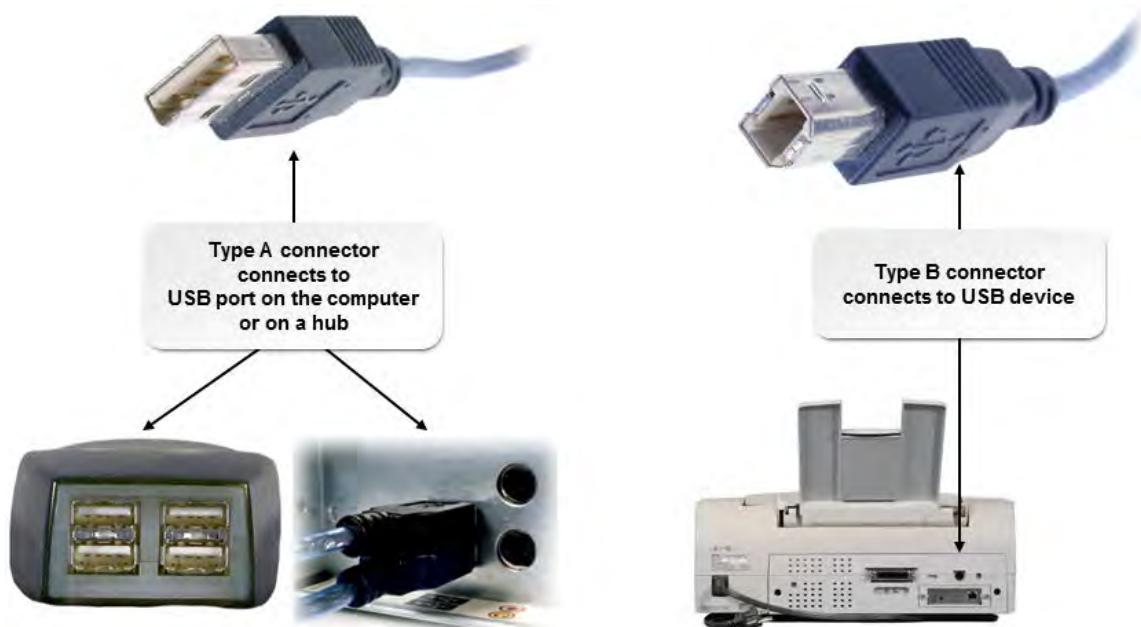
A *universal serial bus (USB) connection* is used to connect multiple computer peripherals to a single port that provides high performance and minimal device configuration. USB standards delineate high-speed wired communication between a host computer and device peripherals. USB connections support two-way communications and hot-plugging, which allows you to install peripherals without powering down the computer. All PCs today have multiple USB ports and can, with the use of USB hubs, support up to 127 devices per port.

A USB interface consists of ports, cables, and connectors. The USB Implementers Forum (USB-IF) standardized the interface and the original standard defined two types of connectors: the 4-pin Type A and Type B. Type A connectors are used only on host devices that provide power, such as the USB ports on the back of a computer or the side of a laptop. Type B connectors are used for peripheral devices that receive power, such as printers.

There are several versions of USB connectors. The standard for USB 2.0 defined a smaller, 5-pin version of the Type B connector called the Mini-B connector, for use with personal electronic devices such as digital cameras and mobile phones. An update to the specification defined the Micro-A and Micro-B connectors, which also have five pins and are widely used in thinner smartphones, GPS units, digital cameras, MP3 players, game controllers, readers, tablets, and other mobile devices. The Micro-A connector plugs into a computer or AC charger, and the Micro-B connector connects to the peripheral device.

A supplement extends the USB 2.0 standard to enable point-to-point communication between two USB devices: one USB On-The-Go (OTG) device and another OTG or standard USB device. OTG-enabled devices, also called dual role devices, can function either as the host or peripheral when cabled together or when a device like a flash drive connects directly to another device such as a smartphone. OTG devices have an AB socket that accepts an OTG micro USB A or B plug.

The USB 3.0 standard boasts high data transfer rates and uses USB 3.0 Type A and Type B connectors, which have five more connection pins recessed in the connector. The pins consist of differential transmit and receive pairs and a ground. Also, the pin design allows for backward compatibility with USB 2.0 and 1.1. USB 3.0 supports high-performance SSD drives, video, and audio equipment.



*Figure 1–19: USB connections.*



*Figure 1–20: USB connection types.*

USB connections transfer data serially, but at a much faster throughput than legacy serial connections. USB devices also incorporate Plug-and-Play technology that allows devices to self-configure as soon as a connection is made.

There are currently three versions of the USB standard: 1.1, 2.0, and 3.0.

- The original USB 1.0 standard, also called low-speed, has a data transfer speed of 1.5 Mbps, which was suitable for non-gaming USB mice and keyboards. USB 1.0 is deprecated.
- USB 1.1, also called full-speed, is still commonly found in devices and systems. USB 1.1 uses half-duplex communication.
- USB 2.0, also called high-speed, was released in April 2000, and is the most commonly implemented standard. USB 2.0 supports low-bandwidth devices such as keyboards and mice, as well as high-bandwidth devices such as scanners, multi-function printers, and high-resolution webcams. A USB 2.0 device connected to a USB 1.1 hub or port will communicate at only USB 1.1 speeds, even though it might be capable of faster speeds. Generally, the operating system will inform you of this when you connect the device. USB 2.0 uses half-duplex communication.
- The USB 3.0 specification, also called SuperSpeed USB and identified as Gen1 was released in November 2008. It is 10 times faster than the USB 2.0 standard, has enhanced power efficiency, and is backward compatible with USB-enabled devices currently in use. USB 3.0 provides full

duplex communication by using two unidirectional data paths for sending and receiving data simultaneously.

- The USB 3.1 specification, identified as Gen 2 or SuperSpeed +, was released in July 2013, and supports speeds up to 10 Gbps with the ability to provide up to 100 watts of power to connected devices.

Characteristics of each version are described in the following table.

<b>Characteristic</b>	<b>USB 1.1</b>	<b>USB 2.0</b>	<b>USB 3.0</b>	<b>USB 3.1</b>
Analog or digital?	Digital	Digital	Digital	Digital
Distance limitations	Maximum cable length 3 meters with devices operating at low speed (1.5 Mbps); maximum cable length of 5 meters with devices operating at full speed (12 Mbps)	Maximum cable length 5 meters	Maximum cable length recommended 3 meters	Maximum cable length recommended 3 meters
Data transfer speed	Up to 12 Mbps	Up to 480 Mbps when connected to USB 2.0 hubs or ports Up to 12 Mbps when connected to USB 1.1 hubs or ports	5.0 Gbps	Up to 10 Gbps
Quality	Low speed mode is less susceptible to electromagnetic interference (EMI) half-duplex communication	Poor signal integrity at its highest data transfer speed due to reflections.	Very short latency and brief jitter.	Very short latency and brief jitter.
Frequencies	48 MHz	48 MHz	Uses spread spectrum clocking on its signaling, which produces a broad spectrum of radio frequency (RF) radiation energy over a large frequency band. This can create noise in the 2.4 GHz band used widely for wireless peripheral devices.	Uses spread spectrum clocking on its signaling, which produces a broad spectrum of radio frequency (RF) radiation energy over a large frequency band. This can create noise in the 2.4 GHz band used widely for wireless peripheral devices.



**Note:** For USB 1.1 and 2.0, to work around the distance limitations, you can use up to five hubs to create a chain to reach the necessary cable length.

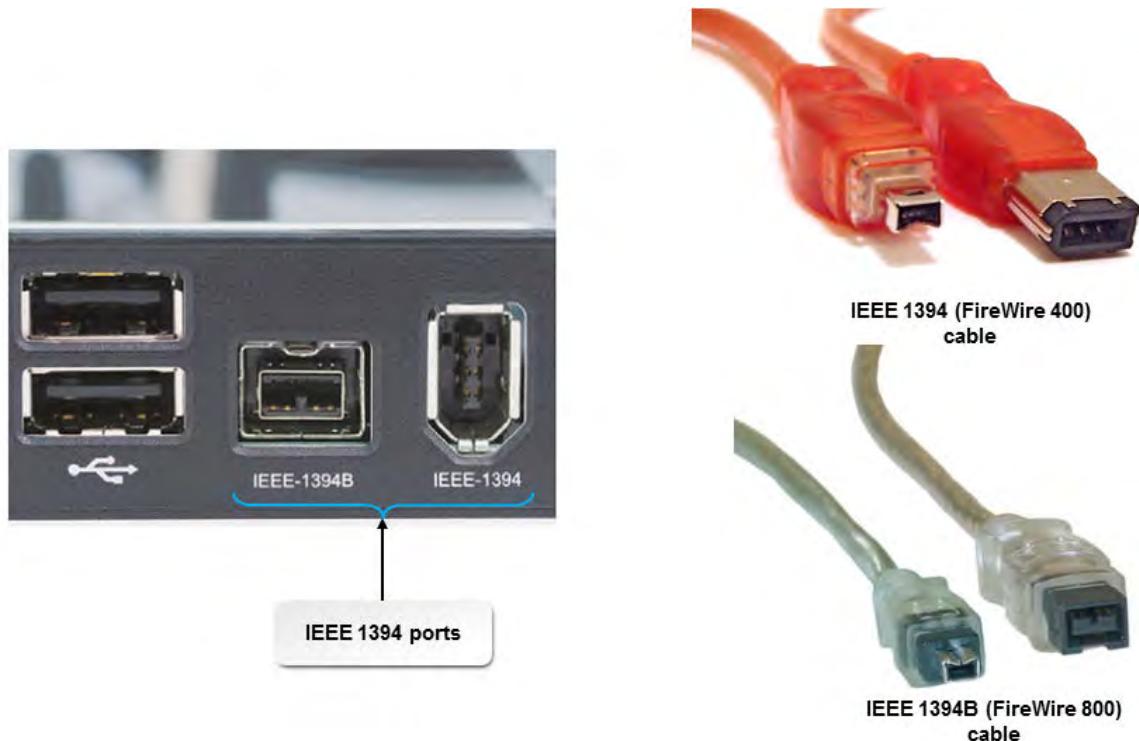
## IEEE 1394 Connections

An *IEEE 1394 connection* is a PC connection that provides a high-speed interface for peripheral devices that are designed to use the *Institute of Electrical and Electronic Engineers (IEEE) 1394 standard*. Products that conform to this standard include Apple Inc.'s FireWire®, Texas Instruments' Lynx™, and Sony Corporation's i.LINK®.

IEEE 1394 can support up to 63 devices on one port, supports Plug-and-Play device discovery, supports hot plugging, and can provide power to devices. IEEE 1394 is often used to connect peripherals such as external hard drives, digital cameras, and digital video camcorders.

Like USB, IEEE 1394 encompasses multiple versions of standards.

- The original 1394 standard was released in 1995 and is now more commonly referred to as FireWire 400. It specified the 6-conductor alpha connector.
- IEEE 1394a was released in 2000. In addition to feature enhancements, it introduced the 4-conductor alpha connector.
- IEEE 1394b was released in 2002 and is more commonly known as FireWire 800. It introduced the 9-pin beta connector, which is incompatible with legacy cables. Bilingual cables are available to overcome this limitation.



**Figure 1-21: IEEE 1394 ports and connectors.**

Characteristics of each version are described in the following table.

Characteristic	IEEE 1394	IEEE 1394B
Analog or digital?	Digital	Digital
Distance limitations	Maximum cable length 4.5 meters	Maximum cable length 100 meters

<b>Characteristic</b>	<b>IEEE 1394</b>	<b>IEEE 1394B</b>
Data transfer speed	400 Mbps	800 Mbps
Quality	Can use isochronous data transfer to coordinate data flow rates and application timing. This reduces buffering in multimedia applications, video and audio streams.	Reduced buffering using isochronous data transfer.
Frequencies	33 MHz	25 MHz

## Thunderbolt Connections

A *Thunderbolt connection* is a high-speed I/O technology interface that consists of a host controller that joins together PCI-Express data and/or DisplayPort video. The combined signal is sent via a full-duplex pair of differential signals. that supports connecting a wide variety of peripheral devices to PCs. Cabling is available in both optical fiber and copper wire. A Thunderbolt connection can support up to six peripheral devices, including full 4K video displays, audio, external graphics, and storage devices.



Figure 1-22: Typical Thunderbolt connections.

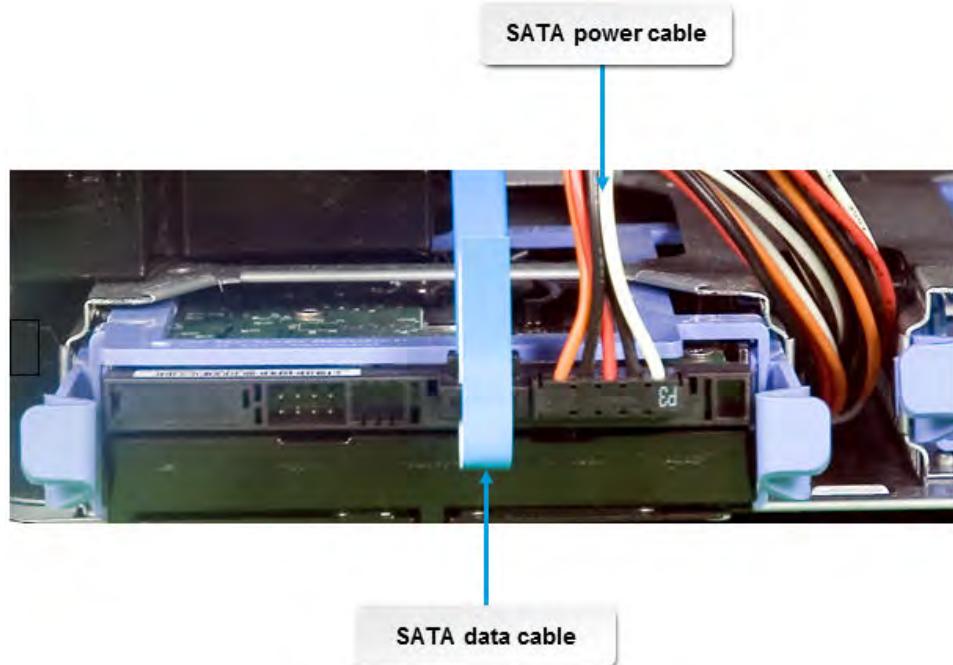
The following table describes the characteristics of Thunderbolt connections.

<b>Characteristic</b>	<b>Value</b>
Analog or digital?	Digital
Distance limitations	<ul style="list-style-type: none"> <li>For copper wire: 3 meters.</li> <li>For optical fiber: 60 meters.</li> </ul>
Data transfer speed	<ul style="list-style-type: none"> <li>Version 1: 10 Gbps per channel, for a total of 20 Gbps.</li> <li>Version 2: 20 Gbps per channel, for a total of 40 Gbps.</li> <li>Version 3: 40 Gbps per channel, for a total of 80 Gbps.</li> </ul>
Quality	Thunderbolt devices transfer isochronously (steady stream), making both audio and video very precise in real-time.
Frequency	430 kHz fixed switching frequency

## SATA Connections

A *SATA connection* is a drive connection standard that provides a serial data channel between the drive controller and the disk drives. SATA transfer speeds are much higher than legacy hard drive

connections for the same drive technologies. SATA's physical installation is also easier because the SATA power and data cables are much smaller, thinner, and more flexible than legacy ribbon cables. SATA connectors have seven pins.



**Figure 1-23: SATA connections.**

External SATA (*eSATA*) is an external interface for SATA connections. Like USB and IEEE 1394, it provides a connection for external storage devices. eSATA connections provide fast data transfers without having to translate data between the device and the host computer. eSATA interfaces do require an additional power connector to function. You can provide eSATA functionality by installing eSATA cards in systems.

Characteristics of SATA connections are described in the following tables.

Characteristic	Value
Analog or digital?	Digital
Distance limitations	1 meter

Data transfer speeds vary with the version of SATA being used.

Version	Characteristics
SATA 1.5Gb/s (SATA I)	<ul style="list-style-type: none"> <li><b>Frequency:</b> 37.5 MHz</li> <li><b>Transfer speed:</b> 1.5 Gb/s</li> <li><b>Interface throughput:</b> 150 MB/s</li> </ul>
SATA 3Gb/s (SATA II)	<ul style="list-style-type: none"> <li><b>Frequency:</b> 75 MHz</li> <li><b>Transfer speed:</b> 3.0 Gb/s</li> <li><b>Interface throughput:</b> 300 MB/s</li> <li>Backwards-compatible with SATA 1.5Gb/s</li> </ul>

<b>Version</b>	<b>Characteristics</b>
SATA 6Gb/s (SATA III)	<ul style="list-style-type: none"> <li>• <b>Frequency:</b> 150 MHz</li> <li>• <b>Transfer speed:</b> 6.0 Gb/s</li> <li>• <b>Interface throughput:</b> 600 MB/s</li> <li>• Backwards-compatible with SATA 1.5Gb/s and SATA 3Gb/s</li> </ul>
SATA 16Gb/s (version 3.2)	<ul style="list-style-type: none"> <li>• <b>Transfer speed:</b> 16.0 Gb/s</li> <li>• <b>Interface throughput:</b> 1969 MB/s</li> </ul>
eSATA	<ul style="list-style-type: none"> <li>• External SATA connectivity</li> <li>• <b>Transfer speed:</b> 3.0 Gb/s</li> <li>• <b>Interface throughput:</b> 30 MB/s</li> </ul>

## Display Cables and Connector Types

Several types of cables and connectors are used to connect display devices to PCs. Here are the most common:

- *Video Graphics Array (VGA)* is a display standard that is implemented with a 15-pin DE-15 connector. You can find this connector type on many video cards, computer monitors, and high definition television sets. On laptop computers and other small devices, a mini-VGA port is sometimes used in place of the full-sized VGA connector.
- *High Definition Multimedia Interface (HDMI)* is a proprietary audio/video interface for transferring uncompressed video data and compressed or uncompressed digital audio data from a display controller to a compatible peripheral device (such as a display monitor, a video projector, digital TV, or digital audio device) over a single HDMI cable.
- *Digital Visual Interface (DVI)* is a video standard for transferring both analog and digital video signals. You can find this connector type on high-definition TVs, DVD players, home theater systems, and computer monitors.

Characteristics of these display connections are listed in the following table.

<b>Characteristic</b>	<b>VGA</b>	<b>HDMI</b>	<b>DVI</b>
Analog or digital?	Analog	Digital <ul style="list-style-type: none"> <li>• HDMI Video Card</li> <li>• Connectors:</li> <li>• Type A: 19-pin connector that supports all High Definition (HD) modes; electrically compatible with single-link DVI-D connectors</li> <li>• Type B: A 29-pin connector; double video bandwidth of Type A; supports very high resolutions</li> <li>• Type C: Mini-HDMI connector used in portable devices</li> <li>• Type D: Micro-HDMI is the smallest connector and also is used in portable devices</li> </ul>	<ul style="list-style-type: none"> <li>• Analog: DVI-A</li> <li>• Digital: DVI-D</li> <li>• Both: DVI-I: Digital and analog</li> <li>• DVI-DL: Doubles the number of transition minimized differential signaling (TMDS) pairs which doubles video bandwidth. TDMS is a high-speed serial link. There are dual-link versions for digital DVI-I and DVI-D</li> <li>• M1-DA (also called M1): Can support digital, analog, and USB control signals</li> </ul>
Distance limitations	30 meters for low resolutions; 5 meters for higher resolutions	5 meters	15 meters for low resolutions; 5 meters for higher resolutions
Frequencies	Need a frequency of at least 60 Hz (refreshing the screen 60 times per second so the images appear constant to the human eye). To make a full frame of pixels fit within one sixtieth of a second, the speed at which pixels are transmitted needs to be adjusted. This speed is called the pixel clock.	HDMI 2.0 specification (2013) increases bandwidth to 18 Gbps; supports resolutions up to 4K (4 times the clarity of 1080 p/60 video resolution; up to 1536 kHz audio sample frequency	In single-link mode, the maximum pixel clock frequency is 165 MHz that supports a maximum resolution of 2.75 megapixels at 60 Hz refresh
Connector			

## Other Connections

In addition to the connectors and cables already discussed in this topic, you are likely to encounter other types of connectors and cables for attaching peripherals to PCs, the most common of which are described in the following table.

Connector	Description
-----------	-------------

Analog audio connectors	Analog audio splits sound into "Left" and "Right" components, or stereo sound. Analog audio cables are split with red and white RCA-style connectors at the end.
-------------------------	--



**Note:** RCA cables with three connectors, where the third connector is yellow or black, are used for audio/video connections.

Characteristics:

- Analog or digital: Analog
- Distance limitations: Depends on cable capacitance and the source impedance of the device, but a practical maximum cable length is around 30 meters.
- Data transfer speed: Varies by interface
- Quality: Unless using a well-shielded cable, prone to EMI interference which can show up as static, popping noises, or hissing sounds, The voltage-based signal degrades after 30 meters.

<b>Connector</b>	<b>Description</b>
Digital audio connectors	Digital audio transmits Dolby® Digital, which can support front center, right, and left speakers as well as rear right, left, and center speakers. Digital audio cables and connectors are generally either coaxial or optical (TOSLINK).



**Coaxial cable and connectors for digital audio**



**Optical cable and connectors for digital audio**

#### Characteristics:

- Analog or digital: Digital
- Distance limitations: 3 meters for coaxial; 15 meters for optical
- Data transfer speed: Maximum data rate of 125 Mbps
- Quality: TOSLINK optical cables are immune to interference and optical audio connections do not suffer from distortion or signal losses from resistance or capacitance unlike copper-based connections.

<b>Connector</b>	<b>Description</b>
RJ-45 connectors	<p>The RJ-45 is an eight-pin connector found on twisted pair cables that are used in networking.</p>  <p>Characteristics:</p> <ul style="list-style-type: none"> <li>• Analog or digital: Digital</li> <li>• Distance limitations: 100 meters for Category 5 Ethernet cabling</li> <li>• Data transfer speed: Depends on the type of cabling the connector is attached to</li> <li>• Quality: The strip-line flex technology within RJ45 jacks lowers the impedance path significantly. This virtually eliminates crosstalk within the connector.</li> <li>• Connector and cable specifications for frequencies: <ul style="list-style-type: none"> <li>• Cat 5: Up to 100 MHz</li> <li>• Cat 5e: Up to 100 MHz</li> <li>• Cat 6: up to 250 MHz</li> </ul> </li> </ul>
RJ-11 connectors	<p>The RJ-11 connector is used for telephone system connections. However, because the RJ-11 connector is similar in appearance to the RJ-45 connector, they are sometimes confused. RJ-11 connectors are smaller than RJ-45 connectors, and have either four or six pins.</p>  <p>Characteristics:</p> <ul style="list-style-type: none"> <li>• Analog or digital: Analog</li> <li>• Distance limitations: Average of 100 meters</li> <li>• Data transfer speed: 10 Mbps</li> <li>• Frequency: supports Transmission speed of 16 MHz</li> <li>• Quality: Transmission errors if pushed to faster speeds.</li> </ul>

<b>Connector</b>	<b>Description</b>
PS/2 connectors	The PS/2 connector is a legacy connection technology used primarily to connect keyboards and mice to system units.



Characteristics:

- Analog or digital: Digital
- Distance limitations: 7.6 meters
- Data transfer speed: 2 Kbps
- Quality: Lower latencies for keyboards than early USB (specification 1.0) because USB polls the host controller and ps/2 does not.

## SPDIF and TOSLINK

SPDIF (also written as S/PDIF) stands for Sony Phillips Digital Interconnect Format, also known as Sony Phillips Digital Interface. SPDIF is a digital format signal used to carry digital audio. It is used to connect audio devices to output audio signals over a short distance. SPDIF can be used with optical fiber TOSlink (Toshiba Link) cables or with coax cables that have RCA connectors. Typically, these connections are found on home audio equipment, but some home theater computers also include SPDIF connections. It is often used to carry 5.1 or 7.1 signals in a surround sound home theater setup.

## Adapters and Converters

With the various types of connections available for PCs and their peripheral devices, you are very likely to encounter situations where you might have a cable that is not compatible with the port to which it needs to connect, or situations where a signal needs to be modified to transfer among different hardware components. The most common adapters and converters include those described in the following table.

Adapter or Converter	Description
----------------------	-------------

DVI to HDMI adapter      A DVI to HDMI adapter enables you to connect a PC that has a DVI port to a HD TV that has an HDMI port. You can connect the adapter to either a DVI cable or an HDMI cable.



DVI to VGA converter      A DVI to VGA converter enables you to convert a DVI (digital) video signal so that it can be displayed on a VGA (analog) monitor.



HDMI to VGA converter      An HDMI to VGA converter enables you to convert an HDMI (digital) video signal so that it can be displayed on a VGA (analog) monitor.



<b>Adapter or Converter</b>	<b>Description</b>
PS/2 to USB adapter	A PS/2 to USB adapter enables you to connect a PS/2-type keyboard or mouse to a computer that has no PS/2 ports. The adapter connects the PS/2 wires to the approximate USB wires. These adapters do not use specific software drivers.



PS/2 to USB converter	A PS/2 to USB converter uses an integrated circuit (pre-programmed chip) to actively translate the PS/2 keyboard signal and convert it into a USB keyboard signal. This allows the PS/2 keyboard to be automatically recognized by the operating system as if it were a standard, modern USB keyboard. A well-designed active PS/2 to USB converter will use the built-in operating system drivers for a USB keyboard.
-----------------------	--



Thunderbolt to DVI adapter	A Thunderbolt to DVI adapter enables you to connect a digital display device to a PC with a Thunderbolt port.
----------------------------	---



<b>Adapter or Converter</b>	<b>Description</b>
USB to Ethernet adapter	A USB to Ethernet adapter enables you to connect to a wired network through a USB port.
	
Audio to USB adapter	An audio to USB adapter enables you to connect a headset and microphone to a PC through a USB port.
	
USB A to USB B adapter	USB A to USB B adapters come in several configurations to enable you to connect USB devices that have different connector types. For instance, you can buy a USB A Female to USB B Male connector, or a USB A Female to USB B Female connector.
	



**Note:** Some adapters are implemented as dongles. A dongle is a device that connects to one of the existing ports and provides additional functionality. Examples include USB to RJ-45 and USB to Wi-Fi.

## Wireless Device Connections

Wireless is rapidly becoming the primary connection method for connecting all sorts of computer components, as well as for connecting computing devices to each other. Popular connection methods are described in the following table.

<b>Connection Method</b>	<b>Description</b>
<i>Radio frequency (RF)</i>	<p><i>Radio networking</i> is a form of wireless communication in which signals are sent via RF waves, in the 10 KHz to 1 GHz range, to wireless antennas.</p> <p>An antenna transmits by converting electrical energy into an RF wave. When an antenna receives a transmission, it converts the RF wave into electrical energy.</p> <p>In wireless communication, low-frequency data or voice signals are transmitted through high-frequency radio waves by superimposing data on them.</p>
<i>Bluetooth</i>	<p>Bluetooth® is a wireless technology that facilitates short-range wireless communication between devices, such as PCs and some of their components, laptops and some of their components, mobile phones, and gaming consoles and other gaming peripherals. Both voice and data information are exchanged among these devices at 2.4 GHz within a range of approximately 30 feet.</p> <p>Bluetooth transmits data in low-power radio waves and contains a tiny chip with a Bluetooth radio and software. Devices need to "pair" to talk to each other and exchange data. Bluetooth uses frequency-hopping spread spectrum technology to avoid interference, and it operates in the frequency range 2.402 to 2.483 GHz.</p> <p>A maximum of eight Bluetooth devices can be connected to each other at a time; this connection of two to eight Bluetooth-enabled devices is known as a <i>piconet</i>. Bluetooth devices operate at very low power levels of approximately 1 milliwatt (mW).</p>
<i>Near field communication (NFC)</i>	<p>NFC is a wireless communication method that enables wireless devices to establish radio communications by touching them together or by bringing them into close proximity with each other, typically within 10 cm or less. NFC operates at 13.5 MHz and is slower than Bluetooth. However, it consumes less power and does not require pairing.</p>

<b>Connection Method</b>	<b>Description</b>
<i>Infrared (IR)</i>	<p>IR transmission is a form of wireless transmission in which signals are sent via pulses of infrared light. IR is generally used for short-range transmission, because receivers need an unobstructed view of the sender to successfully receive the signal, though the signal can reflect off hard surfaces to reach the recipient. Typically, IR communication takes place in the near-infrared frequency range that is in the visible region of the spectrum. Therefore, in some instances, wireless IR communication is also referred to as wireless optical communication.</p> <p>IR uses electromagnetic waves with frequencies ranging from 300 GHz to 400 THz. Their wavelengths range from approximately 1 mm to 750 nm. IR waves are classified into sub-bands called far-infrared, mid-infrared, and near-infrared. The near-infrared frequencies are visible to the human eye as red or violet light, while the far-IR frequencies are not visible to the human eye but are radiated in the form of heat.</p> <p>IR technology is used in several ways in the computing and telecommunication fields. The primary application is to provide network connectivity in wireless personal area networks. IR devices facilitate short-term wireless connections between two computers or between a computer and a wireless handheld device such as a mobile phone. An IR-powered network can also be used as an extension network for a local area network where installing cable may be difficult. Wireless devices such as wireless mice, keyboards, television remote controls, and game controllers also use <i>IR waves</i> for their operation.</p>

## Allocation of the RF Spectrum

The RF spectrum is classified based on the frequency range.

<b>Frequency Range</b>	<b>Name</b>
3 Hz–30 Hz	Extremely Low Frequency (ELF)
30 Hz–300 Hz	Super Low Frequency (SLF)
300 HZ–3 KHz	Ultra Low Frequency (ULF)
3 KHz–30 KHz	Very Low Frequency (VLF)
30 KHz–300 KHz	Low Frequency (LF)
300 KHz–3000 KHz	Medium Frequency (MF)
3 MHz–30 MHz	High Frequency (HF)
30 MHz–300 MHz	Very High Frequency (VHF)
300 MHz–3000 MHz	Ultra High Frequency (UHF)
3 GHz–30 GHz	Super High Frequency (SHF)
30 GHZ–300 GHZ	Extremely High Frequency (EHF)

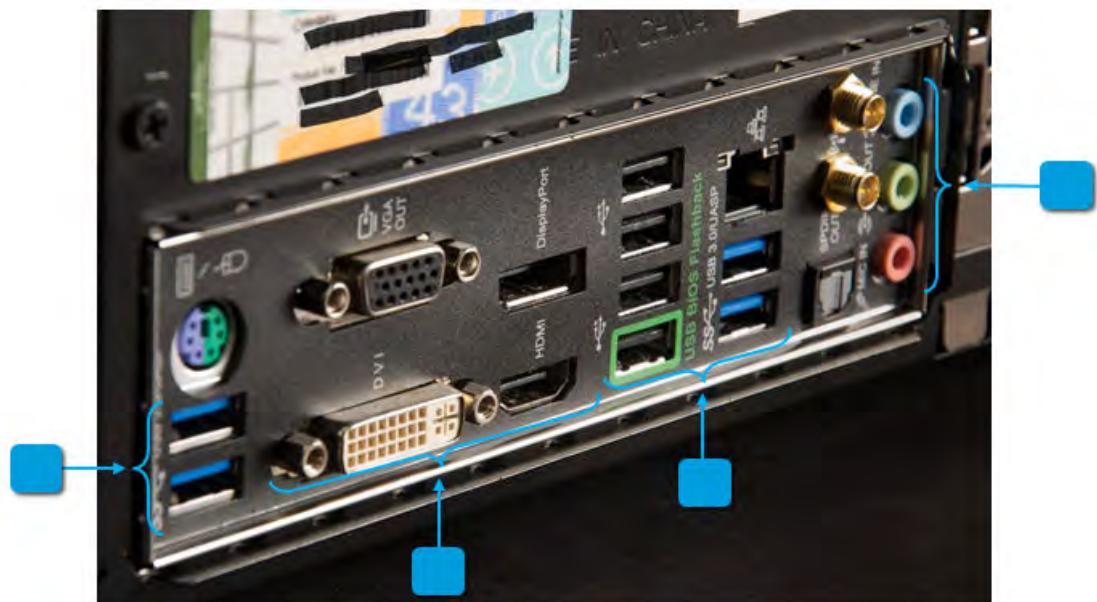
# ACTIVITY 1–4

## Comparing PC and Device Connection Interfaces

### Scenario

In this activity, you will identify and compare PC and device connection interfaces.

1. Your instructor might provide you with examples of device connections and interfaces and ask you or other participants to identify them.
2. In this graphic, identify the (A) audio ports, (B) video ports, and (C) USB ports.



3. Which connection type supports up to 127 peripherals for a single connection?
  - IEEE 1394
  - SATA
  - Parallel
  - USB
4. Which connection interface is compatible with both copper wire and optical fiber cables?
  - IEEE 1393 connection
  - SATA connection
  - Thunderbolt connection
  - DVI-D connection

5. Of the adapters and converters discussed in this topic, which do you think you might use most often?  
Be prepared to share your thoughts.
-

## Summary

In this lesson, you identified some of the hardware components that make up most personal computers, along with the types of connections used to allow the devices to communicate properly. The ability to identify hardware components and how to connect them together enables you to be more efficient when you are installing, upgrading, repairing, configuring, maintaining, optimizing, and troubleshooting PC components.

**How many of the PC components described in this lesson were familiar to you?**

**Which device connections have you used? Which are new to you?**



**Note:** Check your CHOICE Course screen for opportunities to interact with your classmates, peers, and the larger CHOICE online community about the topics covered in this course or other topics you are interested in. From the Course screen you can also access available resources for a more continuous learning experience.

2

# Operating System Fundamentals

**Lesson Time:** 2 hours

## Lesson Objectives

In this lesson, you will identify the basic components and functions of operating systems. You will:

- Identify common PC and mobile operating systems and their features.
- Identify utilities and tools used to manage PC operating systems.

## Lesson Introduction

In the previous lesson, you identified the hardware components of standard desktop personal computers. The other major element of a personal computer is the operating system, which is the software that provides the user interface and enables you to access and use the hardware components. In this lesson, you will identify the basic components and functions of an operating system.

As a professional IT support representative or PC service technician, your job will include installing, configuring, maintaining, and troubleshooting personal computer operating systems. Before you can perform any of these tasks, you need to understand the basics of what an operating system is, including the various versions, features, components, and technical capabilities. With this knowledge, you can provide effective support for all types of system environments.

# TOPIC A

## PC and Mobile Operating Systems

In this lesson, you will identify the basic components and functions of personal computer and mobile device operating systems. The first step is to learn about the various operating systems available today, and to identify those that are commonly used on personal computers, tablets, and smartphones. In this topic, you will identify the most common PC and mobile operating systems and their features.

Aside from hardware, the operating system is the next most important piece of the personal computer system or mobile device. Without a user-friendly operating system, most people would not be capable of using their computers or mobile devices to successfully perform the tasks required of them. As an IT professional, being familiar with the different types of operating systems that can be installed on personal computers and mobile devices can help you to support a variety of computer and mobile device environments.

### Microsoft Windows

Microsoft® Windows® is the single most popular and widely deployed operating system on both desktop computers and server systems in the world today. The various versions of Windows all feature a graphical user interface (GUI), support for a wide range of applications and devices, 32-bit or 64-bit processing, native networking support, and a large suite of built-in applications and accessories such as the Internet Explorer® browser. Windows currently comes pre-installed on many commercially sold PCs.

There have been numerous versions of Windows since its inception. The three most current versions are often deployed on personal and professional computers.

- Windows 8 was released in 2012, with the Windows 8.1 update released in 2013. Windows 8 introduced a new look and feel to the user interface (UI) that is designed to facilitate the use of touch screen devices as well as mouse and keyboard interaction. You can also use the familiar desktop used in previous versions of Windows. Microsoft account integration allows you to use the same settings across all of the Windows 8/8.1 systems you log into.
- Windows 7 was released in 2009. Windows 7 returned to the overall look and feel found in Windows XP in response to the criticism of the Windows Vista® interface. Rather than introduce a multitude of new features like Windows Vista, Windows 7 instead offered many critical upgrades to the system, including application and hardware compatibility, performance improvements, and a redesigned shell.
- Windows Vista was released in 2007 and included many new features, the most noticeable change being to the user interface. While it offered many upgrades to the system, specifically to security features, many were critical of the redesigned interface.



**Note:** Microsoft released the latest version of Windows, Windows 10, in 2015.

### Microsoft Retirement Schedules

To find out when Microsoft products will be retired or how long specific products will be supported, visit the Microsoft Product Lifecycle Search tool at <http://support.microsoft.com/lifecycle/search/>.

## Features of Microsoft Windows

Windows includes several features that distinguish it from other operating systems. Each version of Windows includes a unique combination of many of these features.



**Note:** Other features of the Windows operating system will be covered in more detail throughout this course.

Feature	Description
Start Screen	The central user interface of Windows 8/8.1 that acts as the hub from which you can access all of the capabilities of your computer. From the Start Screen, you can run programs, check email, add contacts, see the latest news, get updates on the weather, change the settings on your PC, sign out of your computer, go online, and much more.
Modern UI	Also known as the Metro UI, this is the user interface for Windows 8/8.1. This includes the Start Screen and its tiles. Some of the tiles change based on the content available and are known as Live Tiles.
File structure and paths	Windows has a file structure that, by default, organizes each drive and partition separately. The root of each drive/partition is assigned a letter and is in the format <letter>:\ where the default installation drive is typically C:\. Additional drives can be assigned to D:, E:, F:, and so on.  Each directory below this root is separated by the backslash character in the directory path, but modern versions of Windows can also recognize a standard slash ("/"). For example, the folder that holds much of the critical operating system files is in the path C:\Windows\system32\ by default. The maximum length for a Windows path is 260 characters.
Side by side apps	You can tile Windows 8/8.1 Modern apps side by side. <ul style="list-style-type: none"> <li>On most monitors, you can tile two apps side by side if your monitor resolution is at least 1024 x 768.</li> <li>You can tile three apps if you have at least a 1600 x 1200 resolution monitor.</li> <li>On larger monitors with at least 2560 x 1440 resolution, you can tile up to four apps side by side.</li> </ul> Each monitor connected to the computer can have side by side apps in these configurations.
Pinning	You can pin your most frequently used applications to the Start Screen or to the desktop taskbar.
Live sign in	The email address you registered with Microsoft to use when you sign in to any Microsoft program or service. This includes Windows 8/8.1 computers, services such as OneDrive or Outlook.com, Windows phones, and even Xbox.
OneDrive	The cloud storage users get with Windows 8/8.1. Saving documents to OneDrive enables users to access those documents on any device they log into using the same Live sign in they used to save the documents.
Windows Store	The application store for Windows 8/8.1, Windows Server 2012, and Windows 8 phone. The apps range from free to \$999.99. Apps in the store have been certified to be compatible with Windows 8.

Feature	Description
Multi-monitor taskbars	If you have multiple monitors, you can choose how you want applications to be listed on the taskbar. By default, all of the taskbar buttons from the main screen taskbar are duplicated on the other monitor. You can change this to show only the applications open on the second screen in that monitor's taskbar, and have all taskbar buttons still be shown on the main monitor. Another option is to only show the taskbar buttons for the applications open on each monitor.
Charms	Hidden on the right side of the screen, the Charms are universal tools that are available from everywhere in Windows 8/8.1 that give you access to key system-wide functions such as printing, searching, and sharing. Charms are dynamic and context sensitive; for instance, using the <b>Search Charm</b> within the Mail app will search through your email messages for the word or phrase you enter; using <b>Search</b> from the <b>Start</b> screen is global and will take you to the <b>All Apps</b> screen, where you can search for apps, files, and PC settings, or begin a search using an app.
Windows PowerShell	A command line interface where you can run PowerShell <i>cmdlets</i> (commandlets). You can also use cmdlets in scripts.
Aero	Windows <i>Aero</i> ® is a color scheme available in Windows Vista and Windows 7. Windows Aero provides a visually rich experience with its glossy and transparent interface. It also provides dynamic visual and animation effects such as Live Preview of taskbar buttons and a Flip 3D view of open windows. You can choose one of the predefined color schemes available in Windows Aero, or you can create a custom color scheme using the color mixer. Each color has a default transparency level that you can change for both predefined and custom color schemes. This feature was not carried over to Windows 8/8.1.
Gadgets	The Desktop Gadget Gallery is a Windows Vista and Windows 7 feature that displays different <i>gadgets</i> , which are mini applications that can perform information-display tasks, including displaying the date and time, central processing unit (CPU) usage, stock information, and user-selected news headlines. If a gadget for a particular need is not available from Microsoft or from a third-party developer, users can create their own. Available gadgets are stored in the Gadget Gallery, which provides a link to download additional gadgets. This feature was not carried over to Windows 8/8.1.
Sidebar	The <i>Sidebar</i> is a designated area of the Windows Vista and Windows 7 desktop that is displayed vertically along the side of the desktop. Users can add gadgets to the Sidebar to provide information and access to frequently used tools or programs.
BitLocker	Windows <i>BitLocker</i> ® is a security feature introduced with Windows 7 and Windows Server® 2008. This security feature provides full disk-encryption protection for your operating system, as well as all the data stored on the operating system volume. BitLocker encrypts all data stored on the operating system volume and is configured by default to use a Trusted Platform Module. This feature ensures the protection of early startup components and locks any BitLocker-secured volumes in order to prevent access or tampering when the operating system is not running.
Shadow Copy	The <i>Shadow Copy</i> technology is available on Windows Vista and newer versions. It creates backup copies or "snapshots" of the system's data and stores them locally or to an external location of the user's choosing. You can perform Shadow Copy operations manually, or you can set up automatic backups at scheduled intervals.

Feature	Description
System Restore	The <i>System Restore</i> utility is available in Windows Vista and Windows 7. It monitors the system for changes to core system files, drivers, and the Registry. It automatically creates a <i>system restore point</i> , which is a snapshot of the system configuration at a given moment in time that contains information about any changes to system components. Restore points are stored on the computer's hard disk, and you can use them to restore system settings to an earlier state without affecting changes in user data since that time.
ReadyBoost	ReadyBoost® is a performance enhancer that is available for Windows Vista and newer versions that enables the user to supplement the computer's memory with an external storage device such as a flash drive.
Compatibility mode	Compatibility mode enables older programs or applications to run on a newer version of Windows. You can configure compatibility for specific applications or programs by using the <b>Properties</b> options for the applications. Windows 7 can accommodate legacy applications dating back through Windows 95.
Windows XP mode	Windows <i>XP mode</i> is a download that is available for Windows 7 versions and that is designed to enable users running Windows 7 to access and use Windows XP-compatible software and programs directly on their desktops.
Windows Defender	<i>Windows Defender</i> is the antispyware software that is included with Windows Vista and newer versions. You can configure Defender to scan for malicious materials at scheduled intervals, automatically remove any spyware detected during a scan, or even alert you in real time if spyware installs or runs on the computer.
Category view and classic view	<p>In Windows Vista and Windows 7, you can configure the <b>Start</b> menu, <b>Control Panel</b>, and other interface elements by using two options:</p> <ul style="list-style-type: none"> <li>• Category view, which is the default setting, displays the options available divided into high-level categories. For instance, in category view, the <b>Control Panel</b> displays categories of options such as <b>Appearance and Themes</b> or <b>Performance and Maintenance</b>.</li> <li>• Classic view displays a more traditional view from earlier versions of Windows, in which all of the available options are displayed, either in a list or icon form.</li> </ul> <p>Windows 8/8.1 does not have the <b>Start</b> menu, but you can still configure the <b>Control Panel</b> to display in Category view or with Large or Small icons.</p>
Action Center	A centralized point of contact for security and maintenance items on your system that require your attention. It can be accessed through the Control Panel, or if there are items that currently need your attention, the Action Center flag will appear in the notification area on the taskbar.

## Versions of Microsoft Windows

Microsoft creates different versions or editions of their operating systems so the end user can purchase the edition most appropriate to how they will use their computers. To keep costs down for home users, a basic edition of each Windows operating system is available, but it doesn't have all of the features that the professional or enterprise edition will have.

Microsoft Windows 8 and 8.1 is available in several different editions.

<b>Edition</b>	<b>Features and Requirements</b>
Windows 8 RT	Windows 8 RT is only available pre-installed on devices that use the ARM 32-bit architecture. It only supports up to 4 GB of RAM. Only Windows Store apps can be installed on this edition. It comes with the Office 2013 Word, Excel, PowerPoint®, and OneNote® applications. Drive encryption is supported.
Windows 8/8.1	Windows 8 and 8.1 is the edition aimed at the home user. It comes pre-installed on many computers and can also be purchased separately if you need to perform an upgrade from a previous Windows version or if you are building a computer from components. It offers basic operating system functions and features. It does not include Office 2013. You can install Windows Store apps and traditional desktop-style applications. It can be installed on computers that use the Intel or AMD 32-bit or 64-bit architecture.
Windows 8/8.1 Pro	Windows 8 and 8.1 Pro is the edition aimed at the business user. This edition enables the system to be part of a Windows Server domain, to use remote desktop connections, use Hyper-V virtualization features, and use Group Policy.
Windows 8/8.1 Enterprise	Windows 8 and 8.1 Enterprise edition is for large organizations that use volume licensing. It has the same features and requirements as the Pro edition.



**Note:** A complete feature comparison between Windows 8.1 and Windows 8.1 Pro can be found at <http://windows.microsoft.com/en-US/windows/compare>.

Windows 7 is also available in several different editions.

<b>Edition</b>	<b>Features and Requirements</b>
Windows 7 Starter	Windows 7 Starter is a simple, basic edition with very few features and limited customization. Windows Aero and the majority of the visual styles included on the higher versions are not included in Starter. Unlike the other versions of Windows 7, it is only available in a 32-bit version.
Windows 7 Home Premium	Windows 7 Home Premium is a low-cost edition for beginners and home users. This edition offers basic OS functions such as Windows Explorer and Internet Explorer 8, and support for other productivity software.
Windows 7 Professional	Windows 7 Professional enables users to run programs in Windows XP mode, connect to domains, and back up data to a network location.
Windows 7 Enterprise	Windows 7 Enterprise is available for enterprise organizations that need large volumes of Windows licenses for employee use. Enterprise features include support for multiple languages through the Multilingual User Interface (MUI), BitLocker, and compatibility with UNIX applications that may be present in the corporate environment.
Windows 7 Ultimate	Windows 7 Ultimate offers the same features as Windows 7 Enterprise, but is available for individual licensing for personal home use.

Windows Vista is also available in several different editions.

<b>Edition</b>	<b>Features and Requirements</b>
Windows Vista Home Basic	Windows Vista Home Basic is a lower-budget OS for beginners and home users who do not require advanced multimedia capabilities and who do not require networking more advanced than a workgroup.

<b>Edition</b>	<b>Features and Requirements</b>
Windows Vista Home Premium	Windows Vista Home Premium adds a media center, High Definition TV (HDTV) support, backup scheduling, and more support for alternate displays. It also includes the Windows Aero interface.
Windows Vista Business	Windows Vista Business offers the same features as Vista Home Basic, plus additional business-focused features such as Remote Desktop, an encrypting files system, and the ability to join a Windows Server domain.
Windows Vista Enterprise	Windows Vista Enterprise adds features to the Vista Business edition, including UNIX application support, BitLocker drive encryption, and multilingual user interfaces.
Windows Vista Ultimate	Windows Vista Ultimate combines all of the features of the other editions, plus additional features, with support for up to 128 GB of Random Access Memory (RAM) but only in 64-bit.

## Running Windows Compatibility Mode

You can either run the **Program Compatibility** wizard to automate the process of running programs in compatibility mode (by selecting **Start**→**Control Panel**→**Programs**→**Run programs made for previous versions of Windows**) or you can manually change the compatibility settings for a specific program. You can do this by right-clicking a program's executable (.exe) file, selecting **Properties**, and changing the appropriate settings on the **Compatibility** tab.

## Other PC Operating Systems

There are several other PC operating systems available.

<b>OS</b>	<b>Description</b>
UNIX	UNIX® is a trademark for a family of operating systems originally developed at Bell Laboratories beginning in the late 1960s. All UNIX systems share a kernel/shell architecture, with the kernel providing the core functionality and the interchangeable shells providing the user interface. Unlike many operating systems, UNIX is portable to different hardware platforms; versions of UNIX can run on everything from personal computers to mainframes and on many types of computer processors. UNIX also incorporates built-in multitasking, multiuser support, networking functions, and a robust platform for software development.

OS	Description
Linux	<p><i>Linux</i> is an open-standards UNIX derivative originally developed and released by a Finnish computer science student named Linus Torvalds. The Linux source code was posted publicly on a computing newsgroup, and the code was developed and tested cooperatively all over the world. Because the source code is open, it can be downloaded, modified, and installed freely. However, many organizations prefer to purchase and implement a <i>Linux distribution</i>. A Linux distribution is a complete Linux implementation, including kernel, shell, applications, utilities, and installation media, that is packaged, distributed, and supported by a software vendor.</p>

Linux features include:

- Multiple desktops: Also known as virtual desktops, is used in Linux GUI environments. A workspace switcher is used to switch between the various desktops.
- Keychain: The keychain feature in Linux is different than the Mac feature of the same name. In Linux, it is a manager for the ssh agent and is typically run from the `~/.bash_profile`.
- iCloud: Support has been added to iCloud so that it can be accessed from a Linux system.
- Gestures: On most Linux systems, the basic scrolling and tap gestures will work on touch pads, but you will need to configure multi-touch gestures through configuration files.
- Remote Disk: To access remote disks from a Linux system, you can use command-line commands such as `rdesktop` and `ssh`.
- Command line and GUI: Linux is often used from the command line, but a variety of GUI interfaces can also be used with most distributions. You can also configure your Linux system to use a variety of GUI desktops.



**Note:** For more information about Linux and its versions, see the Linux home page at [www.linux.org](http://www.linux.org).

OS	Description
OS X	<p>OS X® is the operating system developed by Apple® Computing, Inc. OS X is a Linux derivative, and consists of UNIX-based operating systems and GUIs. This proprietary operating system is included on all Macintosh® computer systems.</p> <p>OS X features include:</p> <ul style="list-style-type: none"> <li>• <i>Mission Control</i>: A feature that allows users to use multiple Spaces that can be thought of as multiple desktops.</li> <li>• <i>Keychain</i>: The keychain feature in OS X is different than the Linux feature of the same name. In OS X, it is a password management system.</li> <li>• <i>Spot Light</i>: A feature that enables users to search for apps, documents, images, and other files. With Mountain Lion or later, you can also search Wikipedia, news sites, Maps, iTunes, movie listings, and other files and other searchable content.</li> <li>• <i>iCloud</i>: A cloud storage solution accessed with the user's Apple ID. iCloud can also be used with non-Apple operating systems.</li> <li>• <i>Gestures</i>: Using one or more fingers on the Mac Multi-Touch trackpad, Magic Trackpad, or Magic Mouse, users can scroll, zoom, and navigate desktop, document, and application content. For a full list of gestures, refer to <a href="https://support.apple.com/en-us/HT204895">https://support.apple.com/en-us/HT204895</a>.</li> <li>• <i>Finder</i>: The file and folder management app on Mac computers.</li> <li>• <i>Remote Disc</i>: A remote disk feature that enables users to access external drives or share disks from another computer. This is especially useful for Macs that don't have an optical drive built in.</li> <li>• <i>Dock</i>: A bar along the bottom or side of the screen that contains icons for apps that come with the Mac. Users can also add apps to or remove apps from the Dock. Documents and folders can also be added to the Dock.</li> <li>• <i>Boot Camp</i>: An app that enables users to install Microsoft Windows on their Mac, then switch between OS X and the Windows operating systems.</li> </ul>



**Note:** With the release of the OS X version Mountain Lion in 2012 and with the increased use of iOS for mobile devices, Apple officially dropped "Mac" from its operating system's name. It is now known simply as OS X, pronounced "OS 10."

## Popular Linux Distributions

There are many Linux distributions. Some are designed for end users and others are designed more for servers. Some popular distributions include Red Hat® Linux®, SUSE®, CentOS Linux®, Mandriva Linux, Debian®, Gentoo Linux™, and Kali Linux®.

## Mac OS Versions

There have been several versions of the Macintosh operating system. El Capitan refines and improves features and performance, rather than introducing new features. Yosemite improved integration between iOS and Mac features. Mavericks was a free upgrade to any system with Snow Leopard or later and a 64-bit Intel processor. Other previous versions included Mountain Lion, Lion, Snow Leopard, Leopard, and Tiger.



**Note:** For additional information, check out the LearnTO **Use OS X Features** presentation in the LearnTOs for this course on your CHOICE Course screen.

## Popular Mobile Operating Systems

There are three primary operating systems utilized in most mobile devices today: Android™, Apple® iOS, and Microsoft® Windows® Phone 8.1. These mobile OS user interfaces support direct touch, multitouch, and using the *accelerometer*.

Here are some common features among the three operating systems.

- Interface control elements consist of switches, buttons, and sliders.
- The response to user input is immediate and provides a fluid interface that includes swiping, tapping, pinching, and reverse pinching, all of which have specific definitions within the context of the mobile operating system and its multitouch interface.
- Screen orientation is facilitated using an accelerometer or gyroscope so that you can use the device in the portrait or landscape orientation. When the device is tipped to the opposite orientation, the display is turned so it remains right-side up.
- The mobile devices have GPS capabilities to facilitate geotracking.
- Emergency notification is enabled by default, but can be configured so that only certain types of notifications are delivered to your device.
- If the mobile device fails to detect your touch, or it thinks you have touched a different area of the screen, you might need to perform screen calibration. Refer to the documentation for your mobile device to determine how to perform screen calibration on your device.
- In addition to cellular connections on phones and on some tablets, mobile devices can connect to Wi-Fi networks to enable you to take advantage of Wi-Fi calling. You can use apps such as Skype to call so you don't use up the minutes on your plan.
- Mobile payment is available on each of the three mobile OSs. These are:
  - Apple Pay for iOS devices.
  - Google Wallet for Android devices.
  - SoftCard for Windows Phone 8.1 devices.

*iOS* is the base software that allows all other applications to run on an iPhone®, iPod touch®, or iPad®. It is a closed source operating system that works only on the devices listed here. The app source for iOS devices is the App Store within iTunes. The virtual assistant for iOS is known as Siri. Apps can be launched from the home screen, the Notification Center, Siri, or Spotlight. You can also install launcher apps to help make accessing and launching apps more efficient and organized.

*Android*, on the other hand, is a layered environment built on the Linux® kernel foundation that includes not only the operating system, but middleware, which provides additional software for the operating system (OS), and additional built-in applications. The Android OS was developed by the *Open Handset Alliance* and is owned by Google. It supports open source-developed applications and functions and comes with basic operating system services, message passing, and so on. Apps can be obtained from Google Play. The virtual assistant on Android devices can be accessed by speaking the words "Okay Google." The Android user interface is referred to as the Android Launcher; other launchers can be used to replace the default launcher.

Windows Phone 8.1 is used by several manufacturers, but it is not an open source OS. It includes some built-in applications. It was developed by Microsoft to be as similar to working in Windows 8.1 on a computer or tablet as possible. It uses the same WinApp UI with the Start screen and tiles. Apps can be obtained from the Windows Store. The virtual assistant for Windows Phone 8.1 is known as Cortana. The Windows Phone user interface is referred to as the Windows Mobile Device Center Launcher.



**Note:** For additional information, check out the LearnTO **Support Mobile OS Device Features** presentation in the LearnTOs for this course on your CHOICE Course screen.

## **Other Mobile OSs**

Additional mobile operating systems are available such as the BlackBerry® OS and HP® webOS. Computers tend to be a separate category and mainly use either one of Microsoft's operating systems or an open-source OS, such as Linux.

## **Mobile OS Differences**

One major difference between Android and iOS is that iOS runs on Apple products only, where the Android OS is used by many different mobile device manufacturers and is more widespread across a number of different mobile devices. Android also enables manufacturers to overlay a suite of applications that they support.

For developers of mobile device apps, obtain the appropriate Software Development Kit (SDK) for your mobile operating system. Apps for iOS devices are built using the iOS SDK and use the programming language swift. Windows Phone 8.1 apps are built using the Windows SDK and the programming language is .net. Android devices use a SDK that uses the Java programming language. They can also use the Android Application Package (APK) format to package their apps. An APK file contains all of that program's code, including .dex files), resources, assets, certificates, and manifest files. Similar to other file formats, APK files can be named almost anything, as long as the file name ends in ".apk"

# ACTIVITY 2–1

## Identifying PC and Mobile Operating Systems

### Before You Begin

You have been provided with a computer that has Windows 8.1 installed.

If you have personal mobile devices, your instructor may ask you to share your device with the class.

### Scenario

In order to gain experience in identifying and working with various operating systems, you ask your co-workers and friends if they would be willing to show you some of the features and functions of their devices.



**Note:** Activities may vary slightly if the software vendor has issued digital updates. Your instructor will notify you of any changes.

1. Identify the operating system installed on your classroom computer.
  - a) If necessary, turn on the device.
  - b) If necessary, log in using the credentials provided by your instructor.
  - c) Swipe in from the right edge of the screen to display the **Charms** bar.
  - d) Select **Settings**.
  - e) Select **PC Info**.



**Note:** If **PC Info** is not shown on the **Settings** pane, select **Change PC settings**→**PC and devices**→**PC info**. Opening **PC Info** using this method displays information in the right-hand pane, rather than opening the **System** dialog box.

- f) Review the information displayed in the **System** dialog box. Information about the **Windows edition** is listed at the top of the dialog box, followed by additional information about the system.  
If you are viewing the **PC info** screen, the Windows edition is displayed after the system information.
- g) Close the **System** dialog box.



**Note:** If you are viewing the **PC info** screen, close the **PC Settings** window.

2. Examine a device that uses OS X.
  - a) If necessary, turn on the device.
  - b) If necessary, log in using the credentials provided by your instructor.
  - c) From the menu bar, select the **Apple** icon.

- d) Select **About This Mac**.



- e) Review the information displayed.
3. Examine a device that uses iOS.
- If necessary, turn on the device.
  - If necessary, log in using the credentials provided by your instructor.
  - On the **Home** screen, tap the **Settings** icon.

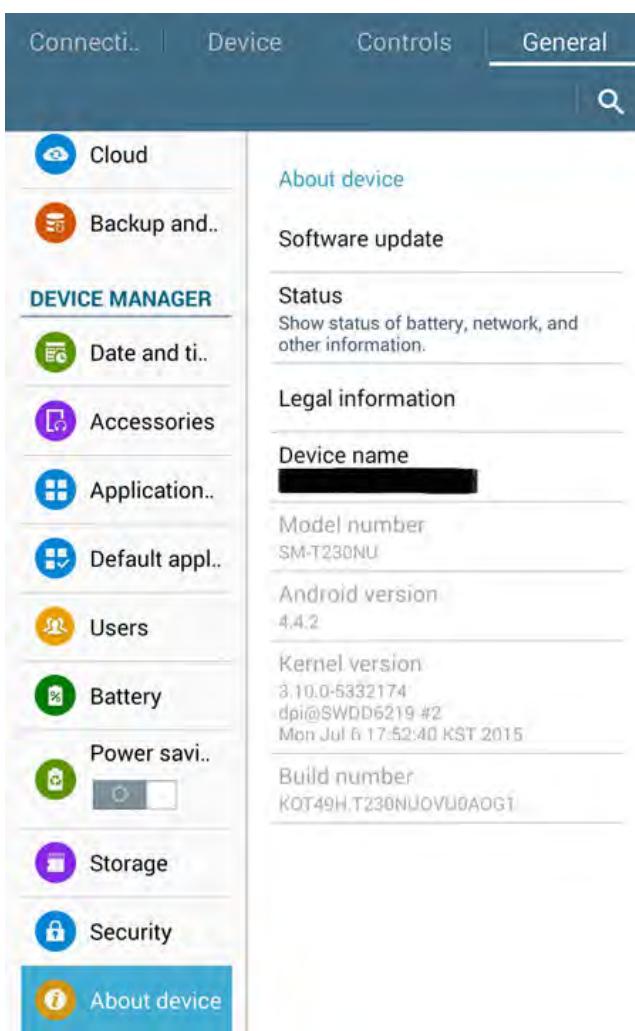
- d) Tap **General** and then tap **About**.



- e) Review the information displayed.

4. Examine a device that uses Android.
- If necessary, turn on the device.
  - If necessary, log in using the credentials provided by your instructor.
  - From the **Home** screen, tap the **Settings** button.

- d) Scroll through the **Settings** until you find a setting that starts with **About**. If you have a phone, it will say **About Phone** and if you have a tablet, it will say **About Tablet** or similar wording.



- e) Review the information displayed. Some devices have more or less information, and on some devices, you might need to select another option to go a level deeper in the menu structure to view the Android version.

## 5. Locate some of the features of the operating system.

- On your device, determine where you need to go to obtain additional apps.
- On your device, change the screen orientation. On most mobile devices, you just need to tip the device 90 degrees. On some laptops, this feature also works, but more likely you will need to access display settings.
- On a mobile phone device, determine how to turn Wi-Fi on and off.
- Determine whether your mobile device includes a mobile payment service option.
- On a mobile device, access the virtual assistant and obtain information about the device using the virtual assistant.

# TOPIC B

## PC Operating System Tools and Utilities

In order to work with your computer, you need to let your computer know who you are. You might log in with administrative capabilities or standard end user capabilities. You will interact with your computer through either a graphic user interface (GUI) for some tasks and through a command line interface for other, often more advanced, set up and configuration tasks. In this topic, you will examine some of the PC operating system tools and utilities for Windows, Mac, and Linux computers.

The various operating systems you might encounter use different tools, but the functionality of those tools is common across all of the operating systems. You will need to access the file and folders, and add or delete users. These are just a couple of the many tasks you will perform.

### User Authentication

*User authentication* is a security measure in which a computer user proves his or her identity in order to gain access to resources. There are many possible authentication methods; one of the most common is a combination of a user name and a password. There are three phases in the user access process that a person or system must perform in order to gain access to resources:

- Identification: The claim of identity made by the user when entering a user name and password.
- Authentication: The verification of that claim.
- Authorization: The action taken as a result of verifying the claim.

Most authentication schemes are based on the use of one or more authentication factors. You can combine these authentication factors for multi-factor authentication. The factors include:

- Something you know, such as a password.
- Something you have, such as a key or an ID card.
- Something you are, including physical characteristics, such as fingerprints.

*Multi-factor authentication* is any authentication scheme that requires validation of two or more authentication factors. It can be any combination of who you are, what you have, what you know, where you are or are not, and what you do. Requiring a physical ID card along with a secret password is an example of multi-factor authentication. A bank ATM card is a common example of this. Keep in mind that multi-factor authentication requires the factors to be different, not just the specific objects or methods.

### Local Users and Groups

Local users and groups are the user accounts and groups that are configured and stored on your computer. Local users and Groups are used in Windows 7 and Windows Server 2008/2012. If you go to another computer, these accounts will not be available. Permissions and rights can be assigned to a local user or group account for the specific computer where they are assigned. Assigning permissions and rights helps you limit which actions users and groups can perform. The permissions are rules about how a file, folder, or printer can be used or if it can be seen and used at all. Rights give the user the ability to take specified actions on the computer, including performing file backups and shutting the computer down.

Local user and group accounts are stored in the local Security Accounts Manager (SAM) on the computer where they were created. Users can see their files under the \Users\user\_name folder.

## Types of User Accounts

The Windows 8 family of operating systems includes three types of accounts, each giving you a different level of control.

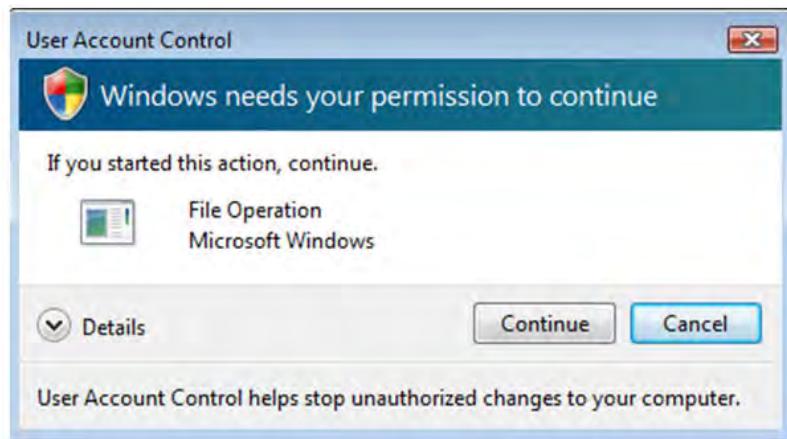
User Account	Provides
<b>Administrator accounts</b>	These accounts give users the most control over aspects of the computer. This type of account is typically created when users first set up a computer. This type of account should only be used when complete control over the computer is required.
<b>Standard accounts</b>	These accounts should be used for day-to-day activities. It is less likely that the user can accidentally delete crucial files or change settings they should not change. If the account is compromised through a security attack, it gives the attacker less access to critical information.
<b>Child accounts</b>	These accounts allow parents or other figures of authority to monitor or limit computer usage. The settings are configured using the Family Safety settings.

Windows 7 includes several built-in user accounts to provide you with initial access to a computer.

User Account	Provides
<b>Administrator</b>	Complete administrative access to a computer. This is the most powerful account on a computer and should be protected with a strong password. In some situations, you might also consider renaming this account.
<b>Standard User</b>	Access to use most of the computing software on the computer. However, higher permission is required to uninstall or install software and hardware. This account also limits the configuration of security settings, operational settings, and deletion of necessary system files. This account is sometimes referred to as a non-privileged user account.
<b>Guest</b>	Limited computer access to individuals without a user account. By default, the <b>Guest</b> account is disabled when you install the operating system. You enable this account only if you want to permit users to log on as a guest.

## Windows User Account Control

*User Account Control (UAC)* is an enhanced security feature of Windows Vista and later that aims to limit the privileges of a standard user unless a computer administrator decides otherwise. The intent is to limit accidental changes to the computer to reduce exposure to malware. Administrators can control access by managing privilege levels, which are not the same as permissions. A user might have administrator permissions, but still needs to be explicitly granted the privilege of running an application.



**Figure 2–1:** The UAC.



**Note:** Complaints from end users against Windows Vista's UAC are common because many tasks that users were able to perform on their own in previous Windows versions require additional privileges in Vista. However, in Windows 7, this issue has been addressed and UAC is now less intrusive.

## Changing UAC Settings

If the UAC is too restrictive for you or for your users, the settings can be changed. Open the Microsoft Management Console (MMC) and open the **Local Security Policy** settings. You must be logged on to the administrator account to modify:

- Whether the UAC is enabled or disabled.
- What the UAC behavior is for administrator or Standard Users.
- Application-specific behavior.

## Tasks Requiring a UAC Prompt

Tasks that are preceded by the **Security Shield** icon will invoke the UAC.

## Group Accounts

Windows includes several built-in group accounts that you can use to control basic system security. Local Windows groups are stored in the registry.

<b>Group Account</b>	<b>Users in this group can:</b>
<b>Administrators</b>	Perform all administrative tasks on the computer. When an account is created during the installation of Windows, it is automatically added to this group by default.
<b>Users</b>	Run applications and perform other day-to-day computer tasks for which the group has been granted permissions.
<b>Guests</b>	Perform any tasks for which the group has permissions. By default, all that members of this group can do is access the system.
<b>Event Log Readers</b>	Read event logs.
<b>Remote Desktop Users</b>	Log on to the system remotely from another system.

Other default groups are also created, and can perform the action indicated by the group name, including:

- Backup Operators who can back up and restore files on the computer.
- Cryptographic Operators who can perform cryptographic operations.
- Distributed COM Users who can start, activate, and use DCOM objects on the computer.
- IIS\_IUSRS used by the Internet Information Services (IIS).
- Network Configuration Operators who can make TCP/IP setting changes as well as release and renew TCP/IP addresses.
- Performance Log Users who can manage performance counters, logs, and alerts on the computer without being a member of the Administrators group.
- Performance Monitor Users who can monitor performance counters on the computer without being a member of the Performance Log Users group.
- Offer Remote Assistance Helpers who can offer Remote Assistance to users of the computer.

## System Files and Folders

*System files* are the files that are required for the operating system to function to its fullest capabilities. These files are typically hidden because their deletion can prevent the computer from working properly. For system files, both the file extension and the location of the file in the system hierarchy are important, as they help the computer recognize it as a system file.

In the file system hierarchy, the terms *folder* and *directory* are used interchangeably to describe a container that is used to organize files and other folders. System software and applications usually create standardized directory structures at the time of installation. Users can also create their own directory structures.



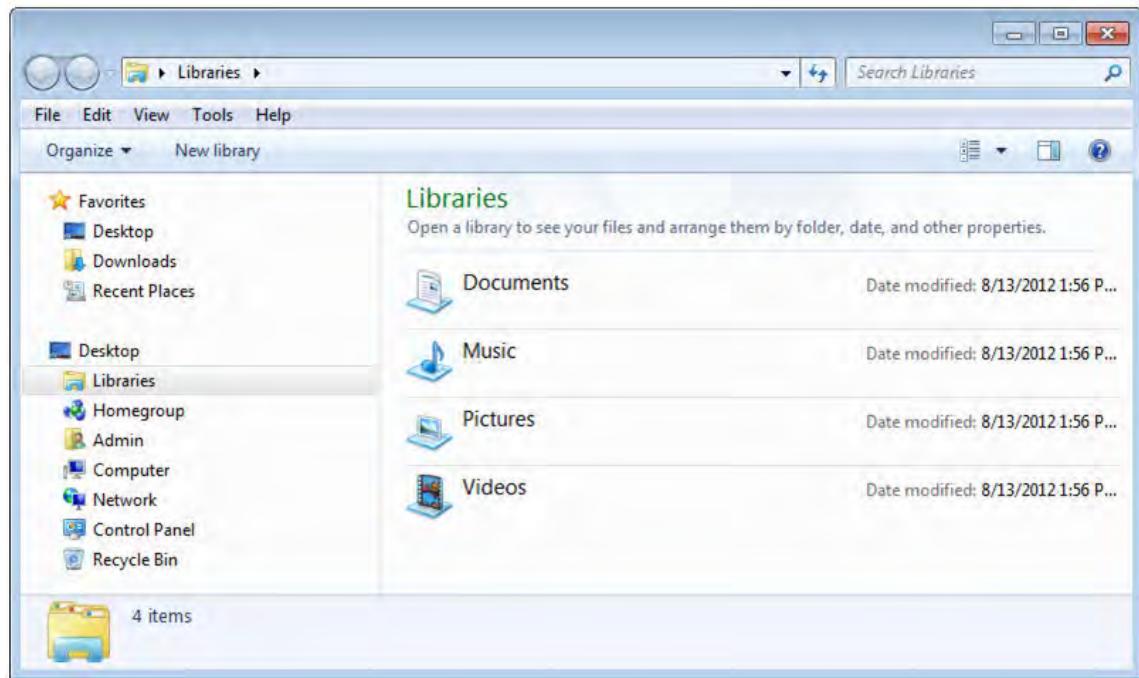
Figure 2–2: System folders on the Windows 7 Desktop.



**Note:** In Windows, the maximum depth of a folder structure is restricted by the 255-character limit in the overall file path, including the character representing the drive and any file name and extension. Otherwise, there is no set limit on the length of a particular file or folder name.

## Windows Explorer and File Explorer

Windows Explorer is a graphical tool in Windows 7 that enables users to manage files and folders on a computer, including the contents of hard disks, floppy disks, CDs, DVDs, USB devices, and any other storage devices attached to the computer. On the left side of Windows Explorer, the **Explorer** bar displays the folder hierarchy tree by default, and the right pane displays the contents of the selected item.

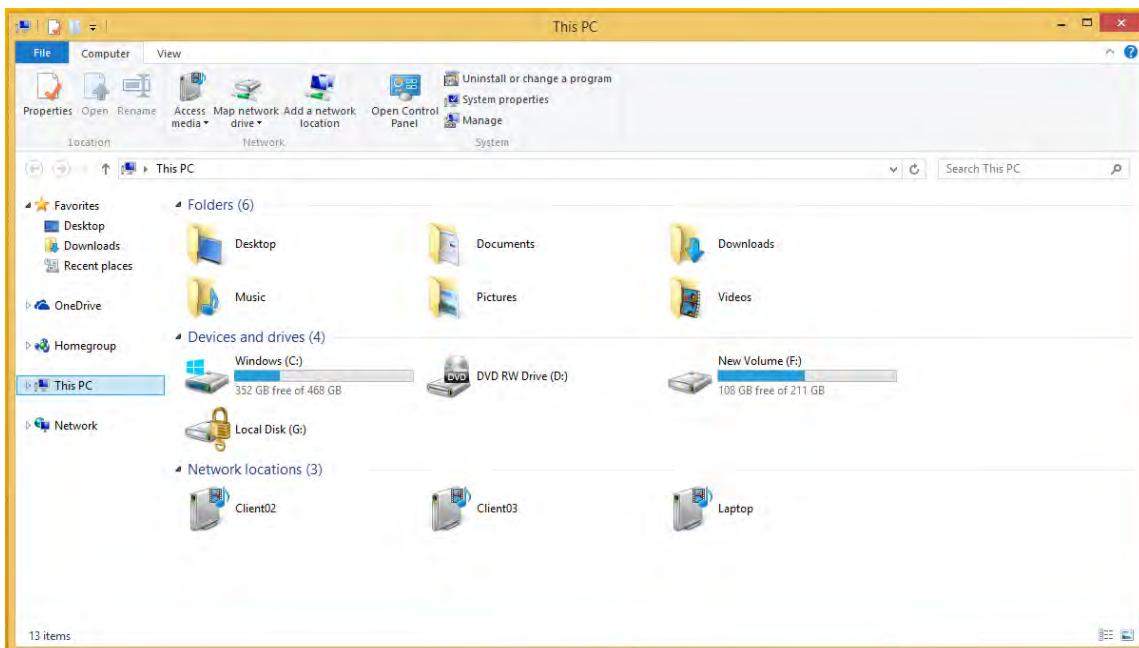


*Figure 2–3: Windows Explorer in Windows 7.*



**Note:** You can run Windows Explorer in Windows Vista and Windows 7 from the **Accessories** group on the **Start** menu. Windows Explorer opens with the object selected in the folder hierarchy. For example, if you display the pop-up menu for the **Start** menu and select **Explore**, Windows Explorer opens and displays the contents of the Start Menu folder on the disk.

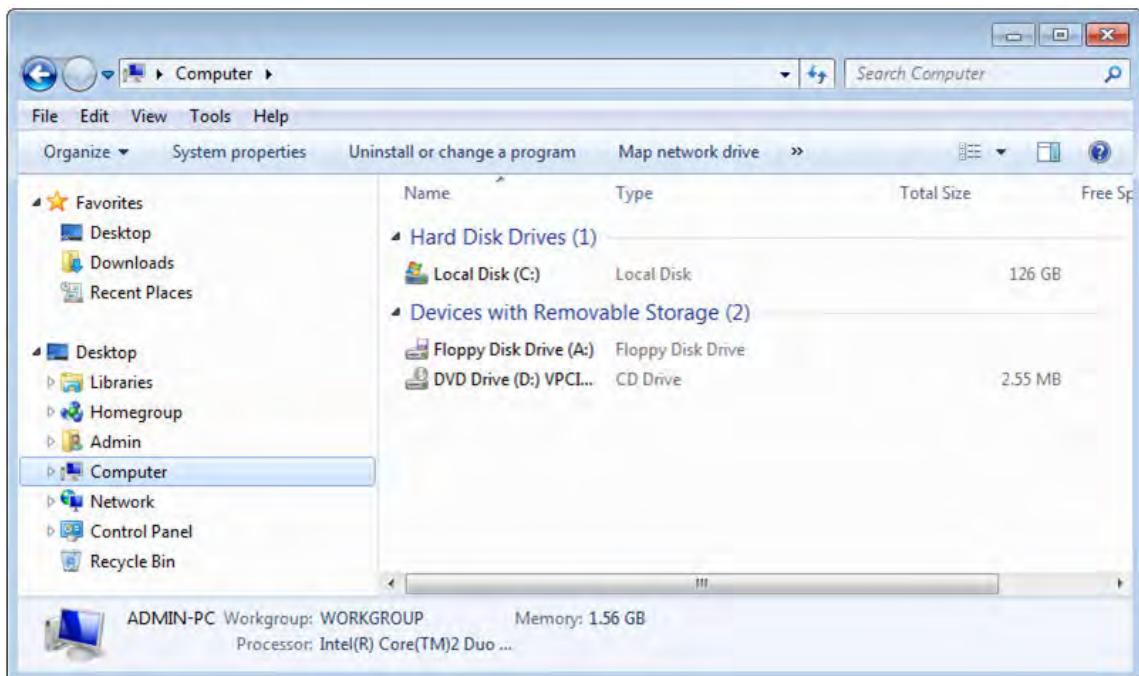
In the Windows 8 family of operating systems, this feature has been renamed to **File Explorer**. You can access it from the **File Explorer** icon on the Desktop taskbar.



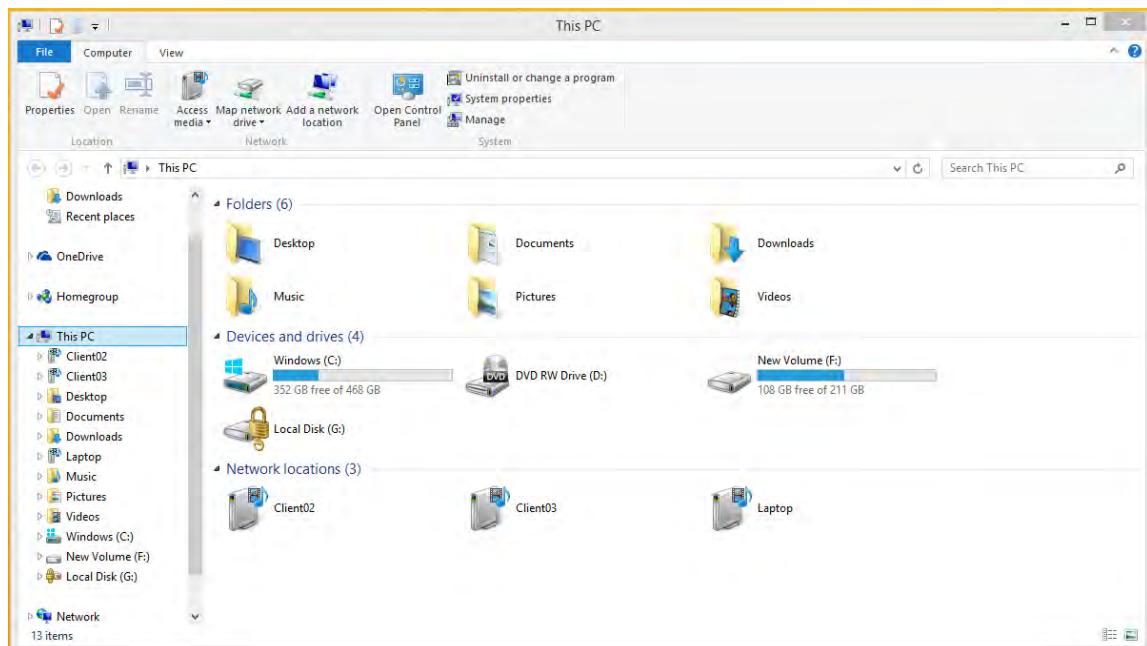
**Figure 2–4:** File Explorer in Windows 8.1.

## Computer and This PC

Like Windows Explorer, **Computer**, or **This PC** as it is called in the Windows 8 family of operating systems, is used to manage files and folders on a computer and on any storage devices attached to the computer. **Computer** or **This PC** can be accessed from **Windows Explorer** or **File Explorer**, respectively.



**Figure 2–5:** Computer in Windows 7.



**Figure 2–6:** This PC in Windows 8.1.

## File Extensions

Standard file extensions that follow the names of files in the Microsoft Windows environment can indicate whether a particular file is a program file or a data file. If it is a data file, the extension can indicate the application category that might be used to edit the file. Many common file extensions are three or four characters long, although there is no longer a strict character limit for the file name or extension in most modern operating systems. A period separates the extension from the file name itself.

Windows uses the file extension to determine how the system will use a file. If you alter a file name extension, you might find that a program file will not execute properly or that a data file will not automatically open in the associated application.

By default, the folder view options in Windows 7, Computer and Windows Explorer, are set so that common file extensions do not display. You can display the extensions by unchecking **Hide extensions for known file types** on the **View** page in the **Folder Options** dialog box. To display file extensions in Windows 8, in File Explorer, from the **View** menu, in the **Show/hide** group, check **File name extensions**.

## File Attributes

*File attributes* are characteristics that can be associated with a file or folder that provide the operating system with important information about the file or folder and how it is intended to be used by system users.

There are several standard attributes that can be enabled for files or folders on Windows systems.

File Attribute	Description
Archive (A)	Indicates that a file has not been backed up. Windows automatically sets the <b>Archive</b> attribute on any file you create or modify. When you back up data, you can choose to back up only the files on which the Archive attribute is set.
Hidden (H)	Hides a file from view in file management tools.

<b>File Attribute</b>	<b>Description</b>
Read-Only (R)	Enables users to read the contents of a file or execute it if it is a program file, but prevents users from changing the contents of a file.
System (S)	Indicates that a file is used by the operating system. Some applications use this attribute to restrict user access to these files. The System attribute in Windows automatically hides the file or folder.
Index (I)	This Windows-specific attribute enables the Windows <b>Indexing Service</b> to create an index of the file to speed up the Search function.

## Viewing and Changing Attributes

You can view or change most attributes of a file or folder object by opening the properties of the object in Windows Explorer. You can view and manage the System attribute at the command line by using the `attrib` command. For information on the functions and syntax of the `attrib` command, see the Windows Help system.

## ACTIVITY 2–2

### Viewing File Extensions and Attributes

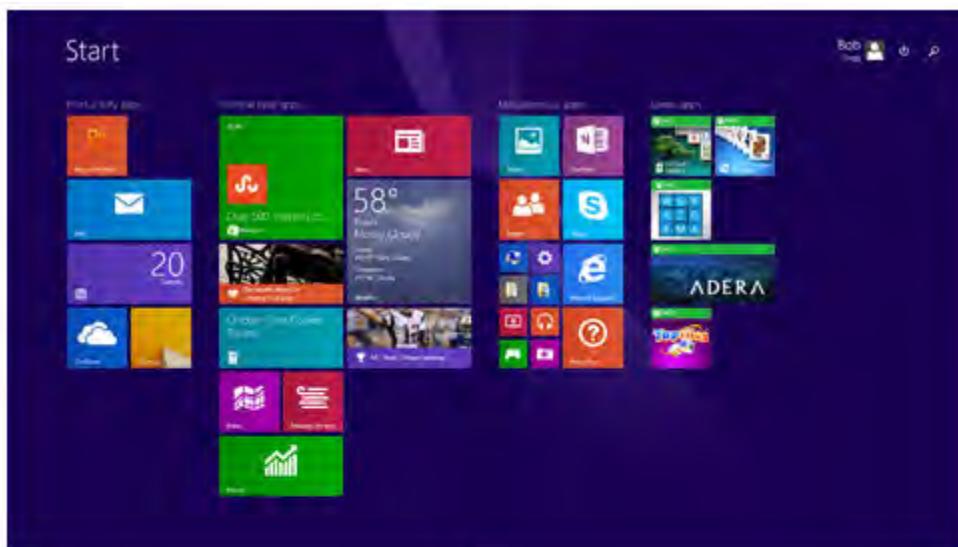
#### Scenario

In this activity, you will view the file extensions and attributes for the files that are stored on your Windows 8.1 system.

1. On your Windows 8 system, open the folder that contains the Windows system files.
  - a) From the **Start** screen, select the **Desktop** tile.
  - b) On the taskbar, select the **File Explorer** icon.
  - c) Double-click **This PC**.
  - d) Double-click the **C** drive.
  - e) Double-click the **Windows** folder.
2. On your Windows 8 system, display the file extensions.
  - a) On the menu bar, select **View**.
  - b) Scroll to see the files.
  - c) In the **Show/hide** group, check **File name extensions**.
  - d) Scroll down to view the files. The first few files in the window have different extensions.
3. Change the display options.
  - a) To see all of the files in a list format, right-click in an open area and select **View→List**.
  - b) To see similar extensions grouped together, right-click in an open area and select **Sort by→Type**.
  - c) To further group like extensions together, right-click in an open area and select **Group by→Type**.
  - d) To return to the list view, right-click in an open area and select **Sort by→Name**. Select **Group by→(None)**.
4. View file and folder attributes.
  - a) Right-click **write.exe** and select **Properties**.
  - b) Observe the **Attributes** section of the **write.exe Properties** dialog box. No attributes have been set for this file.
  - c) Select **Cancel**.
  - d) View the attributes for the **System32** folder.  
This folder has the **Read-only** attribute set.
  - e) Select **Cancel**.
  - f) Close the window.

#### Types of User Interfaces

All of the modern computer operating systems can be accessed from the GUI interface or from a command line interface. The GUI interface can be navigated using a mouse or other pointing device as well as by keyboard. A command line interface only uses keyboard input.



GUI



CLI

*Figure 2-7: User interfaces.*

## Windows Tools

Both command line and GUI tools are used to administer, configure, and work with Microsoft Windows operating systems.

- Some of the GUI tools are available from the **Start** menu or **Control Panel**, while others are accessed by opening the **Run** dialog box and entering the command name.

You can open the command line interface from the **Run** dialog box and entering **cmd**. You can also open it from the Windows 7 **Start** menu by selecting **All Programs**→**Accessories**→**Command Prompt**.

In Windows 8, on the Desktop, right-click the **Start** icon and select either **Command Prompt** or **Command Prompt (Admin)**.

Several of the commonly used GUI tools are grouped together in the **Administrative Tools** folder (select **Start**→**All Programs**→**Administrative Tools**).

- Some commands, such as **sfc**, can only be run in a command prompt window that has been opened with elevated administrator privileges, while others are available to users with standard privileges.

- Another method for opening some tools is through the Microsoft Management Console (MMC). In Windows, the commands are not case sensitive.
- If you know the name of the tool you need, which often will have the .msc extension, you can also search for and then select the file name to open the tool.

Windows PowerShell is a powerful command line tool designed for scripting as an alternative to some of the GUI tools. PowerShell ISE (Integrated Scripting Environment) is a GUI version of PowerShell in which you can write, run, and test script using tools that aren't available in the Console (command line) version of PowerShell. Most of the commands that can be used at the Command Prompt command line can also be used at the PowerShell command line.



**Note:** If you are interested in learning more about using PowerShell ISE, visit <https://technet.microsoft.com/library/dd819514.aspx>.

## Common Windows Command Line Tools

Common Windows command line tools include those described in the following table.

<b>Command</b>	<b>Description</b>
md	The <b>Make Directory</b> command creates a folder with the specified name.
rd	The <b>Remove Directory</b> command deletes the specified folder and its contents.
cd	The <b>Change Directory</b> command moves the command prompt to the specified folder.
del	The <b>Delete</b> command deletes the specified file.
copy	The <b>Copy</b> command copies the specified file(s) to a different location. The other location can be a different file name in the current folder or the same or a different name in another folder.
xcopy	The <b>Xcopy</b> command copies the specified file(s), and if desired, a directory tree, to the specified destination.
robocopy	The <b>Robust Copy for Windows</b> command offers many more options than either XCOPY or COPY. With the robocopy command, you specify the source directory, followed by the destination directory, then the file(s) and any options you want to use.
dir	The <b>Directory</b> command lists the contents of the specified folder.
help	The <b>Help</b> command by itself lists the available commands. To get information on a specific command, enter <b>help command_name</b> .
<i>command /?</i>	Displays the same information as <b>help command_name</b> .

## Linux Tools

Most of the Linux tools you will use are command-line-based tools. Some tools might also be available as GUI applications depending on the Linux distribution you have installed and which GUI you are using.

The types of Linux tools you will most often encounter as an A+ technician include:

- Backup and restore.
- Image recovery.
- Disk maintenance.
- Screen sharing.
- Application management.

Specific tools and applications will be covered in detail later in this course.

## OS X Tools

Most OS X tools are run from the GUI on a Mac. Some commands are accessed from a command line terminal user interface. OS X is a UNIX-based operating system, so the command line commands are UNIX commands. You can enter `man command_name` to get help on using a specific command.

As with Linux, the types of OS X tools you will most often encounter as an A+ technician include:

- Backup and restore
- Image recovery
- *Disk maintenance*
- Screen sharing
- Application management

Specific tools and applications will be covered in detail later in this course.



**Note:** For additional information, check out the LearnTO **Use Linux and OS X Tools** presentation in the LearnTOs for this course on your CHOICE Course screen.

# ACTIVITY 2–3

## Exploring Windows Tools

### Scenario

You have been reading about some of the tools used to manage and configure Windows. You would like to become familiar with how they are accessed and how to view help about some of the tools.

1. Examine the **Control Panel** utilities.
  - a) Right-click the **Start menu button** and select **Control Panel**. The **Control Panel** tools are grouped by function.
  - b) Select **Appearance and Personalization**.
  - c) Select **Taskbar and Navigation**. The **Taskbar and Navigation properties** dialog box opens.
  - d) Select **Cancel** to close the dialog box.
  - e) Select the **Back** button .
  - f) Examine the other categories in the **Control Panel**.
2. Pin items for easy access.
  - a) In the **Search Control Panel** box, type **administrative tools**
  - b) Right-click the **Administrative Tools** link, and select **Pin to Start**.
  - c) Right-click the **Administrative Tools** link, and select **Pin to Taskbar**.
  - d) Close the **Control Panel** window.
  - e) Pin the **Command Prompt** to the Taskbar.
  - f) Pin the **Control Panel** to the Taskbar.
3. Open the command prompt.
  - a) Right-click the **Start menu button** and use the **Search** feature to locate **command prompt**
  - b) From the results, select **Command Prompt**.
  - c) Maximize the command prompt window.
  - d) Enter **attrib** to view file attributes.
  - e) Enter **cls** to clear the screen.
4. View the available commands.
  - a) At the **C:\Users\username** prompt, enter **help**
  - b) Scroll through the list of commands.
5. Get help on an individual command.
  - a) Enter **cd /?** and examine the help information.
  - b) Display help for the **md** command.
  - c) Display help for the **copy** command.
  - d) Display help for another command of your choice.
6. Close the command prompt.

## Summary

In this lesson, you identified features of various PC and mobile operating systems and some of the PC operating system tools and utilities. By comparing functions and features of common operating systems and the tools used in each of them, you have prepared yourself to be more effective in selecting the operating system that is most appropriate for a specific situation.

**With which type of operating system (mobile, desktop, or web-based) do you have the most experience?  
Which do you have the least experience using?**

**How will you remember which commands and tools are used with which operating systems? Why do you think this is important?**



**Note:** Check your CHOICE Course screen for opportunities to interact with your classmates, peers, and the larger CHOICE online community about the topics covered in this course or other topics you are interested in. From the Course screen you can also access available resources for a more continuous learning experience.



# 3

# Networking and Security Fundamentals

**Lesson Time:** 1 hour, 30 minutes

## Lesson Objectives

In this lesson, you will identify networking and security fundamentals. You will:

- Identify common network types.
- Identify network components.
- Identify the properties and purpose of services provided over a network.
- Identify basic cloud concepts.
- Identify basic concepts related to security.

## Lesson Introduction

So far you have looked at hardware and operating system fundamentals. In this lesson, you will examine some basic networking and security fundamentals.

Having a basic background in networking and security fundamentals will help you as you begin installing and working with your computer. In today's computing environment, stand-alone computing is a rarity. Almost from the moment you begin installing the operating system, you are connected to a network. Knowing how the computer connects to the network and making sure it is safe from predators is an important first step in having a secure and functional computer.

# TOPIC A

## Network Types

In this lesson, you will identify networking and security fundamentals. To start, you will identify common network types. Recognizing network models and coverage types will help you determine the best approach to identifying the scope of network issues.

### Networks

A *network* is a group of connected computers that communicate and share resources such as files, printers, Internet connections, and databases. Whether wired or wireless, most networks will include network media, such as a cable to carry network data; network adapter hardware to translate the data between the computer and the network media; an operating system to enable the computer to recognize the network; and a network protocol to control the network communication. All these components work together to enable a fully functioning computer network. Any computing device that will communicate with a network will also include a *network interface card (NIC)* that is usually built into most devices. Older devices may require an adapter card that can be inserted into an expansion port or slot.

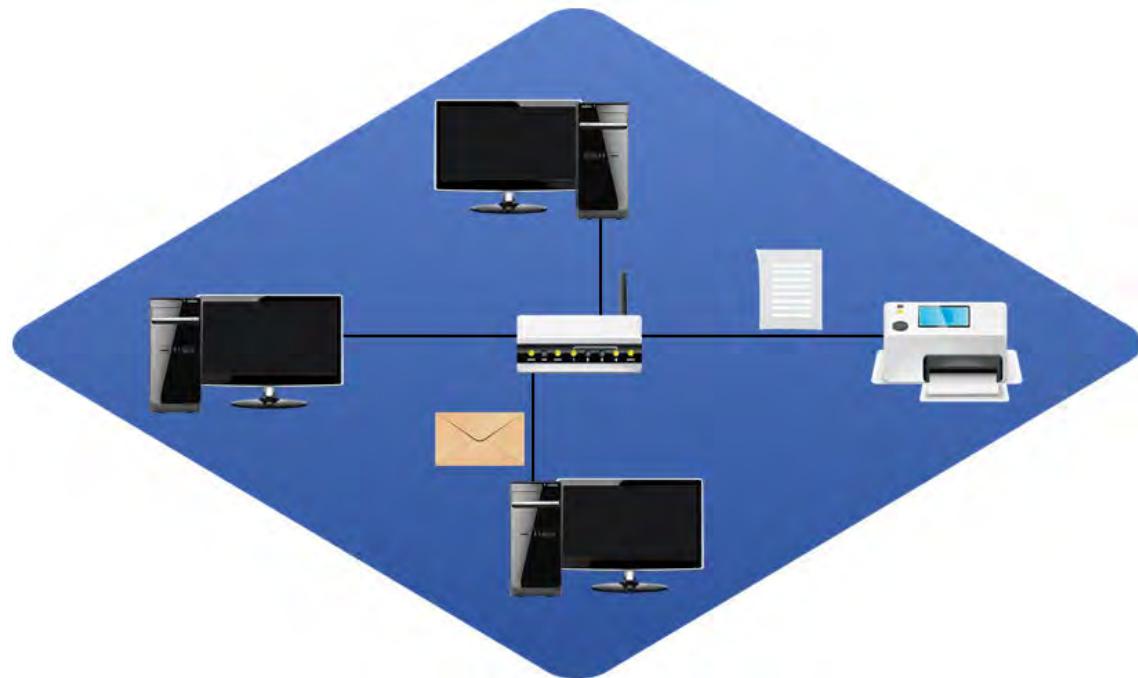


Figure 3-1: A network.

### Network Models

There are two primary network models, which are design specifications for how the computers and other *nodes* on a network can interact.

Network Model	Description
Client-server	A <i>client/server network</i> is a network in which computer functionality is divided into two roles: <i>server</i> computers, which provide services and control network operations, and <i>client</i> computers, which use the services provided by the servers. Typically, there is at least one server providing central authentication services. Servers also provide access to shared files, printers, hardware, and applications. In client/server networks, processing power, management services, and administrative functions can be concentrated where needed, while clients can still perform many basic end-user tasks on their own. Microsoft® Windows Servers® support a client/server network type known as a domain.
Peer-to-peer	A <i>peer-to-peer network</i> is a network in which resource sharing, processing, and communications control are completely decentralized. All clients on the network are equal in terms of providing and using resources, and users are authenticated by each individual workstation. Peer-to-peer networks are easy and inexpensive to implement. However, they are practical only in very small organizations, due to the lack of central data storage and administration. In a peer-to-peer network, user accounts must be duplicated on every workstation from which a user accesses resources. Such distribution of user information makes maintaining peer-to-peer networks difficult, especially as the network grows. Consequently, peer-to-peer networks should not exceed 10 computers. A Windows® workgroup is an example of a peer-to-peer network.

## LANs

A *Local Area Network (LAN)* is a self-contained network that spans a small area, such as a single building, floor, or room. In a LAN, all parts of the network are directly connected with cables or short-range wireless media.

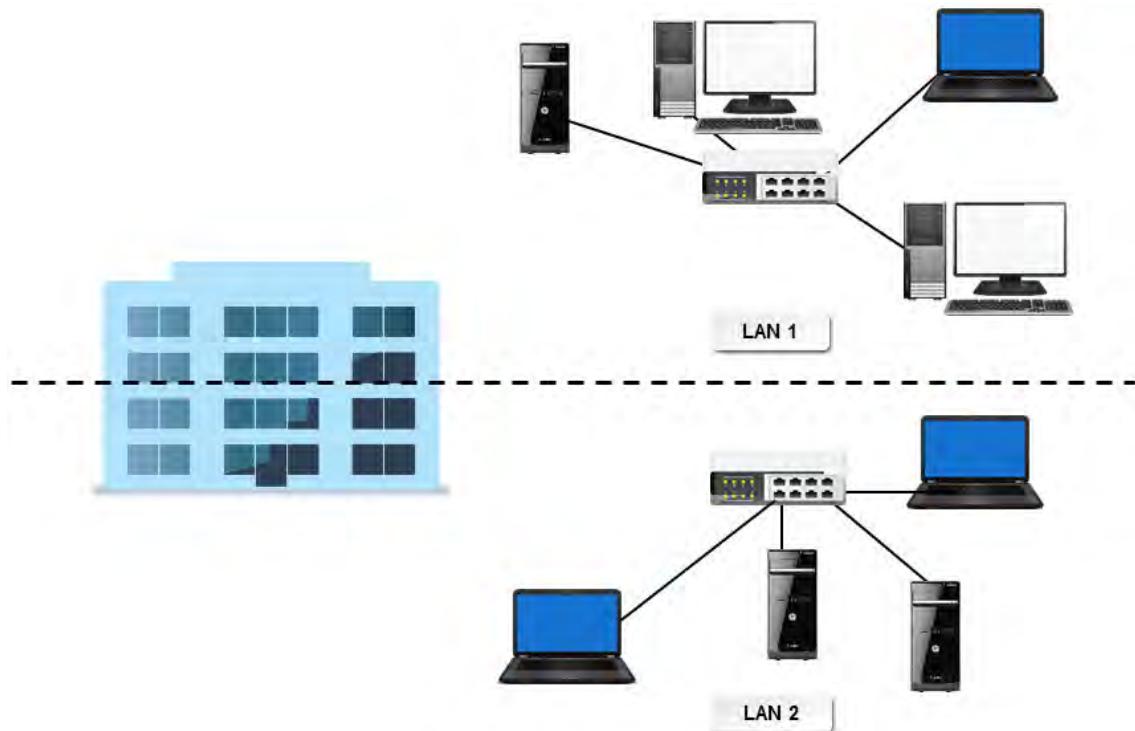
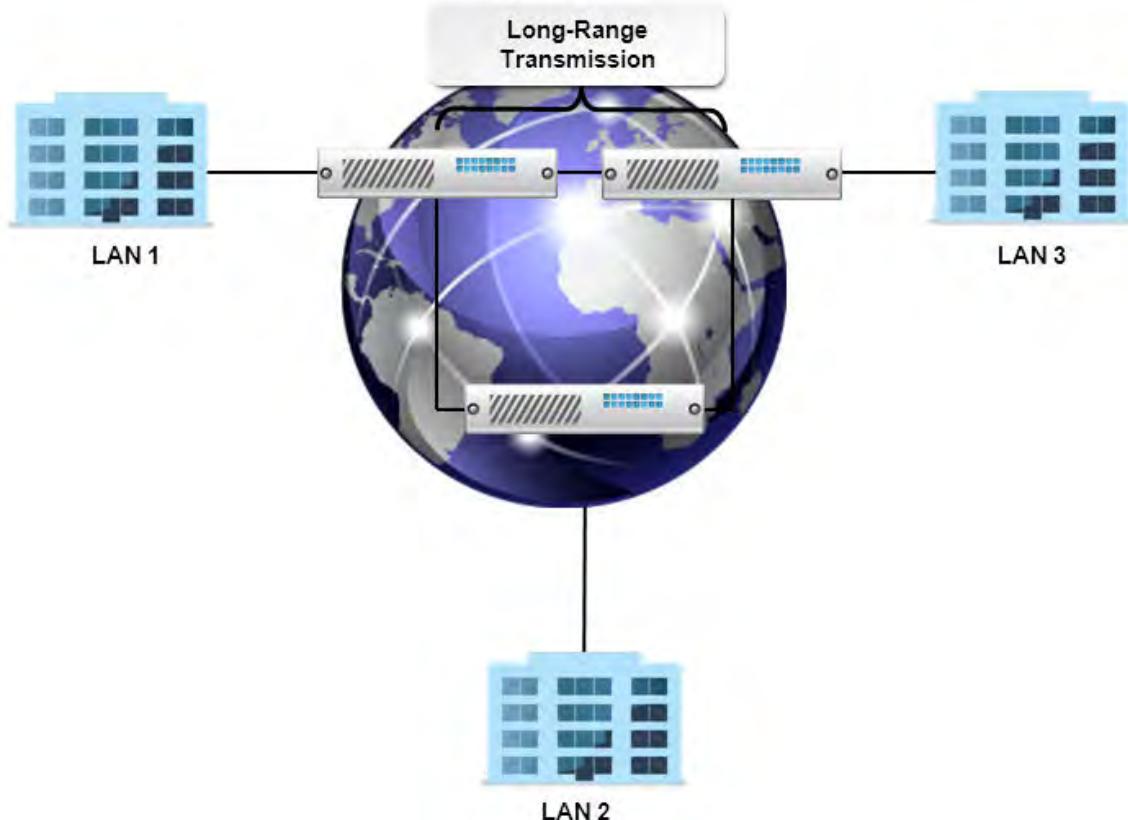


Figure 3–2: LANs within a building.

## WANs

A *Wide Area Network (WAN)* is a network that spans multiple geographic locations. WANs typically connect multiple LANs using long-range transmission media. Such a network scheme facilitates communication among users and computers in different locations. WANs can be private, such as those built and maintained by large, multinational corporations, or they can be public, such as the Internet.



*Figure 3–3: A WAN.*

## PANs

A *Personal Area Network (PAN)* connects two to three devices together for use by one person using a router with cabling; most often seen in small or home offices.

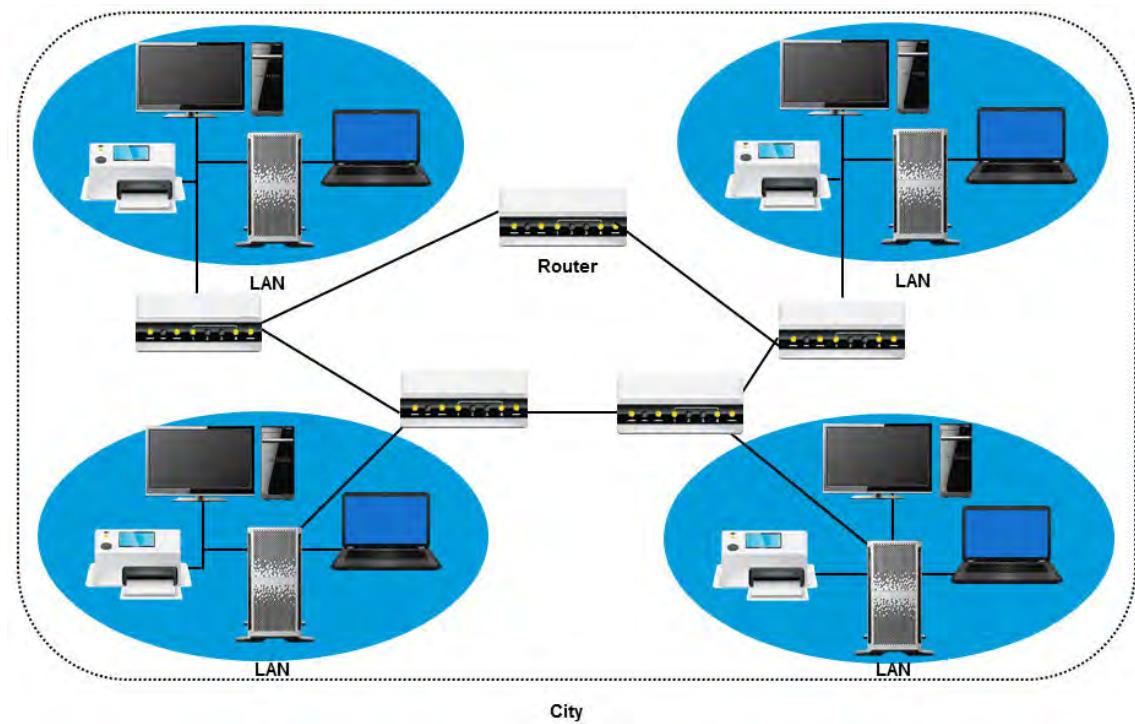
A *Wireless Personal Area Network (WPAN)* is a network that connects wireless devices in very close proximity but not through a Wireless Access Point (WAP). Infrared and Bluetooth are some technologies used for connecting devices in a WPAN.



Figure 3–4: A PAN.

## MANs

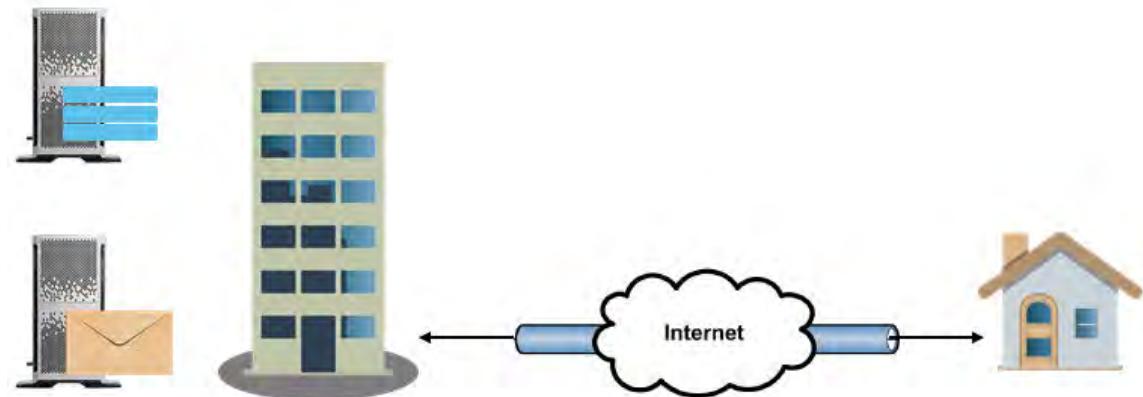
A *metropolitan area network (MAN)* covers an area equivalent to a city or other municipality. In many cases, the MAN connects multiple LANs.



**Figure 3-5: A MAN.**

## VPNs

A *virtual private network (VPN)* is a private communications network transmitted across a public, typically insecure, network connection such as the Internet. With a VPN, a company can extend a virtual LAN segment to employees working from home or other remote locations by transmitting data securely across the Internet.



**Figure 3-6: A typical VPN configuration.**

# ACTIVITY 3–1

## Identifying Network Types

### Scenario

Your manager wants to make sure that all of the interns are using the same terminology when discussing network types, so he asked you to prepare a presentation on the various network types. As a follow up to the presentation, you created some questions to make sure everyone understands the terminology.

1. What is the one component that any device that connects to a network requires?
2. Which network model does a Windows workgroup use and which model does a company-wide server use?
3. Your company has a global presence where all of the locations can communicate. Within each site, there is a network, and that network connects to the overall organizational network. In some locations, there are multiple sites within the city. Identify each type of network described here.

# TOPIC B

## Network Components

Before you start setting up a network, you need to be aware of the devices that you need on a network. In this topic, you will identify several types of network devices and other components.

Switches and routers are fundamental network connectivity devices, so you are likely to encounter them in the network environments that you support. In addition, there are other types of networking devices that you might be asked to support. Understanding the capabilities of these devices will prepare you to support a wide variety of network environments.

### Network Devices

There are many network devices that you can use to connect devices to a network. Typically, you will find devices such as switches, routers, and access points. Patch panels are often used to distribute access throughout the building. You might also encounter older technology such as hubs, bridges, and repeaters.

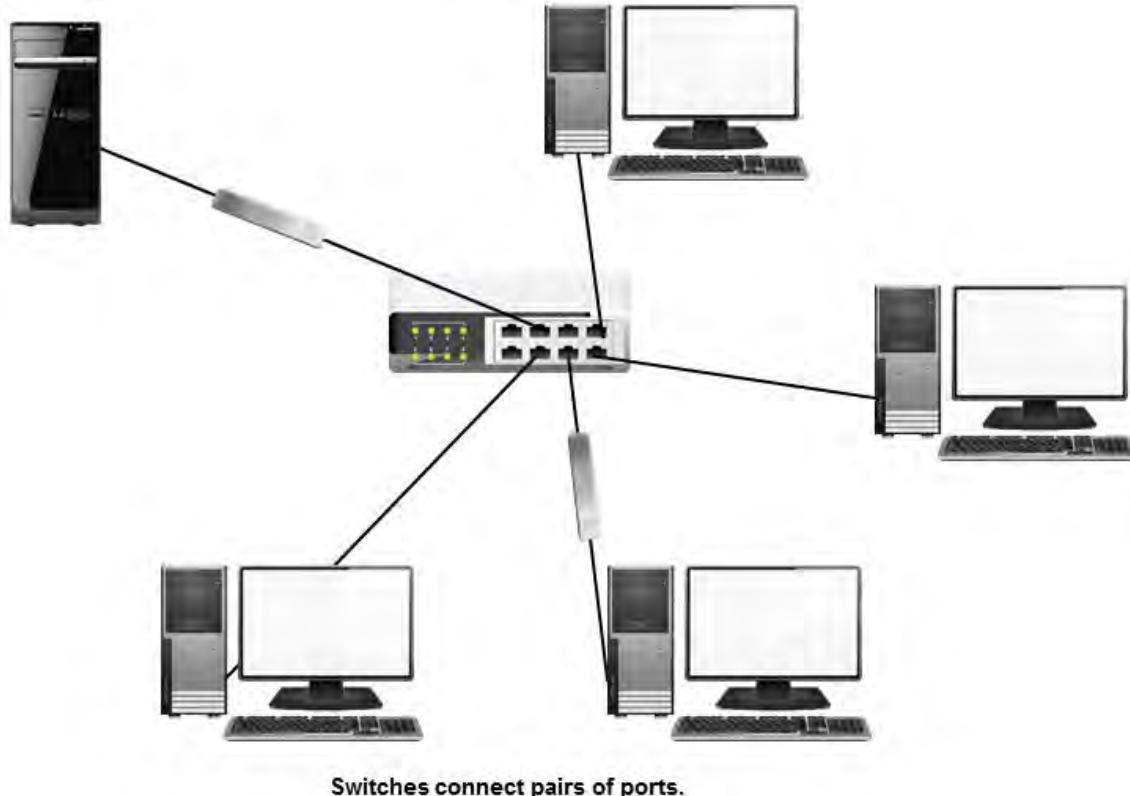
### Legacy Devices

Some of the network devices that you might encounter are older, or legacy devices, such as hubs, bridges, and repeaters.

<b>Device</b>	<b>Description</b>
<i>Hub</i>	<p>A hub, or multiport repeater, is a networking device used to connect the nodes in a physical star topology network into a logical bus topology. A hub contains multiple ports that you can connect devices to. When data from the transmitting device arrives at a port, it is copied and transmitted to all other ports so that all other nodes receive the data. However, only the specified destination node reads and processes the data while all other nodes ignore it.</p> <p>Two common types of hubs used were passive and active.</p> <ul style="list-style-type: none"> <li>• A passive hub simply has its ports wired together physically. It connects devices plugged into it without the use of power. Acting like a patch panel, it merely makes the electrical connection without repeating or transmitting any frames.</li> <li>• An active hub is a true multiport repeater. It receives incoming data and retransmits it out all ports with a signal boost.</li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <b>Note:</b> In today's networks, hubs have been replaced by switches.     </div>
<i>Bridge</i>	A bridge is an older version of a switch. It has the same basic functionality of a switch, but it has fewer ports and is software-based, rather than hardware-based.
<i>Repeater</i>	A repeater, sometimes referred to as a signal extender, is a device that regenerates a signal to improve signal strength over transmission distances. By using repeaters, you can exceed the normal limitations on segment lengths imposed by various networking technologies.

## Switches

A *switch* is a network hardware device that joins multiple computers together within the same LAN. Unlike a hub, switches forward data only to the intended destination. Because of this, they are slightly "smarter" than hubs, and are more common. Switches can also be connected to other switches, thus increasing the number of devices on a LAN without sacrificing performance. Troubleshooting a switch is easier because of the status indicator lights on the individual ports.



**Figure 3-7: Switches in a network**

### PoE

Power over Ethernet (PoE) uses the IEEE 802.3af standard for transferring both electrical power and data to remote devices over twisted-pair cable in an Ethernet network. This technology allows you to place devices such as network switches, VoIP phones, wireless access points, and cameras in locations where it would be inconvenient or impossible to run electrical power for the device. PoE provides up to 15.4 W of power and requires CAT 5 or higher copper cable.

The updated IEEE 802.3at standard, also known as Power over Ethernet+ (PoE+), provides up to 25.5 W of power per port and is backward compatible with all existing IEEE 802.3af devices. PoE+ allows for a broader range of devices to be powered such as:

- Cameras with pan/tilt/zoom capabilities.
- Door controllers.
- Point of Sale terminals.

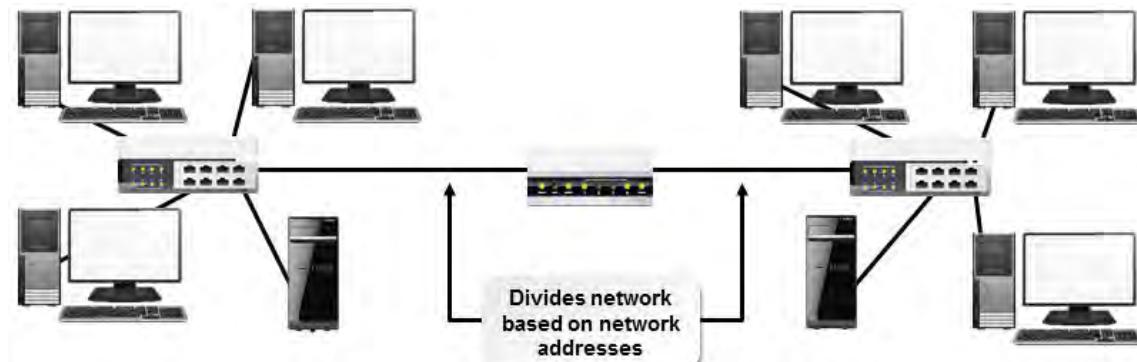
Many switches provide PoE directly from their switch ports. This is used to power Voice-over-IP (VoIP) phones that are plugged into the switch.

Another common implementation is a midspan device that plugs into AC power at the wall, such as an external PoE injector. A PoE injector enables PoE-compliant devices such as IP cameras and wireless access points to connect to a non-PoE switch.

The PoE injector inserts the DC voltage onto the Ethernet cable that leads to the PoE device, allowing the camera or access point to be mounted on a pole or under the eave of a roof, where power is not normally available. Typically, the injector itself is located in the wiring closet near the switch.

## Routers

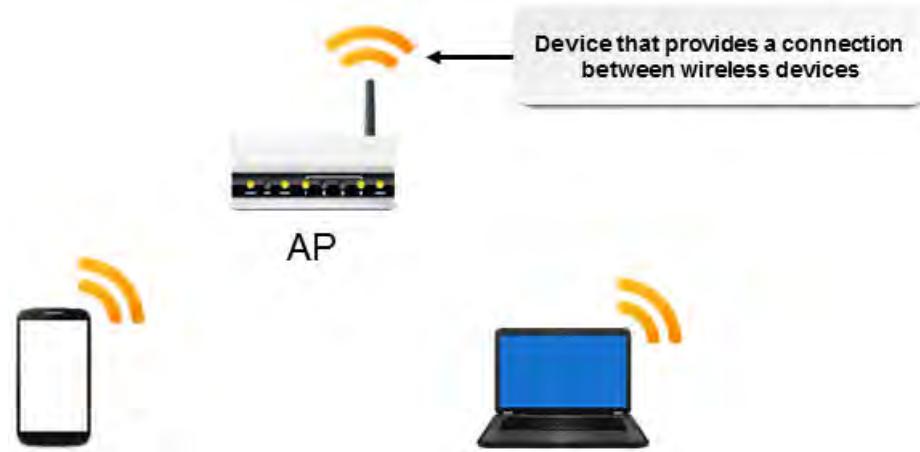
A *router* is a networking device that connects multiple networks. Traffic from one network to another does not always have to travel between the same routers. On the Internet, for example, traffic is routed according to the best available path at the time. Troubleshooting a router is made easier by the use of status indicator lights on the various ports.



*Figure 3–8: Routers connect different networks.*

## Access Points

An *access point (AP)* is a device or software that facilitates communication and provides enhanced security to wireless devices. It also extends the physical range of a WLAN. The AP functions as a bridge between wireless STAs (stations) and the existing network backbone for network access.



*Figure 3–9: Access points connect wireless devices.*

## Repeaters and Extenders

Repeaters are used frequently with coax media, such as cable TV, and were also deployed in networks that used coax cabling. On today's networks, repeaters are not commonly needed because other devices perform that function, but they are sometimes used in Fiber networks. Wireless

network repeaters and bridges are frequently used to extend the range of a WAP. Repeaters are not needed in twisted pair networks because other devices act as repeaters.

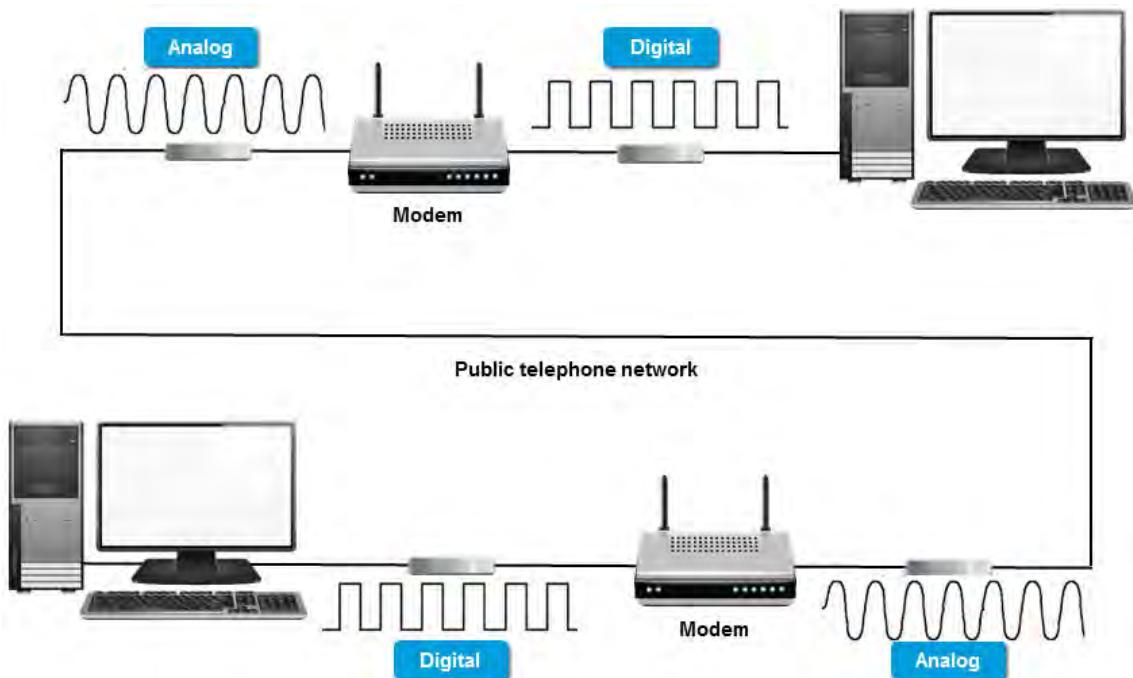


**Figure 3-10: A Wi-Fi repeater expands the effective wireless network coverage area.**

## Modems

A *modem* is a device that modulates and demodulates digital data to an analog signal that can be sent over a telephone line. Its name is a combination of *modulate* and *demodulate*.

Use a modem to connect to the Internet and to translate digital information to and from your computer. Depending on the type of connection used, you will use either a cable modem, a DSL modem, a wireless modem, a voice modem, or a radio modem. A laptop modem can be an internal device, or you can add it to a system as an external device by using an expansion card.



**Figure 3-11: Modems.**

## Firewalls

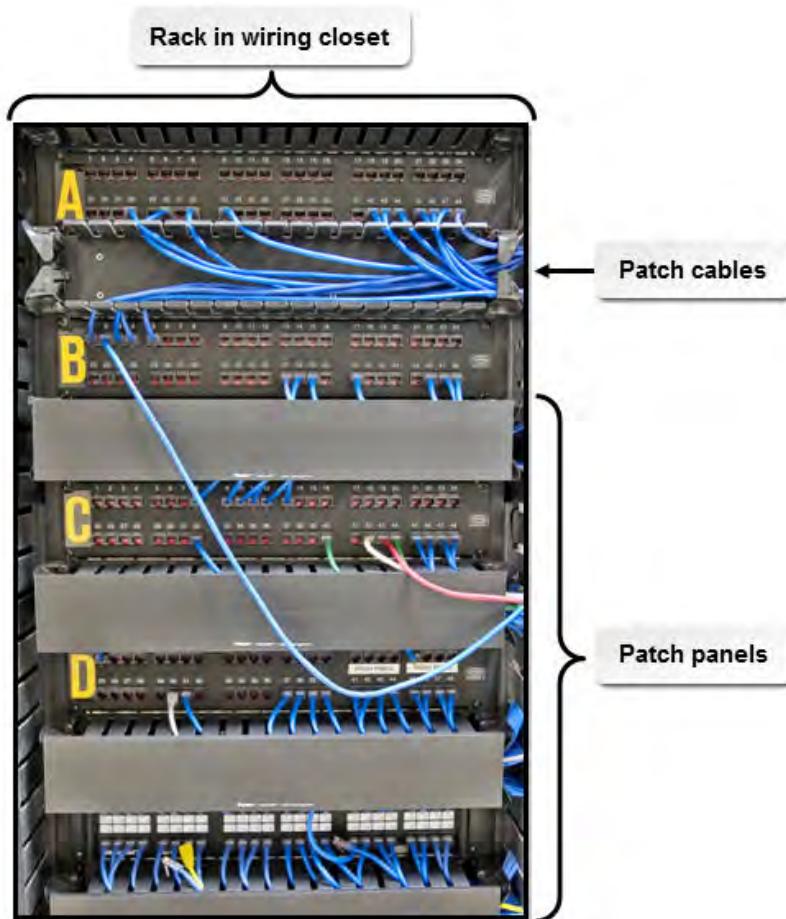
A *firewall* is a software program or hardware device that protects networks from unauthorized data by blocking unsolicited traffic. Firewalls allow incoming or outgoing traffic that has specifically been permitted by a system administrator and incoming traffic that is sent in response to requests from internal systems.

## Patch Panels

A patch panel is connection point for drop and patch cables. Typically, a patch panel has one or more rows of RJ-45 or other connectors. Drop cables are connected to the connectors. Cables run between the connectors to connect drop cables as needed.

Patch cables plug into the patch panel to connect two drop cables. They are most often stranded, and not solid core cables.

A wiring closet, network closet, or telecommunications closet is a small room in which patch panels are installed. Drop cables radiate out from the wiring closet to the components on the network.



*Figure 3–12: Patch panels in a wiring closet.*

## ACTIVITY 3–2

### Identifying Network Components

#### Scenario

You continue to work on the presentation you started earlier and have included some network components that your manager asked you to include. To wrap up this section of the presentation, you decide to make sure everyone can identify various network components.

- 
1. Examine the network devices available to you.
    - a) Determine which device you are viewing.
    - b) Determine whether it is an outdated technology or a current device.
    - c) Determine whether this is the best choice for connecting devices to the network in your location.
  2. Which network device would you recommend to someone who needs to control surveillance cameras that need to pan, tilt, and zoom?
  3. What situations would be best for wired or wireless networks?
-

# TOPIC C

## Common Network Services

So far in this lesson, you have identified common network types and the components that make them functional. Now it's time to examine what this network can provide to you and other users. In this topic, you will identify the properties and purposes of services provided over a network.

### Server Roles

In most organizations, the network will have several servers, each taking on a different role. In smaller networks and test environments, one server might perform several roles.

The following table includes some of the common server roles you are likely to encounter.

<b>Server Role</b>	<b>Description</b>
Web server	A <i>web server</i> provides access to personal, corporate, or education website content. This service is provided primarily to external users, such as customers or students, who access the Web services from the Internet. Web servers typically provide Web services to external users, although intranet servers can provide Web services to internal users.
File server	<i>File servers</i> are computers that store the programs and data files intended to be shared by multiple users. Many file servers use high-speed LAN or WAN links to keep data moving at optimal rates. Simply put, a file server acts like a remote disk drive.  A file server might also be combined with a print server. In this case, it provides access to shared files, such as documents, pictures, spreadsheets, and graphics, as well as access to laser and inkjet printers.
Print server	A <i>print server</i> enables many network users to share the common printers. The printers might be directly attached to the network or attached to the server.
DHCP server	A <i>Dynamic Host Configuration Protocol (DHCP)</i> server runs software that automatically assigns IP addresses to client stations logging on to a TCP/IP network. It eliminates the need to manually assign permanent IP addresses. DHCP software typically runs on servers and is also found in network devices such as firewalls, ISDN routers, and modem routers that allow multiple users access to the Internet.
DNS server	<i>Domain Name System (DNS)</i> is a protocol that provides common naming conventions across the Internet. This distributed database supports a hierarchical naming system. DNS provides name resolution for IP networks, including the Internet. The DNS server maintains a database of domain and host names, and their corresponding IP addresses.
Proxy server	A <i>proxy server</i> is a system that isolates internal clients from the servers by downloading and storing files on behalf of the clients. It intercepts requests for web-based or other resources that come from the clients, and, if it does not have the data in its cache, it can generate a completely new request packet using itself as the source, or simply relay the request. In addition to providing security, the data cache can also improve client response time and reduce network traffic by providing frequently used resources to clients from a local source.

<b>Server Role</b>	<b>Description</b>
Mail server	A <i>mail server</i> , also called the message server, provides post office facilities by storing incoming mail or messages for distribution to users and forwarding outgoing mails or messages through appropriate channels. Many of today's mail servers also provide other services such as document collaboration, chat, web access, and file storage. The term may refer to just the software that performs this service while residing on a machine with other service functions.
Authentication server	An <i>authentication server</i> contains an application that has an access list and identifies the permitted access credentials. The authentication server can be on a separate server or it might be part of another server, a switch, or an access point.

## Internet Appliances

An *Internet appliance* is a relatively inexpensive PC that enables Internet access and a specific activity. Often used by organizations to ease remote management and to cut costs, Internet appliances lack many of the features of a fully equipped PC, and they provide a complete solution consisting of limited hardware and software that is needed to perform a single or specialized set of functions. This hardware device allows for quick installation, ease-of-use, and low maintenance, and is typically managed through a Web browser. Common Internet appliances are described in the following table.

<b>Internet Appliance</b>	<b>Description</b>
IDS	An <i>Intrusion Detection System (IDS)</i> is software or hardware, or a combination of both, that scans, audits, and monitors the security infrastructure for signs of attacks in progress and automates the intrusion detection process. It is used to quickly detect malicious behavior that compromises the integrity of a computer so that appropriate action can be taken. IDS software can also analyze data and alert security administrators to potential infrastructure problems. An IDS can comprise a variety of hardware sensors, intrusion detection software, and IDS management software. Each implementation is unique, depending on the security needs and the components chosen.
IPS	An <i>Intrusion Protection System (IPS)</i> , also referred to as a Network Intrusion Prevention System (NIPS), is an inline security device that monitors suspicious network and/or system traffic and reacts in real time to block it. An IPS may drop packets, reset connections, and sound alerts, and can at times even quarantine intruders. It can regulate traffic according to specific content because it examines packets as they travel through the IPS. This is in contrast to the way a firewall behaves, which blocks IP addresses or entire ports.
UTM	A <i>Unified Threat Management (UTM)</i> appliance is a security device that combines the features of a firewall, gateway antivirus, and IDS/IPS into a single device.

## Legacy Systems

You might encounter some older, legacy systems. These are often for specific functions in an organization. For example, a manufacturing device might only run on a DOS-based system, so the organization might need to keep this old system running in order to use a device.

## Embedded Systems

Some consumer products, such as the set-top box for a television, often use an operating system that is contained on a chip or set of chips that is embedded inside the device. Often, this is a Linux-based system.

## ACTIVITY 3–3

### Discussing Common Network Services

#### Scenario

Your consulting group has been asked to prepare an overview of the network services you would configure for a new organization. This organization is a non-profit that will not have a web presence at the current time, but might in the future. They will be using cloud storage and hosted email addresses. They will have confidential information they need to store locally and also want to be able to share a color laser printer between the 25-30 employees they anticipate working out of this office.

1. What are the minimum network services you would recommend for this organization based on the requirements given in the Scenario?
2. After some discussion amongst the members of the organization, they have decided that they do need a web site. However, they have no one in-house that can create and maintain the web site. Will they need web services on their server? Why or why not?
3. Discuss any other network services you feel the organization should implement at this time, or should plan for in the future.

# TOPIC D

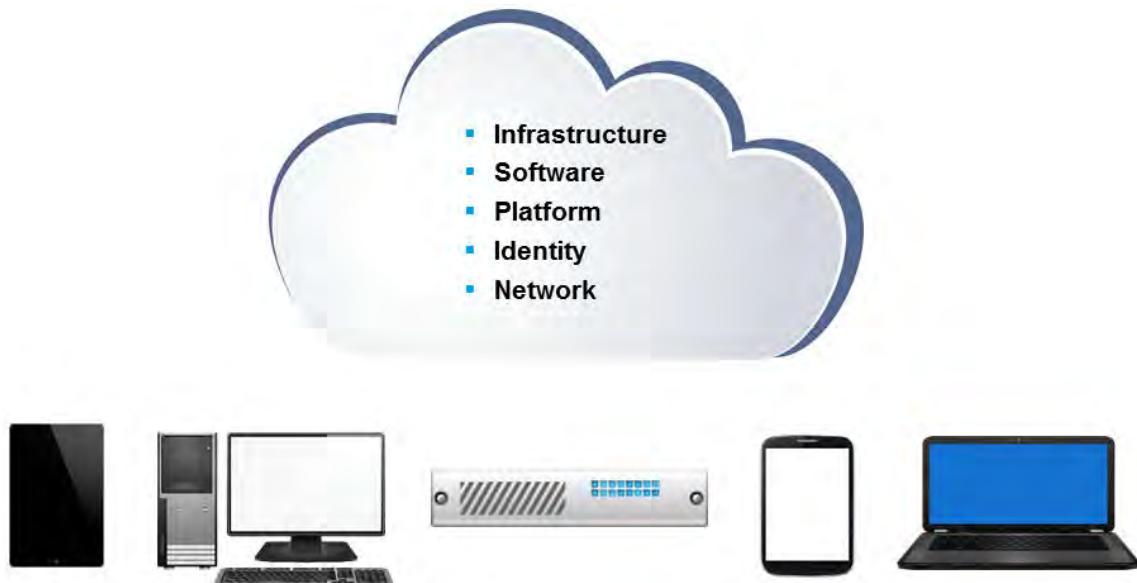
## Cloud Concepts

So far, you've examined network types, components, and services. One of the latest trends in networking is to outsource part of an organization's IT infrastructure, platforms, storage, or services to a cloud service provider. In this topic, you will identify basic cloud concepts.

### Cloud Services

Cloud computing is a model for providing or purchasing off-premise computing services over the Internet. In broad terms, cloud computing is a service (that you purchase or set up on your own) by which you can dynamically expand or contract computation or storage capabilities on an as-needed basis.

The National Institute of Standards and Technology (NIST) defines several components of cloud computing services. Resource allocation is available through rapid elasticity and resource pooling. Automated service changes are covered through on-demand self service. The capabilities of cloud systems and the footprint of the overall service is referred to as broad network access. The provider's ability to control a customer's use of resources through metering is referred to as measured service.



**Figure 3–13:** Cloud services.

### Types of Cloud Services

There are several common types of services that are normally associated with cloud computing.

Type	Description
IaaS	<p>Infrastructure as a Service (IaaS) is an arrangement where, rather than purchasing equipment and running your own data center, you rent those resources as an outsourced service. In an IaaS arrangement, you are typically billed based on the resources you consume, much like a utility company bills you for the amount of electricity you use.</p> <p>Examples of IaaS include Rackspace's CloudServers offering, in which you rent a virtual server running an operating system of your choice. You then install the applications you need onto that virtual server. Other examples include Amazon's Elastic Compute Cloud (EC2) service and Amazon's Simple Storage Service (S3).</p>
PaaS	<p>Platform as a Service (PaaS) enables you to rent a fully configured system that is set up for a specific purpose.</p> <p>An example is Rackspace's CloudSites offering, in which you rent a virtual Web server and associated systems (such as a database or email server). Amazon's Relational Database Service (RDS) enables you to rent fully configured MySQL and Oracle database servers.</p>
SaaS	<p>Software as a Service (SaaS) enables a service provider to make applications available over the Internet. This capability eliminates the need to install software on user computers, and it can be helpful for mobile or transient workforces.</p> <p>Perhaps the most well-known SaaS example is the Google Apps suite of office applications. Other notable SaaS examples are the Zoho suite of applications and Microsoft's Office Web Apps.</p>

## Types of Clouds

Cloud computing can be deployed following a public, private, or mixed model.

Cloud Type	Description
Private cloud	<p>A private cloud is a cloud infrastructure operated solely for a single organization. It can be managed internally or by a third party, and hosted either internally or externally. A private cloud project requires a significant degree of engagement to virtualize the business environment. The OpenStack project (<a href="http://www.openstack.org">www.openstack.org</a>) is the key example of a technology you could use to implement your own cloud computing infrastructure.</p>
Public cloud	<p>A public cloud provides its services over a network that is open for public use. There may be little or no difference between public and private cloud architecture, however, since the services are made available for a public audience over a potentially non-trusted network, security consideration may be substantially different. Rackspace or Amazon are examples of public clouds.</p>
Community cloud	<p>A community cloud is where multiple organizations from a specific community with common interests share the cloud infrastructure. They can be managed internally or by a third-party, and either hosted internally or externally. The costs are spread over fewer users than a public cloud, but more than a private cloud.</p>
Hybrid cloud	<p>A hybrid cloud is a combination of two or more clouds that remain distinct but are bound together, offering the benefits of multiple deployment models. Google's "Gov Cloud" is an example. This cloud can be used by government branches within the U.S., but it is not available to consumers or businesses.</p>

## Benefits of Cloud Computing

The following table describes some of the major benefits of cloud computing.

<b>Benefit</b>	<b>Description</b>
Rapid elasticity	To end users, cloud storage often appears to be unlimited storage space. This is due to <i>rapid elasticity</i> . Users request additional space, and the provider allocates additional resources seamlessly to the end user. This can often be done dynamically without any need for the user to contact the hosting provider.
On-demand	On-demand cloud services enable end users to request and access cloud resources as they are needed. This type of cloud service is useful for project-based needs, giving the project members access to the cloud services for the duration of the project, and then releasing the cloud services back to the hosting provider when the project is finished. This way, the organization is only paying for the services for the duration of the project.
Resource pooling	Resource pooling enables the cloud services provider to service multiple customers to suit each customer's needs without any changes made to one customer affecting any of the other customers. Customers can change their service dynamically through on-demand self-service of their accounts.
Measured service	Measured service refers to the cloud provider's ability to monitor and meter the customer's use of resources. This supports the customer's ability to dynamically make changes to the resources they receive. Based on the metered and measured information, the provider knows what resources the customer has used and can then bill for those resources during the next billing cycle.

# ACTIVITY 3–4

## Discussing Cloud Services

## Scenario

There has been a lot of talk around the office recently about cloud services. You have heard some other people touting this as the only way to go for storage. In order to be sure of yourself before you join in these conversations, you wrote down some questions and did a little research about them to make sure you know what you are talking about.

1. How do the five components of cloud computing defined by the NIST work together to provide users with cloud computing services?
  2. Which types of services would your organization be likely to use?
  3. Which type of cloud would your organization be likely to use?

# TOPIC E

## Security Fundamentals

This lesson has introduced you to the basics of networking. Any time that users are sharing files and resources, there is a chance that a security incident can occur. In this topic, you will identify basic concepts related to security.

### Corporate Security Policies

A corporate *security policy* is a formalized statement that defines how security will be implemented and managed within a particular organization. It describes the tasks the organization will undertake to protect the confidentiality, availability, and integrity of sensitive data and resources, including the network infrastructure, physical and electronic data, applications, hardware, computing devices, and the overall physical environment of an organization. It often consists of multiple individual policies that relate to separate security issues, such as password requirements and acceptable use of hardware guidelines. All security measures and controls should conform with all of the security policies enforced by an organization.

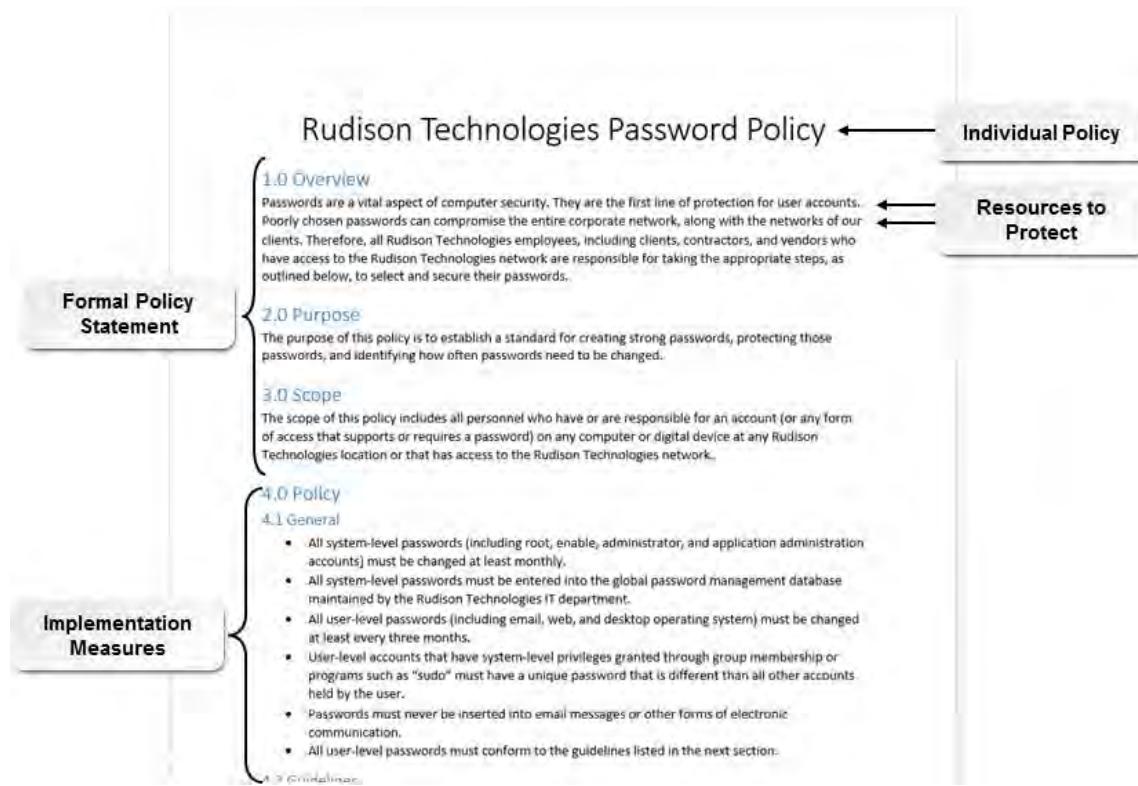


Figure 3-14: A security policy.

### Security Compliance

Security compliance refers to an organization's efforts to enforce its security policies. To ensure data sensitivity and security, many organizations will include the following guidelines in a security policy:

- Patch management guidelines.
- User account and group management.
- Access Control List (ACL) verification.
- Auditing of both systems and data.

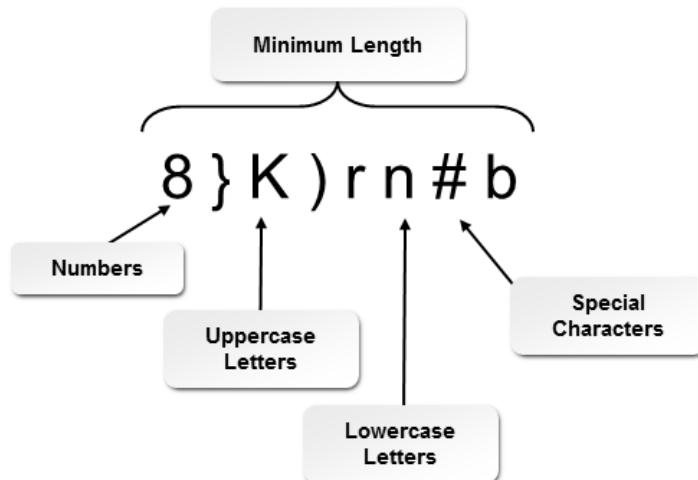
- Security testing.
- User education materials, such as documentation, resources, and training schedules.

## Strong Passwords

A *strong password* is a password that meets the complexity requirements that are set forth by a system administrator and documented in a security policy or password policy. Strong passwords increase the security of systems that use password-based authentication by protecting against password guessing and other password attacks.

Strong password requirements should meet the security needs of an individual organization, and can specify:

- The minimum length of the password.
- Required characters, such as a combination of letters, numbers, and symbols.
- Forbidden character strings, such as the user account name, personal identification information, or words found in a dictionary.



*Figure 3–15: Strong password requirements.*

## User Education

The best protection against *malicious software* or any other security threat is user awareness and education. Providing end users with information about common threats, hoaxes, and security warning signs will enable them to recognize and delete hoax email messages, avoid unauthorized software, and keep antivirus definitions updated. You must support and encourage users to follow security trends and use the organization's resources to stay up-to-date on all recent security incidents and preventative actions. User education is the best defense against data compromise or system damage.

## The Principle of Least Privilege

The principle of *least privilege* dictates that users and software should only have the minimal level of access that is necessary for them to perform the duties required of them. This level of minimal access includes facilities, computing hardware, software, and information. Where a user or system is given access, that access should still be only at the level required to perform the necessary task.



**Figure 3-16: Least privilege.**

## Common User Security Practices

Most security incidents are a result of a user error or unauthorized user action. User errors do not always happen on purpose; sometimes they happen by accident or users are fooled by an attacker. Users need to be aware of their specific security responsibilities and habits. As an A+ technician, you will need to be aware of common security practices used to prevent both types of user security incidents so that you can make sure that all hardware and software implementations support common goals.

Security Area	Employee Responsibilities
Physical security	Employees should not allow anyone in the building without an ID badge. Employees should not allow other individuals to tailgate on a single ID badge. Employees should be comfortable approaching and challenging unknown or unidentified individuals in a work area. Access within the building should be restricted to only those areas an employee needs to access for job purposes. Data handling procedures of confidential files must be followed. Employees must also follow clean desk policies to ensure that confidential documents and private corporate information are secured and filed away from plain sight.
System security	Proper password behaviors can be crucial in keeping systems resources secure from unauthorized users. Employees must use their user IDs and passwords properly and comply with the ID and password requirements set forth by management. Password information should never be shared or written down where it is accessible to others. All confidential files should be saved to an appropriate location on the network where they can be secured and backed up, not on a hard drive or removable media device.
Device security	Employees must follow the correct procedures to log off all systems and shut down computers when not in use. Wireless communication and personally owned devices must (or at least should) be approved by the IT department and installed properly. Policies might be in place to specify how and when personal devices can be used. These devices can be a gateway for attackers to access corporate information and sensitive data. Portable devices, such as laptops and mobile devices, must be properly stored and secured when not in use.
Social networking security	Employees must be made aware of the potential threats and attacks that target social networking applications and websites. The use of these applications can lead to potential breaches in security on an organization's network. Security policies should include guidelines and restrictions for users of any social networking application or website.

## Authentication Methods

Most organizations will employ a variety of authentication methods in order to prevent unauthorized access to the physical building, infrastructure, and resources. Common authentication methods include the following.

<b>Authentication Method</b>	<b>Description</b>
User name and password	In this system, a user or computer must have a valid user name and an associated secret password. The user submits the user name/password combination to an authenticating system such as a network directory server, which validates the credentials against a database and verifies the user's identity. The security of the system can be breached if the authentication database is altered or compromised, whether accidentally or maliciously, or if the credentials, particularly the password, are lost, stolen, or guessed by a third party.
Biometrics	Biometrics are authentication schemes based on individuals' physical characteristics, such as fingerprints or vocal patterns. Biometrics require specialized equipment and software to store, access, and verify the physical information. As biometric authentication becomes less expensive to implement, it is becoming more widely adopted.
Tokens	<i>Tokens</i> are physical or virtual objects, such as <i>RSA tokens</i> , smart cards, and ID badges that store authentication information. Tokens can store personal identification numbers (PINs), information about the user, or passwords. For example, a <i>smart card</i> is a plastic card containing an embedded computer chip that can store different types of electronic information. The contents of the card are read with a special device called a smart card reader, which can be attached to a PC. When used for authentication, the smart card will store user credentials or private information such as a password or PIN. The user must present the smart card as a token of the user's identity, and so smart cards are sometimes classified as a form of token-based authentication.
Multi-factor authentication	An authentication scheme with just one factor can be called single-factor authentication, while a two- or three-factor authentication scheme can simply be called <i>multi-factor authentication</i> . It can be any combination of what you are, what you have, and what you know. System designers determine what specific factors are required during the design phase.  If a user is required to pass a fingerprint scan as well as to enter a password to gain access to a secure facility, this would combine the "who you are" and "what you know" factors. Multi-factor authentication enhances the security of using any single factor alone. Token-based or biometric-based authentication are rarely deployed alone; more frequently, they are used in addition to user name and password authentication.
Mutual authentication	<i>Mutual authentication</i> is a security mechanism that requires that each party in a communication verify its identity. First, a service or resource verifies the client's credentials, and then the client verifies the resource's credentials. Mutual authentication prevents a client from inadvertently submitting confidential information to a non-secure server. Any type or combination of authentication mechanisms can be used.

### Biometric Authentication Methods

Biometrics are used often in high security areas where there is a restricted security clearance, such as in government offices and financial institutions. There are several categories of biometric authentication.

<b>Biometric Authentication Method</b>	<b>Description</b>
Fingerprint scanner	A user's fingerprint pattern is scanned and stored. To authenticate, the user scans a finger again and the print is compared to the stored image in the authentication database. The fingerprint scanner can be a small separate hardware device, and is even built into some laptops, mice, and universal serial bus (USB) flash drives.
Hand geometry scanner	An individual's hand geometry can also be used for authentication. Hand scanners have pegs between which users insert their fingers. Once the initial scan is stored, and then used to authenticate, subsequent scans are compared to the stored scan in the authentication database.
Retinal scanner	The pattern on a user's retina is scanned and stored. To authenticate, the user scans an eye again and the pattern is compared to the authentication database.
Voice recognition	The user provides a speech sample that is analyzed with voice-recognition software and stored. To authenticate, the user speaks again and the speech patterns are analyzed by the software and compared against the stored sample in the authentication database.
Face recognition	A digital image of the user's face is analyzed with face-recognition software and stored. To authenticate, the user's face is scanned digitally again and the facial appearance is compared against the stored image in the authentication database.
Biometric authentication tokens	Biometric user data can be scanned and encoded once and then stored on a chip on some form of portable electronic security token, such as a smart card or a digital key fob. To authenticate, the user presents the token instead of submitting to another biometric scan. Because the token could be lost or stolen, it is best to combine this type of authentication with a password or PIN, or at least to include a user photograph on the card for visual confirmation of the user's identity.

## Encryption

*Encryption* is the process of converting data into a form that is not easily recognized or understood by anyone who is not authorized to access the data. Only authorized parties with the necessary decryption information can decode and read the data. Encryption can be one-way, which means the encryption is designed to hide only the cleartext and is never decrypted, or it can be two-way, in which the encryption can be decrypted back to cleartext and read.

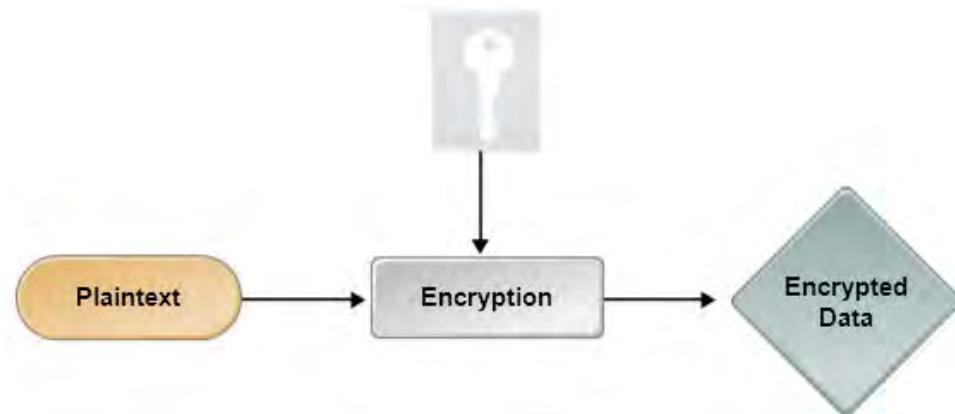


Figure 3-17: Encryption.

## Malware

*Malware* is any unwanted software that has the potential to damage a system, impede performance, or create a nuisance condition. The software might be introduced deliberately or inadvertently and might or might not be able to propagate itself to other systems.

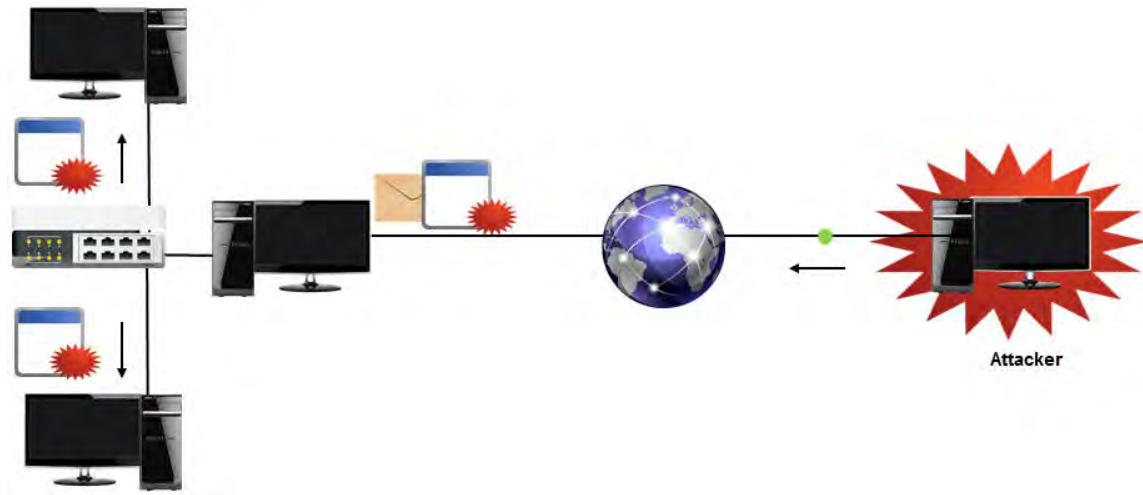


Figure 3-18: Malware.

# ACTIVITY 3–5

## Identifying Security Concepts

### Scenario

In this activity, you will identify common security concepts.

1. Katie works in a high-security government facility. When she comes to work in the morning, she places her hand on a scanning device in her building's lobby, which reads her hand print and compares it to a master record of her hand print in a database to verify her identity. This is an example of:
  - Biometric authentication
  - Multi-factor authentication
  - Data encryption
  - Tokens
2. How does multi-factor authentication enhance security?
3. While assigning privileges to the accounting department in your organization, Cindy, a human resource administrative assistant, insists that she needs access to the employee records database in order to fulfill change of address requests from employees. After checking with her manager and referring to the organization's access control security policy, Cindy's job role does not fall into the authorized category for access to that database. What security concept is being practiced in this scenario?
  - The use of strong passwords.
  - User education.
  - The principle of least privilege.
  - Common user security practices.

## Summary

In this lesson, you got a brief introduction to network and security concepts and features. Every organization will implement these features and concepts in one way or another, depending on their needs.

**Which of the network features presented in this lesson does your organization currently use and support? Which ones do you think they should use if they are not currently using them?**

**How do the security fundamentals presented in this lesson support the network components and services and cloud features presented in this lesson?**



**Note:** Check your CHOICE Course screen for opportunities to interact with your classmates, peers, and the larger CHOICE online community about the topics covered in this course or other topics you are interested in. From the Course screen you can also access available resources for a more continuous learning experience.

# 4 Safety and Operational Procedures

**Lesson Time:** 1 hour, 30 minutes

## Lesson Objectives

In this lesson, you will identify the operational procedures that should be followed by professional PC technicians. You will:

- Identify basic tools and techniques for maintaining PCs, mobile devices, and printing devices.
- Identify best practices to follow to ensure personal and electrical safety.
- Identify best practices to follow to ensure environmental safety and the proper handling of potentially harmful materials.
- Identify best practices for entry-level IT professionals to use for appropriate communication with clients and colleagues.
- Identify common organizational policies and procedures that deal with computer use.
- Explain troubleshooting theory.

## Lesson Introduction

In the previous lessons, you gained fundamental knowledge about personal computer hardware components and operating systems. In addition to that information, every PC technician also needs a working knowledge of tools, safety and environmental precautions, and when professional conduct is important in the workplace. In this lesson, you will identify the operational procedures that you should follow to ensure a safe working environment.

As an A+ technician, you will be asked to install, configure, maintain, and correct problems with a variety of PC components. To work with these components without damaging them or causing physical injury to yourself or others, there are several tools to use and operational procedures to follow in order to get the job done quickly, safely, and correctly.

# TOPIC A

## Basic Maintenance Tools and Techniques

In this lesson, you will identify the operational procedures that can help ensure your success as an A+ certified professional. To begin, it's critical to select the right tool or technique for the job. In this topic, you will identify common hardware and software tools, maintenance techniques, and resources that are used by professional PC technicians.

When it comes to computer maintenance, having the right tool will save time, trouble, and money. Having a good collection of software and hardware tools at your disposal, a foundational knowledge of maintenance techniques, and access to documentation or resources when you need assistance is essential to help you perform your job tasks efficiently.

### Types of Hardware Toolkits

Because of the complexity of personal computers, there are several types of hardware toolkits that are commonly used in PC maintenance and repair.

- A basic toolkit should contain the tools necessary to remove and install computer components. Each tool should be demagnetized, and the tools should be stored in a case to protect and organize them. Basic toolkits should include:
  - Pen and/or pencil.
  - Phillips screwdrivers (small and large, #0 and #1).
  - Flat-blade screwdrivers (small and large, 1/8-inch and 3/16-inch).
  - Flashlight.
  - Container for screws.
  - Nut driver.



**Figure 4-1: A basic toolkit.**

- An extended toolkit builds on the basic toolkit by including additional items such as:
  - Additional sizes of drivers and screwdrivers.
  - Torx driver (size T8, T10, and T15).
  - Tweezers.

- Three-prong retriever.
- Ratchets.
- Allen wrenches.
- Cotton swabs.
- Batteries.
- Anti-static cleaning wipes.
- Anti-static wrist band.
- Compressed air canister.
- Mini vacuum.
- Pen knife.
- Clamp.
- Chip extractor.
- Chip inserter.
- Multimeter.
- Soldering iron and related supplies.
- Spare parts container.
- Circuit tester.
- Drive adapters (USB to IDE/SATA and SATA/PATA/IDE to USB).



**Figure 4-2: An extended toolkit.**

- A network toolkit contains specialized tools to make and install network cables. Prices for these toolkits can vary widely depending on the number and quality of the tools included. Network toolkits typically include:
  - Cable crimper with dies for a variety of cable styles.
  - Wire stripper for flat and coax cable.
  - Precision wire cutters.
  - Cable tester.
  - Punch down tool.
  - Curved forceps.
  - Multi-network Local Area Network (LAN) cable tester.
  - Digital multimeter.

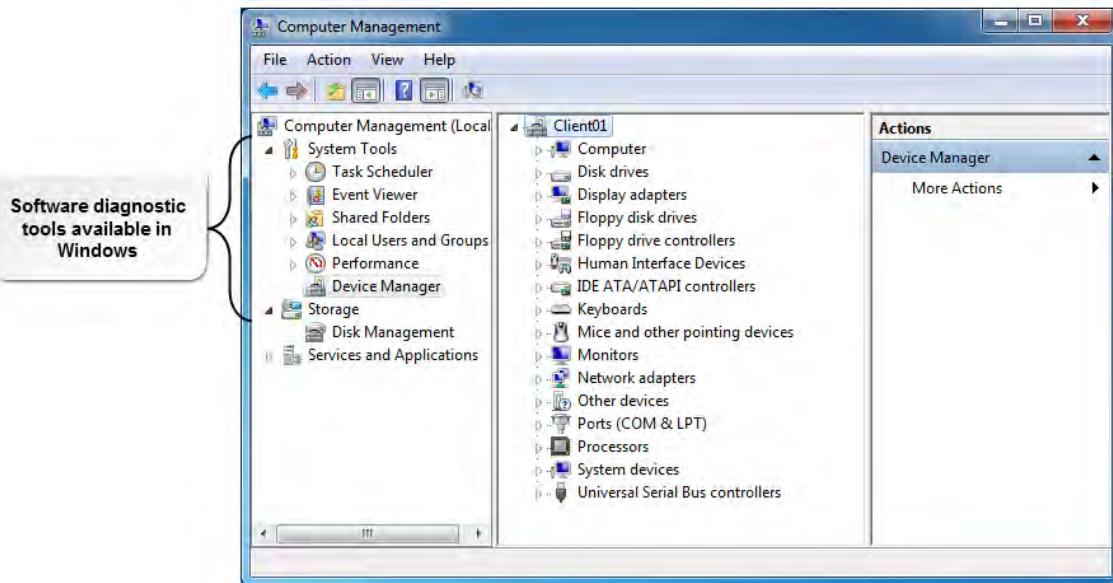


**Figure 4–3:** A network toolkit.

## Software Diagnostic Tools

A *software diagnostic tool* or utility is a computer repair program that can analyze hardware and software components and test them for problems. Some software diagnostic tools can repair software problems and optimize settings. Most operating systems include several software diagnostic tools integrated into them. In addition, most computer stores have at least one aisle dedicated to utility software that has been developed by other software manufacturers.

Microsoft® Windows® provides a few different software diagnostic tests that you can use to identify and repair computer hardware and software issues. For example, you can automatically fix file system errors on any disk in the PC by using the **Disk Management** tool.



**Figure 4–4:** Software diagnostic tools.

## Hard Drive Self Tests

Most hard disk drive manufacturers provide a diagnostic tool that enables the drive to test itself when you start up a PC. Some of these hard drive self-tests are built into the firmware for the hard disk drive, while others are separate utilities that are available for download from the drive manufacturer's website. Make sure that you download the test utility that was designed to be used with your hard disk drive.

## Software Diagnostic Tests

Software diagnostic tests are available from many different manufacturers, and they vary widely in their capabilities, but they can all assist you in detecting, repairing, and preventing hardware and software problems. The Windows operating systems also come with their own sets of diagnostic tools that can help you detect problems.

There are many applicable software diagnostic tests that you can use to troubleshoot computer problems.

<b>Hardware Component</b>	<b>Examples of Software Diagnostics Test</b>
Entire system	PC-Doctor Service Center, PC-Diag, Norton™ SystemWorks, QuickTech Pro, McAfee® System Mechanic, CheckIt Diagnostics, DirectX Diagnostic Tool, Windows <b>Device Manager</b> , Windows <b>Performance Monitor</b>  There are many additional antivirus and anti-malware software solutions provided that detect and remove viruses, malware, and spyware.
Motherboard	Motherboard Diagnostic Toolkit, Power-On Self Test (POST), Basic Input/Output System (BIOS) setup
Central processing unit (CPU)	x86test, POST, BIOS setup
Memory	Memtest86+, DocMemory Diagnostics, POST, BIOS setup
Fan	SpeedFan, BIOS setup
Video adapter card	Video Card Stability Test, DirectX Diagnostic Tool, POST, BIOS setup
Network adapter card	3Com Dynamic Access Managed PC Boot Agent (MBA), Intel® PROset II Utility, DirectX Diagnostic Tool
Modem	Modem Doctor Diagnostics, DirectX Diagnostic Tool, Windows Device Manager, Windows Performance Monitor
Optical drive	CDRoller, Windows Device Manager, Windows Performance Monitor

## Maintenance Techniques for Computer Components

You can choose from several maintenance techniques to maintain PC components.

<b>Maintenance Technique</b>	<b>Description</b>
Use proper power devices.	Use a surge protector or <i>uninterruptible power supply (UPS)</i> to protect the computer from power surges, spikes, brownouts, and power failures.
Clean peripheral components.	Use to prevent problems with the computer's peripherals resulting from dust buildup.
Clean internal system components.	Use to prevent problems with internal computer components resulting from dust buildup.

## Cleaning Materials

Cleaning materials for computers range from standard household cleaning supplies to supplies specifically designed for computers and electronics.

<b>Cleaning Supply</b>	<b>Description</b>
Wipes and cloths	<p>There are several types of wipes and cloths that you can use to clean displays, keyboards, and other equipment.</p> <ul style="list-style-type: none"> <li>Monitor cleaning wipes are alcohol-based, lint-free, pre-moistened wipes for cleaning monitor screens. Use these only on cathode ray tube (CRT) or TV monitors and not on plastic-coated liquid crystal display LCD screens.</li> <li>Keyboard cleaning wipes are pre-moistened wipes for cleaning keyboards.</li> <li>You can use microfiber cloths to lightly remove dust and smudges from LCD displays. You can also use an LCD cleaning solution with the cloth to remove particles and smudges that are stuck to the screen.</li> <li>If you choose not to use pre-moistened wipes, you can use rubbing alcohol applied to a lint-free cloth to wipe down screens and keyboards. You can also use this to clean other components.</li> <li>A toner cloth is a special cloth that you stretch that picks up toner particles that are either in the printer or around the printer. Be careful if you are using it inside the printer so that the cloth does not get caught on any components and leave fibers behind.</li> </ul>
Cleaning solutions	<p>There are a variety of cleaning solutions that you can use to clean displays, keyboards, and other equipment.</p> <ul style="list-style-type: none"> <li>You can use rubbing alcohol on cotton swabs or lint-free cloths to clean many components.</li> <li>You can use mild household cleaner to keep the exterior of computer components clean. This helps prevent dirt and debris from getting inside the equipment. Never spray the cleaner directly on the equipment. Avoid using ammonia-based cleaners around laser printers; the ammonia may react chemically with the toner.</li> <li>For older monitors, especially plastic monitors, read the device's manual to determine the cleaning method recommended by the manufacturer. While some recommend water or isopropyl alcohol (IPA), others claim it is acceptable to use volatile chemicals such as hexane or petroleum benzene, a soft detergent such as Palmolive and water, no suds, or nothing but a dry soft cloth. While some recommend a top-down motion, others subscribe to the circular method.</li> <li>For flat screens such as LCDs, light emitting diodes (LEDs), and plasmas, you can use distilled water, or an equal ratio of water and vinegar on a microfiber or lint-free cloth. There are also specialized cleaners available for flat screens, but make sure to check the manufacturer's instructions before use.</li> <li>In some cases, you can use standard household window cleaner on components if you spray it on a lint-free cloth first. You can use this to clean smudges from optical discs. Never use window cleaner on plastic monitor screens, and even on glass screens; this cleaner might strip off the anti-glare protection. The best option is a damp, clean, soft cloth with water or a cleaner specifically made for monitors (or one that states it is safe for use with monitors) and will not damage anti-glare finishes.</li> </ul>

Cleaning Supply	Description
Cleaning tools	<p>Several tools are optimal for cleaning computer components.</p> <ul style="list-style-type: none"> <li>Tightly wound cotton swabs are useful in getting cleaning solution into tight places. They are also useful when used dry to get dust and debris out from between keys and around buttons or other tight areas.</li> <li>Toothpicks come in handy in getting dirt out from around keys, buttons, and other tight spaces. They are also useful for removing the debris that builds up on the rollers inside of a mouse.</li> <li>You can use a small paint brush to remove dust from between keys on a keyboard. If the brush has long bristles, they can reach under the keys where other cleaning objects would not be able to reach.</li> </ul>
Compressed air canister	<p>A canister with a nozzle that can be aimed at components to blow dust out. This is often used when removing dust from the interior of a computer or laptop. Be sure to blow the dust away from the power supply and drives. You can also use it to blow dust out of the power supply fan area, from keyboards, and from the ventilation holes on various components.</p> <p>Use caution when working with compressed air. Read the instructions on the can and follow them carefully. Tipping the can too much, which is easy to do when you are trying to maneuver the can into place, can cause the propellant to leave the can in liquid form and at sub-freezing temperatures. The freezing could easily damage components, particularly those that may still be hot from use. There is also the issue of the corrosiveness of the chemical damaging components later on. Also, some delicate components on the motherboard can be damaged (literally blown off the board) if compressed air is used too close to a component.</p> <p>If you use compressed air, take the equipment to a different location, preferably outside, so that the dust does not simply disperse into the air in the work area and settle back on the computer equipment or other devices.</p>
Computer or electronics vacuum	<p>A non-static vacuum that you can use on system components such as the power supply, fans, and in printers. (Regular vacuum cleaners can create static, which will damage computer equipment.) The vacuum should have a filter and bag fine enough to contain toner particles so that you can use it to clean up toner spills from laser printers or photocopiers. These vacuums can often be used to blow air as well as for suction, so they can replace the need for compressed air canisters for blowing dust out of machines. Sucking the dust up is usually better, though, since blowing the dust can cause it to get onto or into other components. Sucking it up into a vacuum cleaner bag gets it out of the system without the chance of it getting into something else.</p>
Mask and gloves	<p>A mask that fits over your mouth and nose should be worn when you are using a compressed air canister or working around toner spills. This will keep the particles out of your body. You should also wear latex gloves when cleaning up a toner spill.</p>



**Note:** For additional information, check out the LearnTO **Clean a Desktop Computer** presentation in the LearnTOs for this course on your CHOICE Course screen.

## Documentation and Resources

There are several types of documentation and resources that you might find helpful when you are dealing with common hardware and operating system problems. You can also share documentation and resources with users as a means of assisting and educating them.

<b>Resource</b>	<b>Description</b>
User/installation manuals	User and installation manuals can provide you with basic guidance for installing, configuring, and troubleshooting hardware and software.
	By providing users with various user and installation manuals, users can fix minor issues and problems before requesting additional assistance from a technician. Examples include installing company-specific applications, installing network printers, and mapping drives.
Internet/web-based resources	Internet and web-based resources can provide a wealth of information on installing, configuring, and troubleshooting hardware and software. Many hardware and software manufacturers maintain knowledge bases and wikis to share information about both common and unusual issues that can arise with PC hardware and software.
	Internet and web-based materials can also provide users with quick reference materials for dealing with everyday issues on their own. Some organizations provide a web page or wiki with user-specific information and reference materials.
Training materials	Most major hardware and software manufacturers provide training materials on how to install and use their products. These materials can be helpful for both new and experienced technicians.
	You can provide training materials for various tasks that users may need to complete on their own, such as virus scans, computer maintenance tasks, and PC clean-up tasks. By providing training materials, you empower users to be proactive in maintaining their systems.

## Compliance and Governmental Regulations

In the United States and many other nations, your employer is obligated to comply with governmental regulations that apply to its specific business. The most common regulations are those issued by the federal government, such as the Occupational Safety and Health Administration (OSHA), and state standards regarding employee safety. OSHA-compliant employers must provide:

- A workplace that is free from recognized hazards that could cause serious physical harm.
- Personal protective equipment designed to protect employees from certain hazards.
- Communication—in the form of labeling, Material Safety Data Sheets (MSDSs), and training about hazardous materials.

Your responsibility—to yourself, your employer, your coworkers, and your customers—is to be informed of potential hazards and to always use safe practices.

Protection of the environment is another area that is regulated by the federal and local governments in the United States and many other nations. Many municipalities have regulations that control the disposal of certain types of computer equipment. Your responsibility is to be aware of any environmental controls that are applicable to your workplace, and to be in compliance with those regulations.

## ACTIVITY 4-1

### Discussing Basic Maintenance Tools and Techniques

#### Scenario

In this activity, you will examine the various tools and techniques used to maintain computer equipment and the workplace environment.

1. You are asked to correct a network cabling problem at a customer site. Which set of tools would be best suited for the task?
  - Phillips screwdriver (#0), torx driver (size T8, T10, and T15), tweezers, and a three-prong retriever
  - Wire strippers, precision wire cutters, digital cable tester, and cable crimper with dies
  - Chip extractor, chip inserter, ratchet, and Allen wrench
  - Anti-static cleaning wipes, anti-static wrist band, flashlight, and cotton swabs
2. You suspect that contaminants from the environment have prevented the fan on a PC from working optimally. Which set of tools would be best suited to fix the problem?
  - Phillips screwdriver (#0), torx driver (size T8, T10, and T15), tweezers, and a three-prong retriever
  - Wire strippers, precision wire cutters, digital multimeter, and cable crimper with dies
  - Chip extractor, chip inserter, ratchet, and Allen wrench
  - Anti-static cleaning wipes, anti-static wrist band, flashlight, and cotton swabs
3. True or False? Windows includes software diagnostic tests that help you find and correct hardware problems.
  - True
  - False
4. Examine the tools that are available to you in class. Discuss how and when they may be used to repair, fix, or maintain computer equipment.

# TOPIC B

## Personal and Electrical Safety

In the previous topic, you identified basic maintenance tools and techniques that you will use as a PC technician. In addition to these basic maintenance practices, you need to be aware of specific tools and techniques that are available to promote electrical safety. In this topic, you will identify the best practices for PC technicians to follow to promote electrical safety.

The most prevalent physical hazards that computer technicians face are electrical hazards. Electricity is necessary to run a computer, but it can also damage sensitive computer equipment, and in some cases, pose a danger to humans. Following established best practices for promoting electrical safety will protect not only the computer equipment that you work on, but also your personal safety and the safety of others.

### Static Electricity

*Static electricity* is a build-up of electrical potential energy that is caused by bringing two different materials into contact. Rubbing those materials together increases the frequency of the contact, and this produces static electricity through *triboelectric generation*. When two materials are in contact, one can attract more electrons than the other. Separate the materials, and some electrons can transfer to the material that attracts them most strongly. That leaves one material with extra electrons (and negatively charged) and the other material with fewer electrons (and positively charged). This accumulated imbalance of charges on an object is static electricity.



**Note:** Static charges can be as small as the sparks that come off a dry blanket in the wintertime or as massive as a lightning strike, with its millions of volts.

### ESD

*Electrostatic discharge (ESD)* occurs when a path is created that allows electrons to rush from a statically charged body to another with an unequal charge. The electricity is released with a spark. The charge follows the path of least resistance, so it can occur between an electrical ground, such as a doorknob or a computer chassis, and a charged body, such as a human hand. ESD can damage sensitive computer equipment.

Because air has very high resistance, a static electric discharge usually requires contact with the statically charged object. For a static discharge to arc through the air, it requires a very high voltage, and no other path to the ground with lower resistance. You can feel a static discharge starting at around 3,000 volts (V). The drier the air, the greater the resistance, which is why static shocks on dry winter days can fall within the range of 10,000 to 20,000 V. Keeping a room humidified is one way to reduce the risk of static electricity.

If 120 V from a household electrical outlet can kill you, why does a static spark of 20,000 V just startle you? Because, while the voltage might be high, the current is very low; very few total electrons are transferred in a static spark. All the energy of all the electrons in a spark added together cannot hurt you, even though it may surprise you. Each electron in a static discharge has extremely high energy, but the human body is just too big for the very small number of electrons involved in the spark to cause widespread damage. A few cells in your fingertip may be damaged, but they easily grow back.

### ESD Prevention Techniques

Charges as low as 10 to 100 V can damage or destroy sensitive electronic circuits and components. This is why ESD is such an enemy of integrated circuits. Static charges can build up on both

conductors and insulators, as well as in the human body. When you work with computer equipment, you must take steps to protect against ESD.

There are several prevention techniques that you can use to protect yourself and equipment when you are working with computer components.

<b>Prevention Technique</b>	<b>Description</b>
Eliminate activities and tasks	By eliminating unnecessary activities that create static charges and by removing unnecessary materials that are known charge generators, you can protect against ESD-related damage and injuries.
Use self-grounding methods	Use grounding conductive materials and self-grounding methods before touching electronic equipment. You can prevent ESD injuries by using ESD straps that can be attached to your ankle or wrist.
Use equipment grounding methods	Grounding equipment made up of <i>dissipative material</i> can also be used to avoid a static shock. A dissipative material is a conductor, but with high resistance. It loses its electrical charge slowly, so when you touch it, the electron flow is spread over time and you do not feel a shock. Prevent ESD damage to equipment by: <ul style="list-style-type: none"> <li>• Using anti-static vacuums for cleaning computer components (such as system units, power supplies, and fans).</li> <li>• Using ESD mats and materials such as electric grounded flooring, work benches, or surfaces.</li> <li>• Using anti-static bags to store computer components that are particularly sensitive to ESD, such as RAM and power supplies.</li> </ul>
Maintain air quality	You can maintain air quality and prevent a high-ESD work environment by: <ul style="list-style-type: none"> <li>• Using an air ionizer, which releases negative ions into the air. They attract positively charged particles and form neutrally charged particles.</li> <li>• Humidifying the air to speed up the static discharge from components. When the air is extremely dry, more static is likely. A higher humidity is best for ESD prevention. A rate of 50 to 60 percent is comfortable for both computers and technicians.</li> </ul>

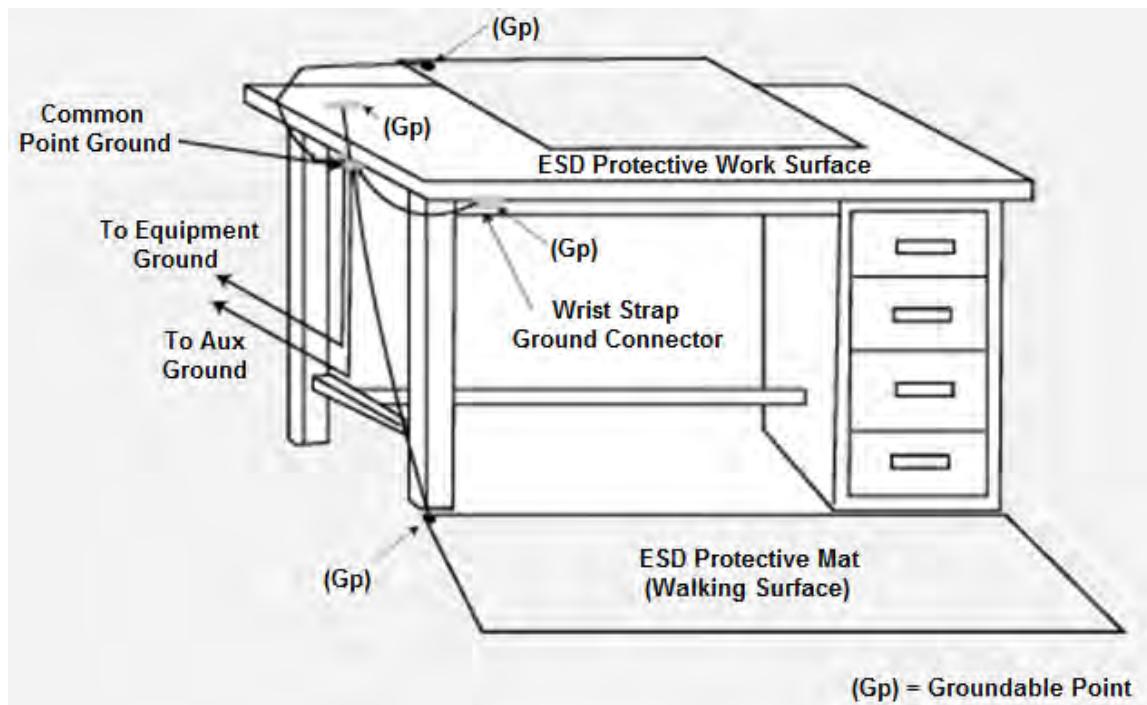
## Anti-static Bags

Anti-static bags that are used for shipping components actually conduct electricity, so keep them away from equipment that is powered on.

## ESD Tools

Some people who work on computer equipment never use a single piece of ESD safety equipment. They discharge themselves by touching an unpainted metal part of the computer case before touching any components. In other instances, a company policy might require that you use a properly equipped ESD-free work area. The minimum equipment in this case would be a grounded wrist ESD strap. Other ESD-protection equipment includes leg ESD straps, anti-static pads to cover the work surface, and grounded floor ESD mats to stand on. The mats contain a snap that you connect to the wrist or leg strap. Anti-static bags for storing components might also be included in an ESD toolkit. If the technician's clothing has the potential to produce static charges, an ESD smock, which covers from the waist up, can be helpful.

To ensure that the ESD equipment remains effective, you should test it frequently. A minor shock that you cannot feel can compromise ESD-sensitive equipment.



**Figure 4-5: An ESD-free workspace.**

## EMI

*Electromagnetic interference (EMI)* occurs when a magnetic field builds up around one electrical circuit and interferes with the signal being carried on an adjacent circuit, causing network communication interference issues. All current-carrying devices generate magnetic fields, and fluctuating magnetic fields generate electrical current in nearby wires. While ESD is the primary electrical danger to computer equipment, EMI also causes problems with microcomputer circuitry and data transmissions between computing devices.

EMI-related issues can also be a result of magnets being placed too close to computer systems. Magnets can be harmful to computer components, and components should not be placed in close proximity to any magnets or items that contain magnets. It's important that you inform users to keep magnets away from their computer equipment.

## Electrical Hazards

Because computers are powered by electricity, there are some common potential electrical hazards that you should be aware of when you are servicing them.

<b>Electrical Hazard</b>	<b>Description</b>
Electric shock	If you touch a high-voltage source, and if you are either grounded or in contact with another electrical circuit, your body may complete an electrical circuit, permitting electrons to flow through you. Water is a better conductor than air or dry skin, so touching an electrical contact with wet hands reduces resistance and increases the current flow even more. Depending on the conditions, this may cause pain, burns, or even death.

Electrical Hazard	Description
Electrocution (fatal shock)	Electrocution results when the body is exposed to a lethal amount of electrical energy. For death to occur, the body must become part of an active electrical circuit with a current capable of overstimulating the nervous system or damaging internal organs. The extent of injuries received depends on the current's magnitude (measured in amperes), the pathway through the body, and the duration of flow. The resulting damage to the human body and the emergency medical treatment determine the outcome.
Burns	<p>Contact with a source of electrical energy can cause external and internal burns. Exposure to higher voltages will normally result in burns at the sites where the electrical current entered and exited the body. High-voltage contact burns may display only small superficial injuries; however, the danger of these deep burns is destruction of internal tissues.</p> <p>Electricity can hurt you even if you are careful and avoid becoming part of an electrical ground circuit. The heat generated by an electric arc or electrical equipment can burn your skin or set your clothes on fire.</p>
Collateral injuries	Collateral injuries occur when involuntary muscle contractions caused by the shock cause the body to fall or come in contact with sharp edges or electrically live parts. You instinctively pull your hand back from the doorknob when you get a static shock. Electricity flowing through your body can also cause your muscles to twitch uncontrollably. These motions can cause you to hurt yourself on objects around you.

## Power Supplies and Electrical Hazards

Most of the internal circuitry in a computer is low voltage (12 V or less) and low current, so there is not much of a threat to your personal safety. However, there are exceptions to this, and these exceptions can be very dangerous. The main exceptions that you need to be aware of are power supplies. The computer's power supply outputs a relatively low voltage, but the high-voltage input can be hazardous. PC technicians who have diagnosed a bad power supply should simply replace it, rather than open it to troubleshoot the internal components.

## Laser Printer Electrical Safety

Laser printers contain high-voltage electronic components inside the case, and these components can be harmful if not handled properly. Components such as the rollers and wires can hold a charge, and you should avoid contact with them. Follow proper cleanup and safety guidelines to prevent electrical shock when you are working with laser printers.

## ESD and Electrical Hazards

All of the precautions that you use to prevent ESD *increase* your danger when you work near high voltages. An anti-static wrist band is specifically designed to provide a low-resistance path for electricity to a ground. If there were ground problems or shorts, your body and your static protection equipment could provide a path from the problem device to ground—the circuit would be completed through your body, causing electrocution.

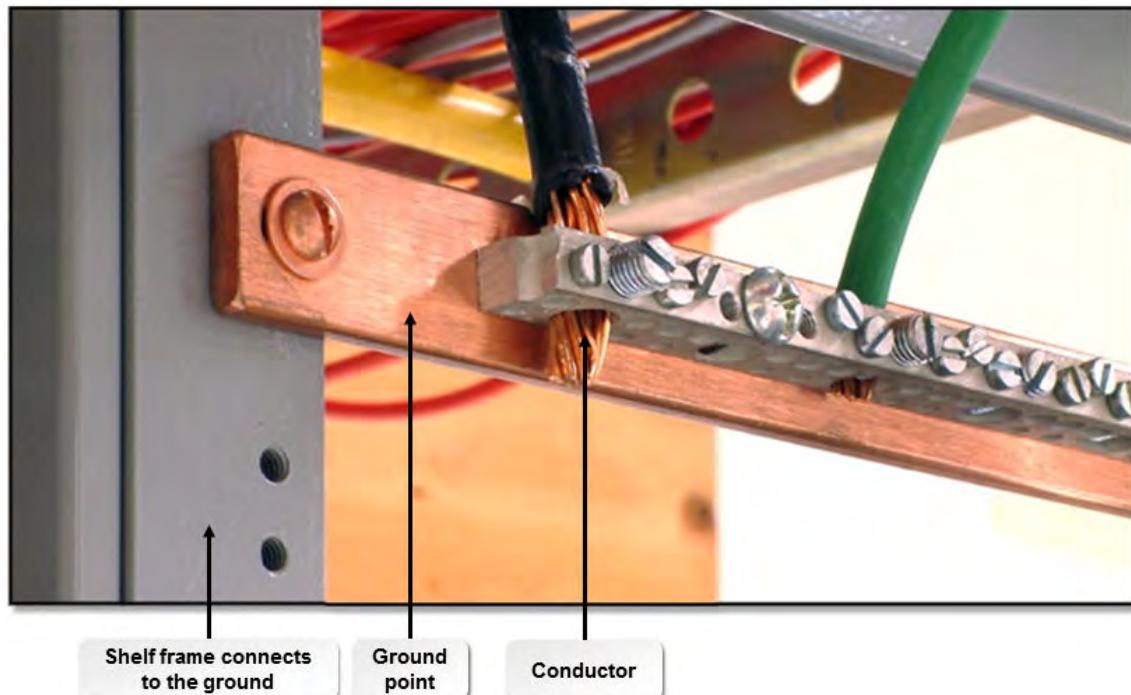
This is precisely why you must unplug devices that you are servicing. Even when devices are turned off, the power supplies in most devices continue to produce voltage if the device is plugged into an outlet. You and your anti-static devices could provide a better path to ground than the device's wiring, leading to your electrocution. If there is a chance of coming in contact with a high-voltage source, you are advised to insulate yourself from ground by wearing rubber-soled shoes or standing on a rubber mat, and avoiding contact with any other grounded mass.

## Power Inverter Electrical Safety

A power inverter converts direct current (DC) voltage to AC voltage. For example, you can use a power inverter in a car to provide a normal wall-style outlet for a laptop. The power inverter unit has no user-serviceable parts within it, so after you determine that the inverter is a problem, there is no need for further diagnosis and troubleshooting; the unit must be replaced.

## Equipment Grounding

Grounding is the connection of a shield or conductor to an electrical ground point, such as a pipe or wire that is in contact with the ground. Grounding at one point in a segment helps prevent noise on the data conductor by shunting noise signals to ground. Connecting to ground at multiple points can introduce noise onto the line, degrading network performance.



*Figure 4-6: Grounding using a shelf frame.*

Electrical devices often must be connected to a ground point for safety. In these situations, the ground connection serves as a way to direct high voltages safely away from humans and other devices, sending them instead into the ground.

You should ground networking and other sensitive electronic equipment to dedicated ground points rather than to pipes and conduits. Electricians refer to this sort of ground connection as an isolated ground and will use an orange socket for such circuits.

## Personal and Electrical Safety Precautions

Working on a computer can be safe and enjoyable if you protect yourself from electrical hazards by using some common sense and by taking appropriate precautions.

<b>Category</b>	<b>Guidelines</b>
Personal safety	<ul style="list-style-type: none"> <li>• Make sure that you disconnect the power before repairing computer equipment.</li> <li>• Do not attempt repair work when you are tired; you may make careless mistakes, and your primary diagnostic tool, deductive reasoning, will not be operating at full capacity.</li> <li>• Do not assume anything without checking it out for yourself.</li> <li>• Remove jewelry or other articles that could accidentally contact circuitry and conduct current.</li> <li>• Wear rubber-soled shoes to insulate yourself from ground.</li> <li>• After turning off the device and removing the power source, press the power button again to drain any residual power.</li> </ul>
Environment conditions	<ul style="list-style-type: none"> <li>• Suspend work during an electrical storm.</li> <li>• Do not handle electrical equipment when your hands or feet are wet or when you are standing on a wet surface. Perform as many tests as possible with the power off.</li> </ul>
Anti-static equipment	<ul style="list-style-type: none"> <li>• Prevent static electricity from damaging components by standing on a totally insulated rubber mat to increase the resistance of the path to ground. In some cases, workstations are located in areas with grounded floors and workbenches, so static electricity has a low-resistance, non-destructive path to ground.</li> <li>• When removing circuit boards, place them on a dissipative ground mat or put them in an anti-static bag.</li> <li>• Use an anti-static wrist strap when you are handling static-sensitive components such as system boards, sound cards, and memory chips.</li> </ul>
Disassembly safety	<ul style="list-style-type: none"> <li>• After cleaning a component, be completely sure it is dry before powering it up.</li> <li>• Label wires and connectors as you detach them, and make sure that you plug them back into the proper sockets in the proper order.</li> <li>• When you replace the computer's case, make sure that all of the wires are inside. The case may have sharp edges that can cut through exposed cables.</li> </ul>
Power supply safety	<ul style="list-style-type: none"> <li>• Power supplies have a high voltage in them any time the computer is plugged in, even if the computer power is turned off. Before you start working inside the computer case, disconnect the power cord and press the power button to dissipate any remaining power in the system circuitry. Leave the power off until you are done servicing the system unit.</li> <li>• Never stick anything into the power supply fan to get it to rotate. This approach does not work, and it is dangerous.</li> </ul>

<b>Category</b>	<b>Guidelines</b>
Electrical fire safety	<p>Electrical fires in computer facilities are especially dangerous. The damage done to computers is extremely expensive, and the chemicals used in the machines may emit toxic substances. It is not practical to fight these fires with small extinguishers or to douse fires with water. Special gases should be used to extinguish fires in computer facilities. To prevent electrical fires:</p> <ul style="list-style-type: none"> <li>• Check the electrical wiring of computer systems and components regularly.</li> <li>• Implement a strategy to make sure any old, worn, or damaged cables, network appliances, and computer systems are checked and replaced regularly.</li> <li>• Verify that smoke detectors are installed to sense the presence of smoke.</li> <li>• Use heat sensors that are triggered either when a target temperature is reached or when there is a high rate of increase in temperature.</li> <li>• Use flame detectors with optical sensors to record incoming radiation at selected wavelengths.</li> </ul> <p>Commercial fire detection systems should be connected to a central reporting station where the location of the suspected fire is indicated. In some cases, the detection system or monitoring station is connected directly to a fire department.</p>

## ACTIVITY 4-2

### Discussing Personal and Electrical Safety Issues

#### Scenario

In this activity, you will identify electrical safety issues.

1. **True or False? If you are using an anti-static ESD floor mat, you do not need any other ESD safety equipment.**  
 True  
 False
2. **Electrical injuries include electrocution, shock, and collateral injury. Would you be injured if you are not part of the electrical ground current?**
3. **Which computer component presents the most danger from electrical shock?**  
 System boards  
 Hard drives  
 Power supplies  
 System unit
4. **Have you had any personal experience with any of the electrical hazards covered in this topic? What safety precautions could have prevented the incident?**

# TOPIC C

## Environmental Safety and Materials Handling

In the previous topic, you identified best practices for safely dealing with electricity. Electrical safety is just one factor that you need to consider to ensure a safe work area. In this topic, you will identify best practices for promoting environmental safety and proper materials handling.

In addition to electrical issues, there are other environmental issues that computer technicians must deal with on a regular basis. The health and safety of you and those around you should always be your highest priority. Recognizing potential environmental hazards and properly dealing with them in a safe manner is a critical responsibility for an A+ technician.

### Environmental Considerations

Certain environmental conditions can be extremely dangerous to you and those around you.

<b>Consideration</b>	<b>Description and Controls</b>
Ozone gas	Laser printers produce ozone gas, usually when the corona wire produces an electrical discharge during printing. Depending on the levels, ozone can be a mild-to-severe irritant. Regulatory agencies have established limits regarding the amount of ozone that employees can be exposed to. Be sure that your laser printers operate in a well-ventilated area. Some laser printers have a filter to control ozone emissions.
Temperature and humidity	Computer equipment and performance are both affected by temperatures and humidity levels. <ul style="list-style-type: none"> <li>Too much moisture can be problematic and cause physical damage to equipment. On the other hand, low humidity can contribute to more electrostatic charge into the air. High humidity levels can also have an effect on tapes and paper media.</li> <li>Extreme temperatures can also be an issue. Low temperatures can cause condensation on computer system components that generate heat while turned on, while high temperatures can cause the components to overheat. Proper ventilation systems must be used to help prevent overheating of computer systems.</li> </ul> Be aware of the humidity level and temperatures of the environment where devices will be installed and running to prevent these types of issues.
Dust and debris	Dust can be a more subtle hazard. The buildup of dust particles over time can cause problems with different types of equipment. Dust buildup causes resistance in moving parts, such as fans, drives, and printer motors. Dust buildup on circuit boards, heat sinks, and vents creates insulation that reduces heat dissipation. Dusting equipment often with compressed air and vacuums can prevent these types of issues. Make sure that printers and paper products are kept in a separate area from computer equipment to prevent paper dust from getting into the equipment.

<b>Consideration</b>	<b>Description and Controls</b>
Airborne particles	<p>The conditions surrounding computer equipment can be an issue when there is a large number of airborne particles flowing in and around various devices. Contaminants can be either gaseous, such as ozone; particles, such as dust; or organic, which comes from industrial processing of fossil fuels, plastics, etc. All these contaminants can cause damage to computer equipment, such as corrosion and overheating. To protect your computing environment and yourself from airborne particles, you can:</p> <ul style="list-style-type: none"> <li>• Install computer equipment enclosures that will prevent contaminants from entering the devices.</li> <li>• Install air filters throughout the facility to catch excess particles as the air flows through the heating, ventilation, and air conditioning (HVAC) system.</li> <li>• Consider using safety goggles and an air filter mask to prevent particles from entering your eyes and lungs.</li> </ul>

## Workplace Safety Issues

Various workplace situations can be a hazard to you and your coworkers.

<b>Safety Issue</b>	<b>Description</b>
Falling and tripping	<p>Within your work area alone, a number of things can cause you to fall or trip. While working with computer equipment, you need to keep in mind the location of hardware, cables, and devices. If cords and cables must traverse a floor area where people need to walk, it is recommended that cord protectors be used to shield the cords and cables from being damaged by pedestrian traffic, as well as to minimize the chance of someone tripping on the cords and cables.</p> <p>You can also use cable management techniques and tools to group and organize cables together to keep them out of the way and hidden from the general working space.</p>
Equipment storage	CPUs and other hardware should not be stacked on top of one another. Make sure the equipment is secure, whether it is on the floor or on a desk or shelf.
Component handling and protection	Whenever you are handling computer equipment, you must follow the proper handling guidelines. Use an anti-static bag to store any computer component that can carry ESD. For example, when you are removing or replacing RAM, motherboards, or CPUs from inside a computer, immediately place the component in an anti-static bag until it is either replaced or disposed of.

<b>Safety Issue</b>	<b>Description</b>
Lasers	<p>Lasers are used in printers, CD drives, DVD drives, and Blu-ray drives and players. Laser is an acronym for Light Amplification by Stimulated Emission of Radiation. A laser produces an intense, directional beam of light by stimulating electronic or molecular transitions to lower energy levels. This powerful beam can cause damage to the human eye or skin. Lasers have many uses and, like other tools, are capable of causing injury if improperly used. The most likely injury is a thermal burn that will destroy retinal tissue in the eye. Because retinal tissue does not regenerate, the injury is permanent.</p>
	<p>Precautions include the following:</p>
	<ul style="list-style-type: none"> <li>• Never point a laser beam in someone's eyes.</li> <li>• Never look directly at a laser beam.</li> <li>• Never disable safety mechanisms when servicing a device with an embedded laser.</li> </ul>
Repetitive strain injury (RSI)	<p>Repetitive strain injuries involve damage to muscles, tendons, and nerves caused by overuse or misuse. Any or all of the following symptoms may appear in any order and at any stage in the development of an injury of RSI:</p>
	<ul style="list-style-type: none"> <li>• Aching, tenderness, and swelling</li> <li>• Pain, crackling, and tingling</li> <li>• Numbness and loss of strength</li> <li>• Loss of joint movement and decreased coordination</li> </ul>
	<p>If an individual has even mild RSI symptoms, action should be taken. Rest, medication, therapy, or even surgery might be prescribed to RSI sufferers. The best treatment for RSI, of course, is prevention through proper arrangement of computer workstations and reasonable project design.</p>
Eye strain	<p>Many computer tasks are done at a close working distance, requiring the eyes to maintain active focusing. This can cause stress and strain on the eyes and the muscles that control them. A very common health problem reported by users of computer monitors is eye strain. Symptoms include blurred vision, difficulty focusing, double vision, tiredness, headaches, and burning, sore, or itchy eyes.</p>
	<p>A vision examination is recommended. A specific eyeglass prescription for computer use may help compensate for the strain involved in looking at a close and fixed point for periods of time.</p>
	<p>Dry eyes can also be a concern for computer operators. The eye surface becomes dry because computer users tend to blink less and tears evaporate faster during monitor use. Symptoms associated with dry eyes are redness, burning, and excess tearing.</p>
	<p>Artificial tears—used to supplement the eye's natural tear film and lubricate the dry surface—alleviate dry-eye symptoms for some computer users.</p>
Noise	<p>Noise levels produced by computers and most printers are well below those that cause adverse health effects. The equipment has minor noise sources such as the hum of cooling fans and the clicking of keys. Excessive noise from a computer may indicate an internal malfunction. Certain industrial high-speed line printers may produce noise at a level which is uncomfortable for prolonged exposure; in these cases, sound-deadening covers are often used, or the printers are placed in areas well away from operators.</p>

<b>Safety Issue</b>	<b>Description</b>
Hot components	Hot computer components within the system unit can be problematic. For example, any component carrying a high electrical voltage can get very hot and could cause burns. High-speed processors are also known heat generators; heat sinks and fans keep them cool enough to prevent a burnout, but they may still be uncomfortably hot to touch. You must exercise caution when working with any part of a computer or printer that may be hot to the touch, or that might be holding an electrical charge.
Food and drink	Eating and drinking around computer equipment can be problematic. Food particles and liquids can get inside and harm the inner mechanics of the hardware. Your employer may have policies in place that prohibit eating and drinking around computer equipment for these reasons.
Moving equipment	<p>Lifting and moving computer equipment can be one of the more strenuous parts of your job. For example, when you need to work on a CPU, you may have to lift and relocate the machine to your work area. Always assess the situation first to determine if you can lift or move items safely.</p> <p>Before lifting anything:</p> <ul style="list-style-type: none"> <li>• Know your own strengths and weaknesses. You need to be aware of what your weight limitations are, as well as any weight limitations set forth in your job description.</li> <li>• When you lift, use proper lifting techniques. Bend at your knees and not at your waist. This will prevent strain on your back muscles and pressure on your spine.</li> <li>• Assess the equipment you are moving. If you feel that physically the equipment is too heavy or awkward for you to move alone, then get help from a coworker, or use a cart to relocate the equipment. If you use a cart, make sure the equipment is tightly secured during transport.</li> <li>• The equipment may be unstable for lifting. You may need to take special precautions and may require help moving it to a cart.</li> <li>• Equipment should never be stacked too high while moving to avoid hardware falling and breaking on the floor. This can cause damage to other devices or to you.</li> <li>• Plan ahead. While moving equipment from one area to another, be aware of narrow doorways or columns that you will encounter on the way. Also, make sure to prep the space before delivering the equipment so that you are not trying to reconfigure the space with all the equipment in the way.</li> </ul>

## Laser Safety Standards

To provide a basis for laser safety, standards are established for Maximum Permissible Exposure (MPE). Lasers and laser systems and devices are grouped into four classes:

- Class 1 lasers do not emit harmful levels of radiation and are exempt from control measures.
- Class 2 lasers are capable of creating eye damage if viewed directly for extended periods of time; this class includes bar code readers.
- Class 3 lasers pose severe eye hazards when viewed through optical instruments (for example, microscopes) or with the naked eye.
- Class 4 lasers pose danger to eyes and skin, and are fire hazards.

Frequently, lasers are embedded in laser products or systems with a lower hazard rating. For example, laser printers, CD drives, and DVD drives are Class 1 laser products; however, they contain Class 3 or Class 4 lasers. When the printer or drive is used as intended, the controls for the device's class (Class 1) apply. When the system is opened—for example, for service—and the

embedded laser beam is accessible, precautions must be based on the classification of the embedded laser (Class 3 or 4).

Precautions include the following:

- Never point a laser beam in someone's eyes.
- Never look directly at a laser beam.
- Never disable safety mechanisms when servicing a device with an embedded laser.

## General Power Issues

Power issues can cause a number of problems for computer equipment and the working environment. Computer equipment, printers, network devices, and other resources require power, so any disruption in electricity will present a number of issues. There are several power problems that can occur.

<b>Power Problem</b>	<b>Description</b>
Blackout	A <i>blackout</i> involves a complete loss of power.
Brownout	A <i>brownout</i> is a temporary power reduction that is often used by electrical power companies to deal with high power demands. It is called a brownout because the lights dim during the event.
Sag	A <i>sag</i> is a momentary low-voltage power failure.
Spike	A <i>spike</i> is a very short increase in the electrical supply voltage or current carried on any wire such as a power line, phone lines, and network lines. Usually lasts only a few milliseconds.
Surge	A <i>surge</i> is a sudden sharp increase in voltage or current that can last up to 50 microseconds.

## Power Protection Systems

There are several protection systems that can restore power to some operational capacity, decrease failures, or monitor power sources.

<b>Power Protection System</b>	<b>Description</b>
UPS or battery backup	An <i>uninterruptible power supply (UPS)</i> , also referred to as a <i>battery backup</i> , is a device that continues to provide power to connected circuits when the main source of power becomes unavailable. Depending on the design, UPSs can be battery operated, AC powered, or both. They are meant for temporary use and are intended to support computer systems until they can be powered off normally. Power is likely to be interrupted when the batteries or other power sources are discharged.
Generators	A <i>generator</i> creates its own electricity through the use of motors. Generators provide long-term power and are often started while a UPS system supports equipment through the initial power loss. Generators can fail when motor fuel runs out or when a mechanical failure occurs.
Surge suppressor	A <i>surge suppressor</i> is a device that provides power protection circuits that can reduce or eliminate the impact of surges and spikes.

## UPS Types

Depending on the needs of an organization, different types of UPSs might be used. Common types include:

- A standby UPS, which is primarily AC-powered, until the power source fails. When the power source fails, it switches to the backup power source or battery. This UPS is used most often with personal computers.
- A line interactive UPS is commonly used in smaller business settings to provide power through a constant AC connection. When the AC power fails, the inverter switches to battery power. This UPS is unique in that while the AC power is available, it is used to also charge the battery.

## Liquid Hazards

There are many different professional situations when you may come in contact with a hazardous liquid. Some such compounds are used to clean or condition equipment, including the computer's case, adapter card contacts and connections, and glass surfaces. They may present safety or environmental problems. Make sure you read the labels and follow the instructions carefully when you are disposing of hazardous materials.

## Chemical Hazards

Working with personal computers can cause you to come in contact with some chemical hazards.

<b>Chemical Hazard</b>	<b>Description</b>
Laser printer toner	Made of fine particles of iron and plastic, toner presents its own set of problems due to its reactions with heat. If you spill toner, do not clean it up with a regular vacuum; the particles will get into the motor and melt. Do not use warm water to wash toner off your hands or arms; the toner could fuse to your skin. Instead, brush off as much as you can with a dry paper towel, rinse with cold water, and then wash with cold water and soap. In addition, do not use ammonia-based cleaners on or around laser printers, as the ammonia may react chemically with the toner.
Batteries	Batteries maintain the data in complementary metal oxide semiconductor (CMOS) chips and supply power to remote controls, portable computers, and other devices. These batteries may contain mercury, cadmium, and lithium, as well as other dangerous chemicals.
Capacitors	Capacitors store electricity by using two or more conducting plates separated by an insulator. There are capacitors in various personal computer components, including microprocessors. The electrolytes in capacitors are very caustic; treat them as you would any hazardous chemical. Thoroughly wash your hands after handling ruptured capacitors.



**Caution:** The capacitors in power supplies and monitors do not discharge when they are turned off or unplugged, and contain enough charge to kill you. Do not open or attempt to service internal components of power supplies or monitors.

## MSDS Documentation

A *Material Safety Data Sheet (MSDS)* is a technical bulletin that is designed to give users and emergency personnel information about the proper procedures for the storage and handling of a hazardous substance. This applies to any situation in which an employee is exposed to a chemical under normal use conditions or in the event of an emergency. The manufacturers supply MSDSs with the first shipment to a new customer and with any shipment after the MSDS is updated with

significant and new information about safety hazards. You can get MSDSs online; the Internet has a wide range of free resources. OSHA regulations govern the use of MSDSs and the information an MSDS must contain.

MATERIAL SAFETY DATA SHEET		Page: 1			
Metal Cleaner					
	Revision: 1/29/2016 Printed: 2/1/2016 Date Created: 1/5/2015				
<b>1. Product and Company Identification</b>					
Product Code:	DK579				
Product Name:	Metal Cleaner				
Manufacturer Name and Address					
Company Name:	PPG Industries, Inc. 4325 Rossana Drive P.O. Box 9 Alison Park, PA 15101				
Emergency Contact 1	Emergency Medical/Spill Info:	(304)842-1300			
Information Contact	Technical Information:	(614)363-0610			
Chemical Family:	ACID				
<b>2. Composition/Information on Ingredients</b>					
Hazardous Components (Chemical Name)	CAS #	Percentage	OSHA TWA	ACGIH TWA	Other Limit
1. Ethanol, 2-Butoxy-	111-762	10.0 - 20.0 %	≤ 25 ppm	≤ 25 ppm	No data.
2. Dibutyl-glycol monobutyl-ether	112-345	10.0 - 20.0 %	Not Estab.	Not Estab.	No data.
3. Phosphoric acid	7664-382	30.0 - 40.0 %	1 mg/m3	1 mg/m3	No data.
<b>3. Hazards Identification</b>					
<b>Emergency Overview</b>					
Harmful or fatal if swallowed. May be corrosive. This product contains a material which causes skin burns. This product contains a material which causes irreversible eye damage. May be harmful if absorbed through the skin. Vapor and/or spray may be harmful if inhaled. Vapor irritates eyes, nose, and throat. Vapor generated at elevated temperatures irritates eyes, nose, and throat.					
Route(s) of Entry:	Irritation? No	Skin? No	Eyes? No	Ingestion? No	
<b>Potential Health Effects (Acute and Chronic)</b>					
(Information from Material Safety Data Sheet)					

**Figure 4-7: An MSDS.**

### Required Information in an MSDS

Every MSDS is required to include information about the following items:

- Physical data
- Toxicity
- Health effects
- First aid
- Reactivity
- Storage
- Safe-handling and use precautions
- Disposal
- Protective equipment
- Spill/leak procedures

## Incident Reports

An *incident report* is a record of any instance where a person is injured or computer equipment is damaged due to environmental issues. The report is also used for accidents involving hazardous

materials, such as chemical spills, that could have an impact on the environment. Any time an accident occurs at a work site, you should submit an incident report. Reporting these occurrences is often part of company policy and can help provide protection against liability.

<b>Rudison Technologies</b>	<b>Office Use Only</b>	Incident # _____		
	Actions taken:	Copies to:		
<b><u>Computer Safety Incident Report</u></b>				
Fill out as completely as possible				
1. Nature of incident: _____ 2. Location of incident: _____ 3. Time of incident: _____ 4. Date of incident: _____ 5. Your name, position, and phone number: _____ 6. Date and time this report was filed: _____ 7. Was there any injury? Place an "X" after one – Yes ___ or No ___ – and elaborate in description below. 8. Is there an ongoing hazard? Place an "X" after one – Yes ___ or No ___ – and elaborate in description below.				
<b>Names, addresses, phone numbers, and ID numbers of individuals involved.</b> Please identify as complainant(s), perpetrator(s), witness(es).				
Name	Address	Phone Number	Employee Number	Status (Employee, Guest, Client)
Sequence or Description of Events. Be concise yet thorough.				

**Figure 4–8: Sample incident report.**

## Hazardous Materials Handling and Disposal

Proper disposal of hazardous materials is an essential part of maintaining a safe work environment.

<b>Hazardous Material</b>	<b>Disposal Recommendations</b>
Liquid cleaning materials and empty containers	Follow your company's guidelines for disposing of liquid cleaning materials and their containers. Each municipality has its own disposal regulations that you must learn and follow. You can find out about these regulations by contacting your local government's environmental office or department for trash disposal and recycling.
Toner	Empty toner cartridges should not be discarded in the trash because of the damage that the residual chemicals can do to the environment. Used toner cartridges should be refilled or returned to the manufacturer for recycling and/or disposal. Follow your company's guidelines for disposal procedures.
Display devices	The CRT's in older computer monitors contain lead, which is considered a hazardous material. Follow your company's guidelines for disposing of display devices. Many municipalities have regulations for disposal and recycling of old monitors and television sets; contact your local government's environmental office or department for trash disposal and recycling to determine if there are specific rules you need to follow.

<b>Hazardous Material</b>	<b>Disposal Recommendations</b>
Ozone filter	Follow the manufacturer's recommendations for replacement and disposal of a laser printer's ozone filter.
Batteries	Used batteries should not be discarded in the trash; they should be recycled or disposed of following your company's guidelines.

## ACTIVITY 4-3

### Discussing Environmental Safety and Materials Handling

#### Scenario

In this activity, you will identify the best practices for promoting environmental safety and proper handling of materials.

1. You are on a service call, and you accidentally spill some liquid cleaner on the user's work surface. What actions should you take?
  - Refer to the MSDS for procedures to follow when the material is spilled.
  - Wipe it up with a paper towel and dispose of the paper towel in the user's trash container.
  - Report the incident.
2. Ozone is classified as an environmental hazard. Which device produces ozone gas?
  - Laser printer
  - CPU
  - Laptop
  - Power supply
3. What item reacts with heat and ammonia-based cleaners to present a workplace hazard?
  - Capacitor
  - Laser
  - Toner
  - Battery

# TOPIC D

## Professionalism and Communication

So far in this lesson, you have identified best practices for working directly with computer equipment. On almost every service call, you will also need to interact with users who are experiencing problems. In this topic, you will identify best practices for PC technicians to use to communicate appropriately with clients and colleagues and to conduct business in a professional manner.

You are a representative of your profession, as well as your company. Working with customers is a fundamental job duty for every A+ technician. How you conduct yourself will have a direct and significant impact on the satisfaction of your customers, and your level of professionalism and communication skills can directly affect whether or not you will do business with them again.

### Communication Skills

Using the proper communication skills when dealing with clients and colleagues creates a professional environment that is conducive to solving the problem at hand. Some of the communication techniques you should master include:

- Use proper language. Avoid the use of jargon, acronyms, and slang when applicable.
- Maintain a positive attitude and project confidence.
- Actively listen to the customer. This might include taking notes and avoiding interrupting the customer.
- Be culturally sensitive to the customer. In some cases this can include the use of appropriate professional titles. Also, different cultures define personal space differently, so be aware of how close or far you are from the customer.
- Be on time. If you are unavoidably detained, contact the customer to let them know you will be late. In some cases you will need to reschedule your appointment with the customer.
- Avoid distractions. This includes not taking personal calls, texting, or visiting social media sites while with a customer. Also, avoid talking to co-workers while interacting with customers or letting personal interruptions affect the client interaction.
- Deal appropriately with a customer's confidential and private materials. This includes items located on their computer, on their desk, on a printer, or elsewhere.

When you meet with a customer, be sure that the expectations and timeline are set and met. If resolution of the issue is going to take a considerable amount of time, be sure to communicate the status of the issue with the customer. You might need to offer different repair or replacement options if the user is going to be without their device for awhile. Always provide the proper documentation on the services you provide to the customer. Be sure to follow up with the customer at a later date to verify their satisfaction with your work and that the issue has been successfully resolved.

Some customers or situations are more intense than others. A customer might become difficult if you cannot instantly resolve their problem. When dealing with a difficult customer or situation:

- Do not argue with the customer or be defensive.
- Avoid dismissing customer problems.
- Clarify customer statements by asking open ended questions to help narrow the scope of the problem. You should consider restating the issue or question back to the customer to verify understanding.
- Do not disclose experiences via social media sites.

## ACTIVITY 4-4

### Discussing Professionalism and Communication Techniques

#### Scenario

In this activity, you will examine different professionalism and communication techniques.

1. Select the correct response.

**Which is a good example of listening skills?**

- Maintain a neat and clean appearance.
- Keep sensitive customer information to yourself.
- Interrupt the customer to ask for more details.
- Let your eyes wander around the room as the customer is speaking.
- Allow the customer to complete statements without interrupting.

2. You have received an off-site service call to service a network printer at a customer location. When you arrive, the user is at the printer and starts talking about how the printer is not working properly, and he cannot get his reports handed in on time. As a result, you start asking more clarifying questions to gather more information, so you can identify the specific issue with the printer. What type of technique are you using to gather information?

- Passive listening
- Non-verbal communication
- Active listening

# TOPIC E

## Organizational Policies and Procedures

In the last topic, you identified best practices for communicating appropriately with customers. You'll also need to deal appropriately with management, particularly when it comes to established protocols for the use and care of computing devices. In this topic, you will identify common organizational policies and procedures that deal with computer use.

By identifying common organizational policies and procedures that deal with computer use, you will be more capable of dealing with compliance issues as they arise and protecting organizational resources.

### Organizational Policies and Procedures of Appropriate Use

*Organizational policies* are documents that convey the corporate guidelines and philosophy to employees. Policies can be either high-level corporate documents distributed to the entire organization, or lower-level operational documents that affect only certain departments, divisions, individuals, or roles in an organization. For example, most organizations will have an *acceptable use policy* (*AUP*) that includes practices and guidelines that management expects all employees to follow when they are using and accessing company-owned computer equipment and information-related resources.

### Acceptable Use Policy

**Overview of Policy**

This policy outlines the general use guidelines of any computer equipment within the organization. The guidelines are in place to protect both the employee and the company. Inappropriate use of equipment and resources can compromise the company network, systems and services.

**Scope**

This policy applies to all employees, clients, contractors, and any other individuals that work within the organization.

**Policy Guidelines**

1. General Use and Ownership Guidelines
  - Use good judgment regarding the amount of use of all company equipment.
  - Systems should be audited on a monthly basis.
  - Properly secure all computer equipment when not in use.
2. Security and Sensitive Information
3. Unacceptable Use Activities
4. Internet and Networking Guidelines

Figure 4-9: An AUP.

### Prohibited Content and Activities

As an A+ technician, you may come across situations when you may encounter prohibited activities, such as viewing pornography on work-issued devices by users either within your organization or by

a customer. There are different levels of prohibited content, which can be described as distasteful, inappropriate, or illegal.

Every organization will have different guidelines and restrictions based on the type of content. For example, some organizations will discourage access to social networking sites, or websites that contain questionable words or phrases, but will not explicitly forbid it. On the other hand, restrictions on content or data that can be categorized as inappropriate or illegal, such as pornography, will be enforced heavily, and accessing such content will have immediate consequences.

In each of these cases, it is your responsibility to follow organizational procedure to report the incident. When reporting potentially illegal activities, you must follow the organization's policy on reporting, collecting, and documenting the specifics of the situation and what evidence was found.

## Guidelines for Dealing with Prohibited Content and Activities



**Note:** All of the Guidelines for this lesson are available as checklists from the **Checklist** tile on the CHOICE Course screen.

Follow these guidelines to deal with prohibited content and activities.

### Identifying and Reporting Prohibited Content

The process of identifying and reporting prohibited content or activities can be complicated, especially when an organization does not have sufficient policies and documented guidelines. There are some fundamental methods that can be applied to help properly report, document, and resolve issues.

Phase	Description
First response	<p><i>First response</i> refers to the immediate actions that follow an incident, as well as the individual or individuals who perform these actions. There are a few actions that take place during the first response to an incident:</p> <ul style="list-style-type: none"> <li>• Identifying the data and/or hardware.</li> <li>• Reporting the details of the discovery and evidence through the proper channels. This will vary depending on the specific organization's policies and reporting instructions.</li> <li>• Preserving the data and/or device as evidence. This is also called computer forensics.</li> </ul>
Chain of custody	<p>The <i>chain of custody</i> is the record of tracking evidence from collection through presentation in court. The evidence can be hardware components, electronic data, or telephone systems. The chain of evidence reinforces the integrity and proper custody of evidence from collection, to analysis, to storage, and presentation in a court of law. Every person in the chain who handles evidence must log and document the process, methods, and tools they used.</p>
Documentation	<p>In the process of identifying and reporting incidents with prohibited content, you should follow the organization's documented procedures to ensure that you are carrying out the correct response tasks and guidelines. You must also be aware of any changes made to the documentation so that you are always following the right procedures in handling incidents, managing evidence, and reporting findings to the appropriate individuals.</p>

### Removing Computers

When computer crimes are reported, one of the first response activities is removing computers from the crime location. They are tagged with a chain of custody record to begin the process of making the evidence secure for future presentation in court.

## Computer Forensics

*Computer forensics* is the practice of collecting and analyzing data from storage devices, computer systems, networks, and wireless communications and presenting this information as a form of evidence in a court of law. Primarily, forensics deals with the recovery and investigation of potential evidence. Computer forensics is a fairly new field, so there is little standardization or consistency in practicing it across organizations and courts. Basically, computer forensics is a blend of the elements of law with computer science in analyzing evidence in a way that is permissible in the court of law.

Forensic response procedures for IT help security professionals collect data evidence in a form that is admissible in a court of law.

<b>Forensic Response Procedure</b>	<b>Description</b>
Capture system image	One of the most important steps in computer forensic evidence procedures is to capture exact duplicates of the evidence, also known as forensic images. This is accomplished by making a bit-for-bit copy of a piece of media as an image file with high accuracy.
Examine network traffic and logs	Attackers always leave behind traces; you just need to know how and where to look. Logs record everything that happens in an intrusion prevention system (IPS) or intrusion detection system (IDS), and in routers, firewalls, servers, desktops, mainframes, applications, databases, antivirus software, and virtual private networks (VPNs). With these logs, it is possible to extract the identity of hackers and provide necessary evidence.
Capture video	Video forensics is the method by which video is scrutinized for clues. Tools for computer forensics are used in reassembling video to be used as evidence in a court of law.
Record time offset	The format in which time is recorded against a file activity, such as file creation, deletion, last modified, and last accessed, has developed to incorporate a local time zone offset against GMT. This makes it easier for forensic examiners to determine the exact time the activity took place, even if the computer is moved from one time zone to another or if the time zone has deliberately been changed on a system.
Take hashes	Federal law enforcement agencies and federal governments maintain a list of files such as files relating to components of Microsoft® Windows® and other application software. The hash codes generated by a file or software can be compared to the list of known file hashes and hacker tools if any are flagged or marked as unknown.
Take screenshots	You should capture screenshots of each and every step of a forensic procedure, especially when you are retrieving evidence by using a forensic tool. This will ensure that data present on a compromised system is not tampered with and also provides the court with proof of your use of valid computer forensic methods while extracting the evidence.
Identify witnesses	Courts generally accept evidence if it is seconded by the testimony of a witness who observed the procedure by which the evidence was acquired. A computer forensics expert witness is someone who has experience in handling computer forensics tools and is able to establish the validity of evidence.

<b>Forensic Response Procedure</b>	<b>Description</b>
Track man hours and expense	When the first incidents of computer crimes occurred, it would usually take less than 40 man hours to complete a forensic investigation because incidents usually involved single, standalone computers. Now, with advances in technology and the advent of new digital media such as voice recorders, cameras, laptop computers, and mobile devices, computer forensics procedures can require a much greater amount of time and expense. Also, the increase in storage device capacities and encryption affect the amount of man hours that it can take to assess any damage, and consequently increase the expenses incurred in any computer forensics investigation. Capturing this expense is part of the overall damage assessment for the incident.

## Privacy

All organizations must consider their legal obligations, rights, liabilities, and limitations when creating policies. Because incidents can potentially be prosecuted as technology crimes, organizations must be prepared to work with civil authorities when investigating, reporting, and resolving each incident. Information security practices must comply with legal requirements that are documented in other departmental policies, such as human resources. A company's response to any incident must conform to the company's legal limitations as well as the civil rights of individuals involved.

Legal issues can affect different parties within each organization.

<b>Affected Party</b>	<b>Legal Considerations</b>
Employees	<ul style="list-style-type: none"> <li>• Who is liable for misuse of email and Internet resources—the organization, the employee, or both?</li> <li>• What is the extent of liability for an organization for criminal acts committed by its employees?</li> <li>• What rights to privacy do employees have regarding electronic communications?</li> </ul>
Customers	<ul style="list-style-type: none"> <li>• What customer data is considered private and what is considered public?</li> <li>• How will a company protect the privacy and confidentiality of customer information?</li> </ul>
Business partners	<ul style="list-style-type: none"> <li>• Who is liable if the data resides in one location and processing takes place in another location?</li> <li>• Who is responsible for the security and privacy of the information transmitted between an organization and a business partner—the sender or the receiver?</li> </ul>

## PII

One of the more common types of information that is protected by organizational policies is personally identifiable information (PII). *Personally identifiable information* (PII) is any information that can be used by itself or in combination with additional information as a way to identify, contact, or find a single person, or to identify a particular individual by using the various pieces of information together to determine the person's identity. The definition of what PII is can differ by legal jurisdiction.



**Note:** Although the abbreviation PII is widely accepted in the U.S., the phrase it abbreviates can have four variations depending on the chosen forms of the words personal (or personally) and identifiable (or identifying). These variants are not identical from a legal standpoint. Each term's definition can change depending on the jurisdiction and the reason the term is being used.

PII can include a user's full name, fingerprints, license plate number, phone numbers, street address, driver's license number, and so on.

## Software Licensing

Most software has a software license agreement that allows the user to install and use the software on a single computer. Unless the license explicitly states that the software can be used on more than one computer, installing it on additional computers is illegal. Also, be sure that you are buying legitimate copies of the software and not bootlegged copies.

Two terms you often encounter when discussing licensing are Digital Rights Management (DRM) and End User License Agreement (EULA). DRM is a copy protection method used for digital content and devices. EULA is a legal contract specifying what the purchaser is allowed to do with the software. Many users acknowledge the DRM and EULA as part of software installation without actually reading the content of those two legally binding documents. Be sure you know what you are agreeing to when you acknowledge those items.

Open source software is free to use, can be modified, and can be shared. Open source software licenses approved by the Open Source Initiative state that the software meets the requirements of being free, open to modification, and being shared. Many open source applications use the GNU General Public License. The full content of the GNU GPL can be found at [opensource.org/licenses/GPL-3.0](http://opensource.org/licenses/GPL-3.0).

Commercial licenses can be found in both proprietary closed-source and open-source software. Some software may be free to use for personal use, but if you want the software to be used in a business, you might need to purchase the application or contact the publisher or author of the software to make arrangements for its use.

A personal license for an application means that you can use the software for your own use, but not for any commercial application of the software.

An Enterprise license might be available for applications and closed-source operating systems for large organizations. These are often sold in increments of 50-100 users, 100-500 users, 1000-5000 users, and so forth. Enterprise licensing makes it easier for large organizations to make sure they are in compliance with having enough licenses for all of their users without needing to purchase and track individual licenses for each user.

## ACTIVITY 4–5

### Discussing Organizational Policies and Procedures

#### Scenario

In this activity, you will examine organizational policies and procedures as they relate to computers and data.

1. Thinking about your organization's acceptable use policy, based on the information covered in this course, do you feel any changes need to be made? Discuss your thoughts with the class.
2. Share any experiences you have had (or read about) where computer forensics was employed to deal with prohibited content or activities.
3. Share with the class your experience with ensuring that software licensing policies are adhered to.
4. **While answering a service call on a computer that is located in a common area of the office, you come across information showing that some unauthorized websites have been viewed. The activity has been linked to a particular user account. What is the appropriate action to take?**

# TOPIC F

## Troubleshooting Theory

Often, computer technicians spend a large percentage of their time troubleshooting various software and hardware components used in computers and printers. Before you can even begin to troubleshoot a physical problem with a piece of hardware, you need to understand the basics of troubleshooting and some best practices used. In this topic, you will apply troubleshooting theory.

The most elaborate toolkit and expensive diagnostic software can be useless if you do not have a consistent plan of attack for solving problems. Even experienced technicians can sometimes overlook obvious problems or solutions. Troubleshooting can be extremely challenging and not always easy, but if you follow common best practices and basic troubleshooting procedures, you will often be able to determine the specific cause of a problem, as well as possible solutions to the problem.

### The CompTIA Troubleshooting Theory

A logical, methodical approach to troubleshooting usually leads to quicker solutions, so there are certain general factors that will apply in any troubleshooting situation.

Factor	Description
Identify the problem	<p>Identify the issue or problem. Ask questions and try to extrapolate key information that will help you identify any anomalies.</p> <p>Make sure to perform backups before making any changes. This will allow you to restore any information that may be lost during the troubleshooting process.</p> <p>Use open-ended questions when working with users to help identify the issue behind the symptoms. For example, instead of asking if the user can start the computer, try asking what happens when the user tries to start the computer.</p> <p>Use following questions to help identify the problem:</p> <ul style="list-style-type: none"> <li>• <i>Were you able to complete this task before?</i> If not, maybe the system is simply unable to perform the task without additional hardware or software.</li> <li>• <i>If you could do the task before, when did you notice there was an issue?</i> If you can identify what happened immediately before the problem, then it could lead you right to the issue.</li> <li>• <i>What types of changes have you noticed since the last time you completed this task?</i> If you cannot get a specific answer from the user, then you may need to follow up with a few more targeted questions such as "Did something get added to the computer?" or "Did you follow the exact same procedure or did you do this task differently?"</li> <li>• <i>Were error messages displayed?</i> If you can get the exact text of any error messages displayed, you can try searching the manufacturer's website (or just a general Internet search) to get an explanation of the message and to see if any problem reports have been logged related to this message.</li> </ul>

<b>Factor</b>	<b>Description</b>
Establish a theory	<p>Establish a theory. Verify anything that may seem too obvious. Make no assumptions and check everything that may seem too simple and easy. Always verify that components are plugged in, connected, and powered on.</p> <p>Oftentimes, problems are the result of simple things.</p> <ul style="list-style-type: none"> <li>• If applicable, try to re-create the issue so that you can experience it for yourself and can see exactly what the results are. If you can, observe the user as they complete the steps to verify that they are following the proper procedures.</li> <li>• Depending on the issue, develop a theory and determine how the problem may be corrected. Use your personal experiences, refer to support websites and online forums, and discuss theories with your colleagues to build possible resolutions and how they may be implemented.</li> </ul>
Test the theory	<p>Test the theory to determine the cause by testing related components; inspecting connections, hardware and software configurations; and consulting vendor documentation, to solve the problem or identify a likely solution.</p> <p>Once the theory is confirmed, if the problem is not resolved, then determine what the next steps will be. If the theory is not confirmed, then determine what the next steps are to resolve the problem. In some cases, you may need to escalate the issue to a designated party or individual.</p>
Establish a plan	<p>Establish a plan of action to resolve the problem and implement the solution. You may need to conduct further research and establish new ideas and determine priorities. Research and planning may result in using a different approach that may need detailed planning. You may also end up with more than one plan depending on what the possible causes are, so prioritize and execute each plan carefully. During this process, you need to make sure that productivity does not suffer and that any downtime is limited.</p>
Verify	<p>When the issue is resolved, verify full system functionality and, if applicable, implement preventative measures. This part of the process may also involve consulting with colleagues or vendors to communicate known issues, solutions, and preventative measures. Preventative measures might include applying system updates and installing antivirus software.</p> <p>Once the issue has been resolved, make sure that the solution implemented is actually working the way you intended and did not cause any additional or new issues. Always make sure that the user or customer is completely satisfied with the results.</p>
Document	<p>Document your findings, actions, and outcomes. Documentation of computer problems and their solutions can be a helpful part of the overall documentation plan for your company's computers. Not only will this provide you with an ever-growing database of information specific to the computers you are responsible for, but it also will be valuable reference material for use in future troubleshooting instances. In addition, documenting as you troubleshoot enables you to capture each step of the troubleshooting routine, as well as the outcome, for future reference.</p>

## Troubleshooting Software Tools

In addition to tools such as screwdrivers, ESD wrist straps, and wire crimpers, your tool kit should also include some software tools. Typically this includes a media source with the operating system

available so you can reinstall it if needed, software for removing viruses or other malware, drivers for the common hardware used in your organization, and other software specific to your needs.

Another piece of software that can be considered part of your toolkit is a tracking database where incidents that occur can be documented with the information about the call, including the hardware or software affected, who performed the troubleshooting and resolved the issue, and what the resolution was. This might be a simple spreadsheet or database, or it might be a complex help desk management tracking application; it all depends on the needs of your organization.

# ACTIVITY 4–6

## Examining Troubleshooting Tracking Software

### Before You Begin

You will need a functional computer with Internet access for this activity.

### Scenario

Your organization has come a long way in tracking help desk calls. Originally there was no tracking, then paper forms were used and placed in 3-ring binders based on the type of call. Then, one of the technicians created a simple Access database in which the information could be recorded. As your organization has continued to grow, you have found that you need a better solution, so your manager has asked you to research what help desk tracking software is available.

1. Search for comparison charts and reviews of help desk software.
  - a) Log in to your computer.
  - b) Verify that you are connected to the Internet.
  - c) Open a web browser and open your preferred search site.
  - d) Search for help desk software.
  - e) Locate reviews and comparison charts for help desk software.
2. Determine which help desk software best follows the troubleshooting method described in this topic.

## Summary

In this lesson, you identified best practices that are followed by professional PC technicians. With the proper tools, awareness of safety and environmental issues, basic communication skills, and a solid method to use when troubleshooting, you are prepared to do your job in a safe, effective, and professional manner.

**Which of the best practices discussed in this lesson apply in your workplace?**

**Have you ever been in a situation where you uncovered inappropriate conduct or prohibited activity?**



**Note:** Check your CHOICE Course screen for opportunities to interact with your classmates, peers, and the larger CHOICE online community about the topics covered in this course or other topics you are interested in. From the Course screen you can also access available resources for a more continuous learning experience.

# 5

# Supporting Display Devices

**Lesson Time:** 1 hour, 30 minutes

## Lesson Objectives

In this lesson, you will install, configure, and troubleshoot display devices. You will:

- Install display devices.
- Configure display devices.
- Troubleshoot common video, projector, and display issues.

## Lesson Introduction

So far in this course, you have identified the hardware and software that makes up a personal computer system and examined some general best practices for working with them. Now that you have a solid base of background information, it is time to roll up your sleeves and start working with some of those hardware components. In this lesson, you will install, configure, and troubleshoot display devices.

Much of the work that you will perform as a PC technician will involve installing and configuring various hardware and software components. As an IT professional, you will often find yourself setting up end-user workstations or helping those end users with the hardware they need to make their daily lives easier. Installing and configuring display devices is one of the more common tasks that you will perform.

# TOPIC A

## Install Display Devices

Generally, one of the most common peripherals that you will be asked to install is the display device. In this topic, you will install display devices.

The display device provides visual output from the computer system. Without the display device, you can't see any images on screen to guide your interactions with programs or see the results of your input. Correctly installing the display device enables you to meet the basic user need to see what you are working on.

### Display Device Types

There are several different types of display devices that you might be asked to install or configure.



**Note:** Depending on available space and user preferences, users might select larger or smaller monitors. Technical needs might also affect the choice of which monitor to purchase.

Display Device	Description
LCD	<p>Liquid crystal display (LCD) flat-panel displays are compact and lightweight, energy efficient displays. They are composed of millions of liquid crystals arranged in a grid pattern. When electricity is applied to the grid, the crystals twist or realign themselves in a manner that allows backlight to pass through to create the images shown on screen.</p> <p>LCD monitors use either <i>cold cathode fluorescent lamp (CCFL)</i> or strips of LEDs as the backlight source. CCFLs use electrodes and mercury vapor to create ultraviolet light that is used as the light source. CCFL backlights are thicker, heavier, more expensive, use more power, have a lower <i>brightness</i>, and a shorter lifespan than LED backlights.</p> <p>LCD monitors typically use either <i>Twisted Nematic (TN)</i> or <i>In-Plane Switching (IPS)</i> technology. TN has fast response times, high brightness, less power draw, and are inexpensive to manufacture in comparison to IPS. TN tends to have more color shift and distortion when viewed at an angle compared to IPS. IPS provides better color reproduction and better viewing angles. Originally, TN offered better contrast and better blacks than IPS, but newer IPS monitors have overcome these limitations.</p> <p>Touch screen monitors enable input by touching images on the screen. This technology is used in bank ATMs, some point-of-sale terminals at fast food restaurants, and other situations where a separate keyboard for input is not appropriate. Touch screens are also found on many smartphones, tablets, and laptops sold for general public use.</p> <p>Virtual reality games and special-purpose imaging needs led to the development of glasses/goggles that substitute for a monitor. The glasses or goggles are composed of one (for both eyes) or two (one for each eye) LCD displays inside a head mounted display. These newer devices tend to be quite expensive; over time, the prices are likely to drop.</p>

Display Device	Description
OLED	<p><i>Organic light emitting diode (OLED)</i> displays utilize the same technology as LED displays, but use organic compounds such as carbon and hydrogen that emit light when subjected to an electric current as the light source.</p>
	<p>OLED screens can be used in a larger variety of dimensions than LED screens, and are currently utilized in computer monitors, television screens, tablets, and mobile phones. OLED is considered a green technology.</p>
Plasma	<p><i>Plasma displays</i> use xenon and neon rays and a flat panel of glass to provide visuals with high contrast, brightness, and vibrant colors that can be viewed from a multitude of angles.</p>
	<p>However, plasma displays are currently only available in very large dimensions, typically 40 inches or more, and are mostly marketed and utilized as television displays. They can also be incredibly heavy and cumbersome due to the technology. For these reasons, plasma displays are typically not practical for workstations.</p>
	<p>Early plasma displays were susceptible to image burn-in, caused by phosphors aging unevenly and creating a permanent outline of an image. This is less likely now because phosphors are faster and more efficient. However, burn-in is not impossible even with advances in plasma displays.</p>
Projector	<p>Video projectors are often used to display the video output onto a whiteboard or other surface so that a larger audience can see it.</p>
	<p>Video display systems can be used to display one image to several monitors (often used in training situations) or to display an image covering a huge screen (often used at trade shows).</p>

## Legacy Display Technology

Legacy display technology includes CRT and LED displays,

- Cathode ray tube (CRT) displays use electron beams within a vacuum tube to create images on a fluorescent screen. The intensity of three electron beams, one for each primary color (red, blue, and green), are manipulated to display the image on the screen.

CRT monitors are larger, heavier, and boxier than their more modern counterparts due to the components used to build them, especially the thick glass used for the screen. The screen may be curved or flat, but CRTs are not considered flat-panel monitors.

CRT monitors have for the most part been replaced by more modern and efficient displays like LCD, LED, or plasma screens, though they may still be in use in organizations that have yet to upgrade their devices.

- Light emitting diode (LED) displays use the same screen as an LCD display, but use a different backlighting technique/technology. Instead of the CCFLs used in LCD, LED screens use one of two types of light emitting diodes as a backlighting source: dynamic RGB LEDs, which are located behind the panel; or white edge-LEDs, which are located around the edge of the screen and use a diffusion panel to evenly distribute the light source.

LED displays consume even less power than LCD displays. However, LED displays can be more expensive to purchase.

## Display Device Connections

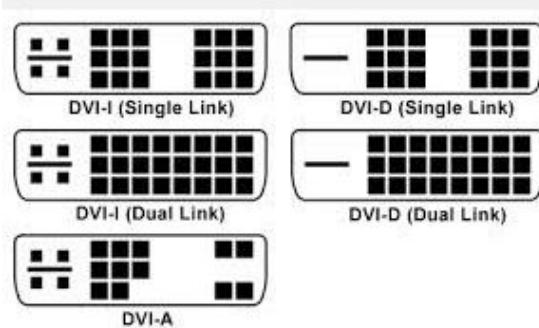
Display devices can use several different types of cables and connectors.

Cable and Connector Type	Description
Video Graphics Array (VGA)	The DB-15 high-density VGA connector is the most common cable used for LCD monitors. It contains three rows of five pins. You might also see the terms HD15 or DE15 used to describe this cable and connector type.



Mini-VGA is used on smaller devices, such as laptops, in place of the standard full-sized cables.

<b>Cable and Connector Type</b>	<b>Description</b>
<b>Digital Video Interface (DVI)</b>	<p>The DVI specification was developed to enable both analog and digital display devices to use a single connector.</p> <p>DVI cables use a technology called Transition Minimized Differential Signaling (TMDS) to transmit large amounts of digital data from the computer to a digital display such as a flat-panel LCD monitor.</p> <p>Single-link cables use one TMDS link to carry data. Each link has three data channels for RGB information, with a maximum bandwidth of 165 MHz. Bandwidth for a single-link connection supports resolutions up to 1920 x 1010 at 60 Hz. DVI dual-link cables use two TMDS links at 330 MHz each. Dual-link connections can support resolutions up to 2048 x 1536.</p> <p>DVI cables come in three configurations:</p> <ul style="list-style-type: none"> <li>• DVI-analog (DVI-A) is an analog-only format. It requires a DVI-A supported interface. The connector does not support dual link technology. It is commonly used to connect VGA devices to a computer using a DVI-A adapter.</li> <li>• DVI-digital (DVI-D) is a digital-only format. It requires a video adapter with a DVI-D connection and a monitor with a DVI-D interface. For DVI-D dual link, the connector contains 24 pins, arranged in three horizontal rows of 8 pins. To the side of the 24-pin grouping is a flat pin called a ground bar. For DVI-D single link, the connector has 18 pins arranged in two groups of nine pins and a flat-pin ground bar is off to one side. This cable type is used with DVI-to-HDMI adapters.</li> <li>• DVI-integrated (DVI-I) supports both digital and analog transmissions. This gives you the option to connect a monitor that accepts digital input or analog input. In addition to the pins/receptacles found on the DVI-D connector for digital support, a DVI-I connector has four additional pins/receptacles to carry an analog signal. For single-link support, the connector contains 18 pins/receptacles, and four additional pins for analog transmissions.</li> </ul>



<b>Cable and Connector Type</b>	<b>Description</b>
<i>High Definition Multimedia Interface (HDMI)</i>	<p>HDMI is the first industry-supported uncompressed, all-digital audio/video interface. HDMI uses a single cable composed of copper wires to provide an interface between any audio/video source, such as a set-top box, DVD player, or A/V receiver and an audio and/or video monitor, such as a digital television (DTV). The connector is made up of 19 pins and can support a number of modes such as High Definition TV (HDTV), Standard Definition TV (SDTV), and Enhanced Digital TV (EDTV), and can run to 50 feet or more in length.</p> <p>HDMI has largely superseded DVI and is compatible with the DVI standard. It can be used with PC systems that support DVI.</p>



<i>Mini-High Definition Multimedia Interface (Mini-HDMI)</i>	Mini-HDMI is similar to the full size Type C HDMI connector, except that it is specified for use with portable devices. The connector is a smaller version of the full size with the same number of pins. The difference between the full size and the mini is that some of pins have different transmission functions. A micro-HDMI cable is also available for portable devices such as the original Microsoft Surface RT tablet and some smartphones.
--	--



Cable and Connector Type	Description
DisplayPort	DisplayPort is a digital display standard that aims to replace DVI and VGA standards. DisplayPort is not backward compatible with DVI and HDMI and is a royalty-free standard. However, by using special dual-mode ports and suitable adapters, it may be possible to use DVI and HDMI signals with DisplayPort. Like HDMI and DVI, DisplayPort uses TMDS link technology to send high bandwidth audio and video signals. DisplayPort uses a 20-pin connector. Similar to <i>Peripheral Component Interconnect Express (PCIe)</i> , DisplayPort also supports high-quality gaming and other applications that use high-end graphics.



Component	Component video is a color video analog format that separates video signals into three or more channels. The wires are identified as Y, Pb, and Pr. Y consists of luminance and represents the brightness of the image; Pr consists of Red minus luminance; and Pb consists of Blue minus luminance. Sometimes component video refers to RGB signals, and the three wire analog RGB cable is often used for high-end video cameras.
-----------	---



Composite video	Composite video is an analog video format that combines video information on one single channel.
-----------------	--



<b>Cable and Connector Type</b>	<b>Description</b>
---------------------------------	--------------------

*Radio Corporation of America (RCA)*

RCA cables and connectors are used to carry audio and video transmissions to and from a variety of devices such as TVs, digital cameras, and gaming systems. In some cases, the RCA cable may also be used as a power cable, a loud speaker cable, and to carry digital audio. The female jacks on the devices are colored to provide a guide as to what type of connector can be attached. Common colors found are:

- Yellow for various composite connections.
- Red for the right channel of the audio transmission.
- White or black for the left channel of audio transmission.

*Coaxial cable*

A coaxial cable, or coax, is a type of copper cable that features a central conducting copper core surrounded by an insulator and braided or foil shielding. An insulator separates the conductor and shield, and the entire package is wrapped in an insulating layer called a jacket. The data signal is transmitted over the central conductor. The outer shielding serves to reduce electromagnetic interference.

*Bayonet Neill Concelman (BNC)*

The BNC connector is used with coaxial cable to carry radio frequencies to and from devices. The BNC cable can be used to connect radio equipment, aviation electronics, and to carry video signals. The actual BNC connectors come in two versions.



Cable and Connector Type	Description
miniDin-4	MiniDIN-4 connectors are used for <i>S-Video</i> connections. S-Video is an analog video signal that carries the video data as two separate signals (brightness and color). S-Video works in 480i or 576i resolution. Older systems from the 1980s used different sized DIN connectors for various connections, including video connections.

 **Note:** Mini-DIN-6 connectors were most notably used for IBM PC compatible PS/2 keyboard and mouse ports.

## Video Adapters and Converters

Computers with built-in video or video cards and monitors need to have a common connector type in order to connect a monitor to the system. Not every monitor has every type of connector and not every computer comes with every type of connector port. You can add a new video card that has the appropriate connector type, but you might be able to save some money using a converter or adapter.

Some of the adapters are just a small plastic housing with both types of connections on it. Others are cables with one connector type on one end and the other end has the other connector type.

Some of the adapters or converters you might use include:

- DVI to HDMI.
- DVI to VGA.
- Thunderbolt to DVI.
- HDMI to VGA.

## Aspect Ratios

The *aspect ratio* is the ratio of width to height of a display. The aspect ratio is found by determining the proportion of the number of pixels across the screen to the number of pixels down the screen. For example, a resolution of 640 x 480 has a 4:3 aspect ratio.

Resolution	Number of Pixels	Aspect Ratio
320 x 200	64,000	8:5
640 x 480	307,200	4:3
800 x 600	480,000	4:3
1,024 x 768	786,432	4:3
1,280 x 1,024	1,310,720	5:4
1,600 x 1,200	1,920,000	4:3

<b>Resolution</b>	<b>Number of Pixels</b>	<b>Aspect Ratio</b>
1,600 x 900	1,440,000	16:9
1,920 x 1,080	2,073,600	16:9
1,680 x 1,050	1,764,000	16:10
1,920 x 1,200	2,304,000	16:10



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Install Display Devices.

# ACTIVITY 5–1

## Installing Display Devices

### Before You Begin

You have a working monitor that uses a 15-pin VGA-style connector, the 29-pin DVI connector, High-Definition Multimedia Interface (HDMI) connector, or a universal serial bus (USB) display. The computer is turned off and the monitor is unplugged.

### Scenario

The marketing department of your company is moving to new offices, and you have been assigned the task of setting up the computers in their new offices. The computers and monitors have been delivered to each office. Employees want to begin using their computers as soon as possible.

1. Install the monitor.
  - a) Verify that the power is off at the computer.
  - b) Locate the monitor cable and examine the connector.
  - c) Locate the VGA, 29-pin DVI, HDMI, or the USB port on the computer.
  - d) Insert the monitor connector into the appropriate port, being sure to align the pins carefully.
  - e) Tighten the screws if the connector is equipped with screws. Do not over-tighten them.
  - f) Plug in the monitor power cord to a power source.
2. Verify that the monitor is functional.
  - a) Turn on the computer power.
  - b) Turn on the monitor power.
  - c) After the system has started to boot, verify that the power light on the monitor is green and is not flashing.
  - d) Watch the monitor and verify that the display is clear.

# TOPIC B

## Configure Display Devices

You have installed a display device. It might work just fine using the default configuration, but you may need to configure it. Correctly configuring the display device enables you to meet users' requirements for their particular usage. In this topic, you will configure display devices.

### Display Device Settings and Features

You can configure several features and settings for a display device, either through the **Control Panel** utility in the Windows® system or through controls on the physical device.

<i>Display Setting or Feature</i>	<i>Description</i>
<i>Resolution</i>	The number of <i>pixels</i> that make up the dimensions of a display. The resolution value is given as the number of horizontal pixels by vertical pixels, or width by height, traditionally in the ratio of 4:3. For wide screen displays, the ratio is 16:10. Common resolutions are 640 x 480, 800 x 600, 1024 x 768, and 1600 x 1200. The higher the resolution, the more objects or information you can fit on the screen at once. Just as widescreen televisions have become popular, video monitors with higher aspect ratio are also becoming more common.
<i>Native resolution</i>	A fixed resolution for LCD or other flat panel display devices. Display devices with native resolution will only display the best quality image when the input signal and the native resolution are the same. Other resolutions may display on a device where that signal input is not the same as the native resolution, but it will result in image quality loss.
<i>Refresh rate</i>	The number of times per second that a CRT monitor is “refreshed,” or the screen redrawn, expressed in <i>hertz</i> (Hz). A refresh rate of 60 Hz (a common value) means that the monitor will redraw the screen 60 times per second. Adjusting the refresh rates for laptop LCD screens or flat-panel LCD monitors is not necessary. Sometimes referred to as “frame rate.”
<i>Brightness</i>	The amount of light that is being emitted from a display device. Brightness is measured in <i>lumens</i> , which is the unit of measurement for visible light that is being emitted from a light source. On a display device, brightness can be increased or decreased for the display. If the brightness is set too high, you might get an aura effect displayed on the screen. If it is set too low, you might not see anything on the screen.
Analog vs. digital	Depending on the type and make of the display device, it may support either analog or digital inputs. Most devices providing the input signals (like a computer) are inherently digital. Display devices such as LCD or LED can innately support digital input signals, and do so via Digital Video Interface (DVI) connections between the input device and the display device.

<b>Display Setting or Feature</b>	<b>Description</b>
Privacy/antiglare filters	<p>Privacy or antiglare filters are physical accessory screens that can be attached onto or over a display device and provide a number of benefits:</p> <ul style="list-style-type: none"> <li>• Reduces glare from the screen for the user sitting in front of the display device.</li> <li>• Protects the display device screen from scratches or dust.</li> <li>• Prohibits others not sitting in the front of the device from viewing information being displayed, protecting confidentiality and providing privacy.</li> </ul>
Color depth (quality)	The number of bits used to store the color of a pixel: the more bits per pixel, the more colors can be displayed.

## Contrast Ratio

The contrast ratio is a metric of a display system, defined as the difference (in luminance) as expressed as a ratio: the "white" brightness divided by the "black." For example, a contrast ratio of 500:1 means the "white" areas are 500 times the brightness of the "black." High contrast ratio is a desired aspect of any display.

## Multiple Displays

Many users choose to use more than one display device to increase the amount of display space. The typical setup is two displays, though more than two displays can be configured with the appropriate expansion card that can support that setup. Multiple displays are most commonly used for either a professional computer workstation or for gaming environments, where an extended desktop is useful.

Within the monitor's display properties, you can designate one of the two monitors as the primary monitor, which controls where the desktop administrative features (**Start** menu, taskbar, and so on) appear. The other monitor would contain extra desktop space. While it is far more common to have the desktop span both monitors and contain a different window in each, it is also possible to have the two monitors display the same image, which is useful for presentations.

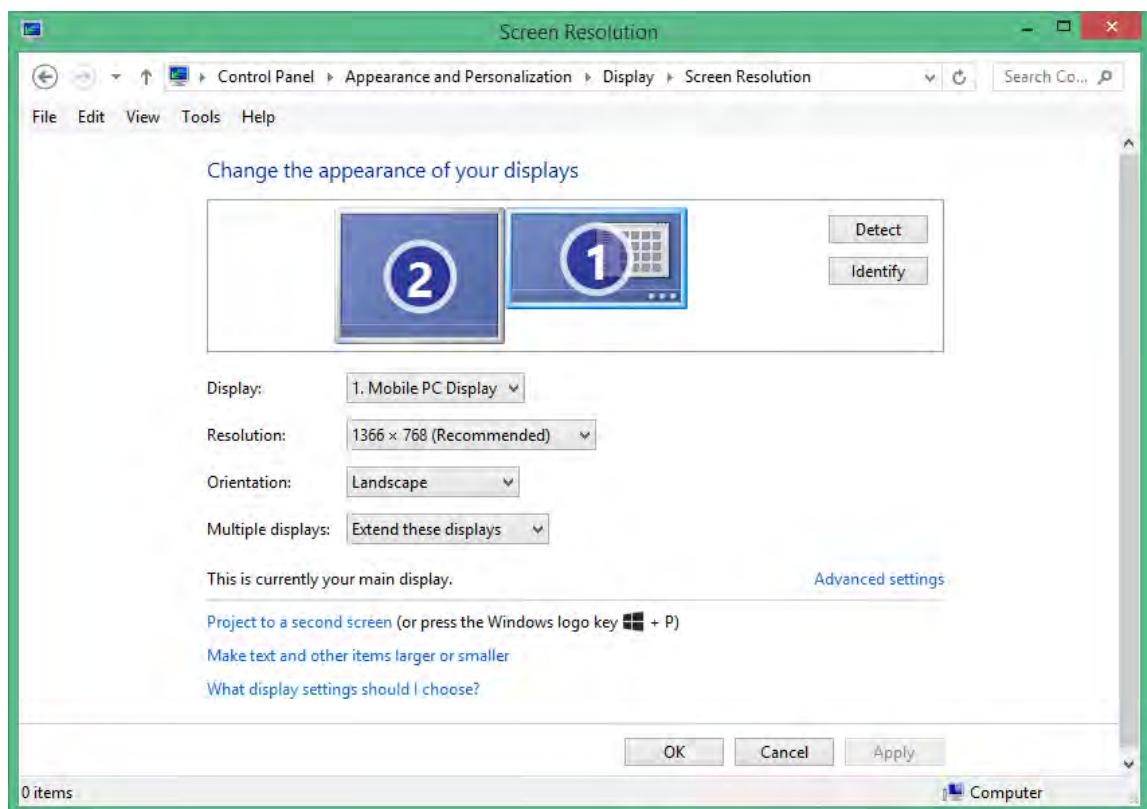


Figure 5–1: Control Panel settings for dual monitors.

## Windows Display Configuration Tools

You can configure the display device settings and features using the Windows display configuration tools. For Windows Vista, Windows 7, and Windows 8, you can configure display properties using the Control Panel. In Windows 8 you can also configure display settings through the PC Settings option from the Charms bar.



# ACTIVITY 5–2

## Configuring Display Devices

### Before You Begin

You have a display device installed.

### Scenario

You want to try out some of the settings and features you recently learned about. You know that customers will be asking you to adjust their displays, so you want to become familiar with how the settings are changed and the results of making those changes.

1. View the current display settings.
    - a) Open **Control Panel**.
    - b) From the **View by** menu, select **Small icons**.
    - c) Select **Display**.
    - d) Select **Adjust resolution** and record the current settings.
    - e) Select the **Back** button.
    - f) Select **Change display settings** and record the current settings. Return to the **Display** settings in **Control Panel**.
    - g) Select **Adjust ClearType text** and work through the wizard to adjust the display. Return to the **Display** settings in **Control Panel**.
  2. Adjust the display device configuration settings
    - a) Change the size of text and items on the screen then select **Apply**.
    - b) Try out different resolutions supported by your monitor to see how they look.
    - c) Accept the new resolution or return to the previous setting as needed.
    - d) Try out different brightness settings.
- 

**Note:** Depending on your system, this might be done through buttons and menus on the monitor, or through Control Panel settings, or even through an application that is installed from the monitor manufacturer.
- e) Accept the new settings or return to the previous setting as needed.

# TOPIC C

## Troubleshoot Video and Display Devices

In this lesson, you have installed and configured display devices. The final major task in supporting display devices is to identify and resolve issues related to display devices. In this topic, you will troubleshoot display devices.

### Common Video and Display Issues

When it comes to display devices, you will encounter a number of issues that are fairly common and can be resolved quickly. Common issues and solutions include the following.

<b>Issue</b>	<b>Possible Problems and Solutions</b>
Dark screen	<p>A dark screen, or an indicator light that is not lit, can indicate general power problems, such as the power is not turned on, the power cable is disconnected, or the power is on but the display is plugged into a power strip, surge protector, or uninterruptible power supply (UPS) that is not turned on.</p> <p>To correct the problem, turn on the power or power strip and reconnect the cables and cords at both ends. If a circuit breaker has tripped, reset it. Press or joggle the power button on the monitor itself.</p>
Dim image or no image in screen	<p>If there is no power light, check for and correct power problems.</p> <p>The data cable to the Video Graphics Array (VGA), Digital Video Interface (DVI), High-Definition Multimedia Interface (HDMI), or display port on the PC may be disconnected. Except on very old displays, you will see an On Screen Display (OSD) message in this case, indicating a signal problem. Connect or re-seat the cables and connectors. If the cable is disconnected, and you do not see an OSD message, the display may be bad.</p> <p>Brightness or contrast may be adjusted improperly. Adjust the settings using the display controls. (The OSD message is not affected by brightness or contrast.)</p> <p>The display may be in power saving mode. The power light will typically change from green to solid or blinking orange. Press a key or move the mouse to wake up the monitor.</p>

Issue	Possible Problems and Solutions
Flickering or distortion on CRT monitors	<p>The display cable may need to be adjusted so that it is more securely connected to the video port. This might also imply that there are bent or broken pins. Try to straighten any bent pins and re-connect the cable. Use caution; a severely bent pin may break, in which case you will need to replace the monitor. Sometimes the cable is removable, in which case you can replace it.</p> <p>This could also be an incorrect display adapter used with incorrect device drivers. If you can see the Power-On Self Test (POST), but the image goes black when the system starts up, try booting the device into VGA Mode and verify that the correct adapter and device drivers are being used.</p> <p>The refresh rate may be too low or too high. The refresh rate should be set to as high as the display and the adapter card can support. If the rate is set too high, then you risk damaging the display.</p> <p>If the display is placed in close proximity to other electronic or magnetic equipment, then interference may cause damage. In this case, move the equipment so that there is adequate space between devices.</p> <p>Check the color depth setting on the display device. The settings may be incorrect. If needed, make the necessary adjustments to the color depth settings for the display.</p>
Display turns itself off	<p>In this case, power management may be enabled. You can adjust this in complementary metal oxide semiconductor (CMOS) settings or in the operating system's display properties.</p> <p>Another reason might be that the display's video card is overheating, causing it to shut down. You can replace the card with one that has a better cooling system, or you can install additional fans to cool the entire system.</p>
Application problems	<p>If the screen goes blank, flickers, or acts erratically when a specific application is active, the application may require different color depth or screen resolution. Right-click in a free area on the desktop and select <b>Screen Resolution</b>. Adjust the settings on this page to suit the user's requirements.</p>
Defective pixels	<p>The pixels that make up a liquid crystal display (LCD) output sometimes do not display as they should. There are generally two types of pixels issues:</p> <ul style="list-style-type: none"> <li>• <i>Dead pixels</i> are pixels that do not display the light as expected. This is shown visually when the LCD is displaying a picture, and there are black spots shown with no light.</li> <li>• <i>Stuck pixels</i> are pixels that only show light, so they appear out of place when the display is on. Light colors can vary from red, to blue or green.</li> </ul> <p>Fixing defective pixels can be difficult to accomplish. It is recommended that you contact the display manufacturer to check for warranty information. If the monitor is an older one, you can attempt to fix the pixels by:</p> <ul style="list-style-type: none"> <li>• Using pressure against the screen using the blunt end of an object.</li> <li>• Using heat to apply pressure to the defective pixels. You must protect yourself with gloves and protect the screen by placing a hot, wet cloth within a plastic bag before placing it on the screen.</li> <li>• Using a defective pixel software utility, such as JScreenFix, Dead Pixel Tester 3, and PixelRepairer.</li> </ul>
Color issues	<p>If the color patterns are incorrect on the display, then you may need to adjust the tint in the display settings. If you notice discoloration of a CRT display, then that could be a sign that you need to degauss the monitor.</p>

Issue	Possible Problems and Solutions
Physical damage	If there is noticeable physical damage to the display device or you know of internal physical damage, you may not be able to repair it. In general, most damaged display devices will need to be replaced, rather than repaired.
Distorted geometry	Running at resolutions that are not in the monitor's memory will cause geometric distortion; however, you should be able to use the monitor controls to address this issue. Magnetic interference can also cause distortion or tilted images.
Burn-in	Image burn-in (also known as image persistence) can happen with any type of display, but it is less prevalent with LCD displays than with CRTs and plasma-based monitors. In addition, burn-in on an LCD display is more likely to be correctable (and preventable) by using a screensaver that changes constantly.
Oversized images and icons	When screen items are too large, it is likely that the screen resolution needs to be adjusted.
Video card issues	<p>There are some specific problems that can cause a number of specific symptoms:</p> <ul style="list-style-type: none"> <li>• If the computer will boot only to VGA Mode (a legacy mode that uses minimal video drivers and a screen resolution of 640 x 480), it is possible that the drivers for the video card are missing or corrupted.</li> <li>• <i>Visual artifacts</i> are errors or anomalies in the visual display of a picture.</li> <li>• A Windows® system stop error (known as the Blue Screen of Death, or BSOD) can be a indicator that there is an issue with your graphics card.</li> <li>• Distortions, such as curves, waves, or other patterns show in the video image.</li> </ul> <p>Additional troubleshooting steps to take in the case of a video card issue include:</p> <ul style="list-style-type: none"> <li>• Check to make sure that the actual video card is seated correctly on the motherboard.</li> <li>• Always verify that you are running the latest drivers for the video card and the chipsets on the motherboard.</li> <li>• Check for interference with other devices within a close proximity. Try removing devices that you suspect may be causing issues.</li> <li>• Check to make sure you are not overclocking the system beyond the capabilities of the card.</li> <li>• Check the power supply and make sure that all connections are secure.</li> <li>• Check to make sure that the fans are operating.</li> </ul>



**Note:** You will work with adapter cards in the next lesson.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Troubleshoot Video and Display Devices.

# ACTIVITY 5–3

## Troubleshooting Video and Display Devices

### Before You Begin

Your instructor has altered the display settings for your monitor. The computer is running and the **Welcome** screen is displayed.

### Scenario

An employee recently had to move the location of his workstation. The employee reports that, since the move, the display does not appear in the center of the monitor. The images are too dark, making them difficult to see, and he cannot see as much on the screen as he would like. The employee needs you to resolve these issues so that he can get back to work.

1. Adjust the monitor display.
  - a) Referring to the monitor's documentation as necessary, locate the physical controls to adjust the brightness of the display image.
  - b) Adjust the brightness so that the monitor is comfortable to view.
  - c) Adjust the contrast so that you can view all the screen elements easily.
2. Change the resolution.
  - a) To open the **Screen Resolution** window, right-click the desktop and select **Screen resolution**.
  - b) In the **Resolution** section, select the current resolution to display the drop-down list.
  - c) In the **Screen Resolution** window, drag the slider or click to select the appropriate resolution.
  - d) Select **OK**.
  - e) In the **Display Settings** message box, select **Keep changes** to set the new resolution.
3. Adjust the horizontal and vertical positions of the image.
  - a) Referring to the documentation as necessary, locate the controls to adjust the size and centering of the display image.
  - b) Adjust the vertical display position so that the display is centered top-to-bottom on the screen.
  - c) Adjust the horizontal display position so that the display is centered side-to-side on the screen.
  - d) Adjust the height and width of the image so that there is either no border or the smallest border allowed.

## Summary

In this lesson, you supported display devices by installing, configuring, and troubleshooting them. It is likely that you will be called upon to support display devices often as a computer technician.

**What types of monitors do you have experience with? What types of connections have you used to connect those monitors to computers?**

**In your current job role, have you had to troubleshoot display device problems? If so, what did you do and how did you resolve the issues?**



**Note:** Check your CHOICE Course screen for opportunities to interact with your classmates, peers, and the larger CHOICE online community about the topics covered in this course or other topics you are interested in. From the Course screen you can also access available resources for a more continuous learning experience.

# 6

# Installing and Configuring Peripheral Components

**Lesson Time:** 1 hour

## Lesson Objectives

In this lesson, you will install and configure peripheral components. You will:

- Install and configure input devices.
- Install and configure output devices.
- Install and configure input/output devices.
- Install and configure PC expansion cards.

## Lesson Introduction

So far in this course, you have identified the hardware and software that makes up a personal computer system and examined some general best practices for working with them. Now that you have a solid base of background information, it is time to roll up your sleeves and start working with some of those hardware components. In this lesson, you will install and configure peripheral computer components.

Much of the work that you will perform as a PC technician will involve installing and configuring various hardware and software components. As an IT professional, you will often find yourself setting up end-user workstations or helping those end users with the hardware they need to make their daily lives easier. Installing and configuring peripheral components—like display devices, keyboards, and mice, or even more specialized devices—are some of the more common tasks that you will perform.

# TOPIC A

## Install and Configure Input Devices

In the previous lesson, you examined display devices and how to install and configure them so that users can see the computer system's output. Users also need to be able to interact with the computer system by using input devices. In this topic, you will install and configure input devices.

Computers need user input such as directions or commands and user interaction with the programs that are included in order to produce something of use. Keyboards and pointing devices are the standard input devices for personal computers these days, but there is an ever-growing number of input devices available for the user to interact with in a variety of ways. As an A+ technician, part of your responsibilities will include installing and configuring all types of input devices.

### Keyboards

Keyboards are a standard input device. They include letters, numbers, and special characters on dedicated keys. Keys can also be used in combination to create additional characters. Special keys such as the Shift, Ctrl, Alt, Esc, and Windows keys can be combined with other keys on the keyboard to issue special commands to the operating system or application.

When selecting a keyboard for a user, in addition to considering its ergonomics, you should also consider whether the keyboard offers additional features (such as customizable hot keys and scrolling) as well as wireless connectivity. Many users now prefer to use a wireless keyboard as it gives them the freedom to locate the keyboard anywhere on their desks. In some cases, users might be able to use a Bluetooth-enabled keyboard to communicate with both their desktop computers and a mobile device such as a tablet or a smartphone. Be sure to determine the potential keyboard's connector requirements; if the keyboard uses USB, you will need to make sure the user's computer has an available USB port.

<i><b>Input Device</b></i>	<i><b>Description</b></i>
Standard keyboard	<p>Standard keyboards have varying numbers of keys depending on the manufacturer, whether it is a compact keyboard or regular sized keyboard, or if it is a keyboard with specialized keys. Other ways that standard keyboards might vary include:</p> <ul style="list-style-type: none"> <li>• Being wired or wireless. Wireless keyboards typically use a USB transceiver to connect with the keyboard. Others might use Bluetooth connections which might or might not require an adapter.</li> <li>• Wireless keyboards might be powered by standard AA or AAA batteries, rechargeable batteries, or via solar power.</li> <li>• Some of the specialized keys might include programmable keys for engineers, graphic designers, or gamers.</li> <li>• Some might include security features such as fingerprint scanners.</li> <li>• Some might include integrated pointing devices such as track pads.</li> </ul> 

<b><i>Input Device</i></b>	<b><i>Description</i></b>
Ergonomic keyboard	<p>Natural or ergonomic keyboards usually split the keyboard in half so each hand can comfortably use its own set of keys. Built-in wrist rests are common, and some ergonomic keyboards also have an integrated pointing device such as a trackball or touch pad.</p> 
Dvorak keyboard	<p>Dvorak keyboards rearrange the keys into a more efficient arrangement that makes faster typing possible for users who have become familiar with it.</p> 

## Pointing Devices

A wide variety of pointing devices are available to accommodate the comfort and space needs of users. The most common pointing device is the mouse. Other pointing devices include game pads, joysticks, and touch pads. Most users prefer wireless mice over wired mice because of the freedom it gives them to move around while working. Choosing between a mouse, a trackball, and a touch pad usually comes down to the personal preference of the user.

Input Device	Description
Mouse	<p>A mouse is a small object that runs across a flat surface and has buttons that send electronic signals to the graphical user interface (GUI). The name is derived from its original appearance: a small rounded rectangle shape with a single cord attached at one end. Most mice today are optical; a laser detects the mouse's movement. Optical mice have no mechanical moving parts, and they respond more quickly and precisely than mechanical types of mice.</p>
	<p>Wired mice typically connect to a USB port and wireless mice connect to a transceiver connected to a USB port. Wireless mice can alternatively use a Bluetooth connection.</p>
	<p>Mice have varying numbers of buttons depending on their manufacturer and purpose. The mouse that comes with a Mac computer has only one button, while most mice that come packaged with other computers typically have two buttons. Specialized mice for gaming might have anywhere from 4 to as many as 24 buttons that can be programmed for specific functions. Some mice include two buttons on the top and buttons on the side dedicated to things like moving back or forward one page on screen.</p>
Trackball mouse	<p>A trackball is basically an upside down mouse. The ball is mounted on the top of the case instead of the bottom and signals are sent to the computer by moving the ball with your thumb, fingers, or palm instead of by rolling the ball across a flat surface. Like a mouse, a trackball has at least one button that is used to send electronic signals to the computer.</p>
Touch pad	<p>A touch pad is a small, touch-sensitive pad where you run your finger across the surface to send electronic signals to the computer to control the pointer on the screen. Touch pads can have buttons like a mouse or trackball, or the touch pad can be configured to detect finger taps on its surface and process those signals like button clicks.</p>

<b>Input Device</b>	<b>Description</b>
Trackpoint	<p>A <i>trackpoint</i>, or pointing stick, is most commonly found on laptops. Located in the center of the keyboard, the trackpoint is a small joystick-like button that responds to user force in all directions in order to move the mouse pointer on screen.</p> 
Gamepad	<p>A gamepad is a game controller used to interact with a video game console or program, typically held and manipulated with two hands. It uses a number of buttons and toggles, each of which controls a different action within the program.</p> 
Joystick	<p>The latest versions of many gamepads also include sensors and pointing devices that sense directions of movement and rotation, and use a combination of these movements to control actions within the game program.</p> <p>Gamepads typically connect to a device via a USB connection. The latest technology in gamepads is unique in its wireless capabilities: many gamepads do not attach to a device via a connector, but rather transmit inputs wirelessly to the receiving device or console.</p> <p>A joystick is a pivoting stick or lever attached to a base that is used to control movement on a device. It typically also includes push buttons, toggles, or switches that control other actions associated with the program or device that the input is controlling. The joystick inputs the angle and direction of a desired movement.</p> <p>Joysticks are most commonly used to control video games or other computer programs, but are also used to control machines and devices such as cranes and unmanned vehicles.</p> <p>Legacy joysticks connected to a computer via a game port, a device port designed specifically for connecting this input device. However, most modern joysticks connect to the device via a USB connection.</p>

## Optical Input Devices

Optical input devices provide a method of getting information from a paper source into a digital format the computer can work with. Some of the optical input devices you might encounter are listed in the following table.

<b>Optical Input Device</b>	<b>Description</b>
Scanner	<p>A scanner is used to take a photo-identical copy (scan) of a physical hard copy of any kind of document, such as a piece of paper or a photo, and create a digital-format copy of the document.</p> <p>A scanner is similar to a photocopy machine or copier, but with a much smaller footprint. Scanners can be attached directly to a personal computer to import scanned copies of documents. With the proper software or program installed, scanned versions can be manipulated and edited once they have been imported.</p> <p>A scanner typically uses a USB or high-speed USB connection to connect between devices.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <b>Note:</b> Many printers are multi-function devices and include a built-in scanner. Printers and scanners are covered in depth later in the course.       </div>
Barcode reader	<p>Barcodes provide a simple and inexpensive method of encoding text information that is easily read by inexpensive electronic readers. A barcode reader decodes a barcode by scanning a light source across the barcode and converting the pattern of reflected light to an electronic signal that is decoded back to the original data by electronic circuits. There are currently four different types of barcode readers available: pen-type readers (or barcode wands), laser scanners, Charge Coupled Device (CCD) readers, and camera-based readers.</p> <p>Barcode scanners or readers connect to a device via a USB connection or are wireless.</p>

## Multimedia Input Devices

A *multimedia device* is a computer peripheral or internal component that transfers sound, images or a combination of both to or from a personal computer. Multimedia devices can be input devices or output devices.

Common multimedia input devices include different types of cameras and sound devices.

<b>Multimedia Input Device</b>	<b>Description</b>
Digital camera	<p>A digital camera uses electronic signals to capture and store photographic images or video images. The resulting files are often stored on embedded memory cards, removable memory cards, or optical discs. Connecting the digital camera or its removable memory card to a PC enables you to save, transfer, print, and otherwise work with the images.</p>  <p>If the digital camera has a removable memory card, the card itself may need to be connected to a computer through a media reader. Most digital cameras also offer USB and FireWire cables and connections.</p>

Multimedia Input Device	Description
Camcorder	<p>A video recording camera captures and stores visual images and sounds in the form of either analog or digital signals. Video files are stored either on an internal storage device or on removable memory cards.</p>  <p>Most digital camcorders available for personal (commercial) use also offer USB and FireWire cables and connections. If the camcorder has a removable memory card, the card itself may need to be connected to a computer through a media reader. Professional-grade cameras are more likely to use tapes or disks that will need an alternate transfer method, often including digitizing.</p>
Webcam	<p>A web camera, or webcam, is used to send periodic images or continuous frames to a website for display. Webcam software usually captures the images as JPEG or MPEG files and uploads them to a web server. Webcam images can also be accessed using some instant messaging software and by some video applications. Some corporations use webcams as a security measure.</p>  <p>Webcams commonly use USB or FireWire cables and connectors.</p>
Microphone	<p>A computer microphone is used to input audio into the device, either for recording the audio as data or for use in real-time, such as the audio input that accompanies a webcam or video conferencing chat.</p>  <p>Microphones can be connected to the microphone port or jack of any sound card. If the card is color-coded, it will be pink. Otherwise, it will be labeled MIC or have a picture of a microphone. Many microphones have a 1/8-inch phono plug built into the attached cable.</p>

## Security Input Devices

Security input devices provide protection against unauthorized access to computing devices and resources. Commonly implemented security input devices include biometric devices and other security devices.

*Biometrics* is an automated method of recognizing a person based on a physiological or behavioral characteristic unique to the individual, such as a retina pattern, fingerprint, or voice pattern. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. Biometric input devices can add an additional layer of physical security or information security by verifying the identity of the person attempting to gain access to a location or device.

Biometric devices will need to be installed and configured, and then initialized for the specific end user who will be using the device. The initial biometric authentication “object” for the user (be it a fingerprint, retina scan, pass phrase, etc.) must first be captured and stored. Then the user will have

to test the device to make sure that it accurately verifies his or her identity against the authentication object, permitting them access to the location or device.

Whether or not a biometric device is being deployed will likely be a decision made based on an organizational security policy or standard. If biometric devices will be deployed at individual workstations, you will need to determine the specific biometric device's connector requirements; as most use a USB connection, you will need to make sure that the user's computer has an available USB port to connect the device.

Several types of security input devices might be used in an organization.

<b>Security Input Device</b>	<b>Description</b>
Fingerprint scanner/reader  	Scans a person's fingerprint(s) and matches it against a database of fingerprints to verify that person's identity. Once verified, that person will be able to access a building, location, or device or can be used with point-of-sale applications to complete a transaction.  If not hard-wired into a system (such as a security system), fingerprint scanners/readers used with smaller devices like a personal computer typically connect via a USB connection.
Retina scanner  	Some laptops have a fingerprint scanner integrated into the system as well, which is usually placed near the keyboard area of the laptop. The scanner is used to verify the identity of the user and grant them the ability to use the laptop.  Scans a person's retina or iris and matches it against a database of retina scans to verify the person's identity. Once verified, that person will be able to access a building, location, or device.  If not hard-wired into a system (such as a security system), a retina scanner used with a smaller device like a personal computer typically connects via a USB connection.

<b>Security Input Device</b>	<b>Description</b>
Voice recognition 	<p>Uses a spoken phrase called the "pass phrase" and compares it against a person's voice print, a recorded and stored version of that person saying the pass phrase, to verify identity. Once verified, that person will be able to access a building, location, or device.</p> <p>If not hard-wired into a system (such as a security system), a voice recognition system used with a smaller device like a personal computer typically connects via a USB connection.</p>
Signature recognition 	<p>Uses a signature pad and a database of approved signatures. A user signs the signature pad, and the recognition system analyzes the individual behavior of the person signing, such as the strokes used and the pressure applied while signing, to verify the identity of the user.</p> <p>If not hard-wired into a system (such as a security system), a signature capture pad used with a smaller device like a personal computer typically connects via a USB connection.</p>
Keyboard 	<p>Using a biometric keyboard, only authorized users would be able to use the keyboard, and only once their identity was verified through the verification program.</p> <p>The keyboard and a special program monitor the individual's typing behaviors, such as key press duration or pressure, key strokes, and so forth, to create a baseline for normal typing for the individual. The program can challenge a user to verify identity by typing, and compares the keystroke behavior of the typist to that stored in a database for the user.</p> <p>Most biometric keyboards connect via a USB connection.</p>

<b>Security Input Device</b>	<b>Description</b>
Mouse  	<p>Using a biometric mouse, only authorized users would be able to use the mouse and access or navigate the computer system, and only once their identity was verified through the verification program.</p> <p>A biometric mouse uses biometric authentication, typically a built-in fingerprint reader, to verify the identity of the user and provide them control over the mouse.</p> <p>Most biometric mice connect via a USB connection.</p>
Storage devices  	<p>Using a biometric storage device, such as a flash drive or hard drive, only authorized users would be able to access files or data stored on the storage device.</p> <p>Biometric flash drives or hard drives use another kind of biometric authentication, typically a built-in fingerprint reader, to verify the identity of the user and provide them access to the flash drive files.</p> <p>Most biometric storage devices connect via a USB connection.</p>
Motion sensor  	<p>Motion sensor peripherals can be used as either a security device or as an input device. In either case, infrared sensors built into the device detect changes in heat as a body, hand, or fingers move in front of it.</p>
Smart card reader  	<p>Smart card readers read the information stored in a microprocessor on a smart card. It is used as a physical authentication token for accessing computers, rooms, or buildings. The smart card is often an employee ID card with the microprocessor embedded in the card.</p>

## Guidelines for Installing Input Devices



**Note:** All of the Guidelines for this lesson are available as checklists from the **Checklist** tile on the CHOICE Course screen.

Before you attempt to install an input device, you should consider certain factors:

- Be sure that you have the most current drivers for the input device for the operating system of the computer on which you plan to install it.
- Either let the PC find the right driver, or restart the computer and see if the device is recognized. If that does not work, you will need to find a driver for the device.
- Review the manual or quick start guide that came with the device. In some cases, the manufacturer might require you to install the device drivers before connecting the device to the computer.



Access the **Checklist** tile on your CHOICE Course screen for reference information and job aids on How to Install Input Devices.

# ACTIVITY 6-1

## Installing Input Devices

### Before You Begin

For this activity, you will need a replacement keyboard and mouse or other pointing device.

### Scenario

You have received a service call to replace a user's mouse and keyboard. The user doesn't like the style of their current keyboard, so they would like to try an alternative keyboard style. The user would also like to try a different style of pointing device than what they are currently using.

1. Replace the keyboard.
  - a) Determine the connection type used by the replacement keyboard.
  - b) Unplug the old keyboard from the system unit.
  - c) If you are using a wireless keyboard, insert batteries and move the switch to the **ON** position.
  - d) Plug the new keyboard or transceiver into the appropriate port.
  
2. Replace the pointing device.
  - a) Determine the connection type used by the replacement pointing device.
  - b) Unplug the old pointing device from the system unit.
  - c) If you are using a wireless mouse, insert batteries or make sure it is charged, and move the switch to the **ON** position.
  - d) Plug the new mouse or transceiver into the appropriate port.
  - e) Start the computer.
  
3. Test the installed devices.
  - a) On the keyboard, press the **Windows** key to access the **Start** page.
  - b) Move the pointing device around to verify that it is working properly.
  - c) Use both the left and right pointing device buttons to verify that their functionality is appropriately configured.

### Windows Input Device Configuration Tools

Depending on which operating system you are using, and what you need to configure, you can use the Windows Control Panel or Windows 8 PC Settings to configure input devices. You can adjust settings for the mouse, touch screen, touch pad, keyboard, and Bluetooth devices.

Some of the configurations you can perform includes:

- Specifying which mouse button is the primary mouse button.
- How fast a double-click is.
- How fast the user types.
- Whether to delay input from the touch pad so that while typing, the touch pad isn't accidentally invoked.
- Calibrate the screen for pen or touch input.
- Configure the meaning of gestures on a touch screen or touch pad.
- Turn Bluetooth on, which allows Bluetooth input devices to find and connect to your system. Turn it off to prevent others from accessing your system through Bluetooth connections.

## Third-Party Configuration Utilities for Input Devices

Input devices often come with their own configuration utilities. These additional third-party device configuration utilities enable users to configure the device beyond the capabilities built into the drivers available through the operating system. You might need to install the third-party utilities before connecting the device. Refer to the documentation for details on when and how to install any configuration utilities that come with the device.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Configure Input Devices.

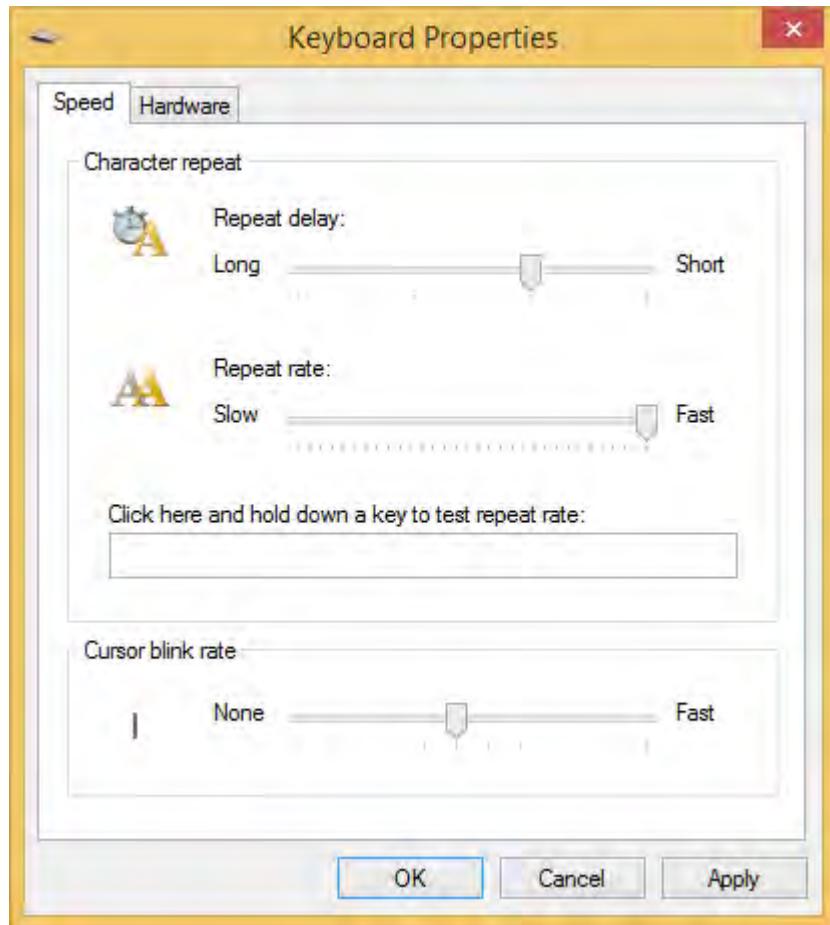
# ACTIVITY 6-2

## Configuring Input Devices

### Scenario

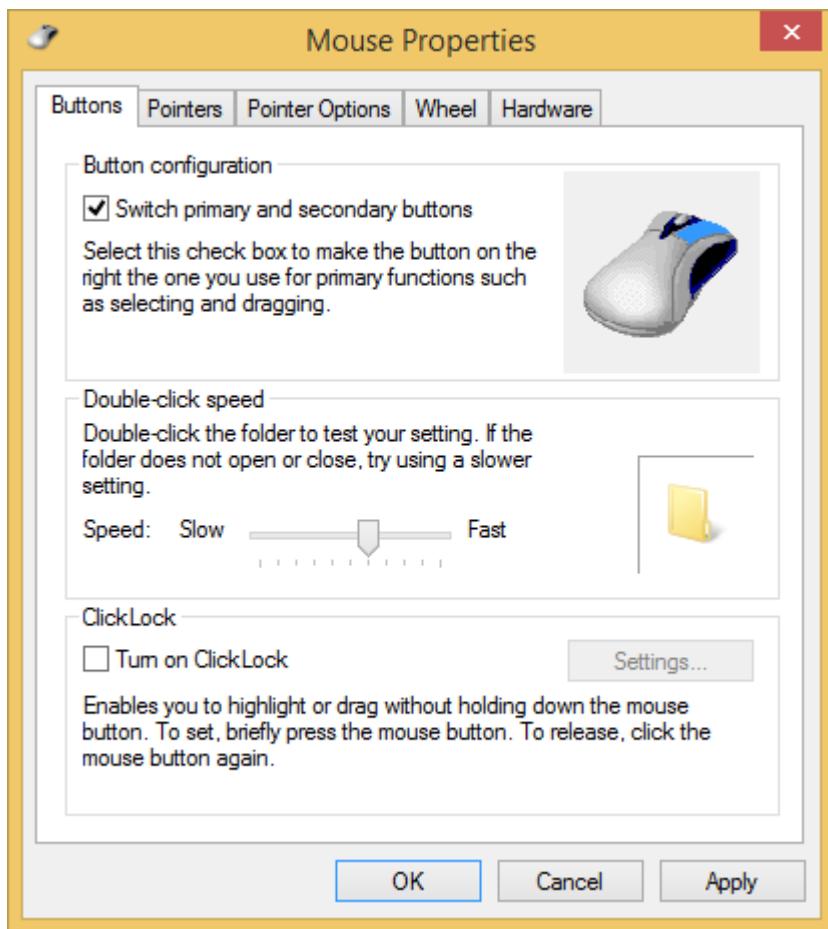
You just replaced a user's mouse and keyboard. The user is left-handed and prefers a slow-blinking cursor. She also has a hard time distinguishing the mouse pointer from other screen elements, and asks if you can adjust the pointer to something more easily discernible.

1. Configure the keyboard settings.
  - a) Open Control Panel.
  - b) In the Control Panel window, in the **Adjust your computer's settings** section, from the **View by** drop-down list, select **Large icons**.
  - c) Select the **Keyboard** link.
  - d) In the **Keyboard Properties** dialog box, on the **Speed** tab, reduce the cursor blink rate by dragging the **Cursor blink rate** slider to the left.

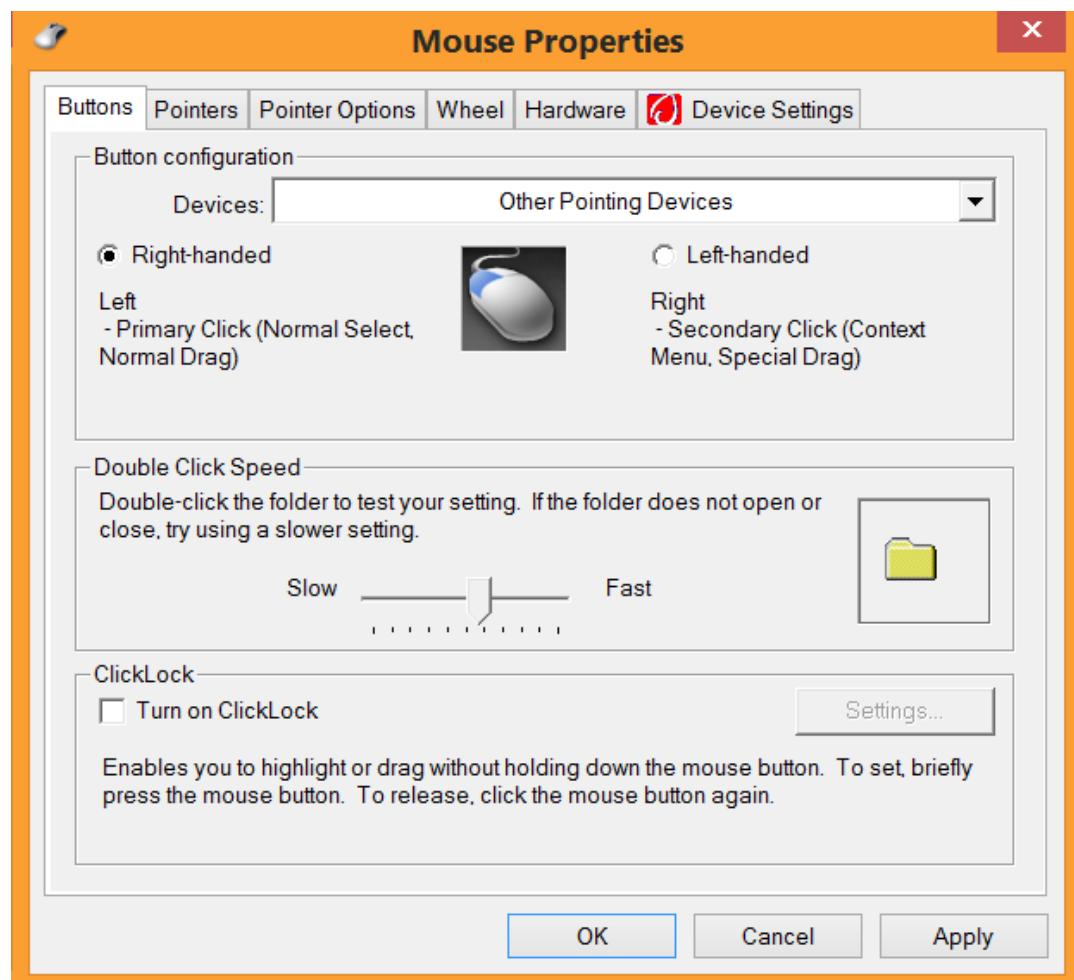


- e) Select **Apply**.
  - f) Select **OK**.
2. Configure the mouse settings.

- a) In the Control Panel window, select the **Mouse** link.
- b) In the **Mouse Properties** dialog box, on the **Buttons** tab, if the options shown in the following image are displayed, check the **Switch primary and secondary buttons** check box.

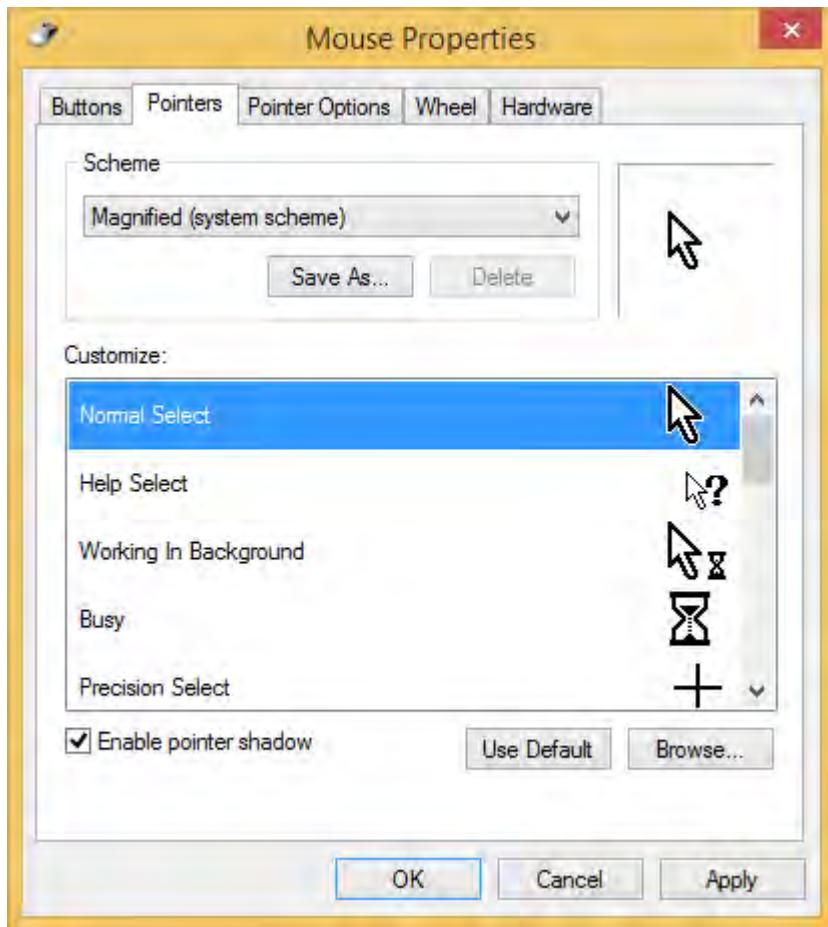


- c) In the **Mouse Properties** dialog box, on the **Buttons** tab, if the options shown in the following image are displayed, select the **Left-handed** radio button.



- d) To verify that the right mouse button is now the primary button, right-click the **Pointers** tab.  
e) Right-click the **Buttons** tab.  
f) Select the **Pointers** tab.

- g) From the **Scheme** drop-down list, select **Magnified (system scheme)**.



- h) Select **OK**.

3. Reconfigure the mouse settings to suit your personal preferences, and close the **Control Panel**.

# TOPIC B

## Install and Configure Output Devices

Earlier in the course, you worked with display devices, which are the most prevalent type of output device. However, you will be responsible for supporting different types of output devices as part of your duties as an A+ technician. In this topic, you will install and configure other output devices.

Although being able to view the user interface and documents is essential to working with a PC, there are other types of output in addition to simple visual display output. By installing and configuring all sorts of output devices, you can be sure that you are appropriately supporting your users' needs.

### Output Devices

Output devices take information stored in the computer and make it available in a visual, audio, or tactile format.

- Probably the most common type of output device is the display device, which you worked with in the last lesson. As you saw, there are a wide variety of device types and associated connection interfaces.
- Another common output device type is the printer, which you will work with in greater depth later in the course. As with display devices, there are many types of printers and related output devices that provide physical output from a PC.
- Another common output device is a pair of speakers, or a set of speakers that you can configure for surround sound effects. Speakers are connected to the **Line Out** port or jack on the sound card or motherboard. Some speaker sets are permanently connected to each other, while other speaker sets are connected by the user to each other or to a subwoofer. A cable runs from one of the speakers to the **Line Out** port to connect both speakers to the computer. If the card or motherboard is color-coded, the speaker port will be lime green. The port might be labeled as **Line Out, Out, Spkr, or Speaker**, or it may have an image with an arrow indicating the direction of the audio (out). Speakers typically have a 1/8-inch phono plug built into the attached cable.
- Headphones are another output device. They might connect to a port on an external speaker, or be connected directly to the speaker port, a **Line Out** port, or a dedicated headphone port.
- For blind or visually impaired users, using a standard monitor display device is not possible. One method for a blind person to access what would usually be displayed on a monitor is to use a screen reader application. This application reads any text on screen and uses information available about graphics and images that are displayed. For example, a well-designed website will have alternate text available for the screen reader to read that describes the image displayed. The information is provided to the user through audio devices such as speakers or headphones.
- Another output device for the blind or visually impaired user is an alternative to a standard printer. Instead of printing with standard ink, raised tactile output is created for Braille reading or raised-line drawing images.

### Surround Sound

Most home audio systems are set up with either 5.1 or 7.1 surround sound. The 5.1 configuration places one speaker at the front center, a pair of speakers to the front side of the listener and another pair to the rear or even with the listener, and a subwoofer speaker anywhere in the room. A 7.1 configuration adds another pair of speakers to the sides, between the front and rear speakers.



**Figure 6-1: Surround sound configuration for a home theater.**

Computers can be connected to more than just a standard pair of PC speakers or a headphone. Some computers include connections for all of the speakers used in a 5.1 or 7.1 surround sound system. Even if the computer doesn't have all of the ports needed to connect the speakers to an audio receiver and its connected speakers, you can use a variety of methods to connect a computer to a home audio system.

Connection Method	Description
Analog cable	In this method, an analog cable with a mini stereo plug on one end plugs into the <b>Audio Out</b> or headphone jack on the computer. The other end of the analog cable is equipped with RCA plugs that can be connected to a port on the audio receiver, typically the auxiliary ports.
USB cable	<ul style="list-style-type: none"> <li>Using a cable that has a USB port on one end and RCA plugs on the other end allows the computer to send audio and visual information to the home audio system.</li> <li>An external digital-to-audio converter (DAC) is often connected to the computer via USB cable and to the home audio system using RCA cables.</li> </ul>
Digital audio cable	<ul style="list-style-type: none"> <li>Some computers have an S/PDIF port. With this port, you can use a coaxial cable with RCA connectors or a TOSLINK cable to connect the computer and the home audio system.</li> <li>Other computers, such as Mac computers, have a digital port for the headphone jack. When a standard pair of headphones or speakers is connected, the port works in analog mode. When a digital cable is connected, the information is sent digitally to the home audio system.</li> </ul>

<b>Connection Method</b>	<b>Description</b>
HDMI	If your computer is equipped with an HDMI port, and your home audio system also has HDMI ports, you can send audio and visual data over the HDMI cable.

You will also need to configure the surround sound through **Control Panel**. You can specify how many speakers there are, what types of speakers each one is, and balance the system for the type of room.

## Device Manager

You can use *Device Manager* to manage and configure hardware devices. In Windows 7, there are several ways to access **Device Manager**:

- Open **Control Panel** and then select **System and Security**→**Device Manager**.
- At a command prompt or in the **Run** dialog box, enter the devmgmt.msc command.
- In the navigation pane of **Computer Management**, select **Device Manager**.

You can use the same methods in Windows 8 to open **Device Manager**. You can also use the **Charms Search** to search for **Device Manager**, or from the **Desktop**, right-click the **Windows** button and select **Device Manager**.

You can use **Device Manager** to:

- View a list of all devices attached to the system.
- See the status of a device. An exclamation point means there is a problem with a device; a yellow question mark means the device has been detected but a driver is not installed, or there is a resource conflict.
- Enable or disable a device. A disabled device appears with a red X.
- Determine the device driver a device is using; upgrade a device driver; roll a device driver back to a previous version.
- Determine any system resources that the device is using, such as interrupt request lines (IRQs) or Direct Memory Access (DMA) ports.
- Uninstall or reinstall devices.

## Device Manager Log On Options

If you are logged on as a standard user, you are notified that you are restricted from changing device settings, and **Device Manager** opens in read-only mode. If you select an option to make a change, you are prompted to log in using administrator credentials to make the change. If you are logged on as an administrator, you can make the desired changes.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Install and Configure Output Devices.

# ACTIVITY 6–3

## Installing and Configuring Output Devices

### Before You Begin

Your instructor will provide you with a pair of speakers, or a 5.1 or 7.1 surround sound system designed for computers if your sound card supports it.

### Scenario

You are working with the team that is presenting a slide show that includes audio portions. You need to verify that the speakers work with the computer.

1. If you were given a pair of speakers, perform this step. If you were given a surround sound system, perform the next step instead.
  - a) Connect the speakers to each other.
  - b) Connect the speakers to the Spkr, Speaker, or Line out port on the computer.
  - c) If necessary, connect the speakers to a power source.
2. If you were given a surround sound system, perform this step.
  - a) Refer to the documentation to see how the speakers should be placed.
  - b) Connect the speakers to each other, to the computer, or both, as indicated in the documentation.
  - c) Connect the surround sound system to a power source.
3. Test the speakers.
  - a) In **Control Panel**, select **Sound**.
  - b) In the **Sound** dialog box, select the **Playback** tab.
  - c) Select **Speakers** and then select **Configure**.
  - d) In the **Audio channels** section, select the speakers you want to test, then select **Test**.  
You can also select individual speakers at the right of the window to play a test sound from the selected speaker.
  - e) Select **Next**.
  - f) On the **Select full-range speakers** page, select the check box for your setup. Select each speaker to test it.
  - g) Select **Next**.
  - h) Perform any additional tests if offered.
  - i) When the **Configuration complete** page is displayed, select **Finish**.

# TOPIC C

## Install and Configure Input/Output Devices

Some devices function as both input devices and as output devices. In this topic, you will install and configure input/output devices.

### Input/Output Devices

An input/output device contains components that enable one device to perform both input and output functions.

<b>Device</b>	<b>Description</b>
MIDI-enabled device	The Musical Instrument Digital Interface (MIDI) connection enables you to connect and control musical devices such as electric keyboards, synthesizers, guitars, drum kits, and mixers. Sound cards usually include built-in synthesizers as well, to produce MIDI sounds. MIDI devices can be connected to each other and then to the computer.  MIDI devices can connect to the computer using a number of ports. MIDI to USB interface, MIDI to serial, or MIDI to FireWire connections are most commonly used, allowing for faster communication between the musical instrument and the computer or controller device.
Multi-function printers	Multi-function printers combine input and output features in one device. They typically include printer (output), scanner (input), and fax (input/output or send/receive) capabilities.
Headset	A headset combines headphones (audio output) with a microphone (audio input). You can use headsets to participate in online meetings, to participate in gaming with other players, and to use with communication applications such as Skype.

### KVM Switches

A *keyboard, video, mouse (KVM) switch* is a device that enables a computer user to control multiple computers with a single keyboard and mouse, with the display sent to a single monitor. This feature is particularly useful in managing multiple test environments, or in accessing multiple servers that have no need for dedicated display or input devices. KVM switches are available with PS/2 or USB connections, and come in desktop, inline, or rack-mount varieties. Higher-end rack-mount models can be uplinked to connect dozens of computers.



**Figure 6-2: A KVM switch.**

## Touch Screens

Touch screen monitors enable input by touching images on the screen. This technology is used in bank ATMs, some point-of-sale terminals at fast food restaurants, and other situations where a separate keyboard for input is not appropriate. Touch screens are also found on many smartphones, tablets, and laptops sold for general public use.

Touch screens enable users to enter inputs by touching areas on a monitor screen. They can be activated by a finger touch or a stylus touch.

Touch screens are composed of:

- Touch sensors. The sensors can be a panel that lays over a standard monitor or can be built into a special touch screen monitor where the user actually touches the surface of the monitor.
- A controller. If using an overlay panel, the controller connects to the panel and then to a PC port. Many use a COM or USB port, although there are special instances where the controller connects to a drive or other device or port. For touch screens with built-in touch sensors, the controller is built into the monitor. In this case, the monitor contains two cables—one to the monitor port and one to the COM or USB port (or other port).
- A device driver or specialized software. This enables the operating system to receive and interpret information from the touch screen device.

## Smart TVs

A *smart TV* is a hybrid device. This is a television set with web and Internet features built into it. You can access the Internet using voice commands or the remote without the need to connect other devices to the TV. It seems like a good idea, but some devices are not being updated as new features from content providers are made available, while other manufacturers are providing updates for apps and firmware.

Another drawback for some smart TVs is that the voice commands are sent to a third party without any security measures in place to protect the information you request. Some manufacturers use the information you send to add additional advertising to your viewing experience. Consult the documentation that came with your smart TV to see if there is a TV privacy policy.

## Set-Top Boxes

A *set-top box* is a device that takes video content and converts it to a format that can be viewed on a television. Set-top boxes are also known as streaming players (streaming TV) or media players.

Traditionally, set-top boxes were used by cable companies to descramble the broadcast signal so that only authorized customers could view the programming offered. Satellite television providers also have a set-top box that acts as a converter to allow over-the-air content to be viewed on televisions.

You can also purchase set-top boxes that are not tied to a cable or satellite television provider. Examples include the Apple TV, Amazon Fire TV, and Google TV set-top boxes. These devices use Wi-Fi or Ethernet connections to connect the television to the Internet so that you can view content from providers such as Netflix, Hulu, or other content sites. Some also have built-in Internet browsers.

These devices connect to the television through coaxial or HDMI connections.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Install and Configure Input/Output Devices.

# ACTIVITY 6–4

## Installing and Configuring Input/Output Devices

### Before You Begin

Your instructor will provide you with one or more input/output devices, appropriate documentation, and cables.

### Scenario

You have installed input and output devices. Now you want to try installing a device which can be both an input and an output device.

1. If you have a MIDI device, connect it through the USB-to-MIDI device or a MIDI expansion card.
  - a) Locate the appropriate port and connect the MIDI adapter to it.
  - b) If necessary, connect MIDI cables to the MIDI adapter.
  - c) Connect the MIDI cable to the MIDI instrument.
  - d) If necessary, install drivers for the MIDI instrument.
  - e) If necessary, install software to work with the MIDI instrument.
  - f) Test the MIDI device by playing a few notes to ensure that it is working properly.
  
2. If you have a KVM switch, working with a partner, connect one set of peripherals to multiple computers.
  - a) Identify the ports on your computer that will connect to the KVM switch so that you can determine the type of KVM switch you need. There are two types of KVM switches available: PS/2 and USB.
  - b) Obtain the appropriate type of KVM switch you need.
  - c) Turn off all the computers that are to be connected.
  - d) Insert the KVM connectors into the appropriate ports on the computer.
  - e) Connect all the computers to the KVM switch in the same way.
  - f) Connect a monitor, keyboard, and mouse in the appropriate ports of the KVM switch.



**Note:** Some KVM switches also have speaker or headphone ports.

- g) Turn on all the computers and monitors.



**Note:** Some KVM switches require a power source and might have a power switch.

- h) Toggle the KVM device through all the connected PCs to check whether it is functioning correctly.

3. Disconnect the devices connected through the KVM switch and connect the devices directly to the computers again.
  
4. If you have a set-top box, refer to the documentation provided to determine how to connect and configure the device to work with the television or computer.



**Note:** Some set-top boxes provide the ability to access the Internet, using your television as the display device. Other set-top boxes allow a computer to receive television signals.

5. Connect a headset to the computer.

- a) Examine the connections on the headset.
- b) Connect the appropriate plug into the headphone jack.
- c) Connect the appropriate plug into the mic jack.
- d) Test the functionality of the microphone and headphones.

Your instructor will guide you through selecting an app or application to use to test the headset.

---

# TOPIC D

## Install and Configure Expansion Cards

In the previous topics, you installed input, output, and input/output devices. These devices typically connect using standard ports that are available on most machines, such as a USB port. You can expand the functionality of your computer by adding expansion cards that provide additional ports for a variety of peripheral devices. In this topic, you will install and configure expansion cards.

Display devices, keyboards, and other pointing devices are the most common devices you are likely to install and configure; these devices are typically included in a standard workstation environment when a PC is requested. When a user needs to connect a peripheral component that doesn't have an existing interface, like a multimedia device, you will need to install an expansion card. As an A+ technician, your responsibilities are likely to include upgrading users' computers by installing a variety of components, including expansion cards.

### Expansion Card Types

Expansion cards extend the capabilities of a computer. There are many different types of expansion cards, each of which provides different capabilities.

<b>Expansion Card Type</b>	<b>Description</b>
Sound cards	A sound card or audio card provides the interface necessary for the input of audio signals to, and output from, the computer.
Video cards	A video card, sometimes called a display card or graphics card, provides the interface necessary to generate the visual output that is sent to the display device.
Network cards	A network card, sometimes called a network interface card (NIC), provides the interface necessary for network communications, whether for wired or wireless connectivity.
USB cards	A USB card provides the interface necessary for the computer to recognize and interact with all devices that connect to the computer via a USB connection. Devices that utilize USB connections include keyboards, flash drives, cameras, and more.
FireWire cards	A FireWire card provides the interface necessary for the computer to recognize and interact with all devices that connect to the computer via a FireWire connection. FireWire is mainly used for high-speed data transfer. Devices that use FireWire connections include external hard drives, video and audio recording devices, and more.
Thunderbolt cards	A Thunderbolt expansion card can be added to systems whose motherboard has a Thunderbolt header. The header needs to match the version of Thunderbolt the card uses. After installing a Thunderbolt card, you can daisy chain up to 9 devices from the port on the card.
Storage cards	A storage card provides the interface for the computer to recognize and interact with a storage device such as a disk. Systems with multiple disk drives, especially of different types, may require multiple storage cards to manage the communication between the disks and the system board.
Modem cards	A modem card provides the interface necessary for remote communications over phone or data lines that have been provided by a cable or Internet service provider.

<b>Expansion Card Type</b>	<b>Description</b>
Wireless/cellular cards	A wireless or cellular card provides the interface necessary for remote communications, such as Internet over mobile phone or wireless data lines such as Wi-Fi, 3G, or 4G Internet that have been provided by a cellular service provider.
TV tuner cards	A TV tuner card provides the interface necessary for the computer to receive television signals and display the output on a display device.
Video capture cards	A video capture card provides the interface necessary for the computer to input video feeds, including digital video, and interact with the software necessary to process and edit video.
Riser cards	A riser card provides the interface necessary for adding expansion cards to a system board while saving space within the system case. A riser card allows the cards to stack horizontally rather than vertically within the system.

## Expansion Card Configuration

Once the expansion card is installed, there are a number of means for configuring it. Depending on the type and manufacturer, you may need to use one or a combination of these methods.

<b>Configuration Method</b>	<b>Description</b>
PnP installation	If the expansion card, the device, the BIOS, and the operating system are all PnP compatible, the expansion card will be automatically configured and the system will automatically assign resources to the card when the system starts.  You can use the <b>Add Hardware</b> wizard to install and configure PnP devices, although to install most unrecognized devices, you will typically just run a setup program provided by the manufacturer. When using the wizard, you should initially let Windows try to scan for new hardware (this is the default selection). If Windows cannot find the device, you can then choose the device from a list of devices offered by Windows and Windows will install the appropriate driver.
Manufacturer driver	If Windows does not automatically detect an expansion card, you can manually install a driver from the manufacturer.



**Note:** Read the installation instructions for the expansion card to determine if any software is required prior to the installation. Failure to do so could cause the installation to fail or the card and system to behave erratically.



**Note:** For additional information, check out the **LearnTO Install Expansion Cards** presentation in the LearnTOs for this course on your CHOICE Course screen.



Access the **Checklist** tile on your CHOICE Course screen for reference information and job aids on **How to Install and Configure Expansion Cards**.

# ACTIVITY 6–5

## Installing Expansion Cards

### Before You Begin

You have open expansion slots on the system board. You have been given one or more expansion card types and device drivers.

### Scenario

You have been asked to install several expansion cards on a user's system. The appropriate drivers for the cards are also available to you should you need them.

1. Open the system cover and access the slots.
  - a) Turn off the system power.
  - b) Unplug the computer from the electrical outlet.
  - c) Unplug peripherals from the system.
  - d) Remove the cover.
  - e) Determine if you need to move or remove any components in order to access the slots.

2. Insert the card in an available slot.



**Caution:** Some manufacturers require installing a driver prior to inserting the adapter card. It is therefore important to read the manufacturer's instructions before installing the card.

- a) Locate an open slot.
- b) Remove the slot cover.
- c) Firmly press the card into the slot.



**Caution:** Do not rock the card side to side when installing or removing it.

- d) Secure the card to the chassis with the screw from the slot cover. Normally, you would now secure the cover back on to the system, but because you will be doing more work inside the system, leave it off.

3. Configure the card for the computer.

- a) Reconnect the peripherals and cables that you disconnected in step 1.
- b) Power on the system.
- c) Install any required drivers.

4. Check whether the card is functioning properly.

- a) Connect any devices to the card that are required for testing the card functionality.
- b) Access or use the device connected to the card.
- c) In **Device Manager**, verify that the device's properties show that the device is working properly and that there are no conflicts, and then select **Cancel**.

## Summary

In this lesson, you installed and configured various types of peripheral computer components, including input and output devices and the expansion cards that may be necessary to connect them. As an IT professional, having the ability to successfully install and configure these components is an integral part of your daily work life, as you will be expected to set up workstations or assist users in installing anything that they may need to perform their job duties effectively.

**What types of peripheral components do you anticipate having to install and configure most often in your current job role?**

**Will there be any specialty input devices that you will need to install or configure at your workplace? How might this affect your day-to-day activities as an IT professional?**



**Note:** Check your CHOICE Course screen for opportunities to interact with your classmates, peers, and the larger CHOICE online community about the topics covered in this course or other topics you are interested in. From the Course screen you can also access available resources for a more continuous learning experience.

# 7

# Managing System Components

**Lesson Time:** 2 hours

## Lesson Objectives

In this lesson, you will manage system components. You will:

- Explain the importance of motherboard components, their purpose, and properties.
- Install various types of CPUs and apply the appropriate cooling methods.
- Install a power supply.
- Troubleshoot common problems related to motherboards, CPU, and power.

## Lesson Introduction

In the previous lesson, you worked with peripheral components such as display devices, input devices, expansion cards, and multimedia devices. As an A+ technician, you are not only responsible for the components outside the system unit, but all the internal components as well. On the job, you may be asked to connect peripheral components for a user, or you may be asked to swap out a motherboard.

A large part of your time as an A+ technician will be spent helping users to install and configure new software and hardware components. Having the knowledge and skills to properly install and configure the internal system components is crucial because, in most cases, users will not have the knowledge or the experience to install the components themselves. It will be your professional responsibility to know the technical specifications for these components and how to manage them appropriately.

# TOPIC A

## Identify Motherboard Components and Features

In this lesson, you will dive inside the computer system and take a closer look at the internal components that enable the computer to run successfully. In this topic, you will start by examining motherboards.

The most important system component in a computer system is the motherboard. Although you can argue a case for almost any system component as being most important, without the motherboard, the computer simply cannot run. As an A+ technician, you must be knowledgeable about motherboards and their purpose within the computer system.

### Motherboards

As you learned earlier in the course, a *motherboard* or *system board* is a circuit board that contains the basic electronic components that form the backbone of a PC.

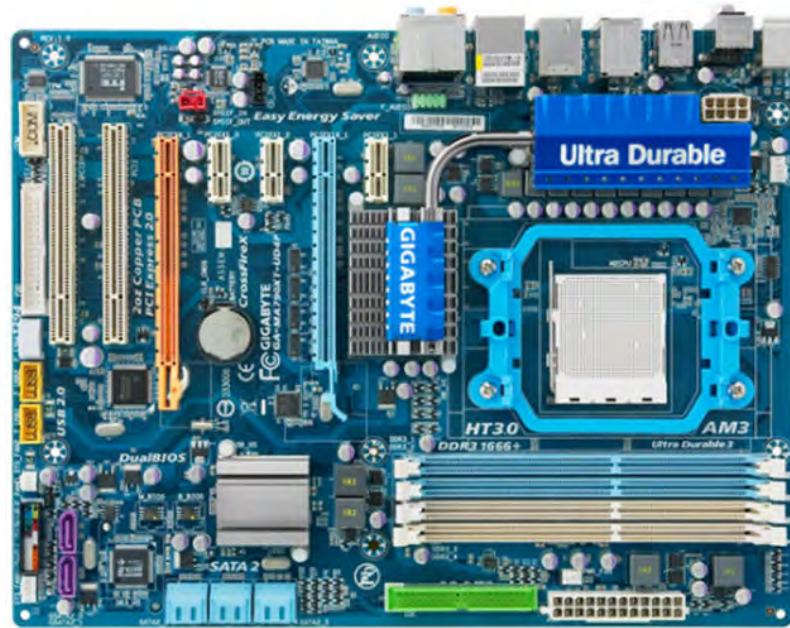


Figure 7-1: A motherboard.

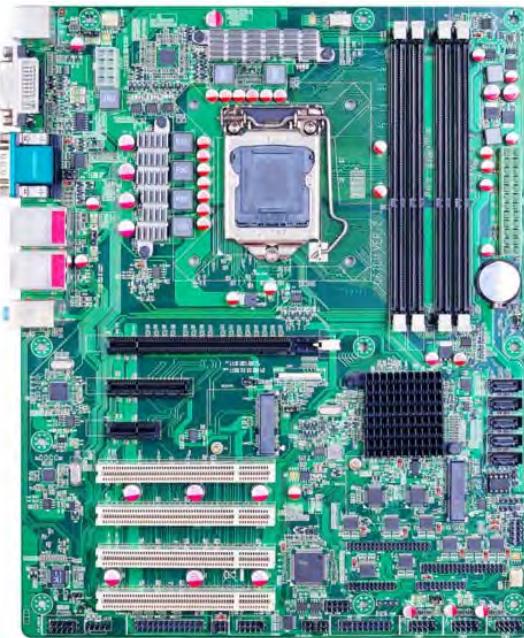
### Motherboard Sizes and Form Factors

Motherboards come in several different sizes. This is often referred to as the board's *form factor*. The form factor describes the size, shape, and configuration of the motherboard.

<b>Motherboard Form Factor</b>	<b>Description</b>
ATX	<p>Advanced Technology eXtended (ATX) boards are an older motherboard standard that was introduced by Intel® in 1995 to provide better I/O support, lower cost, easier use, and better processor support than even earlier form factors. ATX has undergone several revisions. Some of the features of the original ATX form factor are as follows:</p> <ul style="list-style-type: none"> <li>• Power supply with a single, keyed 20-pin connector called the P1 connector. The main power connector to the motherboard provided +3.3 volts (V), +5 V, +5 V, +12 V, and -12 V.</li> <li>• The central processing unit (CPU) is closer to the cooling fan on the power supply. Also, the cooling circulation blows air into the case instead of blowing air out of the case. (Later revisions had fans blowing air out of the case.)</li> <li>• You can access the entire motherboard without reaching around drives. This was accomplished by rotating the board 90 degrees.</li> <li>• This board cannot be used in Baby AT or LPX cases.</li> <li>• This board is typically described as having a maximum size of 12 inches by 9.6 inches or 12 inches by 10 inches, but the actual item dimensions can vary, as long as the mounting holes are in the specified locations.</li> </ul>



<b>Motherboard Form Factor</b>	<b>Description</b>
<i>Mini-ATX</i>	The mini-ATX board has a maximum size of 11.2 inches by 8.2 inches. The main difference between the mini board and the full-size ATX board is its smaller size. For example, it uses the same power supply form factor and case mounting holes as the full-size board.



<b>Motherboard Form Factor</b>	<b>Description</b>
<i>microATX</i>	The microATX board, introduced in late 1997, is often written as µATX, and has a maximum size of 9.6 inches by 9.6 inches. MicroATX boards with integrated graphics are often used by system board manufacturers as a basis for small form factor and home entertainment PCs. MicroATX boards are backward compatible with the full size ATX boards and often use the same chipsets, so they can usually use the same components. However, because the cases are generally smaller, there are fewer I/O ports available than in ATX systems, so it might be necessary to use external USB hard drives, CD burners, and so forth.



<b>Motherboard Form Factor</b>	<b>Description</b>
ITX and <i>mini-ITX</i>	<p>ITX, also known as Embedded Platform Innovative Architecture (EPIA), is a small motherboard originally designed for industrial applications. They are also used in firewalls, home theater PCs, and embedded car computers. The mini-ITX and Pico-ITX motherboards are the most popular versions of ITX motherboards.</p> <p>The mini-ITX motherboards are small, compact boards that fit the same form factor as the ATX and the micro-ATX boards. They have a maximum size of 6.7 inches by 6.7 inches. ITX boards were developed by a company named VIA technologies in 2001 to provide a compact board that does not drain system power. The boards are unique in that they are uniquely designed to consume less power while providing adequate processing power. Because of this, the board itself does not demand excessive cooling components. Due to their small size and low power consumption, the boards can be implemented in a number of cases and electronics and are popular among the industries that purchase motherboards in bulk to be incorporated into a number of different products.</p>



## ATX Power Revisions

ATX has undergone several revisions. The following table highlights the power revisions included in the various versions of the specifications.

<b>ATX Version</b>	<b>Description</b>
ATX 1.0	20-pin P1 motherboard power connector.
ATX 12V 1.0 to 1.3	<ul style="list-style-type: none"> <li>An extra 4-pin, 12V connector, commonly called the P4 connector, was first needed to support the Pentium 4 processor.</li> <li>Added a supplemental 6-pin AUX connector, which provided additional 3.3V and 5V supplies to the motherboard if needed.</li> <li>Increased power on the 12V rail.</li> <li>Both connectors were of Molex Mini-fit Jr. type.</li> </ul>
ATX 12V 1.2	-5V rail no longer required (optional).
ATX 12V 1.3	<ul style="list-style-type: none"> <li>Introduction of Serial ATA power connector (defined as optional).</li> <li>-5V rail prohibited.</li> </ul>

ATX Version	Description
ATX 12V 2.x	<ul style="list-style-type: none"> <li>24-pin P1 connector. The additional pins provide +12V, +5V, and +3.3V pins. This connector is backward compatible with the 20-pin connector.</li> <li>The 6-pin AUX connection was no longer necessary because the extra 3.3V and 5V circuits were incorporated in the 24-pin connector.</li> <li>The most power was provided on the 12V rails.</li> <li>Power on the 3.3V and 5V rails was reduced.</li> <li>The power supply was required to include a serial ATA power cable.</li> </ul>
ATX 12V 2.1	Added a 6-pin connector for PCI Express (PCIe) graphics cards that delivers 75 watts (W). PCIe version 1 defined the 6-pin connector. The connector can also be located on the motherboard.
ATX 12V 2.2	Added an 8-pin connector for PCIe graphics cards that delivers additional 150W. PCIe version 2 defined the 8-pin connector. The connector can also be located on the motherboard.
ATX 12V 2.3	Included efficiency recommendations to align with Energy Star 4.0 mandates.



**Note:** For processor voltage regulators that have been designed for 12V input, an additional 12V power connector was added. ATX power supplies with the 12V connector are designated as ATX 12V.

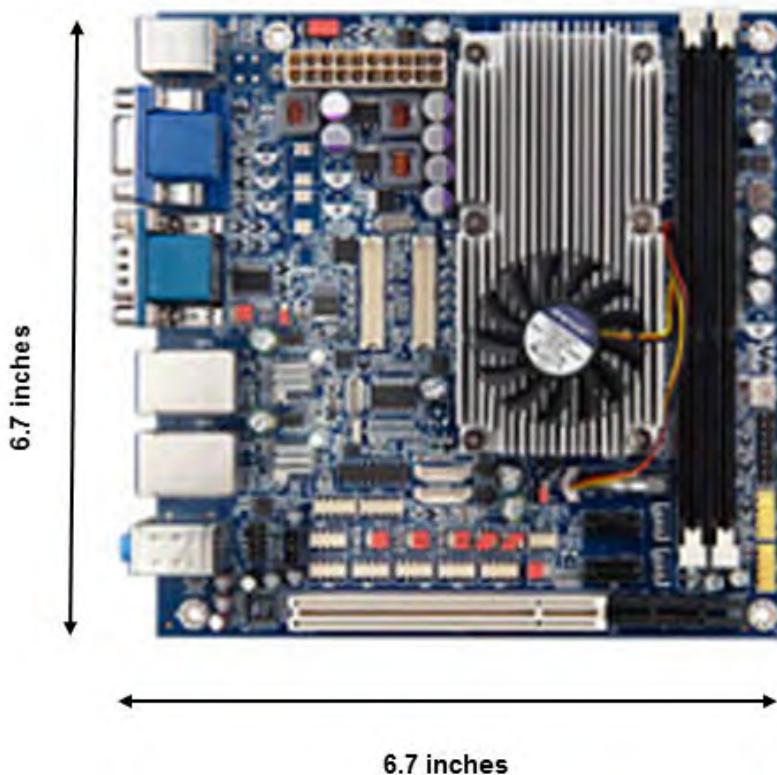
## ACTIVITY 7–1

### Identifying Motherboards

#### Scenario

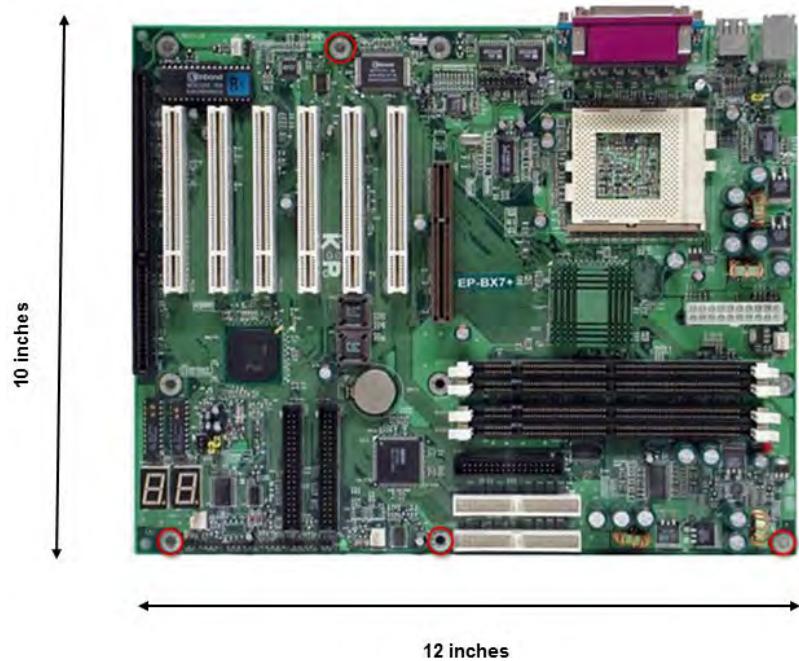
In this activity, you will analyze and identify some of the more common motherboards in use today.

1. Examine the graphic and answer the following question.



What type of motherboard is displayed here, and what characteristics did you use to help you identify the board type?

2. Examine the graphic and answer the following question.



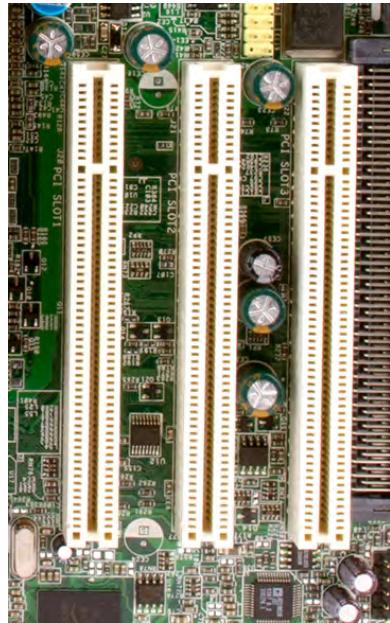
What type of motherboard is displayed here, and what characteristics did you use to help you identify the board type?

3. Take the case off the PC you are using for this course to identify the type of motherboard installed in the PC. Use the descriptions presented in this topic to help you.

## Expansion Slots

Expansion slots allow you to add expansion cards to your motherboard in order to extend the capabilities of a computer system. Motherboards generally include several of these slots so that the adapters can transfer data to and from the different computer components that have been installed in a system.

<b>Expansion Slot Type</b>	<b>Description</b>
PCI	<p>The <i>Peripheral Component Interconnect (PCI)</i> expansion slot is the most common expansion slot used on system motherboards. The specifications include:</p> <ul style="list-style-type: none"> <li>Physical characteristics of cards: operates at 33 or 66 MHz. Up to eight functions can be integrated on one board.</li> <li>A 32-bit PCI card that operates at 33 MHz has a throughput of 133 MBps.</li> <li>A 32-bit PCI card that operates at 66 MHz has a throughput of 266 MBps.</li> <li>A 64-bit PCI card that operates at 33 MHz has a throughput of 266 MBps.</li> <li>A 64-bit PCI card that operates at 66 MHz has a throughput of 533 MBps.</li> <li>Configuration: Supports up to five cards per bus and a system can have two PCI buses for a total of 10 devices per system. Can share interrupt requests (IRQs). Uses Plug and Play (PnP).</li> <li>Number of data lines: 64-bit bus often implemented as a 32-bit bus.</li> <li>Communication method: Local bus standard; 32-bit bus mastering. Each bus uses 10 loads. A load refers to the amount of power consumed by a device. The PCI chipset uses three loads, while integrated PCI controllers use one load. Controllers installed in a slot use 1.5 loads.</li> </ul>



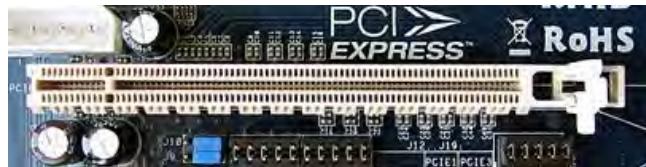
### **Expansion Slot Type Description**

PCI-X	<p>PCI-eXtended (PCI-X) is a motherboard expansion slot that improves upon some of the PCI expansion capabilities and is the latest version of PCI technology. PCI-X uses a parallel interconnect along a 64-bit bus shared with other PCI-X devices. The specifications include:</p> <ul style="list-style-type: none"> <li>Provides increased bandwidth and faster speeds by doubling the bus width from 32 bits to 64 bits.</li> <li>For PCI-X 1.0, the clock rate ranges from 66 megahertz (MHz) to 133 MHz, depending on the card. A 64-bit PCI-X card that operates at 66 MHz has a throughput of 533 MBps, whereas a card that operates at 133 MHz has a throughput of 1.06 GBps.</li> <li>PCI-X 2.0 clock rates are 266 MHz and 533 MHz. Cards that operate at 266 MHz have a throughput of 2.13 GBps due to double-data-rate technology, where data is transferred on the rising and falling edges of the clock cycle. Cards that operate at 533 MHz have a throughput of 4.26 GBps and use quad-data-rate technology.</li> <li>Commonly found in server machines to provide faster transfer rates required.</li> </ul>
-------	--



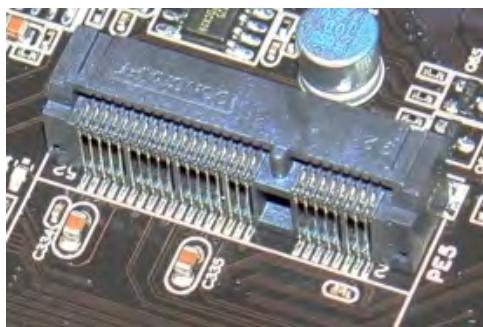
**Note:** Conventional PCI and PCI-X are sometimes called "parallel PCI" to distinguish them from PCI Express, which uses a serial, lane-based architecture.

<b>Expansion Slot Type</b>	<b>Description</b>
PCIe	<p><i>PCI Express (PCIe)</i> uses a different architectural design than PCI and PCI-X and is not backward compatible with either one. PCIe provides full-duplex, high speed communication. PCIe is based on the concept of “lanes.” Lanes can be grouped to increase bandwidth, so when two devices use eight lanes for their connection, it’s an x8 connection. Each device uses two lanes, one to transmit and one to receive (full duplex).</p> <p>PCI and PCI-X use a 32-bit or 64-bit parallel bus, and PCIe uses a serial bus, which is faster than a parallel bus.</p> <p>There are four versions of the PCIe standard—1.x, 2.x, 3.x, and 4.x. PCIe 1.0 and 2.0 use the 8b/10b encoding system (which is the same encoding used by Fast Ethernet for a 100 Mbps network throughput). PCIe version 3.x is the current standard, which will eventually be replaced by version 4.x.</p> <ul style="list-style-type: none"> <li>• Used for high-speed graphics cards and high-speed network cards.</li> <li>• Number of data lines: Each device has a serial connection consisting of one or more lanes. The data rate depends on the PCIe version.</li> <li>• PCIe version 1.x: Clock speed is 2.5 GHz, and each lane offers up to 250 MBps of throughput. An x16 slot (16 lanes) can handle 4 GBps of bandwidth in one direction.</li> <li>• PCIe version 2.x: Clock speed is 5 GHz, and each lane offers up to 500 MBps of throughput. An x16 slot (16 lanes) can handle 8 GBps of bandwidth in one direction.</li> <li>• PCIe version 3.x: Clock speed is 8 GHz, and each lane offers up to 1 GBps of throughput. An x16 slot (16 lanes) can handle 16 GBps of bandwidth in one direction.</li> <li>• PCIe version 4x: Specifications are not yet released, but the transfer rates are targeted to reach 16 gigatransfers per second (GT/s). An x16 slot (16 lanes) will be able to handle 64 GBps in one direction.</li> <li>• Communication method: Local serial interconnection.</li> </ul>



### **Expansion Slot Type Description**

MiniPCI	The PCI industry standard for desktop computer expansion cards applied to the small form factor for notebook expansion cards. Types of Mini PCI devices developed include Bluetooth, modems, Fast Ethernet, sound card, SATA controllers and so on. The cards are attached to the motherboard and are not accessible from the outside of the laptop. There are three card form factors available: <ul style="list-style-type: none"> <li>• Type I: Uses a 100-pin stacking connector</li> <li>• Type II: Uses a 100-pin stacking connector</li> <li>• Type III: Uses a 124-pin edge connector</li> </ul>
---------	--



Features include:

- Upgradeable; Mini PCI cards are removable and easy to upgrade to newer technologies.
- Flexibility: A single Mini PCI card interface can accommodate different types of communication devices.
- High Performance: uses 32-bit, 33MHz bus and support for bus mastering and DMA.
- 2 W maximum power consumption.
- Mini PCI cards can be used with PCI using a Mini PCI-to-PCI converter.

Mini PCI is an older technology; it has been superseded by PCI Express Mini Card.

## ACTIVITY 7–2

### Identifying Expansion Slots

#### Scenario

In this activity, you will examine and identify the expansion slots on your PC's motherboard.

- 
1. With the case removed from your PC, examine the expansion slots on your motherboard.
  2. Try to identify the different types of expansion slots.
- 

#### RAM Slots

RAM slots come in several form factors, and each module will connect to the system board through a RAM slot of a compatible type.

<b>RAM Form Factor</b>	<b>Description</b>
DIMM	Dual In-line Memory Modules (DIMMs) are found in many systems, and they have a 64-bit data path. The development of the DIMM solved the issue of having to install memory modules in matched pairs. DIMMs also have separate electrical contacts on each side of the module, whereas the contacts on older RAM on both sides are redundant. DIMMs have a 168-pin connector, and they generally have 16 or 32 random access memory chips mounted on a small circuit board.
RIMM	Rambus Inline Memory Modules (RIMMs) have a metal cover that acts as a heat sink. Although they have the same number of pins, RIMMs have different pin settings and are not interchangeable with DIMMs. RIMMs can be installed only in RIMM slots on a system board.

## ACTIVITY 7–3

### Identifying RAM Slots

#### Scenario

In this activity, you will examine and identify the RAM slots on your PC's motherboard.

1. With the case removed from your PC, examine the available RAM slots on your motherboard.
2. How many RAM slots are on your motherboard? Are they all being used?

#### Chipsets

The *chipset* is the collection of chips and integrated circuits that support basic functions of the computer. PC chipsets are housed on one to four chips and include built-in controllers for the system board's buses and all the integrated peripherals.



Figure 7–2: A motherboard with a single-chip chipset.

The chipset architecture, including the number, function, name, and placement of the various chips in a chipset, will vary depending on the type and manufacturer of the system board. For example, on many Intel Pentium computers, the two main chips in the chipset are known as the Northbridge and the Southbridge.

- The *Northbridge* controls the system memory and the AGP video ports, and it may also control cache memory. The Northbridge is closer to the processor and communicates directly with it using a 64-bit front side bus.
- The *Southbridge* controls input/output functions, the system clock, drives and buses, advanced power management (APM), and various other devices. The Southbridge is further from the CPU and uses the *PCI bus* to communicate with the Northbridge.

Newer Intel systems employ the Intel Hub Architecture (IHA) chipset. This also has two main chips, now named the Graphics and AGP Memory Controller Hub (GMCH) and the I/O Controller Hub (ICH), which perform functions roughly analogous to the Northbridge and Southbridge, but the communication between the two new chips is designed to be faster.

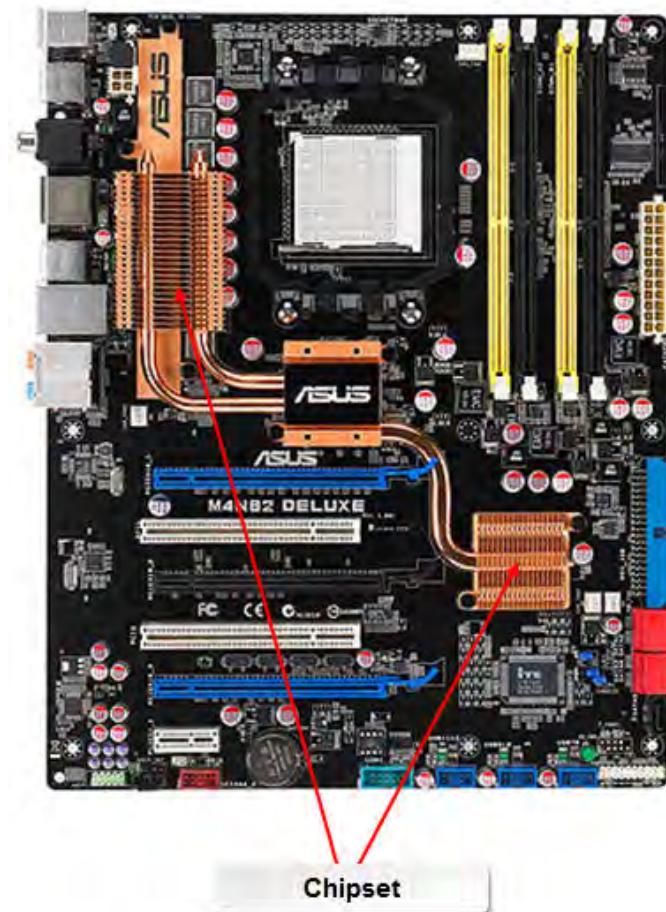


Figure 7-3: A multichip chipset on a system board.

## CPU Sockets

CPUs use either sockets or slots to connect to the motherboard. Older slot-based processors plugged into a system board in much the same way as an expansion board, whereas socketed processors plug into a system board using a pin grid array (PGA). Modern CPUs usually fall into either the AMD or Intel category. Although there are other CPU manufacturer brands available, Intel and AMD technologies tend to dominate in the marketplace.

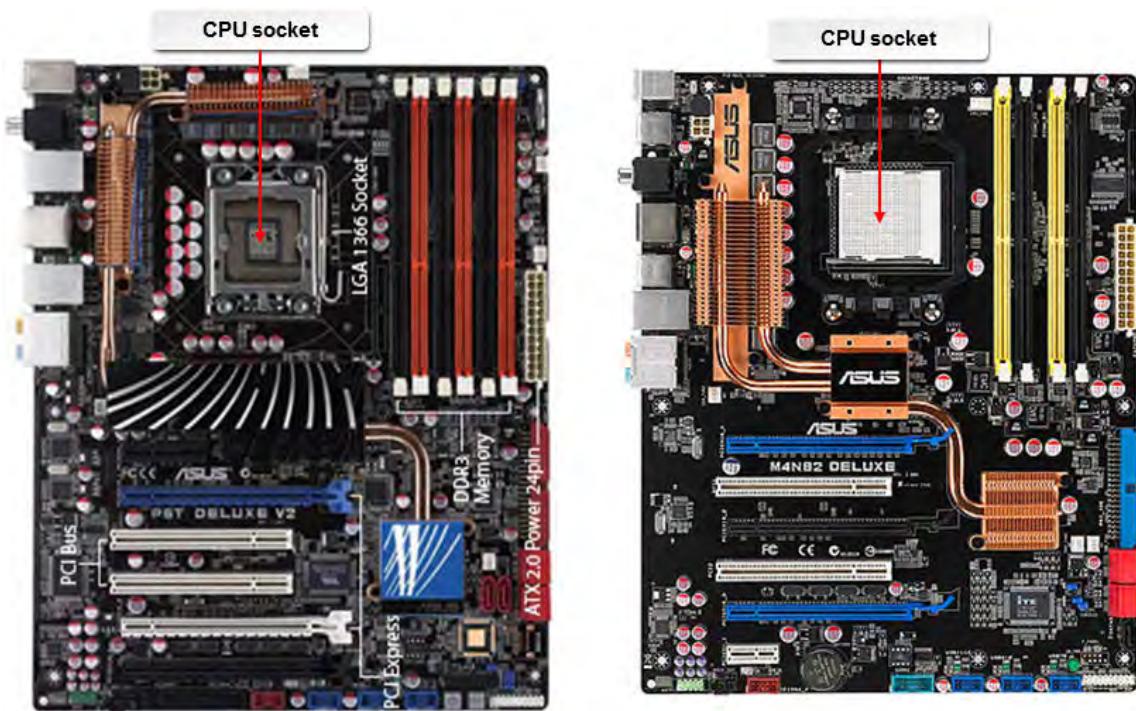


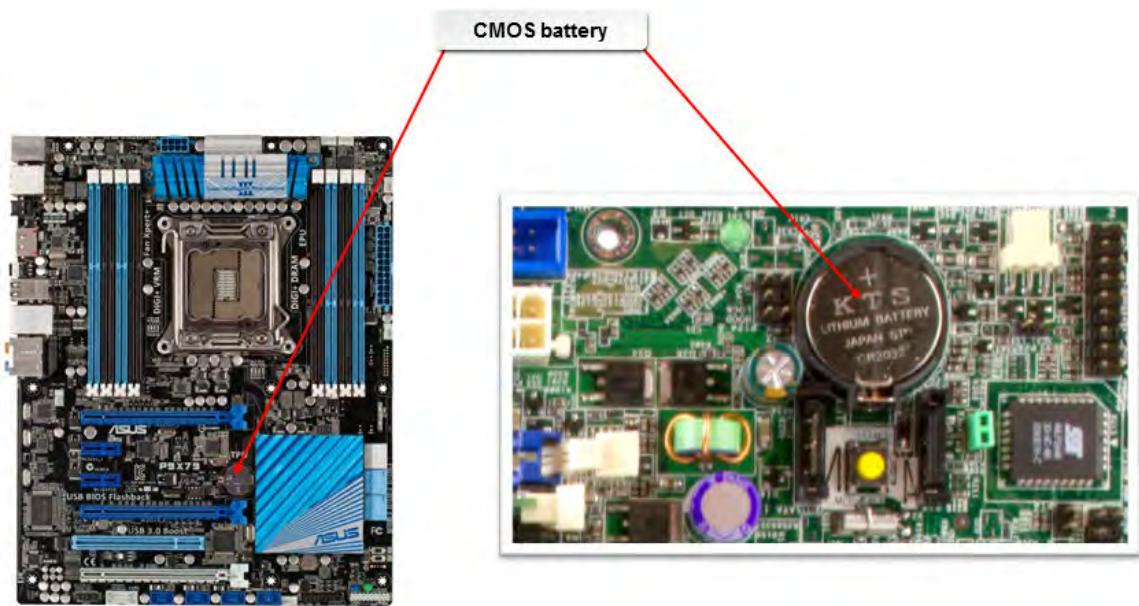
Figure 7-4: CPU sockets.

## Bus Speeds

The motherboard bus speed determines how fast circuits will carry data simultaneously from one area of the motherboard to another. Speed can vary based on the capacity of the specific bus. The bus speed will depend on what components are installed in the computer.

## CMOS Batteries

The *complementary metal-oxide-semiconductor (CMOS)* battery is a small battery on the motherboard that provides power to the real-time system clock when the computer is turned off. You may find cases when the CMOS battery fails, which will result in a CMOS Battery Failure message (or possibly a CMOS Read Error). Replacing a CMOS battery is not difficult, but it is not always necessary. Start by leaving the computer on for a day, and see if this helps the battery recharge. If this does not work, and you need to replace the battery, immediately write down all of your CMOS settings, as you will need to re-enter them later after replacing the battery. Note that not all motherboards can have their CMOS batteries replaced; in these cases you can add a new CMOS battery, but not remove the old one. Consult the documentation for your motherboard.



**Figure 7-5: CMOS batteries.**

## CMOS Settings

CMOS settings can be changed if needed in the system setup program that is loaded from the system firmware setup utility. The CMOS battery supports the BIOS or UEFI utility by providing enough power to save critical system settings.

<b>CMOS Setup Setting Description</b>	
System date and time	You can set the system's real-time clock using DOS date and time commands, or by setting the clock in Windows, which will adjust the real-time clock.
Password	You can specify whether a user or administrator password is required to start up the system.
Boot sequence	You can specify the order that Power-On Self Test (POST) checks drives for an operating system.
Memory	Some systems require you to specify in CMOS how much RAM is installed on the system. You might also be able to specify whether the system uses parity memory or non-parity memory. Most modern systems automatically detect and report the installed RAM.
Hard drive	You can specify the number, type, and size of the hard drives attached to the system.
Display	You can specify the monitor type and port.
Power management	In most modern computers, you can specify settings such as powering down components (such as the monitor, video card, and hard drives) when the components have not been used for a specified time period, as well as options and time limits for <i>standby</i> and suspend modes. You can also disable or enable global power management.

## Power Connections

Every component in a PC requires electrical power, and most components get that power from the PC's power supply. Because all of the components, including the power supply, are connected to the motherboard, you will find several different power connectors on a typical motherboard.

- Main power connector (24 pins)
- CPU power connector (4/8-pin 12V). Lower-end boards supporting CPUs with lower thermal design power (TDP) will likely have a four-pin connector, and boards that support higher-end processors will have an eight-pin connector.
- CPU fan connector (3 or 4 pins). Three-wire connectors are typically used for small chassis fans with low power consumption. The four-wire connectors are for processor fans with higher consumption. Four-pin connectors can control fan speed via pulse width modulation (PWM).
- Legacy ATA ATX P4 or 4-pin connector.
- SATA power connector. SATA power connectors have 15-pins. A difference between a SATA power connector and the four-pin connector is a pin that provides 3.3V of power. Some SATA drives have specific power requirements. SATA drives don't always include a SATA power connector. In that instance, you can attach the legacy ATA four-pin power connector to the drive. However, do not connect a four-pin power connector and a SATA power connector to the drive. This will likely cause the drive to malfunction.
- PCIe 6/8-pin.

## Fan Connectors

There are several uses for fans within a computer. The components installed and how much heat they produce will determine what type of fans you should install. Full-size desktop systems will generally have a case fan that will pull the hot air out, letting cooler air circulate through the chassis. There is no current standard that dictates the size and form factor of the fan connector. Common connectors include:

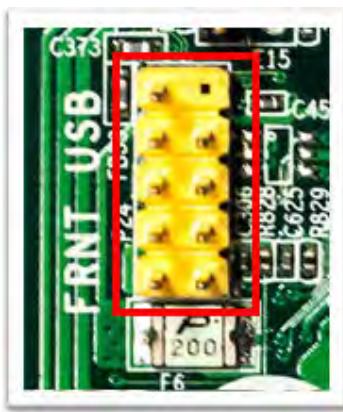
- A 3-pin Molex KK connector, commonly used to connect a fan directly to the motherboard.
- A 4-pin Molex KK connector that is similar in function to the 3-pin KK connector, except that it has an extra pin to provide the ability to control the speed of the fan.
- A 4-pin Molex connector that connects directly to the system's power supply.

In some systems, the system firmware monitors the fan speed. In order for this to happen, the power supply requires an external fan connector that is attached to the motherboard. The fan does not draw power from the connector; it only is used to provide information to the system firmware. Based on the information received, the system can increase the fan speed for improved cooling or decrease the fan speed when less cooling is needed so that the system operates more quietly.

## Front and Top Panel Connectors

Many different components connect to the motherboard. It is important to understand where each component is supposed to be attached. Always check the manufacturer's information for your motherboard before you disconnect or reconnect a component to the pins on the various panels of the board.

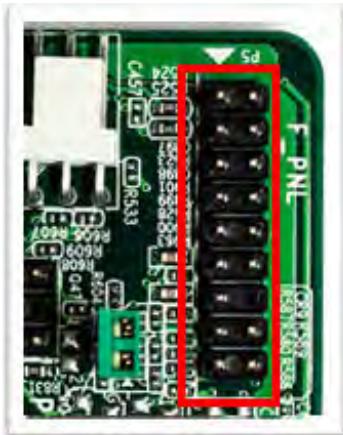
<b>Motherboard Headers</b>	<b>Description</b>
USB header	The USB header contains the pins that the USB cable connects to. This connects the USB drive installed in the computer case directly to the motherboard. USB headers will have one pin missing from the second row on the end. This can be a visual guide when identifying the different headers.



Front panel header

The front panel header of the motherboard contains many system connection pins that are used to connect components installed in the computer case to the motherboard. Most front and top panel headers will include:

- Power switch
- Power light emitting diode (LED)
- Reset switch
- Hard drive LED
- Speaker



Motherboard Headers	Description
Audio header	The audio header contains the pins to connect the system audio cable to the motherboard.



## ACTIVITY 7–4

### Identifying Motherboard Components

#### Scenario

In this activity, you will examine various motherboard components.

---

1. Locate and identify various components on the motherboard of your PC.
    - a) On the motherboard, identify the chipset. How is it configured? Can you see the Northbridge and Southbridge chips? Or does this computer have the newer GMCH/ICH chipset?
    - b) Try to find the CMOS battery on the motherboard.
  2. Identify fan and power connectors.
    - a) Locate the power supply within your PC.
    - b) Trace the connections from the power supply to the motherboard and identify the type of connections made.
    - c) Check for any fans installed within the PC. Locate the case fan and see how it is connected to the motherboard. Also check for any fans connected directly to the motherboard, and identify where the connections are made.
  3. Identify the front and top panel connectors.
    - a) On the motherboard, try to identify the USB headers.
    - b) Identify the front panel header.
    - c) Identify the audio header.
-

# TOPIC B

## Install and Configure CPUs and Cooling Systems

In the last topic, you identified the various types of motherboards used in computer systems. Now that you understand the purpose of the motherboard, you can take a closer look at the components that make up the board. Two of these components are the central processing unit, or CPU, and the cooling systems that service it. In this topic, you will examine CPUs and cooling systems.

Much like the motherboard, the CPU is another important component of the computer system that actually carries out all the tasks requested by the applications installed in the computer. The CPU is a heat generator, so part of understanding the CPU includes understanding how to manage heat inside the computer case by managing the airflow and temperature. Keeping the system cool is an easy but important way to maintain or even increase its productivity. A computer that runs too hot risks damaging its own components. As an A+ technician, you need to be familiar with these essential components of the computer system.

### Intel CPU Socket Types

Although you may encounter older socket types on the job, most computers will use more recent socket types and processors. Common Intel CPU sockets include the following.

<b>Socket Type</b>	<b>Description</b>
LGA 775	<p>The land grid array (LGA) 775 CPU is also referred to as Socket T.</p> <ul style="list-style-type: none"> <li>Supports Intel CPUs from 1.8 to 3.8 GHz with front-side bus frequencies ranging from 533 MHz to 1600 MHz.</li> <li>Uses 775 copper pins with no socket holes to attach to the motherboard's pins. The CPU is connected via a load plate that the CPU attaches to and is lowered onto the board by the load lever.</li> <li>Has 775 contacts in a 33x30 grid array with a 15x14 grid depopulation in the center of the array, and with one corner contact and four contacts on two sides of the socket removed.</li> <li>Base metal for the contacts is high strength copper alloy, and the areas on the socket contacts that mate with the processor are gold-plated.</li> <li>Proper cooling is accomplished by the design of the CPU connection to the motherboard. By using the load plate to connect, the CPU is properly seated into place and is perfectly level. This ensures that the CPU is making full contact with the heat sink or liquid cooling method.</li> <li>Commonly used in consumer desktop computers.</li> <li>Used for Pentium 4, Celeron D, Pentium Extreme Edition, Core 2 Duo, Core 2 Extreme, and Core2Quad processors.</li> </ul>

<b>Socket Type</b>	<b>Description</b>
LGA 1156	<p>The LGA 1156 is also referred to as Socket H or H1.</p> <ul style="list-style-type: none"> <li>• Works with processors with frequencies from 1.86 to 3.46 GHz.</li> <li>• Uses 1,156 copper pins to attach to the processor pads on the motherboard.</li> <li>• Has 1,156 contacts arranged as a 40x40 grid of contacts with a 24x16 section de-populated, and with 60 land contacts removed mainly from the socket corners and socket edges.</li> <li>• Uses the Independent Loading Mechanism (ILM) to keep the processor in place and distribute even force across all socket contacts.</li> <li>• Commonly used in consumer desktop computers.</li> <li>• Designed to replace the LGA 775 socket type.</li> <li>• Used for Core i3, Core i5, Core i7, 3400 series Xeon, dual-core Celeron, and dual-core Pentium processors.</li> </ul>
LGA 1155	<p>The LGA 1155 is also referred to as Socket H2.</p> <ul style="list-style-type: none"> <li>• Uses 1,155 copper pins to attach to the processor pads on the motherboard.</li> <li>• Contacts arranged in two opposing L-shaped patterns within the grid array. The grid array is 40x40 with a 24x16 grid depopulation in the center of the array.</li> <li>• Base material for the contacts is high strength copper alloy and with minimum gold plating where process lands meet.</li> <li>• Designed to replace the LGA 1156 socket type.</li> <li>• Used for Intel's Sandy Bridge and Ivy Bridge microprocessors.</li> <li>• Used for Core i3, Core i5, Core i7, Xeon, Celeron, and Pentium processors.</li> </ul>
LGA 1150	<p>The LGA 1150 is also referred to as Socket H3.</p> <ul style="list-style-type: none"> <li>• Supports Haswell and Broadwell-based processors with 2 or 4 CPU cores.</li> <li>• Uses 1,150 copper pins to attach to the processor pads on the motherboard.</li> <li>• Has 1,150 contacts arranged as a 40x40 grid with a 24x16 section depopulated in the center as well as areas from the socket corners and edges.</li> <li>• Designed to replace LGA 1155 socket type.</li> <li>• Backwards compatible with LGA 1155 and 1156 cooling systems.</li> </ul>
LGA 1366	<p>The LGA 1366 is also referred to as Socket B.</p> <ul style="list-style-type: none"> <li>• Uses 1,366 copper pins that connect to the bottom of the processor.</li> <li>• Has 1,366 contacts arranged as a grid of 43x41 contacts with a 21x17 section de-populated in the center, and with 40 contacts in the socket corners and socket edges removed.</li> <li>• Commonly used in higher-end desktop systems that require high performance.</li> <li>• Used for Intel's Core i7 processor.</li> </ul>

<b>Socket Type</b>	<b>Description</b>
LGA 2011	<p>The LGA 2011 is also referred to as Socket R, and was designed to replace LGA 1366.</p> <ul style="list-style-type: none"> <li>• Uses 2,011 copper pins that connect to the bottom of the processor.</li> <li>• Commonly used in higher-end desktop computers and servers.</li> <li>• Used for Intel's Sandy Bridge and Ivy Bridge microprocessors.</li> </ul>

## AMD CPU Socket Types

Similarly to the Intel socket types, there will be, on occasion, an older socket and processor used, but in more cases, you will be supporting computers that contain newer-model AMD sockets and processors.

<b>Socket Type</b>	<b>Description</b>
AM3	The AM3 was designed to replace AM2+. The socket is not compatible with the previous versions AM2 and AM2+ because of the pin layout being slightly different than the older models. The AM3 has 941 pins, while the AM2+ has 940.
AM3+	The AM3+, also referred to as AM3b, is designed to be more efficient and use less power.
FM1	FMI is AMD's next generation socket type that is designed to be used with the Fusion and Athlon II processors.
FM2	FM2 works with Athlon X2 and X4 processors. It has 904 pins.
FM2+	FM2+ is not compatible with FM2 motherboards. It has 906 pins.

## CPU Characteristics

There are many different characteristics and technologies that can affect a CPU's performance.

<b>CPU Characteristic or Technology</b>	<b>Description</b>
Architecture	<p>The CPU architecture is a description of the width of its front-side bus. A CPU's front-side bus width is either 32 or 64 bits.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <p><b>Note:</b> Starting in 2008, the Intel front-side bus has been replaced with the QuickPath Interconnect (QPI) communication path. QPI is a high speed, packetized, point-to-point interconnect that offers higher bandwidth with low latency compared to wide front-side buses.</p> </div>
Clock speed	<p>The number of processing cycles that a microprocessor can perform in a given second. Some CPUs require several cycles to assemble and perform a single instruction, whereas others require fewer cycles. The clock speed is a technical rating; actual performance speeds can vary from the published clock speed rating. The clock speed is typically referred to as the processor performance.</p>

<b>CPU Characteristic or Technology</b>	<b>Description</b>
Overclocking	Overclocking is configuring your CPU to run at a speed greater than it is rated to handle. Overclocking can be performed on an unlocked processor by adjusting the multiplier of the processor core in the BIOS. Intel, for example, allows you to enable overclocking on some of its processors so you can tune the system for maximum performance. However, in general, overclocking can create problems when pushing a processor beyond frequency tolerances. Overclocking problems include causing the CPU to overheat, to produce random results, or to be damaged or destroyed.
CPU speed	CPU speed is an umbrella term for the overall rate at which instructions are processed. There are two factors that affect the CPU speed. One is the core clock speed, which is the internal speed at which instructions are processed within the CPU. The other is the bus clock speed, which is the actual speed at which instructions are transferred to the system board.
Throttling	Used to adjust CPU speed. A CPU throttle is typically used to slow down the machine during idle times to conserve the battery or to keep the system running at a lower performance level when hardware problems have been encountered.
Hyperthreading (HT)	A feature of certain Intel chips that makes one physical CPU appear as two logical CPUs. It uses additional registers to overlap two instruction streams to increase the CPU's performance by about 30 percent.
Integrated GPU	The graphics processing unit (GPU) is integrated within the die of the CPU to provide an alternative to having a dedicated graphics card.
Virtualization support	Most modern CPUs are virtualization compatible, meaning that they have virtualization software built into the chipset of the CPU. Both Intel and AMD have CPU virtualization built into their chips. This allows the CPU to process instructions from multiple operating systems quickly and efficiently.
Cores	CPU cores read and execute instruction data sent from computer applications. Two or more individual cores can process the workload more efficiently than a single core. A single chip that contains two or more distinct CPU cores that process simultaneously is called a multicore. Options include dual-core (two CPUs), triple-core (three CPUs), and quad-core (four CPUs), though hexa- and octo-core chips are becoming more common. Once you start combining tens or hundreds of cores, the terminology changes from "multicore" and becomes "many-core."
Cache	Dedicated high-speed memory for storing recently used instructions and data.
VRM	A voltage regulator module (VRM) is a replaceable module used to regulate the voltage fed to the CPU.
MMX	Multimedia Extensions (MMX) is a set of additional instructions, called microcode, to support sound, video, and graphics multimedia functions.

<b>CPU Characteristic or Technology</b>	<b>Description</b>
Execute Disable bit (EDB)	The EDB is a hardware-based security feature. It allows the processor to classify and separate memory areas where application code can and cannot execute. Malware programs and worms, when treated as trustworthy data, can exploit and overrun a memory buffer, and the computer may interpret the extra bits as instructions and execute them. The action could range from damaging files to disclosing confidential information and creating an access point. Intel refers to this as the XD bit and AMD refers to it as Enhanced Virus Protection. The operating system must support the NX (no-execute) bit to use this security feature.

## 32-Bit vs. 64-Bit

A 32-bit operating system supports applications that use data units up to 32 bits wide, but no larger. A 64-bit operating system can support applications that use data units up to 64 bits wide, making 64-bit operating systems backwards-compatible (in other words, they are able to support 32-bit programs). A 64-bit operating system requires a 64-bit processor and 64-bit software. A 64-bit processor uses memory more efficiently; since it can use more memory, it can increase the use of RAM and decrease the amount of time spent using the hard disk. A 32-bit processor cannot use more than 4 GB of physical memory, while 64-bit registers (which store memory addresses) can address up to 16 terabytes (TB) of physical memory. Except for Windows 7 Starter, all other versions of Windows come in both 32-bit and 64-bit versions.

## x86 and x64

x86 is the most common and successful instruction set architecture, which supports 32-bit processors. If something is referred to as x86, it supports 32-bit software, and it *might* support 64-bit software. To clarify things, the term "x86-64" (also written as "x64") explicitly refers to a 64-bit x86 architecture.

## Multi-CPU Motherboards

Prior to the development of multicore processors, some hardware manufacturers offered additional processing power by designing motherboards that could hold more than one CPU. With the advent of the multicore processors, these are less common in PCs, but they are still widely used in servers.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Install and Configure CPUs.

# ACTIVITY 7–5

## Planning for a CPU Upgrade

### Before You Begin

You will need a working computer with an Internet connection for this activity, or a hardcopy catalog that contains CPUs.

### Scenario

A user has asked you to upgrade the CPU in her PC. You need to make sure that the CPU you are installing will perform better than the one currently installed, and that it will work with the existing motherboard and other components.

1. Determine which CPU is currently installed in the PC.
  - a) Locate the CPU on the motherboard.
  - b) Look for any markings that indicate which CPU is currently installed.
  - c) Open the **System Information** window on your PC.
  - d) Record the information under **System** next to **Processor**.
  
2. Determine which CPUs would provide better performance in the PC.
  - a) Using the Internet or a hardcopy catalog, locate CPUs that are compatible with the PC.
  - b) If available, review installation instructions for the replacement CPU.

### CPU Cooling Methods

Having the right cooling method can be crucial to reach the optimal performance of a PC's CPU. Many cooling systems will be directly attached to the CPU.

<i>Cooling System</i>	<i>Description</i>
Fans	Computer fans provide cooling by simply blowing regular air across heated components. It is common to see case fans, power supply fans, adapter card fans, and CPU fans.
Vents	Computer cases are designed with vents to facilitate airflow through the case and across all components. A common implementation is to include air vents near the bottom of the front of the case and to place a fan near the top of the rear of the case to pull cooler air through the system.
Heat sinks	A heat sink is designed to provide direct cooling to a system's CPU. Modern CPUs have enormous processing power that requires instant cooling that is attached right to the CPU itself. Heat sinks have metal fins to increase their surface area to aid in heat dissipation. Cool air is blown past it by a fan, removing the heat from the processor.
<i>Thermal paste</i>	Thermal paste is used to connect a heat sink to a CPU. At the microscopic level, when two solids touch, there are actually air gaps between them that act as insulation; the liquid thermally conductive compound gel fills these gaps to permit a more efficient transference of heat from the processor to the heat sink.

<b>Cooling System</b>	<b>Description</b>
Fanless/passive	A fanless CPU cooler passively transfers heat through convection to the area surrounding the CPU. This ensures that hot air can move out of the CPU chassis without the assistance of loud, dust-accumulating fans. The fanless cooler is therefore more silent and efficient than traditional heat sinks.
Liquid-based	<p>CPUs can also be kept cool using a device to circulate a liquid or liquefied gas, such as water or freon, past the CPU. Like an air conditioner, heat from the CPU is absorbed by the cooler liquid, and then the heated liquid is circulated away from the CPU so it can disperse the heat into the air outside the computer.</p> <p>Another benefit of liquid-based cooling is that it can be significantly quieter than fan-based cooling.</p> <p>Liquid cooling systems are not as prevalent as heat sinks in most desktop systems or low-end servers; however, you will probably encounter them if your organization has deployed computers with hexa-core or octa-core processors.</p>



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Install and Configure Cooling Systems.

## ACTIVITY 7–6

### Discussing Cooling Systems

#### Scenario

In this activity, you will discuss cooling systems.

---

1. When might you need more than one cooling system in a computer?
  2. When would liquid cooling systems be more appropriate than adding a fan?
  3. Locate all of the cooling methods used in your PC.
-

# TOPIC C

## Install Power Supplies

In the previous topic, you examined CPUs and cooling systems. The next logical step is to select and install a compatible power supply in the system unit. In this topic, you will take a closer look at the computer's power supply and its connections to the other system components.

The computer's power supply is the main source of power for all components installed within the system unit. Understanding the power requirements of all the components and the maximum power supplied is crucial in managing the overall computer system power needs. Whether you are upgrading or replacing faulty components, you need to effectively manage the capacity of the current power supply.

### Power Supply Specifications

Each component in a personal computer has different power requirements that are required from the power supply, or power supply unit (PSU). The specifications provided will help in determining the right levels of power supplied to all internal computer components.

<b>Specification</b>	<b>Description</b>
Size	<p>Hardware manufacturers across the globe strive to standardize the power supply unit specifications in terms of dimensions and layout to make computer users' lives simpler. This has resulted in a range of power supply unit types that are accepted worldwide. The key to replacing and installing a power supply is to make sure that the form factor matches the case and the motherboard it will connect to. Form factors available today are:</p> <ul style="list-style-type: none"> <li>• ATX, which can be used in ATX and NLX cases and with ATX and NLX motherboards. Dimensions are 150 mm x 140 mm x 86 mm. Found in desktops and towers. ATX power supplies do not have a pass-through outlet, but instead usually have a physical on-off switch.</li> <li>• Micro ATX is essentially the same form factor as ATX, only with fewer expansion slots, which reduces the power supplied to the motherboard, and physical size.</li> <li>• Proprietary, which includes motherboards that do not conform to standards. It is likely that these proprietary system boards will require nonstandard power supply form factors as well, although you might be able to use an ATX power supply.</li> <li>• The number of connectors (pins) is also an important form factor. For example, a 4-pin male connector will not work properly with a 24-pin female connector.</li> </ul>
Connector style	<p>There are generally three types of connectors used to connect different devices in a computer to the power supply:</p> <ul style="list-style-type: none"> <li>• Berg, a square-shaped connector used to supply power to floppy disk drives and some tape drives.</li> <li>• Molex, a round-shaped connector used to supply power to Parallel ATA drives, optical drives, and SCSI drives.</li> <li>• SATA, used to supply power to Serial ATA drives.</li> </ul>

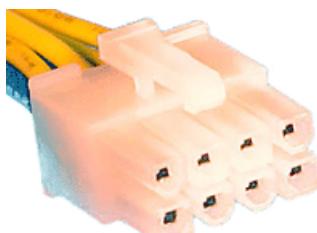
<b>Specification</b>	<b>Description</b>
Voltage	<p>All system components require specific voltages. You must verify that the power supply used can provide the volts demanded by the system.</p> <p>Some power supplies are dual-voltage. They can contain multiple channels that provide discrete voltages, with 5 V, 12 V, 15 V, and 24 V being the most common. These channels are often referred to as rails because although there are multiple wires carrying a specific voltage, they are normally tied to a single rail (or tap) in the PSU. Some PSUs are single rail, meaning that all of the wires carrying a discrete voltage tap into one rail, as described above. Others are dual rail, meaning that the wires carrying a discrete voltage are split into two channels.</p>
Wattage	<p>In order to calculate whether your power supply meets your power needs, you will need to add up the maximum power you might use at one time. A range of maximum power consumption for various components has been established. Most components use much less than the maximum, so by using the published requirements as a guide, you are overestimating the power usage, and therefore making it more likely that you never test the capacity of the power supply. You can check the documentation for the component to determine how much power it actually will use.</p>
	<p>Even some of the most powerful current CPUs only use 1.1 to 1.3 V. The necessary voltage for CPU and RAM is usually detected by the motherboard (system firmware) and configured appropriately, but sometimes you have to manually configure it by accessing the system firmware utility and entering the appropriate values. The power supply will supply 3.3 V for the CPU, RAM, and other devices, but the motherboard regulates how much they actually get. Most power supplies have a voltage selector switch that gives you the option to specify the input voltage to the power supply as 115 V (as used in the US) or as 230 V (as used in other countries).</p>
	<p>Power supply specifications are given in watts. Watts are volts times amps (voltage x current). Older systems typically had power supplies under 200 watts (W) and often even under 100 W. Newer power supplies typically have wattages ranging from 200 to 500 W. Because of their increased power demands, high-powered servers or computers designed for gaming can have power supplies with wattages from 500 W up to 1 kilowatt (kW).</p>



**Note:** Although most devices require specific voltages, some devices have different voltage requirements depending on use. This is particularly true of some memory chips, which vary in voltage requirements from 1.8 V to 3.3 V, and some can actually function at different voltages, or in a voltage range.

## Power Connector Types

One of the first things you will notice about a power supply is the cable that connects it to the components within a computer because there are so many different colored wires and connectors. Every device uses one of several types of connectors to connect to the computer's power supply.

<b>Connector Type</b>	<b>Description</b>
SATA	The 15-pin Serial Advanced Technology Attachment (SATA) connector connects peripheral components to the power supply and has a maximum wattage of 54. The SATA connector provides power at three voltages: <ul style="list-style-type: none"> <li>• +3.3</li> <li>• +5</li> <li>• +12</li> </ul>
	
Molex	Molex connectors are most commonly used to connect hard drives (4-pin) and power supplies (20/24-pin) to a motherboard. The voltage and color configuration of a 4-pin molex connector is as follows: <ul style="list-style-type: none"> <li>• +12 V (yellow)</li> <li>• Ground (black)</li> <li>• Ground (black)</li> <li>• +5 V (red)</li> </ul>
	
4/8-pin 12 V	The 4-pin and 8-pin connectors are similar in that they both provide 12 volts of power to the CPU on the motherboard. The 8-pin was designed to provide power to multiple CPUs in the system. The 4-pin has a maximum wattage of 192, and the 8-pin has a maximum wattage of 336.
	

<b>Connector Type</b>	<b>Description</b>
PCIe 6/8-pin	The Peripheral Component Interconnect Express (PCIe) 6-pin and 8-pin connectors provide power to PCIe slots on the motherboard. Both connectors provide power at 12 V. The 6-pin has a maximum wattage of 75, whereas the 8-pin has a maximum wattage of 150.
Main power connectors	 <p>The main power connector to the motherboard is either a 20-pin or 24-pin ATX connector. The 24-pin connector contains four additional pins to support the requirements for PCI Express slots on the motherboard. The 20-pin connector has a maximum wattage of 72, while the 24-pin has 144. Both connectors provide power at three voltages:</p> <ul style="list-style-type: none"> <li>• +3.3</li> <li>• +5</li> <li>• +12</li> </ul> 

## Power Supply Safety Recommendations

Power supplies can be very dangerous to work with. You should take careful security measures when working with power supplies.

<b>Safety Precaution</b>	<b>Explanation</b>
Check for certification	Be sure to purchase power supplies that are certified by the Underwriters Laboratories, Inc. (UL). UL standard #1950, the Standard for Safety of Information Technology Equipment, Including Electrical Business Equipment, Third Edition, regulates computer power supplies (along with other components). When it comes to electricity, you do not want to take a chance with a non-certified power supply. The risk of electrocution or fire from a malfunctioning power supply is simply not worth saving a few dollars by purchasing a low-quality power supply.
Replace instead of repair the power supply	You run the risk of electrocution if you open a power supply to attempt to repair it. Even when you unplug a computer, the power supply can retain dangerous voltage that you must discharge before servicing it. Because power supplies are relatively inexpensive, it is easier (and safer) to simply replace a failed power supply rather than attempting to repair it.
Keep the computer case on	Make sure that you run computers with their cases on. The fans inside power supplies are designed to draw air through the computer. When you remove the cover, these fans simply cool the power supplies and not the computer's components. Leaving the case open puts the computer at risk of overheating.
Protect the power supply	Use a power protection system such as an uninterruptible power supply (UPS) or surge suppressor to protect each computer's power supply (and thus the computer) from power failures, brownouts, surges, and spikes. You should also make sure that the computer's power cord is plugged into a properly grounded electrical outlet. (Three-pronged outlets include grounding; never use an adapter to plug a computer's power cord into a two-pronged electrical outlet.) You can buy a socket tester (available at hardware stores) to test your outlets if you suspect that they are not properly grounded.

	<p><b>Note:</b> You should also make sure to cover empty slots in the system board with filler brackets. If you do not install a filler bracket, you reduce the efficiency of the power supply's fan and increase the chances of the computer overheating.</p>
	<p><b>Note:</b> For additional information, check out the LearnTO <b>Install a Power Supply</b> presentation in the LearnTOs for this course on your CHOICE Course screen.</p>
	<p>Access the <b>Checklist</b> tile on your CHOICE Course screen for reference information and job aids on How to Install Power Supplies.</p>

# ACTIVITY 7–7

## Calculating Power Requirements

### Scenario

In this activity, you will calculate the power required by the computer you are using for this course. As a guide, you can refer to the following table that includes common component types, example specifications, and required wattages.

<b>Component Type</b>	<b>Example Specification</b>	<b>Example Wattage Required</b>
CPU	Intel Core i7-970, 3.2 GHz	130
Memory	4GB DDR3-1600	8
Video card	NVIDIA GeForce 8800 GTS	220
Motherboard	ASUS P6X58D Premium LGA	36
Hard drive	1 TB SATAII 7200 RPM	6
Optical drive	6x Blu-ray	32
NIC	10/100/1000 Mbps PCI-Express	14
Sound card	SoundBlaster X-Fi Titanium	23
USB wired keyboard	Yes/No	4
USB wired mouse	Yes/No	4
USB flash drive	Yes/No	5
Other external devices	External DVD+R drive	5

1. Examine your PC, and complete the **Specifications** column of the following table. If you have different or additional components in your PC, revise the table accordingly.

<i>Component Type</i>	<i>Specification</i>	<i>Wattage Required</i>
CPU		
Memory		
Video card		
Motherboard		
Hard drive		
Optical drive		
NIC		
Sound card		
USB wired keyboard		
USB wired mouse		
USB flash drive		
Other external devices		

2. If you can, determine the power required by each component, and complete the table. Again, example values have been provided for your reference.
  3. Calculate the total wattage required for your PC. Compare this value with the maximum wattage output listed on the power supply. Does this power supply need to be upgraded?
  4. Add a buffer of 30 percent to the total wattage required for your PC. Will the existing power supply continue to supply enough power if additional components are added to the system?
-

# ACTIVITY 7–8

## Installing a Power Supply

### Scenario

After calculating the power needed for all the components added to a user's system, you have determined that it exceeds the capacity of the installed power supply. You have ordered and received a replacement power supply and now you need to install it.

1. Remove the existing power supply.
  - a) Shut down and turn off the system.
  - b) Unplug the power cord from the electrical outlet.
  - c) On ATX systems, to discharge any remaining electricity stored in the computer's capacitors, toggle the power switch on the computer on and off.
  - d) Remove any components necessary in order to access the power supply and its connection to the system board.
  - e) Unplug all power connections from devices, marking where each connection went to as you go.
  - f) Unplug the power supply from the system board.
  - g) Unscrew the power supply from the case.
  - h) Remove the power supply from the case.

2. Install the replacement power supply.



**Note:** If you don't have another power supply, reinstall the power supply you just removed.

2.
  - a) Insert the power supply into the case. Align the guides on the base of the supply with the base.
  - b) Secure the power supply to the case.
  - c) Plug all power connections into the devices.
  - d) Plug the power supply into the system board.
  - e) Reinstall any components you removed to access the power supply.
  - f) Plug the power cord from the power supply to the electrical outlet.

3. Test the power supply.
  - a) Turn on the system.
  - b) Test all components.

# TOPIC D

## Troubleshoot System Components

So far in this lesson, you have worked with several crucial components that are found inside a computer case. As an A+ technician, it is essential for you to be comfortable working with these components, whether you are installing them, configuring them, or trying to figure out how to resolve issues with them. In this topic, you will troubleshoot system hardware components.

It is only a matter of time before a personal computer's internal system hardware components experience problems, and generally these are problems users themselves cannot fix. As an A+ technician, many of the service calls that you respond to will involve troubleshooting system hardware components, and your ability to quickly and effectively diagnose and solve the problems will be essential in maintaining the satisfaction level of the users you support.

### Common System Troubleshooting Tools

Troubleshooting system devices can be challenging when the problem is not visually detected or obvious. To help you determine where the problem stems from within a computer, you can use a few different tools each with a unique function that will enable you to fix the defective hardware component:

- A *power supply tester* is a tool that connects to the power supply's 24-pin connector that tests the functionality of the unit. These testers can be used to test various power connectors including Berg, Molex, AT, and ATX. You can also use them to test the power supply under load. Some advanced testers can even test the functionality of other drives such as hard drives, optical drives, and floppy drives.
- A multimeter can be used to verify correct voltage ranges for a system's power supply.
- A loopback plug can be used to test port functionality.
- A *POST card* is a card that can be plugged directly into the motherboard in an available expansion card slot, or connected to an available USB port, that can read and display any error codes that get generated during the POST process of a computer. This tool can be extremely useful for determining why a computer will not boot up. The specific error codes will differ depending on the BIOS version and the specific manufacturer. You may need to refer to the manufacturer for an updated error code list before you start using the card in the computer.

Another useful troubleshooting tool are indicator lights. Indicator lights are found on components such as the motherboard, connections from the power supply to indicators on the case, from the hard drive to indicators on the case, and on network cards. The indicator lights provide a visual indication of whether the component or device is functioning properly.

### Common CPU Issues

When troubleshooting central processing units (CPUs), you must be aware of common issues and how to manage them effectively.

<b>Problem</b>	<b>Description</b>
Overheating and failure	Most problems with CPUs can be attributed to overheating or outright failure. The main solution to CPU problems is to replace the CPU. In some cases, you may be able to add additional cooling units to prevent the CPU from overheating and prevent further damage from occurring. Other times, it may be possible to simply pro-actively optimize the existing cooling system, such as by clearing dust from chips, heat sinks, and fans.

<b>Problem</b>	<b>Description</b>
Slot and socket compatibility	<p>Before you replace a processor, you need to make sure you select a processor that matches the type of socket on the system board.</p> <ul style="list-style-type: none"> <li>Some sockets use a pin grid array (PGA) that enables the chip to drop in and ensures that Pin 1 on the processor is properly aligned with Pin 1 on the socket. This method prevents you from bending the pins when removing or inserting the processor. The chip fits easily into the socket and does not need to be forced. Once the chip is in place, the retaining clip is secured.</li> <li>The land grid array (LGA) is another type of socket that contains pins that connect to pads located on the bottom of the processor package.</li> </ul> <p>When examining CPU issues, confirming the socket type may help you to identify any possible CPU connection issues.</p> <p>Not all processors that use a particular socket will be compatible with your system; this is just one of several items you will need to check for compatibility.</p>
Cooling system issues	<p>Because CPUs are prone to damage from overheating, you should always consider the cooling system components when you are troubleshooting CPU issues. For instance, if a user is experiencing intermittent problems during operation, there could be inadequate airflow within the computer chassis that can be corrected by providing space in front of the vents and fans. Also, dust can often accumulate on the CPU's heatsink, and can reduce the efficiency of the heatsink, possibly causing the CPU to overheat.</p> <p>When thermal problems cause a system to shut down or fail to boot, it could be that the overall system cooling is inadequate, a cooling device has failed, or the processor is overclocked, whether intentionally or not.</p> <ul style="list-style-type: none"> <li>If you suspect the cooling system is a problem, you can add more cooling devices, upgrade to more efficient devices, or clean or replace failed devices.</li> <li>If you suspect the CPU is overclocked, check the manufacturer's specifications to determine the supported clock speed. Then, use firmware settings to reduce the CPU speed. If you have an advanced system BIOS, then you may be able to see the actual CPU temperature readings.</li> </ul>
Excess power consumption	<p>Power consumption is a major factor for manufacturers when designing CPUs. When troubleshooting possible CPU issues, keep in mind that because some CPUs operate at higher clock frequencies, they require more power. If not properly cooled, this can result in the CPU overheating. In this case, you may need to either reduce the clock frequency of the processor using <b>Power Management</b>, or install additional cooling devices.</p>



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Troubleshoot CPU Problems.

# ACTIVITY 7–9

## Troubleshooting CPU Issues

### Scenario

You are attempting to resolve problems for a user who has been reporting intermittent but severe system errors, such as frequent unexpected shutdowns. The problems have been getting more frequent, and you have been unable to pinpoint a cause within the system software, power supply, memory, or any adapter cards. You are starting to suspect that there is a bad CPU, and you need to proceed accordingly to get the user back to work with as little downtime and cost as possible.

**1. What initial steps should you take to identify and resolve a potential CPU problem?**

- Replace the CPU with a known-good processor.
- Verify that the CPU fan and other cooling systems are installed and functional.
- Replace the motherboard.
- If the CPU is overclocked, throttle it down to the manufacturer-rated clock speed.

**2. All other diagnostic and corrective steps have failed. You need to verify that it is the CPU itself that is defective. What should you do?**

- Replace the CPU with a known-good chip.
- Remove all the adapter cards.
- Reinstall the operating system.
- Replace the motherboard.

## Common Cooling System Issues

There are a few issues common to computer cooling systems.

Issue	Solution
Dust buildup	Over time, dust will build up on components inside the computer. Dust can act as a thermal insulator once it has gathered on a system's heat sinks and fans. In this case, the dust can act as an insulator and keep heat from escaping from the components, and can inhibit proper airflow within the system. As a result, system components will not perform to capacity and can burn out quicker than expected. Make sure to keep system components clean and free of dust.
Poor airflow	When system components are not properly placed inside the computer's case, the result can be reduced airflow within the system. This can happen when system board components are placed too close together and create too much heat. Another cause for concern is when there is more than one fan used in the cooling system. Both of these examples can create irregular airflow and can also create small pockets of hot air inside the case. Always check the manufacturer information for your system before adding additional components, including core cooling devices such as CPUs and case fans.

<b>Issue</b>	<b>Solution</b>
Poor heat transfer	Thermal compounds are used to aid in the cooling of computer devices. Thermal compounds are often used in conjunction with a heat sink to maximize the cooling effect. In cases when the thermal compound is not applied properly, heat transfer may not be effective and can result in heat damage to the components instead of the heat being properly dissipated.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Troubleshoot Cooling System Issues.

## Common Motherboard Issues

Motherboard problems can be among the most difficult to recognize and diagnose. Typically, the computer will not boot, or the computer will display erratic behavior, or there may be intermittent device failures that cannot be resolved otherwise. If you have eliminated all other hardware components, applications, and the operating system as the source of the problem, then you should check to see if the system board is the cause.

Common sources of system-board-related problems include:

- Computer viruses infecting the system, including the system firmware.
- Loose connections between system components and the system board. For example, front panel connectors may not be secure.
- Out-of-date system firmware. Check the system firmware and the advanced system firmware settings for your system board.
- System firmware memory is not holding configuration information.
- System time and settings reset automatically. This is caused by either a bad CMOS battery, or a faulty motherboard.
- System attempts to boot to incorrect device. This is typically a sign that the system firmware has been set up improperly.
- The CMOS battery is not functioning to keep the system clock information.
- Electrical shorts on the system board due to improperly seated components or power surges. This is the most common cause of system board problems.
- Physical damage to the system board. Physical damage can lead to many issues. If the bus circuits on the board are affected, for example, the result could be slower information transfers by the system bus, and ultimately slower overall system performance.
- Distended capacitors on the system board that can break their casings and leak electrolytes, causing the board to fail.
- Damage to memory and expansion slots when replacing memory and adapter cards.
- Damage to the processor socket when installing a new CPU. This is common when the pins inside the socket get bent or broken when inserting the processor chip in the socket.

## Preventing System Board Problems

When you have to touch the system board, you can prevent damage by handling it with care. When you install components into the system board, be sure not to bend or break any of the pins. This includes the pins on the cards as well as the system board. Also, the system board can crack if you push down too hard on the board itself or the expansion cards. When you secure the system board to the case, be sure not to over-tighten the screws as this could also crack or damage the system board. ESD damage from handling or from electrical surges such as lightning strikes can ruin the system board electronics. Be sure to use proper surge protection as well as ESD-prevention techniques to help prevent such problems.

## Repair vs. Replace

Today's system boards are highly integrated and generally not repairable. When you examine a system board, you will find that there are very few components on the board that are individually repairable. For example, if a built-in input/output (I/O) port fails, you will have to install an expansion card that provides that port's functionality. If the chipset or another integrated circuit fails, you will have to replace the entire system board. Even if you are highly skilled in the use of a soldering iron, in most cases, when a system board fails, you will replace it. Other than replacing the battery, there is virtually nothing on it you can repair.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Troubleshoot Motherboard Problems.

# ACTIVITY 7-10

## Troubleshooting Motherboards

### Scenario

Several trouble tickets related to motherboards have been assigned to you.

- 
- Problem #1** When the user turns on the computer, he sees a message stating that the computer's date and time are incorrect. He must reset this information in the computer's system firmware each time he starts the computer.

**What should you do to resolve this issue?**

- Problem #2** When the user turns on the PC, it does not always come on and sometimes it just shuts itself down abruptly, with no warning. When she turns on the PC again, there is no fan noise. Her data is becoming corrupted from the frequent reboots.

**What should you do to resolve this issue?**

- Problem #3** One of the other hardware technicians has been trying to troubleshoot a power problem. The computer periodically and randomly reboots. The other technician has determined that the user has an ATX motherboard and power supply. You have been assigned to take over this trouble ticket.

**What should you do to resolve this issue?**

---

### Common External Power Source Problems

Problems with external power sources can result in data loss, erratic behavior, system crashes, and hardware damage.

<b>Power Problem</b>	<b>Possible Causes</b>
Line noise	<p><i>Line noise</i> occurs when there is a fluctuation in the electrical current. Causes include:</p> <ul style="list-style-type: none"> <li>• Electromagnetic interference (EMI)</li> <li>• Radio frequency interference (RFI)</li> <li>• Lightning</li> <li>• Defective power supply.</li> </ul>

<b>Power Problem</b>	<b>Possible Causes</b>
Power sag	A <i>power sag</i> is when the power level drops suddenly below expected power levels. Causes include: <ul style="list-style-type: none"> <li>• Many electrical systems starting up at once.</li> <li>• Switching loads at the electric company utility.</li> <li>• Electric company equipment failure.</li> <li>• Inadequate power source.</li> </ul>
Power undervoltage or brownout	This symptom can last from several minutes to several days and can be caused by any of the following: <ul style="list-style-type: none"> <li>• Decreased line voltage.</li> <li>• Demand exceeds power company supply.</li> <li>• Utility company reduced voltage to conserve energy.</li> </ul> A variation on this is switching transient or instantaneous undervoltage that lasts only a matter of nanoseconds.
Frequency variation	Usually occurs when using a small power generator. As loads increase or decrease, the power frequency varies. Generators are not recommended for supplying direct power to computers and other sensitive equipment. The variance in frequency (square wave instead of sinusoidal wave) and the instability of the voltage will cause severe instability in computers, leading to crashes, data loss, and possible equipment damage. Using a power conditioner or an inverter with a generator will prevent these issues by stabilizing the voltage and frequency.
Overvoltage	<i>Overvoltage</i> occurs when power levels exceed acceptable levels. This can be caused by any of the following: <ul style="list-style-type: none"> <li>• Suddenly reduced loads.</li> <li>• Equipment with heavy power consumption is turned off.</li> <li>• Power company switches loads between equipment.</li> <li>• Lightning strikes.</li> </ul>
Power failure	Power failures can be caused by any of the following: <ul style="list-style-type: none"> <li>• Lightning strikes.</li> <li>• Electrical power lines down.</li> <li>• Overload of electrical power needs.</li> </ul>

## Common Power Supply Problems

Power supply damage from overheating, lightning strikes, or short circuits can produce a number of symptoms.



**Note:** POST error codes from 020 and 029 are related to the power supply.

<b>Symptom</b>	<b>Possible Causes and Solutions</b>
Fan will not work.	The fan and openings around the power supply bring in air to cool system components, but they also allow dirt and dust to gather around the power supply. This can cause the fan bearings to wear and the fan to turn more slowly. You can use compressed air to remove this debris from the system. If the fan becomes damaged due to dust, replace the power supply or have qualified personnel replace the fan.

Symptom	Possible Causes and Solutions
No power.	If the computer will not boot, then the first thing to check is that the power supply cable is securely connected at the supply and at the power source. Check to make sure there is power coming from the outlet or power strip. If the connection is secure, then you will need to open the computer case and verify that the motherboard status indicator light is on. The status indicator light is shown when the power is sufficiently supplied to the board. If the light is not on, then you should check the physical power connection from the board to the power supply. Depending on the manufacturer, the power supply itself may also have a small LED light that indicates whether or not the power supply is functioning.
Fans spin but no power to other devices.	This symptom is a sure sign of a power connection issue. Check all connections from the power supply to the internal components. Verify that the motherboard is properly connected to the power supply. Look for the indicator light on the motherboard to confirm the connection is successful and there is power supplied to the board.
Computer will not start or reboots after startup.	<ul style="list-style-type: none"> <li>If the computer does not start at all, make sure that there is power to the outlet. You can check by plugging in a lamp or other device that you know works. If that does not turn on, you know that you have a bad outlet and not necessarily a bad power supply.</li> <li>Check that the connections from the power supply to the system board are secure, especially on ATX systems. Make sure the master switch to the power supply, at the rear of the system, is on before pressing the computer's power button. Also on ATX systems, check the voltage of the power being supplied using a multimeter.</li> <li>A loose power supply drive connector landing on exposed metal can short-circuit the power supply. The power supply can detect this problem and disable itself. If you fix the short (by putting the power cable onto the drive correctly), the power supply should start working again. Unused drive connectors should be either covered (some technicians bring rubber end caps) or tie-wrapped to a safe location (not too tight to avoid damaging the wire). Also check for loose screws or foreign metallic objects that can cause shorts.</li> <li>Check power supply output voltages with a digital multimeter to verify that the necessary voltages are being provided to the board. This will not measure voltage under load, but will allow you to determine whether the output is within the correct range. Most motherboards also provide a voltage reading within the BIOS. If the system boots, access this BIOS option to obtain readings as detected by the motherboard.</li> </ul>
An odor or burning smell is coming from the power supply.	<p>An odor coming from the power supply can be the first sign that there is something wrong. Start by turning off the power, and then visually inspecting the system and looking for any damaged parts or cables.</p> <p>To verify the smell is in fact coming from the power supply, you may need to remove some of the system components. This may include hard drives, the CD-ROM drive, or a DVD burner. Reboot the system from an external drive, and check for the smell once again.</p> <p>Once you confirm that the odor is indeed coming from the power supply, contact the manufacturer first. Some newer systems may have a smell initially, but will eventually fade away. However, in other cases, an odor can be a sign that the power supply is failing, the fan is damaged, or there is a problem with the electricity source going to the system.</p>

Symptom	Possible Causes and Solutions
Smoke coming from computer.	Smoke coming from the computer means there is something seriously wrong with the power supply. Typically, the only component that can generate smoke is a failing power supply. When the wrong power supply is installed in a computer, it can cause issues with not only the supply itself, but it can literally fry the motherboard and connected components. If you see smoke, in most cases you will need to replace the power supply, and possibly the motherboard if there are any other damaged components.
Loud noise is coming from the power supply.	<p>Other components, especially drives, also can sometimes make a lot of noise. Make sure this is not where the noise is coming from.</p> <p>A loud whine or squeal from the power supply area is usually from the fan. A damaged fan with worn bearings will cause a grinding whine that worsens with time. Sometimes, when the bearings begin to fail, the fan blade assembly will shift, rubbing against the fan grill or the case, and produce a high-pitched noise. Also possible, after cleaning with compressed air, a wire inside the power supply unit could be shifted by the forced air and end up touching the fan, causing the very loud grinding noise, possibly stopping the fan altogether. With the power supply off, you can attempt to carefully shift the wire away from the fan by using a plastic tool (metal is not recommended so as to avoid damaging any components).</p> <p>If the noise is not from the fan, but from another power supply component, replace the power supply or take it out and send it for service.</p>

## Power Supply Troubleshooting Considerations

When troubleshooting power supplies, there are a few things you must consider in order to properly identify the issues.

Consideration	Additional Information
Wattages and capacity	You should always verify how much power each system component requires, before installing or replacing a power supply. If you are having issues with a power supply, then verify that the system component usage does not exceed the power supply's capacity. Ideally, you want a power supply that provides more, but not much more, power than the components require. Use proper power calculations to determine the power requirements of the system.
Connector types	Consider the power supply's connection type when replacing the unit. You must verify that the connection type on the system board matches the connection interface on the power supply unit. Also, verify that there are enough of each type of drive connector for the type and number of drives the system will be using.
Output voltage	The output voltage in a power supply is controlled by a feedback circuit inside the unit. Verify that the output voltages are within the range of what is expected.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Troubleshoot Power Supply Problems.

# ACTIVITY 7-11

## Troubleshooting Power Supplies

### Scenario

You have been assigned several power problems to solve.

1. **Problem #1** When the user turns on the PC, it does not always come on and sometimes it just shuts itself down abruptly, with no warning. When she turns on the system again, there is no fan noise. She is using a legacy database application and the data is being corrupted during the improper shutdowns.

**What would you do to resolve this problem?**

2. **Problem #2** A user is reporting an odor coming out of his computer. You have serviced this machine recently and replaced the computer's power supply unit.

**What would you do to resolve this problem?**

3. **Problem #3** One of the other hardware technicians has been trying to troubleshoot a power problem. The system will not come on when the user turns on the power switch. He determined that the user has an ATX motherboard and power supply. You have been assigned to take over this trouble ticket.

- a) Set the multimeter for DC volts over 12 V.
- b) Locate an available internal power supply connector. If none are free, power off the system and unplug it, then remove one from a CD drive, and then power on the system again.
- c) Insert the black probe from the multimeter into one of the two center holes on the internal power supply connector.
- d) Insert the red probe from the multimeter into the hole for the red wire.
- e) Verify that the multimeter reading is +5 V DC.
- f) Move the red probe into the hole for the yellow wire.
- g) Verify that the multimeter reading is +12 V DC.
- h) Check the documentation for the ATX motherboard to see if there is a logic circuit switch that signals power to be turned on or off, that it is properly connected, and how it should be set.
- i) Verify that the motherboard, processor, memory, and video card are all correctly installed and working.

4. **Problem #4** The user turns on the power switch, but the PC does not come on. He does not hear the fan, there is no power light on, and he hears no beeps or other sounds coming from the system. His system is plugged into a surge protector.

**What would you do to resolve this problem?**

---

## Summary

In this lesson, you installed and configured internal system components. In your role as an A+ technician, you will be responsible for helping users with installing and troubleshooting motherboards, CPUs, cooling systems, and power supplies, so having the skills to install and troubleshoot them will be crucial to assisting users.

**In your current job role, what system components have you worked with the most? In future job roles as an A+ technician, what system components do you think you will be working with the most?**

**What types of cooling systems have you worked with? What would you recommend for the average user?**



**Note:** Check your CHOICE Course screen for opportunities to interact with your classmates, peers, and the larger CHOICE online community about the topics covered in this course or other topics you are interested in. From the Course screen you can also access available resources for a more continuous learning experience.

# 8

# Managing Data Storage

**Lesson Time:** 2 hours, 30 minutes

## Lesson Objectives

In this lesson, you will manage data storage. You will:

- Compare and contrast various RAM types and their features.
- Troubleshoot RAM issues.
- Install and configure storage devices.
- Configure settings through BIOS or UEFI tools on a PC.
- Troubleshoot hard drives and RAID arrays using appropriate tools.

## Lesson Introduction

Data storage comes in a variety of types and sizes and for different purposes. Temporary data storage in RAM, long term battery powered storage in CMOS, and permanent storage on disks, in flash memory, and on tape are the main types of storage you will encounter.

# TOPIC A

## Identify RAM Types and Features

In this lesson, you will manage data storage. All PCs have both long-term and short-term data storage. In this topic, you will examine RAM.

Just as some people say you can never be too rich or too thin, you can never have too much memory. Adding memory is one of the simplest and most cost effective ways to increase a computer's performance, whether it is on a brand-new system loaded with high-performance applications or an older system that performs a few basic tasks. Upgrading the memory is a common task for any PC technician.

### RAM Modules

A RAM module, or *memory module*, is a printed circuit board that holds a group of memory chips that act as a single unit. Memory modules reside in slots on the motherboard, and they are removable and replaceable. Memory modules are defined by their design and by the number and type of chips they contain.

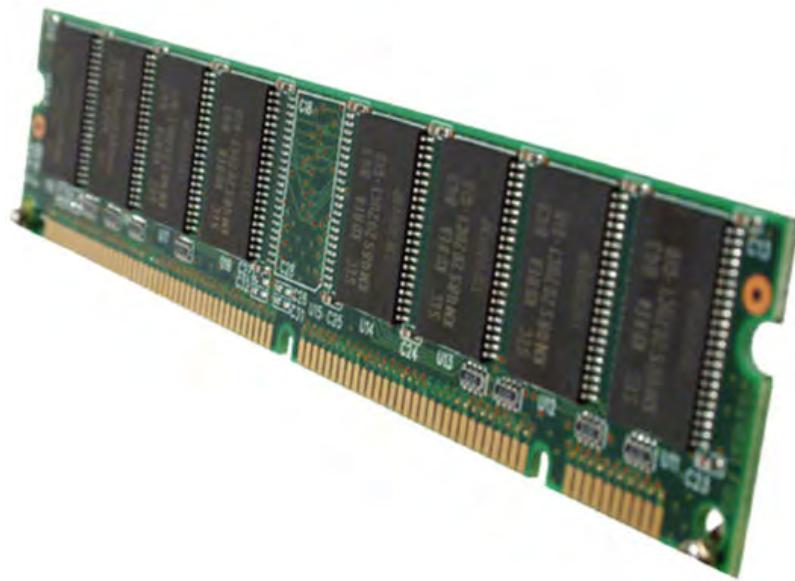


Figure 8-1: A memory module.

### RAM Types

Static RAM (SRAM) is used for *cache memory*, which is high-speed memory that is directly accessible by the CPU. It does not need to be refreshed to retain information. It does not use assigned memory addresses. It is faster than Dynamic RAM, but it is also more expensive. Cache is used for active program instructions that software refers to on a frequent basis. Cache is divided into levels based on how close it is to the CPU. Level 1, or L1, cache is embedded on the CPU chip. L2 cache is memory that resides within the processor package but is not on the processor chip itself. L3 cache is specialized memory designed to improve L1 and L2 cache performance; it is further from the processor core but still within the processor package.

Dynamic RAM (DRAM) is used on single and dual in-line memory modules (SIMMs and DIMMs). It needs to be refreshed every few milliseconds. It uses assigned memory addresses and is used in the memory modules installed in the RAM slots on the motherboard. It uses an asynchronous

interface that operates independently from the CPU. This outdated technology was replaced with Synchronous DRAM (SDRAM), which is synchronized with the system bus, making it less likely that information is lost during transfer and processing by the CPU.

There are several types of RAM modules used for system memory. These all use SDRAM.

Type of RAM	Description
DDR	Double Data Rate Synchronous DRAM (DDR SDRAM) transfers data twice per clock cycle, which means it processes data on the rising side and falling side of the system clock. It is a replacement for SDRAM. DDR uses additional power and ground lines and is packaged on a 184-pin DIMM module.
DDR2	DDR2 chips increase data rates over those of DDR chips. DDR2 modules require 240-pin DIMM slots. Although DDR2 chips are the same length as DDR, they will not fit into DDR slots.
DDR3	DDR3 chips transfer data at twice the rate of DDR2, and use 30 percent less power in the process. Like DDR2, DDR3 chips use 240-pin connections, but cannot be used interchangeably because of differences in notch location and electrical requirements.

## Single-Sided vs. Double-Sided Memory

Single-sided RAM does not refer to the literal number of sides that a RAM module has, but rather it means an expansion bank of RAM has all of its available memory accessible by the computer.

Double-sided RAM might have two banks of memory, but only one can be accessed at a time by the computer.



**Note:** Be sure not to confuse this with single-sided and double-sided media such as CDs and DVDs, which can be written to one side or both sides of the media.

## ECC vs. Non-ECC

*Error Correcting Code (ECC)* is an error correction method that uses several bits in a data string for error checking. A special algorithm is used to detect and then correct any errors it finds.

A DIMM has an even number of chips on the memory module, but a DIMM that supports ECC has an odd number of chips, and the extra chip is the ECC chip. The data path width for DIMMs is 64 bits, but ECC uses an extra 8 bits for error checking, so the data path width is 72 bits. All memory modules must support ECC.

ECC is used only in upper-end systems such as high-end workstations and servers; other desktop systems use non-ECC memory. Non-ECC memory usually employs *parity* to ensure that errors are detected within the data, but does not have the functionality to correct them.

## RAM Configurations

Different chipset configurations used in RAM will determine how fast data can be transferred between the chips on the board. In this context, the number of channels correlate to how many DIMM slots the memory controller can address at one time.

- The slowest configuration is the single channel because the memory controller can access only one DIMM at a time.
- In a dual-channel configuration, the memory controller can access two DIMMs at one time, which doubles the speed of memory access.

- In a triple-channel configuration, the memory controller can access three DIMMs at the same time.
- In a quad-channel configuration, the memory controller can access four DIMMs at the same time.

## Parity vs. Non-Parity

Parity is an older error-checking method that is sometimes used in RAM modules to detect errors that may occur during data transmission. When parity is used, a data transmission contains 8 bits of data with the ninth bit being the parity bit. The parity bit is used to determine whether a piece of data is equal to another piece of data. The parity bit value can be either true, or a 1, or it can be false, or 0. An error is detected if the parity bit values of two data strings do not match.

The controller can detect that an error has occurred, but it cannot correct it. When an error is detected, the system simply tries again after discarding the data. Or, a parity error might cause the system to stop and the screen displays an error message such as: Parity Error 1 (parity error on the motherboard).

Parity memory is rarely used; however, there are usually other system components that are relied on to verify that the data contained in memory is accurate when non-parity memory is used. You will typically find this type of memory used in servers.

## Buffered vs. Non-Buffered

Buffered RAM contains a control chip to assist the memory controller when there is a large amount of memory installed in a system. Buffered memory is typically used in servers to ensure that data is handled correctly. Unbuffered RAM communicates directly with the memory controller. Unbuffered RAM is more appropriate for workstations and computers used for gaming. Buffered RAM introduces some degree of latency due to the extra control chip it contains, making it less than ideal for gaming systems.

Buffered RAM often also contains ECC circuitry. This helps find and correct any errors. These features make buffered RAM more expensive than non-buffered RAM.

You can only use the type of RAM your system is designed to use. The connectors between buffered and non-buffered RAM are not the same.

## RAM Compatibility

If you want to add additional memory or you need to replace the existing memory in your system, the RAM modules you install must be compatible with your motherboard. The technology for each type of memory module (DDR, DDR2, DDR3, and so forth) is not compatible with each other. In addition to the technology, another way memory manufacturers prevent you from accidentally installing the wrong memory modules is by the placement of the notches on the edge of the RAM modules. Even though the modules might be the same physical size, the location of the notches will be different.

Most memory manufacturers have tools on their website to help you identify the RAM you will need for your system. Typically, you need to specify the manufacturer of the computer, the product line, and the model of the system. Some sites will scan your system to see what is currently installed and make recommendations based on the results of the scan.

The best results when installing additional RAM is to install the exact same modules as what is already installed. If that isn't possible, make sure that the new modules have the same specifications. Memory modules of different speeds will cause the faster modules to run at the speed of the slowest module.

<b>Specification</b>	<b>Description</b>
CAS latency	Column address strobe (CAS) is a signal the processor sends to a memory circuit to activate a column address. The latency indicates how many clock cycles it will take for the memory module to read or write a column of data from a memory module and return the data requested by the CPU. Make sure that additional modules have the same CAS latency.
Timing	In addition to the CAS latency timing, the other timings you need to match include: <ul style="list-style-type: none"> <li>• Row Access Strobe (RAS): After sending the memory controller a row address, this is the number of cycles that must pass before the system can access one of the row's columns.</li> <li>• Row Precharge Time (RP): If a row is already selected, this indicates how many cycles must pass before another row can be selected.</li> <li>• Row Active Time: This specifies the minimum number of clock cycles a row needs to be active to make sure there is enough time to access the information stored in the row.</li> </ul>
Voltage	The voltage should be the same as the existing memory modules.

## ACTIVITY 8-1

### Comparing RAM Types and Features

#### Scenario

In order to choose the right type of RAM for a computer system, you typically will compare the various types and features.

- 
1. You have a typical system with RAM that runs at 10 ns, and you add a 12 ns memory module. How fast will the RAM run? Explain your reasoning.
  
  2. When selecting a RAM module, when would you choose RAM enabled with ECC as opposed to RAM with only parity?
-

# ACTIVITY 8-2

## Install RAM (Optional)

### Before You Begin

You will need a working computer with access to the Internet for this activity.

### Scenario

A user has asked you to install additional memory in their PC. You will need to figure out what type of memory is currently installed, then determine which memory modules would be compatible with the existing modules already installed.

1. Determine the specifications for the memory currently installed in the PC.
  - a) Open a web browser and access a search site.
  - b) Search for **RAM finder**
  - c) Select the manufacturer of your choice and access their web page.
  - d) Enter the required information about your PC to find out what memory works in the system.  
This typically includes the computer manufacturer name and the model name or number.
  - e) Determine the maximum amount of RAM that can be installed in the PC.  
This information should be shown in the results from your search.
  - f) View **System** information to see how much RAM is currently installed.

### System

Processor: Intel(R) Core(TM) i7-4510U CPU @ 2.00GHz 2.60 GHz

Installed memory (RAM): 8.00 GB

System type: 64-bit Operating System, x64-based processor

2. Install memory in the PC.



**Note:** If your instructor has additional memory available for you to install in the PC, they will give it to you now. If not, you can remove the existing memory module and reinstall it. Be sure to follow ESD best practices when you work with RAM modules.

- a) Shut down the PC and prepare to work inside the system.
  - b) Locate an empty RAM slot on the motherboard.
- 
- Note:** Refer to any documentation you have about whether modules must be installed in certain slots if multiple slots are available.
- c) Open the retaining clips for the selected RAM slot.
  - d) Holding the RAM by the edges, line up the RAM with the RAM slot, then press down on it until the clips lock the module in place.
  - e) Restart your PC.
  - f) Log in, then view **System** information to see how much RAM is installed.

# TOPIC B

## Troubleshoot RAM Issues

You have identified RAM types and features. Fully functional RAM is essential to the system and to creating a working system. In this topic, you will examine some of the common RAM issues you might encounter and how to resolve those issues.

### Common RAM Issues

RAM problems typically show themselves as memory-specific errors, erratic system behavior, or frequent crashes.

Symptom	Possible Causes
Computer crashes, system lockups, and unexpected shutdowns.	<ul style="list-style-type: none"> <li>ESD, overheating, or other power-related problems that can affect memory.</li> <li>Registry writing to bad memory, General Protection Faults (GPFs), and exception errors caused by software and operating system.</li> </ul>
Memory errors appear on screen.	<ul style="list-style-type: none"> <li>Memory address errors at boot time.</li> <li>Applications that require large amounts of memory or that do not properly release memory.</li> </ul>
Blank screen on bootup.	<ul style="list-style-type: none"> <li>Memory is not correct for the system. For instance, the computer is expecting memory that uses error checking and you installed non-parity memory.</li> <li>Memory module is not fully inserted into the slot.</li> </ul>
Computer does not boot. POST beep codes sound.	<ul style="list-style-type: none"> <li>CPU cannot communicate with memory due to the memory being improperly installed or the BIOS not recognizing the memory. Beep codes are specific to the BIOS manufacturer and the ones for memory can be found in the manufacturer's beep codes list.</li> <li>For additional information on specific beep codes, visit <a href="http://www.computerhope.com/beep.htm">www.computerhope.com/beep.htm</a>.</li> </ul>
Some or all newly installed RAM is not recognized.	<ul style="list-style-type: none"> <li>You exceeded the maximum amount of RAM that can be addressed by the system. Even though the slots can accept Dual In-line Memory Modules (DIMMs) containing more memory, the system can only recognize a certain amount of memory on most systems.</li> <li>The wrong memory type was installed.</li> <li>The memory was not installed in the proper sequence.</li> <li>You might need to leave empty slots between multiple modules, or you might need to install modules containing more memory in lower-numbered slots than smaller modules.</li> </ul>



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Troubleshoot RAM Problems.

# ACTIVITY 8-3

## Troubleshooting RAM Issues

### Scenario

You have been assigned some trouble tickets that deal with memory issues.

- 1. Problem #1** The user is experiencing corrupted data in his database application. The hard drive has been checked and no problems were found with it. The application was reinstalled and the database was re-indexed and all data problems have been corrected. No other users are experiencing this problem when they enter data. He has been successfully entering data until just recently.

After troubleshooting this trouble ticket, you have discovered symptoms of a memory problem. What factors could cause sudden memory problems in this situation?

- New virus
- Power spike
- New memory not compatible
- Power surge

- 2. Problem #2** Additional memory was installed in a user's system, and now it will not boot.

What steps would you take to resolve this trouble ticket?

- 3. Problem #3** The user is complaining of application crashes. He is fine if he is running only his email and word processing programs. If he also opens his graphics program at the same time, then the applications are crashing.

Why is the user experiencing the problem only when additional applications are opened?

- There is not enough memory in the system.
- Memory errors are occurring in one of the higher memory modules.
- The memory modules are incompatible with one another.

# TOPIC C

## Install and Configure Storage Devices

So far in this lesson, you have worked with RAM, which is short-term data storage. Now it's time to look at long-term storage solutions. Storage devices such as hard disks are one of the most common system components you will install. In this topic, you will install and configure storage devices.

Users rely on local storage devices to keep their applications and data current and available. As an A+ technician, your responsibilities are likely to include installing and configuring different types of storage devices to provide your users with the data-storage capabilities that they need to perform their jobs.

### Storage Devices

As you have seen previously in the course, there are several types of storage devices. These include internal and external devices. The data is stored on optical discs, magnetic media, solid state devices, and using RAID.

### Internal Storage Device Considerations

There are several things to consider when you are installing an internal storage device in a computer system. It is not as simple as just plugging the device into the slot inside the case. Make sure you consider each factor before installation.

Consideration	Details
Does the computer have existing internal storage devices?	Do you need to plan for the addition of another controller for an additional device? You might need to purchase an additional SATA controller before you can add another SATA device. In addition, make sure that the computer has an available slot for the controller.
Does the device need additional drivers installed?	Make sure that you have the appropriate operating system device drivers to install the new storage device on the computer. If necessary, download the device drivers from the device manufacturer's website.
Does the computer have an available power supply cable to supply power to the device?	If not, you can purchase splitters to enable two (or more) devices to be connected to a single power connection, but be aware of power consumption. The number of connectors approximates the available power, so make sure that the storage device will not cause the computer to exceed the capacity of its power supply.
Does the computer have an available drive bay for the storage device?	Most hard drives require a 3.5-inch drive bay; most tape drives and optical drives require a 5.25-inch drive bay. If you want to install a hard drive in a 5.25-inch drive bay, you will need <i>drive rails</i> . Make sure you place the storage device where it will get good air flow to avoid overheating the device. Consider the placement of the drives inside the bays with the cable configurations. You may need to adjust the placement of the drives to match the order of cable connectors.
Do you have the necessary data cables to connect the storage device to the controller?	You will need a SATA data cable for each hard drive in the PC. Other types of storage devices might require different types of data cables,

<b>Consideration</b>	<b>Details</b>
Does the placement of the device interrupt the air flow of the case?	Make sure there is enough total air flow to handle whatever heat the new storage device will add to the computer.

## External Storage Device Considerations

External storage devices have a whole set of different considerations than internal devices. Make sure to verify all the factors before selecting and installing a new device.

<b>Consideration</b>	<b>Details</b>
What interface does the external storage device require (USB, FireWire, or eSATA)?	<ul style="list-style-type: none"> <li>If the external storage device uses USB 3.0, does the computer support it?</li> <li>If the external storage device uses FireWire, is there an available FireWire port in the computer? Does the device use FireWire 400 or FireWire 800? If there is no FireWire port, or it is not the right size, you must buy and install an appropriate FireWire controller. Make sure the computer has an available slot for the FireWire controller before purchasing one.</li> <li>If the external storage device uses eSATA, does the computer have an eSATA port?</li> </ul>
Do you need a cable to connect the external storage device to the computer?	Depending on the type of interface used, you will need to make sure that you have a compatible cable to connect to the computer. Common cable connections include: <ul style="list-style-type: none"> <li>USB</li> <li>FireWire</li> <li>eSATA</li> <li>Ethernet</li> </ul>
Do you have an available source of power for the storage device?	Some external storage devices will require an additional power source from the computer. For example, eSATA requires an additional power connection to function.

## USB Performance Factors

To get the best possible performance from a storage device that uses USB as a connection method, connect it to a port or hub that supports USB 3.0. Keep in mind that many hubs drop all ports down to the slower USB 1.1 speed if you connect any USB 1.1 devices. Try not to connect a slower-speed device to the same hub in which you plan to connect a USB 3.0 storage device.



**Note:** For additional information, check out the LearnTO **Install Storage Devices** presentation in the LearnTOs for this course on your CHOICE Course screen.

## Disk Management

**Disk Management** is a snap-in utility for the MMC that you can use to manage all of the drives installed on the system, including hard disk drives, optical disc drives, flash drives, and storage spaces.

The following figure shows a system with a BIOS configuration that uses MBR. GPT is only used on UEFI systems. For GPT drives, you use diskpart to work with the drives.

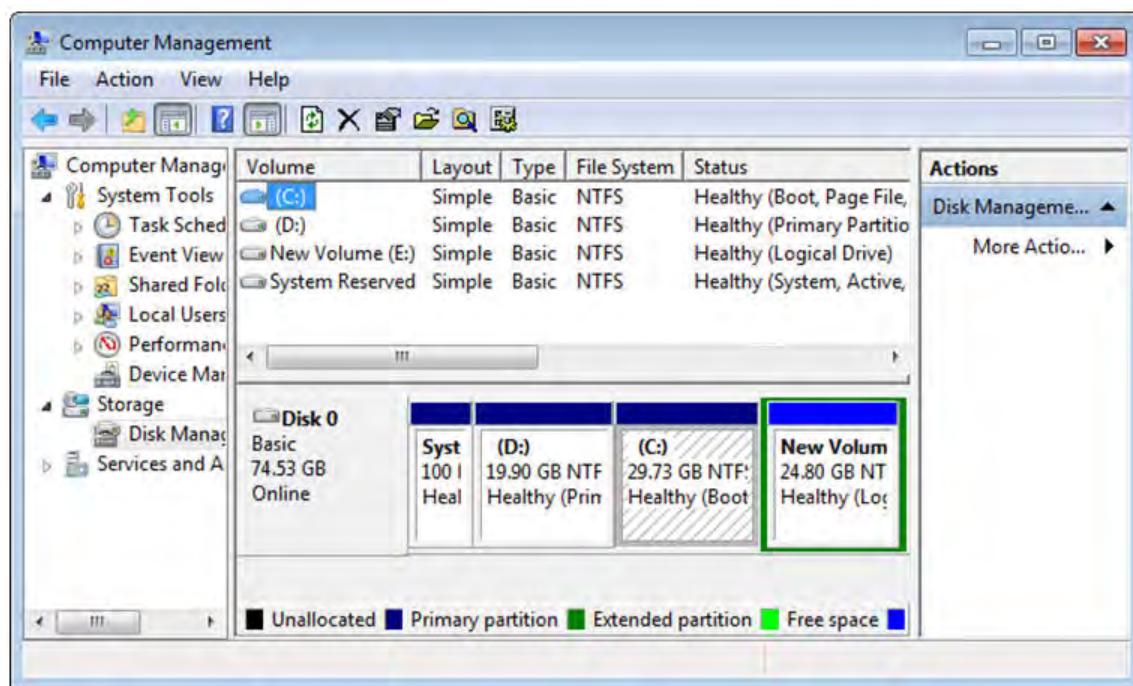


Figure 8-2: The Disk Management utility in Windows 7.

	<b>Note:</b> Although any user can access <b>Disk Management</b> and view information about their drives, only an administrator can use the other disk management tools available through this utility.
Action	Description
Views	Displays all of the drives on the system, the drive letter assigned, the total capacity of the drive and how much free space is available, and the current status of the drive. It also displays the partitions for each drive.
Assign a drive letter	Can be used to assign or change a drive letter for any hard drives, optical drives, or flash drives being used by the system. The drive letter for the partition that Windows is installed on cannot be changed.
Mount a drive	Can be used to create a mounted drive or partition, in which the drive is mapped to an NTFS-formatted folder on the hard drive and is assigned a folder path name rather than a drive letter.
Extend partitions	Can be used to create a container for logical partitions in order to extend the volume of an existing partition, if more than four partitions are desired.
Split partitions	Can be used to shrink or divide a partition on the drive to make room for another partition to be created. You can reduce the partition volume to a desired size to make free space for a new partition to be created.
Add a drive	Can be used to add a drive/disk to the machine. Once the drive has been installed and depending on the history of the drive (already partitioned, never been used, etc.), you can use this utility to initialize the disk or set an offline disk to online.
Add an array	Can be used to create and add an array to the system, including assigning the drive a drive letter, mounting it to a folder, and formatting the volume. An array is more than one physical drive on the machine that is combined and managed as a single logical drive in the <b>Disk Management</b> utility.

## Accessing Disk Management Directly

You can access **Disk Management** by using an MMC snap-in, but you can also access it directly by using the **Run** dialog box and entering the `diskmgmt.msc` command.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Install and Configure Storage Devices.

# ACTIVITY 8-4

## Installing an Internal Storage Device

### Before You Begin

To complete this activity, you will need the following hardware components. If you do not have these available, you can remove and reinstall the existing hardware:

- A second hard drive and an empty drive bay.
- An available power connection for the device you are adding to the system.
- Optionally, rails to allow smaller drives to fit into larger drive bays.

### Scenario

You have been assigned the task of refurbishing a computer for a client. This computer has a single functioning hard drive, and the user needs a significant amount of local storage space.

1. Locate the available bay and the power and data connections for the new hard disk drive.
  - a) Power off the system, unplug all the peripherals and power cord, and open the computer case.
  - b) Locate an available drive bay and determine if the bay is the same form factor as the drive. If you are using a 5.25-inch drive bay and a 3.5-inch drive, you will need to install the drive using rails to adapt the drive to the larger bay.
  - c) Locate an available data connection on the data cable.
  - d) Locate an available power connector.
2. Install the hard disk drive into the system.
  - a) If necessary, attach rails to the drive to fit in the bay.
  - b) Slide the drive into the bay.
  - c) Connect the data cable to the drive.
  - d) Connect the power cable to the drive.
  - e) Secure the drive to the bay chassis with screws.
3. Check whether the drive is accessible.
  - a) Plug all the peripherals back into the system.

 **Note:** You can leave the case open until the end of the activity.

  - b) Restart the computer.
  - c) If necessary, access CMOS, enable the disk, and then exit CMOS and save your settings.
4. Partition and format the new drive as an NTFS drive.
  - a) Log on to Windows with your assigned user name and password.
  - b) On the Desktop, right-click the **Start menu** button and select **Computer Management**.
  - c) In the left pane, select **Disk Management**.
  - d) If the **Initialize Disk** window is displayed, select **MBR** if the new drive is smaller than 2 TB or **GPT** if the drive is larger than 2 TB. Select **OK**.
  - e) If necessary, maximize the **Disk Management** window to view the new drive. It may be labeled **Disk 1 Unallocated**.
  - f) Right-click the unallocated space for the new disk.
  - g) Select **New Simple Volume**. The **New Simple Volume** wizard starts.

- h) Select **Next**.
- i) In the **Simple volume size in MB** text box, type **20000**
- j) Select **Next**.
- k) From the **Assign the following drive letter** drop-down list, select **S**.
- l) Select **Next**.
- m) On the **Format Partition** page, verify that **NTFS** is selected and select **Next**.



**Note:** To save time during class, you can check the **Perform a Quick Format** option.

- n) Select **Finish**.
- o) Close the new drive window.
- p) Close **Computer Management**.
- q) In the **Auto Play** dialog window, click **Open folder** to view files.
- r) Close the **New Volume (s:)** window.

## RAID

The *Redundant Array of Independent Disks (RAID)* standards are a set of vendor-independent specifications for improvements in performance and/or fault-tolerant configurations on multiple-disk systems. In a fault-tolerant configuration, if one or more of the disks fails, data may be recovered from the remaining disks.



**Note:** The original RAID specifications were titled Redundant Array of Inexpensive Disks. As the disk cost of RAID implementations has become less of a factor, the term "Independent" disks has been widely adopted instead.

## RAID Standards

RAID can be implemented through operating system software, but hardware-based RAID implementations are more efficient and are more widely deployed.

Hardware-based RAID requires a card, or controller, to show the different disks to the computer as a single drive. These cards are usually a PCI or PCIe card, but can also be already built into the motherboard.

In the Windows 8 family of operating systems, RAID is known as *Storage Spaces*.

## Common RAID Levels

There are several RAID levels, each of which provides a different combination of features and efficiencies. RAID levels are identified by number; RAID 0, RAID 1, RAID 5, and RAID 10 are the most common implementations.

RAID Level	Description
RAID 0	RAID level 0 implements <i>striping</i> , which is the process of spreading data across multiple drives. Striping can dramatically improve read and write performance. Striping provides no fault tolerance, however; because the data is spread across multiple drives, if any one of the drives fails, you will lose all of your data. You must have at least two physical disk drives to implement striping, and the largest size RAID-0 partition that can be created is equal to the smallest available individual partition times the number of drives in the set. For instance, combining a 37 GB drive and a 100 MB drive in a RAID 0 set would result in a 200 MB partition; the balance of the 37 GB drive could not be included in the set (although it would remain available for use in other partitions).

<b>RAID Level</b>	<b>Description</b>
RAID 1	In RAID level 1, data from an entire partition is duplicated on two identical drives by either mirroring or duplexing. In <i>mirroring</i> , the two disks share a drive controller. In <i>disk duplexing</i> , each disk has its own drive controller, so the controller card is not a single point of failure. Data is written to both halves of the mirror simultaneously. This redundancy provides fault tolerance and provides for quick failure recovery, but the storage overhead consumes half the available space. The work of reading the data can be split between both drives, improving performance. However, with the increased read speed, a RAID 1 implementation loses some write speed.
RAID 5	RAID level 5 spreads data byte by byte across multiple drives, with parity information also spread across multiple drives. You need at least three physical disk drives that have the same capacity and are the same type. If one drive fails, the parity information on the remaining drives can be used to reconstruct the lost data. In the event of a drive failure, data recovery is not instantaneous (as it is in RAID 1); the bad drive needs to be replaced, and then the missing data needs to be reconstructed. With RAID 5, disk performance is enhanced because more than one read and write can occur simultaneously. However, the parity calculations create some write-performance overhead. Storage overhead is at a ratio of one to the number of drives in the set (for example, 1/3 overhead in a three-drive set or 1/10 overhead in a 10-drive set), so the more drives that are in the set, the less overhead, and the better performance. In the event of multiple drive failures, all data will be irrecoverable.
RAID 10	RAID 10, or RAID 1+0, combines two RAID levels into one. It uses RAID 1 and RAID 0 to provide both mirroring from level 1 and striping from level 0. RAID 10 uses a minimum of four disks, in two disk mirrored blocks. This configuration gives you better performance and system redundancy.



**Note:** For additional information, check out the LearnTO **Select the Appropriate RAID Level** presentation in the LearnTOs for this course on your CHOICE Course screen.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on **How to Install and Configure RAID**.

# ACTIVITY 8–5

## Installing and Configuring RAID

### Before You Begin

You have installed a second drive in your Windows 8 computer.

### Scenario

You have had a request from a user to configure RAID 1 on his PC. You already installed a second hard drive for this purpose.

1. Access the **Storage Spaces** utility.
  - a) Display the **Charms** bar.
  - b) Using the **Search** charm, search for **storage spaces**
  - c) From the results, select **Storage Spaces**.
2. Create a new pool and storage space.
  - a) In the **Storage Spaces** window, select **Create a new pool and storage space**.
  - b) In the **User Account Control** dialog box, select **Yes**.
  - c) Check the available formatted drive.
  - d) Select **Create Pool**.
3. Specify a name, resiliency type, and size for the storage space.
  - a) In the **Create a storage space** dialog box, under **Name and drive letter**, in the **Name** text box, type **My RAID Storage Space**
  - b) Accept the default drive letter.
  - c) Verify that the **File system** is set to **NTFS**.
  - d) Set the size as needed, based on information provided by your instructor.
  - e) Select **Create storage space**.
4. Open **File Explorer** and examine the drive.

# TOPIC D

## Configure the System Firmware

In the previous topics, you focused on the basic internal storage devices that enable a computer to run, but what about how the computer communicates with all these devices? In this topic, you will configure settings in the system firmware.

How does the computer know when to start devices within the computer? Without the system firmware managing the system components within the computer system, the devices simply would not be accessible. As an A+ technician, you must fully understand how the system firmware operates and how to configure it to enable a customized computing environment for users.

### System Firmware

*Firmware* straddles a gray area between hardware and software. Firmware is specialized software stored in memory chips that store information whether or not power to the computer is on. It is most often written on an electronically reprogrammable chip so that it can be updated with a special program to fix any errors that might be discovered after a computer is purchased, or to support updated hardware components.

Traditionally, systems booted up using BIOS (Basic Input/Output System) system firmware. However, the limitations such as lack of support for large drives and a plain text non-mouseable interface, meant a new approach to system firmware was needed. UEFI (Unified Extensible Firmware Interface) allows support for larger hard drives, provides a GUI interface, supports remote diagnostic and repair, and paves the way for a more secure system boot.

Most of the functions available in system firmware are available in both BIOS and UEFI. They are implemented differently and may have limitations. They are both interpreters between system hardware and the operating system that run at system startup to initialize hardware and launch the operating system.

- *BIOS memory* stores information about the computer setup that the system firmware refers to each time the computer starts. The BIOS information is stored in non-volatile *Electrically Erasable Programmable Read-Only Memory (EEPROM)*, or flash memory chips. Because you can write new information to BIOS memory, you can store information about system changes, such as new components that you add to your system. The computer will look for the component each time it is turned on.
  - When a system boots using BIOS, the first sector of the boot drive is read. This sector of the drive contains information about the initialization address. The boot device is initialized based on BIOS settings, and then operation is handed off from the system BIOS firmware to the operating system code.
  - BIOS uses the Master Boot Record (MBR), which is a table of 32-bit entries. MBR supports up to 4 physical disk partitions, each with a maximum size of 2 TB. The MBR can use only one bootloader.
  - UEFI stores information in a .efi file on the hard drive in the EFI System Partition (ESP). This partition also contains the bootloader for the OS. UEFI uses a GUID partition table (GPT), which is a table of 64-bit entries. It supports unlimited partitions (although in practice this is limited to 128 partitions), each with a maximum size of about 8 to 9 ZB (Microsoft Windows limits the size to 256 TB). ESP can store multiple bootloaders. This is useful if you have multiple operating systems that use different bootloaders.
  - Many functions are available in the pre-boot environment, including video and storage services.
  - Another advantage UEFI has over BIOS is secure boot. UEFI uses a private key created by the motherboard manufacturer. This secure boot feature is designed to prevent boot-time

viruses from running. Secure boot also helps ensure that the computer boots using only trusted firmware.



**Note:** For additional information, check out the LearnTO **Work with the System Firmware** presentation in the LearnTOs for this course on your CHOICE Course screen.

## Types of ROM

ROM is memory that is non-volatile. The original ROM chips could not be altered after the program code was placed on the ROM chip. As time went on, though, users needed the ability to update the information stored on ROM chips. Over the years, various chips have been created that perform the function of ROM, but can be updated one way or another. These are referred to as programmable ROM (PROM).

EEPROM (electronically erasable PROM) is a chip that can be reprogrammed using software from the BIOS or chip manufacturer using a process called flashing. It is also known as Flash ROM.

## Firmware Upgrades

Updating firmware electronically is called flashing. There are a few reasons why you should consider upgrading the system firmware, including:

- To provide support for new hardware, such as a large hard drive or removable storage device.
- To fix bugs that prevent the operating system from installing or running properly.
- To enable advanced Plug-and-Play or advanced power management features
- To be eligible for vendor support.

The temptation to upgrade the system firmware simply because a newer revision is available should be avoided. Upgrading the system firmware or other firmware can be damaging to the PC if it is not done correctly. If you improperly flash the system firmware, or if the flash process is interrupted by a power failure, or even if you use the wrong BIOS image to flash the system BIOS, you can corrupt the BIOS chip so that the system will no longer boot. Often, your recovery options will be limited, but they should be listed on the manufacturer's support website.

UEFI is updated through package updates. The updates, along with the appropriate updater tool, are downloaded from the manufacturer.

## System Firmware Components

When the system firmware is activated on startup, it determines which components are present and when they are accessed during the boot process. Any time you change a hardware component, you should check the system firmware settings to see if they also need to be changed for the system to recognize the new hardware. Also, you can configure system firmware without needing to open the chassis. Several system components can be configured through the system firmware:

- RAM
- Hard drives
- Optical drives
- CPU

## System Firmware Configuration Options

System firmware configuration options can be altered at any time by changing the settings within the system firmware configuration utility. Many times when you replace or change a hardware component, the system firmware configuration will need to be changed so that the system firmware can recognize the newly installed hardware. System firmware settings can be configured without having to physically open the system case of the computer. The extent to which you can use system firmware to configure a computer depends heavily on the manufacturer of the particular system

firmware; however, in most cases, you should be able to configure at least the following—and possibly much more—by using the system firmware configuration utility.

<b>Configuration Option</b>	<b>Description</b>
General	<p>General settings include:</p> <ul style="list-style-type: none"> <li>• Motherboard information, including the manufacturer, brand, and CPU vendor.</li> <li>• System date and time. You can use the system firmware Setup program to set the PC's real-time clock. (You can also use command prompt date and time commands to reset the real-time clock.)</li> <li>• Boot sequence. You can specify the order that drives are checked for the operating system.</li> <li>• System firmware version. This can be used when looking for firmware updates for the system firmware chip.</li> </ul>
Security settings	<p>You can specify a number of security functions:</p> <ul style="list-style-type: none"> <li>• Manage passwords, including both administrator and system passwords.</li> <li>• Configuring support for full drive encryption.</li> <li>• Enable and disable the trusted platform module (TPM) security feature. When enabled, the system firmware will load the TPM and make it available within the operating system.</li> <li>• In some laptop computers, laptop-tracking software such as LoJack® for Laptops can be configured to help recover lost or stolen laptops.</li> <li>• The Secure Boot feature is part of UEFI. It is designed to ensure that the firmware is authentic and to prevent pre-boot viruses from being launched.</li> </ul>
Enabling and disabling devices	<p>Many devices can be configured by modifying the system firmware settings. You can:</p> <ul style="list-style-type: none"> <li>• Specify the type and size of the hard disk drives attached to the system.</li> <li>• Enable and disable advanced drive settings, such as RAID settings.</li> <li>• Specify the preferred default monitor.</li> <li>• Specify settings such as powering down components (like the display device, video card, and hard drives) when the components have not been used for a specified time period, as well as options and time limits for standby and suspend modes. You can also disable or enable global power management.</li> </ul>
Clock speed	<p>The clock speed for the CPU can be adjusted in the system firmware. In some modern systems, the CPU type and speed is automatically adjusted, but in older systems, you will verify that the clock speed is optimized for the CPU installed on the motherboard.</p>
System configuration	<p>Allows you to configure various system components such as integrated network interface cards (NICs), USB controllers, parallel ports, and serial ports.</p>
Video	<p>Allows you to change the video controller settings when more than one video card is installed.</p>
Performance	<p>Allows you to change CPU settings such as enabling or disabling multicore support and changing processor modes.</p>

<b>Configuration Option</b>	<b>Description</b>
Virtualization support	If the CPU supports virtualization, then you can use the system firmware setup utility to enable or disable the various virtualization settings available. Virtualization support within the system firmware is dependent on the OEM model. Most modern systems will support virtualization.
Power management	Allows you to configure different power options available, such as how the system will recover from a power loss and other advanced power options.
Maintenance	Allows you to verify and set service and asset tags used when a computer needs further maintenance from an outside vendor. The asset tag is used to identify the computer within the system firmware. It is usually a four or five digit number.

## Secure Boot

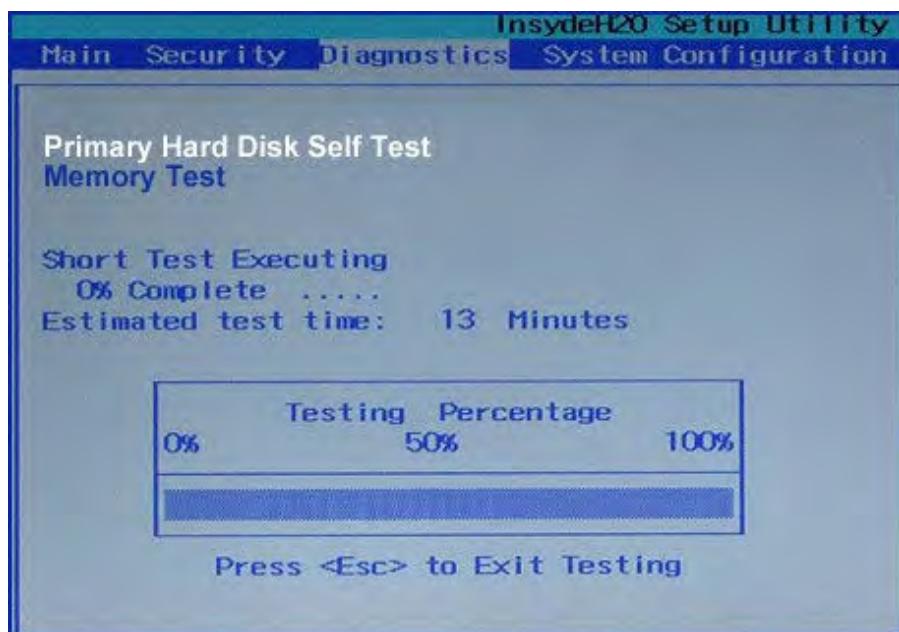
The UEFI 2.2 feature Secure Boot prevents drivers from loading that haven't been signed with an appropriate key. This feature is enabled by default and should not be disabled unless absolutely required. Windows 8 and some Linux distributions make use of the Secure Boot feature.

On Windows 8.1 systems, you might need to disable the Secure Boot feature in order for some hardware to work, or if you are using another operating system such as a previous version of Windows or some Linux distributions. Secure Boot cannot be disabled on Windows RT.

## Built-in System Firmware Diagnostics

Most BIOS and UEFI systems come with a built-in diagnostics utility that can be used to troubleshoot issues and verify proper functionality. Most diagnostic tools allow you to test the system memory and the entire system. The tool will thoroughly test each system component and display test results which are usually a pass or fail. This will help you to identify which component is having issues. Most utilities will run tests on the following components:

- Video cards
- System memory
- Hard drives
- Optical drives



*Figure 8–3: Built-in diagnostics testing the primary hard disk.*

## System Firmware Monitoring Capabilities

Most system firmware has monitoring capabilities built in and can allow you to check a number of system activities for issues. To access the monitoring options, you must enter the system firmware during start up, by pressing one of the function keys. The specific function key will depend on the type of motherboard installed, so verify the key you need to press on startup to access the BIOS or UEFI configuration utility.

<b>Monitoring Capability</b>	<b>Description</b>
Temperature	The temperature of the CPU, motherboard, and overall system can usually be checked within the system BIOS. You can use this option to check for overheating and to verify that the CPU is running within its safe temperature range.
Fan speeds	Within the BIOS, you can verify the fan speed for your CPU, and any system fans installed in the computer. Keep in mind that you must balance the rotations per minute (RPM) speed of the fans with the temperature of the CPU and motherboard.
Intrusion detection/ notification	Most modern BIOS will have some security functions built in. This includes system intrusion detection. The intrusion detection is implemented using a sensor that alerts the system BIOS when the case cover of the system has been removed.
Voltage	The system voltage settings are strictly based on the specific hardware you have installed in the system, such as type of motherboard and CPU. The BIOS allows you to change the voltage configuration for each device installed. Once in the BIOS, you will look for: <ul style="list-style-type: none"> <li>• Vcore, or VCC, which is the CPU voltage reading.</li> <li>• Memory voltage, which displays the RAM voltage settings.</li> <li>• VDD voltage, which displays the motherboard's voltage. This rating is driven by the Northbridge chip of the board.</li> <li>• If there is a graphics card installed, then you will see the AGP voltage setting displayed.</li> </ul>

Monitoring Capability	Description
Clock	You can verify that the BIOS clock is accurate by verifying the time within the system BIOS.
Bus speed	In some cases, you may find the need to monitor the bus speed, and to make sure that the overall CPU speed is in line with the bus speed. Bus speeds are usually set by the manufacturer at a natural clock rate or an enhanced clock rate.  For example, when you have a processor with a CPU speed of 1.82 GHz clock speed, you would need to set the bus speed to 166 MHz with the multiplier of 11. (166 MHz x 11 = 1.826 GHz).



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Configure System Firmware Settings.

# ACTIVITY 8-6

## Exploring and Configuring the System Firmware

### Scenario

In this activity, you will explore the configuration options available to you in the system BIOS or UEFI utility.

1. Explore the system firmware utility.
  - a) Restart your computer system.
  - b) As the computer restarts, press the system firmware access key. You might want to record this key for later use.
  - c) Navigate to the **System Setup** menu option.

Depending on the system firmware installed on your computer, this menu might have a different name.
  - d) Browse through the available configuration options.
  - e) Locate the motherboard settings and record the firmware version.

This information can be helpful if you ever have to update the system firmware to solve a hardware issue.
2. Change the boot order.
  - a) Navigate to the **Boot Sequence** setting.

Depending on the system firmware installed on your computer, this setting might have a slightly different name.
  - b) Examine the current boot order.

In older systems, the floppy drive was often configured as the primary boot device. In newer systems, a USB storage device or the internal hard disk might be configured as the primary boot device.
  - c) Change the boot order to the following:
    - Optical drive
    - Internal hard disk 1
    - Internal hard disk 2
    - USB storage device
  - d) Save the change.
3. Update the system date and time.
  - a) Navigate to the **Date and Time** setting.

Depending on the system firmware installed on your computer, this setting might have a slightly different name.
  - b) Examine the current setting. If the date and time appear to be correct, you can skip this and the next substep. If the date and time are not correct, adjust them to match the current date and time.
  - c) Save your changes.
4. Examine system monitoring options.
  - a) Navigate to the **Hardware Monitoring** menu option.

Depending on the BIOS or UEFI installed on your computer, this setting might have a different name, such as **PC Health**, **CPU Temperature**, or some other name.
  - b) Examine the CPU temperature reading.

Normal CPU temperatures range from 30 to 60 degrees Celsius.

5. Verify the BIOS or UEFI changes.
    - a) Exit the BIOS or UEFI utility.
    - b) Log on to Windows.
    - c) If you changed the date and time, verify that the system date and time has been updated in the taskbar.
-

# TOPIC E

## Troubleshoot Hard Drives and RAID Arrays

So far in this lesson, you've examined the various forms of data storage found in most PCs, and you've performed troubleshooting on RAM. You'll also need to be well versed in troubleshooting other types of data storage options. In this topic, you will troubleshoot hard drives and Redundant Array of Independent Disks (RAID) arrays.

End users rely on the hard drives in their PCs to store important system information and personal or professional data and files. Without a hard drive that works properly, the computer system is essentially worthless. As an A+ technician, you will likely be called upon to fix or troubleshoot common problems with hard drives. In this topic, you will troubleshoot hard drives and RAID arrays.

### Drive and Array Troubleshooting Tools

To resolve hard drive and RAID array problems, there is a variety of different physical tools and software utility tools available.

<i>Tool</i>	<i>Description</i>
Screwdriver	In order to repair a faulty hard drive, you will need a screwdriver to remove the drive from the drive bay within the computer case.
External enclosures	<i>External enclosures</i> protect the hard drive by providing a strong barrier typically made of plastic all the way around the disk. Most enclosures also provide power to the drive through an external connection, typically through a universal serial bus (USB) port.
CHKDSK	This utility is also referred to as Check Disk. It is used to verify the logical integrity of a file system. With the /f switch, chkdsk.exe can repair the file system data. Enter <code>chkdsk "drive letter" /f</code> in the <b>Run</b> dialog box or at the command line. With the /r switch, chkdsk can locate bad sectors on the disk and recover any readable information. Entering <code>chkdsk /?</code> displays a list of all available switches.
BOOTREC	Bootrec.exe is run from within the Windows RE. This is the system recovery done from the Windows Vista or Windows 7 DVD. After booting from the installation media in the DVD drive, selecting <b>Repair your computer</b> , and selecting the operating system to repair, you can open a command prompt and run bootrec.exe. It can be used to fix the master boot record and the boot sector, to rebuild the BCD store, and to scan for items not in the BCD store.
DISKPART	DISKPART is a superset of the commands available in the GUI tool Disk Management. It should be used with extreme caution as you can easily remove a partition that contains data.
FORMAT	The format utility can be used to format partitions to a selected file system. You can run the <code>format</code> command right from the command line, or right-click any drive letter in Windows® Explorer and select the <b>Format</b> option.
FDISK	Use to create and manage partitions on a hard disk. You can run the <code>fdisk</code> command at the command line to open the utility. The tool can be used to not only create partitions, but also to change, delete, and view current partitions.

Tool	Description
File recovery software	<p><i>File recovery software</i> is used to recover deleted files from your computer system. In many cases, files that were moved to the recycle bin, then emptied, can still be recovered. Some files may still live on the hard disk. There are a number of free software programs that will provide recovery functions:</p> <ul style="list-style-type: none"> <li>• Recuva</li> <li>• Glary Undelete</li> <li>• Pandora Recovery</li> </ul>

## Common Hard Drive Symptoms

When you are troubleshooting hard drives, you will run into a number of different issues with numerous potential solutions.

Hard Drive Symptom	Possible Problems and Solutions
Failure to boot	If you receive an error that says "Not Ready—System Halted," then the drive is damaged or a data cable is not connected properly. You should check the drive for physical damage and verify that the connections are properly attached to the drive.
POST error	<p>POST errors in the 17xx range could indicate several different issues, including:</p> <ul style="list-style-type: none"> <li>• 1701: Drive not found</li> <li>• 1702: Hard drive adapter not found</li> <li>• 1703: Hard drive failure</li> <li>• 1704: Hard drive or adapter failure</li> <li>• 1780, 1790: Hard drive 0 failed</li> <li>• 1781, 1791: Hard drive 1 failed</li> <li>• 1782: Hard drive controller failed</li> </ul> <p>You should check for damage to the connections and reconnect the drive. You may need to replace any component that has failed.</p>
Drive not recognized	If your hard drive is not recognized by the system when it boots up, then verify that the system has been set to boot from the hard drive in the system firmware settings in the boot priority list. You may also need to verify that the correct drivers for the hard drive are installed.
Drive read/write failure	<p>The drive might have been infected with a virus. Run an antivirus utility to find and remove any infections.</p> <p>If you suspect that the drive is not writing and reading data properly, then it could mean that there are bad sectors on the drive, the drive has failed, or the drive has been infected by a virus. Sometimes, issues that seem to be device-specific are actually virus infections that can cause physical damage as well, but in most cases, the damage is limited to the data stored on the device.</p> <p>Start by running CHKDSK to attempt to recover data from any damaged sectors of the drive. Use <b>Device Manager</b> to resolve any resource conflicts and indications of drive failure.</p>
Computer will not boot	If the computer will not boot up, then it could be a sign that the drive is disconnected, is damaged, is not recognized by the system firmware, or is not configured properly by the system firmware. Start by enabling the drive in the BIOS or UEFI setup utility and check the startup settings, then visually inspect the drive for damage and reconnect it to the system.

<b>Hard Drive Symptom</b>	<b>Possible Problems and Solutions</b>
Grinding noises	If you hear grinding noises coming from the system, then it could be a sign that the drive is physically damaged. If there is data that needs to be recovered, then power down the system immediately because powering the drive at all will make the damage worse. Next, remove the damaged drive and send it to a suitable recovery facility, where it will be rebuilt in a cleanroom, and the data can be extracted.
Loud clicking noises	Loud clicking noises can be a sign that the drive is trying to park the drive head but cannot park the head. You can try turning off power management to the drive. This will allow the drive to only park its head when the device is shut down.
Possible data corruption	If you suspect that the data is corrupted, then the system may not have been shut down properly or the drive is either in the process of failing or has been infected with a virus. In this case, all you can really do is educate users to be aware of this and make sure that they are shutting the system down properly every time. In the event that it may be a virus, run antivirus software to clean the computer of all infected files.
Slow performance	<p>Slow hard drive performance can mean that the drive is too full or fragmented, the controller is too slow, or the wrong cable type was used to connect the drive. To resolve these issues:</p> <ul style="list-style-type: none"> <li>• Delete all unneeded files.</li> <li>• Defragment the drive.</li> <li>• Verify and replace the hard drive cable, if necessary.</li> </ul>
External drive issues	<p>External drives come with their own types of issues, including:</p> <ul style="list-style-type: none"> <li>• The cable connecting the hard drive to the PC may be bad, so check it for physical damage.</li> <li>• The USB port may not be functioning, so try connecting to another USB port and make sure the connection is successful.</li> <li>• If the drive requires an external power supply, then supply an external power source to the drive.</li> </ul>
Removable drive issues	Removable drives can be problematic if the drive is not configured properly, or the hard drive bay cable is not connected securely to the system board. In some cases, issues can arise due to a power issue.
OS not found	<p>An “Operating system not found” or “Missing Operating System” error can be common after an operating system is either reinstalled or has been reconfigured. In this case, the system BIOS does not detect the hard drive or the hard drive may be damaged or corrupted.</p>
BSOD	<p>Verify that the system BIOS settings are correct and that the hard disk is recognized within the system, or replace the defective hard drive.</p> <p>This may also be a symptom of a Master Boot Record (MBR) problem. The MBR is specific to each operating system, so you will need to check the manufacturer's documentation and website for possible solutions.</p> <p>BSOD, or often referred to as the “Blue Screen of Death,” is a system <i>stop error</i> that is severe enough to stop all processes and shut the system down without warning. BSOD errors can be a sign that the hard drive is damaged or is not working properly.</p>

## SATA Troubleshooting Tips

There are several points to keep in mind when troubleshooting Serial Advanced Technology Attachment (SATA) drive problems.

<b>SATA Issue</b>	<b>Description</b>
Controller card	Not all SATA controller cards are supported on all operating systems. Check the vendor specifications for the operating system or software you are using.
Controller driver	SATA drives themselves do not require drivers, but the SATA controller does. Ensure that you are using the latest version.
Drive not detected	If you install a fresh copy of your operating system and the SATA drive is not detected, then restart the setup process and press <b>F6</b> when prompted to install the driver.
Drive size limitation	If the SATA controller drivers are not loaded during the operating system installation, then the drive will only report the 137 GB capacity supported natively by the operating system.
Speed limitation	1.5 gigabytes per second (GBps) SATA cards do not always auto negotiate with newer 3.0 GBps drives. Use jumper settings on the drive to limit the transfer rate to 1.5 GBps.

## Common Solid State Device Issues

Solid state storage device issues can include:

- Limited and slower erase-write cycles. Flash memory devices do not last as long as traditional hard drives and often performance will suffer because of this. Usually at around 100,000 cycles, the devices will begin to break down.
- Power consumption. Solid State Drive (SSD) devices do not have their own power source and will consume power from the system, so if the main device or system cannot provide the right amount of power, then the SSD will not be accessible.

## Common Array Issues

When configuring RAID arrays, you may come across a number of issues that prevent proper functioning of the drives.

<b>RAID Array Symptom</b>	<b>Possible Problems and Solutions</b>
RAID not found	If RAID is not found when the computer boots up, it could be a sign that either RAID is not configured within the system firmware or that the motherboard does not recognize RAID. You must verify that the motherboard installed in the system does in fact support RAID. You may want to refer to the manufacturer's documentation.
RAID stops working	If RAID stops working suddenly, then that could mean that the settings have changed within the system firmware. If you have made other configurations or replaced a component in the computer, then those configurations may have conflicted with the RAID settings.  In the system firmware configuration utility, verify that the drive configuration is set to RAID. Also check the motherboard documentation to see if RAID is fully supported by the board installed in the computer.  If there is a non-system board RAID controller used, then check the controller's firmware, and verify that the settings are properly configured.

## SMART

*Self-Monitoring, Analysis, and Reporting Technology* (SMART) is a monitoring system that can help anticipate storage drive failures. Indicators of failure that SMART monitors for include excess heat, excess noise, damaged sectors, or read/write errors. Modern SMART systems also include functionality for repairing damaged sectors, and can maintain monitoring functionality even when the drive is not in use.

Most hard drives today run SMART by default. There is no robust program in Windows that allows you to review your drive's SMART data, so you'll need to download a third party program like HD Tune, CrystalDiskInfo, and SpeedFan in order to see detailed information. This information is dependent on the drive manufacturer, but often includes:

- Number of reallocated sectors.
- Number of uncorrectable errors.
- Spin up time.
- Throughput performance.
- Temperature in Celsius.
- Numbered of canceled operations due to drive timeout.

The manufacturer specifies a certain threshold for these statistics, and when the threshold is met, the SMART system will produce an error. If you receive a SMART error, back up your data as soon as possible. Depending on the nature of the error, you may be able to fix the problem. For example, if SMART detects excessive heat, you can try and resolve the issue by improving ventilation around the drive. However, many errors are not easily fixable and will require you to replace the drive.

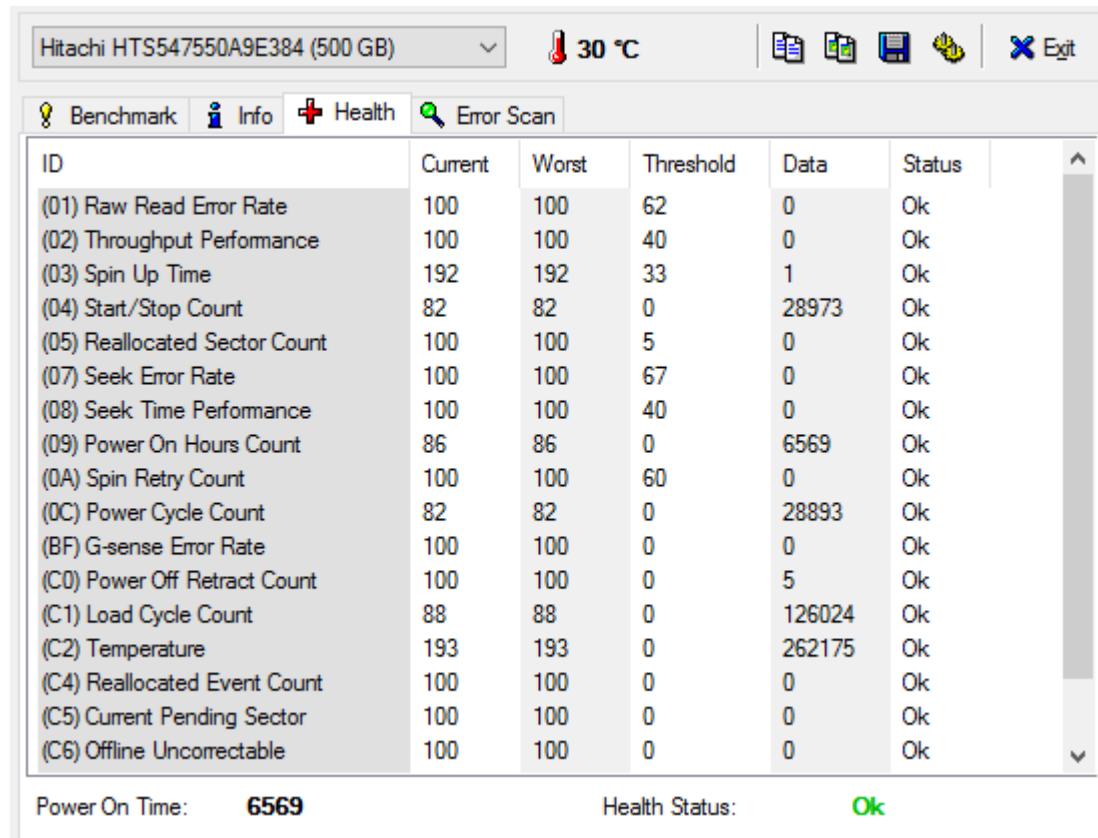


Figure 8-4: A report of SMART data.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Troubleshoot Hard Drives and RAID Arrays.

# ACTIVITY 8-7

## Troubleshooting Hard Drive Problems

### Before You Begin

Your instructor will introduce a drive problem on your system.

### Scenario

In this activity, you will troubleshoot different issues relating to hard drives.

#### 1. Problem #1: Grinding Noises

A user has reported that there are grinding noises coming from her computer case. Once you take a closer look, you suspect that it is the hard drive. What is the possible cause and solution to this type of issue?

- The hard drive is physically damaged, probably due to a head crash, so the drive must be replaced.
- A virus has attacked the hard drive, so use antivirus software to mitigate the issues.
- Data is corrupt on the drive, and has not been shut down correctly.

#### 2. Problem #2: A Computer Won't Start

A user has reported that her computer cannot boot and is getting an error message at POST. Diagnose and correct the issue.

- a) Perform a cold boot.
- b) Verify that BIOS lists the correct drive settings.
- c) Listen to the drive or touch the drive to determine if it is spinning during POST.
- d) Using your multimeter, verify that power connection readings are +12 V for Pin 1 and +5 V for Pin 4. Pins 2 and 3 should be grounded.
- e) Verify that the data cable is correctly oriented.
- f) Check the drive settings
- g) If nothing else corrects the problem, replace the drive.

#### 3. Problem #3: A Second Hard Drive is Not Recognized

You recently installed a second hard drive into a user's system. He is now reporting that the drive is not showing up or is not recognized. You know that one of the things you forgot to check when you first performed the installation was system firmware settings for the drive. What in particular do you need to check in system firmware for this problem?

#### 4. Problem #3: A Second Hard Drive is Not Recognized (Continued)

Another thing you should check when a second hard drive is not recognized is that the drive was installed correctly. What exactly should you be checking?

**5. Problem #4: The Drive Letter for a Second Hard Drive is Not Accessible**

A second hard drive was properly installed, but you cannot access it by its drive letter. What should be your next step?

**6. Problem #5: Hard Drive Data Access Issues**

A user is encountering the following problem: Her computer boots fine and everything works until the user tries to access data on the second hard drive, the D drive. The message "Can't Access This Drive" is displayed when she tries to access the D drive. The user would also like an explanation about what the error message means. List some of the steps you might take to resolve this problem.

**7. Problem #5: Hard Drive Data Access Issues (Continued)**

When a user tries to access the hard drive containing his data, the system locks up and makes a clicking sound. From the command prompt, he can change to drive D, but when he tries to access a file or list the files on the drive, it locks up and begins clicking again. What steps might you take to attempt to resolve this problem? What is the most likely cause of the problem?

**8. Problem #5: Hard Drive Data Access Issues (Continued)**

A user reports that some of his folders have begun disappearing and some folder and file names are scrambled with strange characters in their names. What steps might you take to attempt to resolve this problem? What is the most likely cause of the problem?

**9. Problem #5: Hard Drive Data Access Issues (Continued)**

A user is questioning the difference between the sizes in GB and bytes. Why is there such a big difference? The disk reports in some places as 9.33 GB and in others as 10,025,000,960 bytes. Why is it not 10 GB?

---

## Summary

In this lesson, you managed a variety of data storage methods. You looked at the temporary storage provided by RAM as well as the long-term storage provided by storage devices and the various issues that might arise with these storage solutions. The ability to identify the cause of data storage issues and quickly resolve them will be an important part of an A+ technician's duties.

**Which types of storage devices have you worked with? Have you installed additional hard drives or replaced hard drives?**

**Which system firmware have you worked with, if any? What types of configuration did you perform?**



**Note:** Check your CHOICE Course screen for opportunities to interact with your classmates, peers, and the larger CHOICE online community about the topics covered in this course or other topics you are interested in. From the Course screen you can also access available resources for a more continuous learning experience.



9

# Installing and Configuring Microsoft Windows

**Lesson Time:** 3 hours

## Lesson Objectives

In this lesson, you will install and configure Microsoft Windows. You will:

- Implement client-side virtualization.
- Install the Microsoft Windows operating system.
- Use features of the Windows operating system.
- Configure Microsoft Windows.
- Perform a Windows upgrade.

## Lesson Introduction

So far in this course, you have learned in general about hardware and software, and have installed and configured many of the hardware components required for a computer system. Now it is time to install the most important software component—the operating system—so that all the hardware you've assembled so far can function together.

Since so many computers today come with operating system software installed by the vendor, an ordinary user might never need to install an operating system. As an IT professional, however, you might be called upon to install and configure operating systems for a variety of reasons: if the original installation does not meet a user's needs; if the system needs to be upgraded; if you are redeploying a system from one user to another; or even if you need to complete a brand new build and construct a computer entirely from scratch. In all of these cases, you will need to be able to install, configure, and optimize the computer's operating system.

# TOPIC A

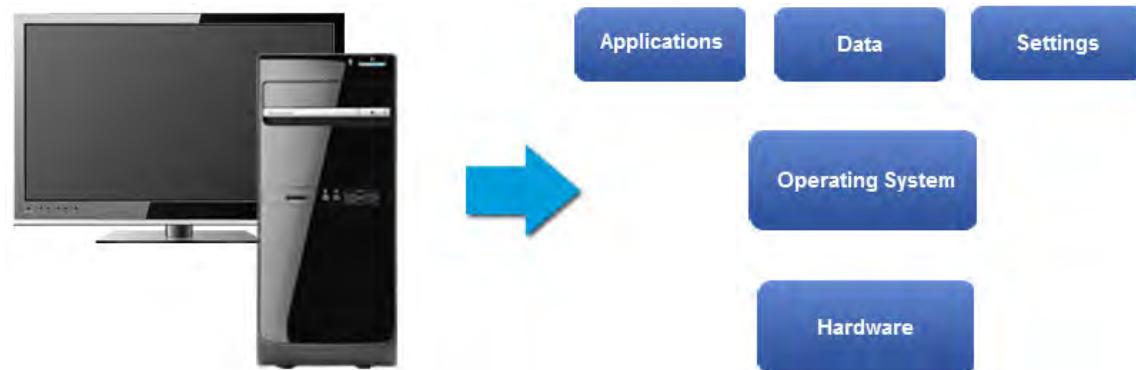
## Implement Client-Side Virtualization

In this lesson, you will install and configure the Windows® operating system. One or more of those operating systems can be leveraged using virtualization to improve performance or increase productivity for one or more computers. In this topic, you will implement client-side virtualization.

As organizations grow in size and scope, there is an increased need for more resources, especially when it comes to computing. Virtualization can help ease the growing pains of an organization by providing the opportunity to leverage one computer and one operating system for use over many systems, and save valuable time and resources when it comes to hardware, software, and personnel. As an A+ technician, you may need to know what is needed to set up a virtualized environment.

### Virtualization

*Virtualization* is the technological process of creating a virtual version of a computing environment by separating the elements of the computing environment—the applications, operating system, programs, documents, and more—from each other and from any physical hardware by using an additional software application. Virtualization can provide flexibility and scalability for organizations where the costs for hardware and software and the IT infrastructure needed to maintain them both continue to increase. It can increase resource utilization by allowing those resources to be pooled and leveraged as part of a virtual infrastructure, and it can provide for centralized administration and management of all the resources being used throughout the organization.



**Figure 9–1: Virtualization.**

Although you can virtualize a stand-alone computer, you will reap the greatest benefits by integrating virtualization into a networked environment.

- *Client-side virtualization* takes place at the endpoints, the desktop environments themselves. Client-side virtualization separates the elements of a user's logical desktop environment—the applications, operating system, configuration settings, and more—and divides them from each other and from the physical hardware or a physical machine. With desktop virtualization, a single user can run multiple operating systems on one machine simultaneously and seamlessly; a single user can interact with their computer and all of their applications remotely from a mobile device; or numerous users can access and maintain their own individual desktop environments via a single and centrally managed physical device which can either be co-located to the virtualized environments or operate from a remote location. This type of virtualization environment allows multiple virtualized machines to run on a single device with no impact on the host's file system, registry, and OS.
- *Server (or server-side) virtualization* takes place centrally at the server or data center. Server virtualization utilizes one logical device, typically the server, to act as the host machine for the

guest machines that virtually use the applications and programs provided by the host. A software application is used to divide the single physical device into multiple isolated virtual devices.



**Note:** For additional information, check out the LearnTO **Identify Server-Side vs. Client-Side Virtualization** presentation in the LearnTOs for this course on your CHOICE Course screen.

## Purposes of Virtualization

Virtualization is a technology through which one or more simulated computers run within a physical computer. Virtualization offers a range of benefits and is a suitable solution largely because many user and system functions typically consume far less than the full power of a modern computer. For example, if a user's activities on her PC use just 30% of the computer's capabilities, 70% is being wasted. Through virtualization, potentially three VMs could be run on a single system at this level of utilization, giving similar performance levels. Full resource utilization takes full advantage of the resources you have available.

Some of the reasons you might use virtualization include:

- Test a new operating system or software application.
- Run software in isolation from the host operating system.
- Create a snapshot of the image, allowing you to restore the image to the virtual machine.
- Create test labs.
- Configure and deploy multiple computing environments.
- Set up and deploy systems for training classrooms.

## Hypervisors

Currently, the most popular virtualization products fall into two general categories:

- Bare metal hypervisors
- Host-based hypervisors

A *hypervisor*, or virtual machine manager, is the core virtualization software that enables multiple virtual computers to run on a single physical host. A bare metal hypervisor is one you install directly on the server's hardware—you don't install an operating system first. Bare-metal hypervisors are also known as native or Type-1 hypervisors.

A host-based hypervisor is one that runs within an operating system—you install the OS first and then install the hypervisor. This is also known as a Type-2 hypervisor.

Linux-based virtualization typically uses either Xen or Kernel-based Virtual Machine (KVM). These are both free hypervisors. Xen is a bare-metal hypervisor with built-in management tools. KVM is embedded in the Linux kernel.

Host-based hypervisors such as VirtualBox, Microsoft Virtual PC, and VMWare Workstation, run on top of an existing OS.

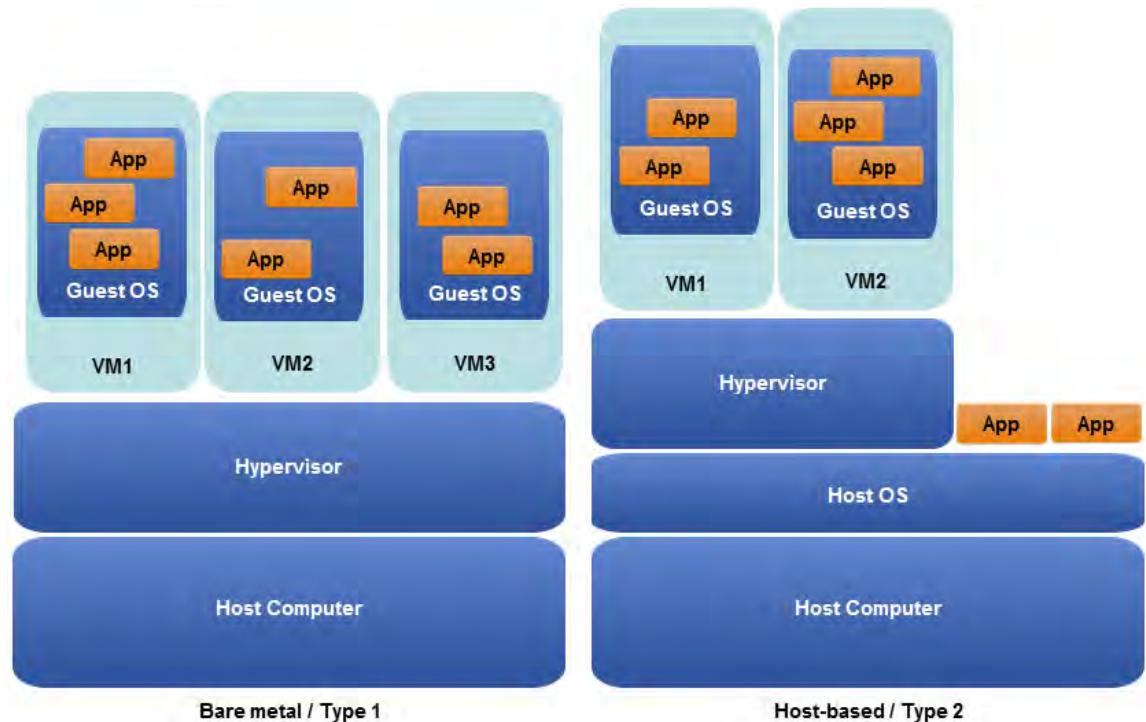


Figure 9–2: Hypervisors.

## Virtualization Resource Requirements

Before planning to migrate a system from a physical environment to a virtual environment, it is essential to ensure that the hardware intended to be virtualized meets the requirements of all virtual machines that are intended to be run on it. Also, the operating system running on the host hardware should be capable of supporting the guest operating systems running on each virtual machine. The resource requirements for virtualization will depend on what virtualization components will be supported within the environment. You should verify that the host computer has the required hardware and software components installed. This can include having enough RAM and hard drive capabilities and CPU power to run the virtualization software.

Early virtualization products required modifications to the guest OS, particularly hardware drivers. Modern CPUs include virtualization support features that enable the host to run unmodified guest operating systems. Intel's Virtualization Technology (VT or VT-x, which stands for Virtualization Technology for x86) and AMD's AMD-V (the V stands for virtualization) are the primary examples of CPU virtualization features.

Intel VT and AMD-V are not compatible, though they provide essentially the same features. Current host OS options typically support both of these virtualization technologies. Citrix XenServer, Oracle's VirtualBox, and Microsoft's Hyper-V are examples of host operating systems (or operating system components) that take advantage of CPU virtualization features and enable virtualization.

You will need to check the documentation for your system to see whether it has support for hardware virtualization. Virtualization support might need to be enabled in the system BIOS in order for it to be used.

## Emulator Requirements

In a client-side virtualization environment, the *emulator* is the software installed that allows the computer to virtually run another operating system or another instance of the same operating system. Each emulator manufacturer will have specific hardware and processor requirements that the client machine must have in order to be able to run the emulation software.

Client-side virtualization capabilities are still growing to meet consumer needs. Recent advances include mobile device hypervisors that give the devices the ability to access corporate resources without having to manage each device individually.

## Virtualization Security Requirements

Security requirements will primarily be based on an organization's security policy. There are, however, general security guidelines that should be followed when configuring a VM:

- Ensure that the VM has been equipped with appropriate antivirus software that is designed to protect both the physical client computer and the VM. Not all antivirus software packages can properly protect against malware on a VM. Always check with the manufacturer of the software before you install any program files on a VM. Issues can arise when the client machine running VM gets infected and there is no control in place to prevent the virus from propagating to the VM.
- Restrict users from copying files and applications from a traditional desktop machine to a VM. This vulnerability can lead to issues if infected files are copied, or sensitive data is copied to a shared VM.
- Regularly update and manage the security patches for both the physical client and the VM running on it.
- Enforce proper management of all VMs installed in client machines to prevent data leakage.
- Ensure that security measures are in place to isolate the VMs from the hypervisor. This prevents any viruses or infections from being spread between VMs and the hypervisor and vice versa.

## Virtualization Network Requirements

Generally for client computers running VMs, the normal network activity load will also suffice for running any VM-initiated network functions. You can create virtual switches to enable the virtual machines to communicate with the host computer, with other virtual machines, or with systems outside the virtualized environment. In Hyper-V, the three types of virtual switches are private, internal, and external.

<b>Switch Type</b>	<b>Description</b>
Private	VMs can communicate with other VMs on the same physical host.
Internal	In addition to communicating between VMs on the same physical host, the VM can also communicate with the host system.
External	In addition to the communication allowed on internal switches, the VMs can also communicate with external systems, outside of the physical host.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Implement Client-Side Virtualization.

# ACTIVITY 9–1

## Installing a Hypervisor

### Before You Begin

Installing Hyper-V on Windows 8 requires that you have the Pro or Enterprise edition.

### Scenario

Part of your job duties include testing new software, updates to operating systems, and other tasks that you don't want to do on your production system. Your usual test computer no longer works, so before you request a new computer, you decide to see if using Hyper-V might meet your needs. So, you decide to install Hyper-V on your Windows 8 Pro (or Enterprise) system. You want to be able to connect to the Internet from the virtual environment, so you will also create an external virtual switch.

1. Verify that your computer can run Hyper-V.
    - a) From the **Start** screen, type **pc info** then from the results, select **PC info**.
    - b) Under **Windows**, verify that the **Edition** is Windows 8.1 Pro or Windows 8.1 Enterprise.
    - c) Close the **PC Settings** window.
    - d) Open a web browser to your preferred search page.
    - e) Search for and download **coreinfo.exe**
    - f) Extract the files from coreinfo.exe to the root of the C drive.
    - g) Open a command prompt window with administrative privileges, then run **C:\coreinfo -v**  
Verify that SLAT support is available.
    - h) Shut down Windows.
    - i) Restart the computer and access the system firmware configuration.
    - j) Verify that virtualization support has been enabled.



**Note:** If your computer does not meet all of the requirements, you will not be able to install Hyper-V on your computer. If you want to use virtualization, you can use another product such as VirtualBox.
  - k) If necessary, save your changes and exit, or simply exit the system firmware configuration utility if no changes were made.
  - l) When the system reboots, log in as **username**
2. Install Hyper-V.
    - a) Using the **Search** charm, search for and select **turn windows features on or off**
    - b) In the **Windows Features** dialog box, check **Hyper-V**. Expand **Hyper-V** and verify that **Hyper-V Management Tools** and **Hyper-V Platform** are also checked, then select **OK**.
    - c) When the message **Windows completed the requested changes** is displayed, select **Restart now** to reboot the computer.
    - d) After the computer boots, log in.
    - e) From the **Start** screen or using the **Search** charm, type **hyper-v** and from the search results, select **Hyper-V Manager**.
  3. Create an external virtual switch.
    - a) In the left pane of **Hyper-V Manager**, select your computer.
    - b) In the **Actions** pane, select **Virtual Switch Manager**.
    - c) Under **What type of virtual switch do you want to create**, select **External**.

- d) Select **Create Virtual Switch**.
  - e) Type **Stu##-ExtSwitch** as the name for the virtual switch
  - f) If multiple network cards are installed, select the desired network card.
  - g) Select **OK**.
  - h) In the **Apply Networking Changes** dialog box, select **Yes** to acknowledge that pending changes may disrupt network connectivity.
-

# ACTIVITY 9–2

## Creating Virtual Machines

### Before You Begin

- You have installed Hyper-V (or another virtualization hypervisor) and created a virtual switch.
- Hyper-V Manager (or the hypervisor manager for an alternative hypervisor) is open.

### Scenario

Now that you have a hypervisor installed, you are ready to set up the virtual machine workspaces for the various operating systems you will install. You anticipate needing virtual machines for Windows 7 and for Linux. You still have some users that use Windows 7, so you want to be able to test software on that environment. Members of the Engineering department have requested that they be allowed to use Linux for some of their work, so you need to test that as well.

1. Create a Windows 7 virtual machine environment using the pre-configured settings.
  - a) In the **Actions** pane, select **New→Virtual Machine**.
  - b) On the **Before You Begin** page of the **New Virtual Machine Wizard**, select **Finish**.  
A virtual machine with 512 MB of RAM and no network connection is created.
  - c) In the center pane, under **Virtual Machines**, right-click **New Virtual Machine** and select **Rename**.
  - d) Enter **Win7Test##**
2. Connect the Windows 7 virtual machine to the virtual switch.
  - a) Select **Win7Test##**, then in the **Action** pane, select **Settings**.
  - b) Select **Network Adapter**.
  - c) Under **Virtual switch**, select **Stu##-ExtSwitch** and select **OK**.
3. Enable Dynamic Memory for the virtual machine.
  - a) Select **Win7Test##**, then in the **Action** pane, select **Settings**.
  - b) Select **Memory**.
  - c) Change the **Startup RAM** value to **2048**
  - d) In the right pane, under **Dynamic Memory**, check **Enable Dynamic Memory**.
  - e) Select **OK**.
4. Create a Linux virtual machine environment with customized settings.
  - a) In the **Actions** pane, select **New→Virtual Machine**.
  - b) On the **Before You Begin** page of the **New Virtual Machine Wizard**, select **Next**.
  - c) On the **Specify Name and Location** page, type **Stu##-Linux** and then select **Next**.
  - d) On the **Specify Generation** page, select **Generation 2** and then select **Next**.
  - e) On the **Assign Memory** page, type **2048** to specify the machine has 2 GB of RAM. Select **Next**.
  - f) On the **Configure Networking** page, connect the network adapter to **Stu##-ExtSwitch**. Select **Next**.
  - g) On the **Connect Virtual Hard Disk** page, accept the default name, location, and size to create a virtual hard disk so you can install an operating system on it. Select **Next**.
  - h) On the **Installation Options** page, select **Install an operating system later**.
  - i) Select **Next**.
  - j) Select **Finish**.

# TOPIC B

## Install Microsoft Windows

In this topic, you will install Windows 7 and Windows 8.1 operating systems. The fundamental installation method is to install the operating system from scratch. In this topic, you will perform a fresh installation of Microsoft® Windows®.

Being able to perform a fresh installation of Windows can be important if you have built a custom computer system from scratch, if the system you purchased from a vendor did not have the correct system installed, or if you are completely redeploying existing hardware from one system to another. The skills and information in this topic will help you plan and perform a fresh installation properly, for whatever your technical and business requirements might be.

### Windows System Requirements

Before installation, you must make sure that your hardware meets or exceeds the minimum requirements for the version of Windows you will install.



**Note:** If you will need to install Service Packs or updates as part of the installation process, you will need more available hard drive space to accommodate those files.

Operating System	Requirements
Windows® 8.1, Professional, or Enterprise	<ul style="list-style-type: none"> <li>• 1 GHz 32-bit (x86) or 64-bit (x64) processor.</li> <li>• 1 GB RAM (32-bit) or 2 GB RAM (64-bit).</li> <li>• 40 GB hard disk with a minimum of 20 GB of available space.</li> <li>• Support for DirectX 9 graphics; some programs may require support for DirectX 10 graphics or higher to provide optimal performance.</li> </ul>
Windows® 7 Home Premium, Professional, or Ultimate	<ul style="list-style-type: none"> <li>• 1 GHz 32-bit (x86) or 64-bit (x64) processor.</li> <li>• 1 GB RAM (32-bit) or 2 GB RAM (64-bit).</li> <li>• 40 GB hard disk with a minimum of 20 GB of available space.</li> <li>• Support for DirectX 9 graphics; some programs may require support for DirectX 10 graphics or higher to provide optimal performance.</li> </ul>
Windows Vista® Home Premium, Business, or Ultimate	<ul style="list-style-type: none"> <li>• 1 GHz 32-bit (x86) or 64-bit (x64) processor.</li> <li>• 1 GB of RAM.</li> <li>• 40 GB hard disk with a minimum of 15 GB of available space.</li> <li>• Support for DirectX 9 graphics and 128 MB of graphics memory available.</li> </ul>
Windows Vista® Home Basic	<ul style="list-style-type: none"> <li>• 1 GHz 32-bit (x86) or 64-bit (x64) processor.</li> <li>• 512 MB of RAM.</li> <li>• 20 GB hard disk with a minimum of 15 GB of available space.</li> <li>• Support for DirectX 9 graphics and 32 MB of graphics memory available.</li> </ul>

## Hardware Compatibility

Prior to installing any versions of Windows, you should check to make sure that your system meets the system requirements and that all your hardware is compatible with the version of Windows you plan to install. You can refer to the retail packaging to determine compatibility or search microsoft.com for information about hardware compatibility for the version of Windows you are installing.

## Boot Methods

The operating system comes loaded onto a boot device, which is connected to the computer and can be used to either launch the OS or, in some cases, install the OS files onto the computer. There are a number of boot methods that can be used to install the operating system.

<b>Boot Method</b>	<b>Description</b>
USB	The operating system files and all necessary support files are loaded onto a USB device, such as a flash drive. The USB is connected to the computer and the operating system is booted and launched via the files on the USB.
CD-ROM/DVD	The operating system files and all necessary support files are loaded onto an optical disc, such as a CD-ROM or DVD. The disk type used will be dependent upon the size of the files on the disk: DVDs can hold more files and larger files than a CD-ROM. Regardless of the type, the disk is inserted into the optical drive of the computer and the operating system is booted and launched via the files on the disk.
ISO	An ISO file contains all of the contents from an optical disc in a single file. ISO files stored on removable media or a host system are often used to install virtual machine operating systems.
Internal storage drive	An internal HDD or SSD can hold all of the operating system's installation files and can be used to install the OS onto a different drive or a different partition on the same drive. You can use a dedicated drive or partition for the purpose of creating multiple operating environments on the same device.
External storage drive	An external HDD or SSD can also be used for OS installation, most commonly over a USB interface. Using an external drive for this purpose makes it easier to physically install an OS on several different computers.
PXE	The operating system files and all necessary support files can be accessed from a Preboot Execution Environment, or PXE (pronounce as "pixie"). With PXE, the operating system and all necessary supporting files are loaded onto a server. The operating system is then booted and launched over a network interface, accessing the operating system files on the server, instead of using a local drive. This method is often used for booting multiple computers that are being managed centrally and accessed by more than one user, such as public computers at a library or school. The network booting technology used by Apple Macs is called NetBoot.

## Factory Configuration

Most computers are factory-configured to boot from CD-ROM or DVD-ROM first, and changing them to boot from hard disk speeds up the startup process. It also reduces the risk of contracting viruses by accidentally booting from an infected disk.

## Device Priority

The BIOS allows a user to specify disk boot order and to provide device priority. By default, the computer might look to boot from the hard disk or a DVD-ROM first. If you prefer to boot from

an operating system contained on a USB device, you can instruct the computer to look to that device first. To change the settings, wait until the computer has performed its POST, press the key (usually a function key, such as **F12**) indicated onscreen, and follow the instructions.

## Installation Types

There are several methods available for installing a Windows operating system.

<b>Installation Method</b>	<b>Description</b>
Clean install	<p>A clean install is used to install the operating system on a brand new computer or to replace the operating system on an older computer in which the hard drive has been completely wiped.</p> <p>If the computer is new or once the old hard drive has been wiped, you can install the operating system using the boot method of your choice.</p> <p>Typically a clean installation will be performed with a local source, likely an installation disk.</p> <p>A clean install on an old system is particularly helpful if the system has been plagued by problems; erasing the hard drive and starting with a clean install can eliminate viruses and corrupted files and allow the computer to work more efficiently. However, it is important to remember that all the settings, preferences, and files will be lost with a clean install to replace an existing system. Some of these settings or files can be migrated after the install using a migration tool.</p>
Unattended installation	<p>An unattended installation is an automated installation method that is most often used to roll out an installation or upgrade of the operating system to multiple systems and with minimal user interaction. An administrator is needed to start the installation, but then tasks that would usually require user input during installation are carried out automatically using an answer file. An answer file is a simple text file that contains all of the instructions that the Windows Setup file will need to install and configure the OS without any administrator intervention, including the product key.</p> <p>Using unattended installation allows for multiple installations to occur simultaneously, can prevent errors during installation, and create more consistency between installations in a large-scale rollout, all while lowering overhead costs and decreasing installation time and effort.</p>
Repair installation	<p>A repair installation is used to fix or repair the operating system that is currently installed on the computer and is experiencing issues. A repair install will replace the system files currently on the system with a fresh set of system files, essentially overwriting the existing system files. A repair install will only work if you are replacing the same version of the operating system; you cannot upgrade in this manner.</p> <p>With a repair installation you can install the operating system using the boot method of your choice.</p> <p>It is important to back up any data that you do not want to lose during the repair install to another <i>disk partition</i>, separate hard drive, or to an external storage device.</p>

<b>Installation Method</b>	<b>Description</b>
Upgrade	<p>An upgrade is used when an operating system is already installed, but the user needs or wants a newer version of the operating system. Upgrades are often provided on a disk or via a download from a vendor's website.</p> <p>It is recommended that you back up any data that you do not want to lose during the upgrade to another disk partition, separate hard drive, or to an external storage device. It is also recommended that files for the upgraded system are placed in a separate directory folder, preserving the current OS files, to ensure that everything is working properly.</p>
Multiboot	<p>Multiboot or dual boot refers to installing more than one operating system on a machine. This may mean more than one type of OS made by different vendors (such as Windows and Unix or Linux OS) installed on a single machine, or could mean having a newer and an older version of the same OS (such as Windows Vista and Windows 8) on a single machine.</p> <p>Multiboot installation requires that the machine either has multiple hard disks or that the hard disk has been partitioned, with a separate partition available for each operating system.</p> <p>Multiboot installations can be completed using the boot method of your choice.</p>
Remote network installation	<p>With remote network installation, copies of the necessary operating system installation files are placed on a server that supports remote installations, and an administrator can remotely initiate the installation over the network onto one or more client computers.</p> <p>Installing an operating system remotely requires the use of PXE as the boot method.</p>
Image deployment	<p>Image deployment provides a rapid way to install a standardized version of an operating system on one or many target computers. The operating system is first installed and configured with any additional software, security settings, or general user settings on a reference computer. A computer image is made of the reference computer's hard disk, including the operating system and all associated files, and then replicated onto the specified target computers.</p> <p>More than likely, the image will be too large to be placed on a CD or standard DVD, and it will need to be saved to a dual-layer DVD or a large flash drive. This installation will likely be completed using a USB drive as the boot method.</p>

Installation Method	Description
Recovery	<p>With a non-destructive refresh, you can repair an installation without disrupting any of the settings, data files, or installed software. This can be performed on Windows Vista, Windows 7, and Windows 8/8.1 systems. For Windows Vista and Windows 7, use the <b>Upgrade</b> option from the installation media. For Windows 8 or 8.1, from the <b>Update and recovery</b> page, select <b>Recovery</b> and then specify the recovery method to use.</p> <p>Windows 8 offers three types of recovery:</p> <ul style="list-style-type: none"> <li>• <b>Refresh your PC without affecting your files</b>, a non-destructive refresh.</li> <li>• <b>Remove everything and reinstall Windows</b>, useful for systems that are being decommissioned. It resets the system to the factory settings.</li> <li>• <b>Advanced startup</b>, allows you to selectively change or restore firmware settings, Windows startup settings, or restore Windows from a system image.</li> </ul>



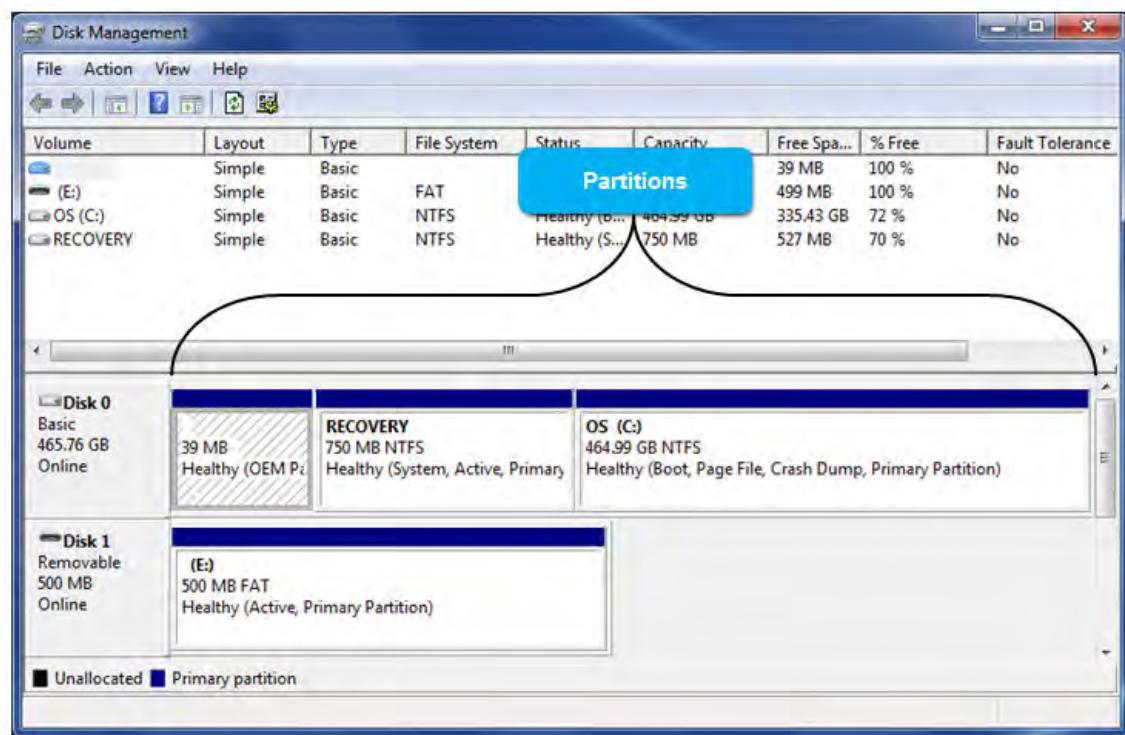
**Note:** If your network environment supports Microsoft Active Directory®, you can use Microsoft's Windows Deployment Services (WDS) to deploy Windows automatically on multiple computers. WDS uses disk imaging (the Windows Imaging format). It will now fully automate the installation of Windows Vista and newer operating systems. WDS is a replacement of the old Remote Installation Services (RIS).

## Third Party Drivers

The installation files for your operating system should include the necessary drivers for the hardware components of the system. However, if you have hardware that has been released more recently than the operating system or have added hardware components to the system that are not traditionally part of the environment, such as a wireless card or printer, then you may need to load alternate third party drivers for these devices during the installation process.

## Partitioning

*Partitioning* is the process of dividing a single hard disk into multiple isolated sections that function like separate physical hard drives, known as *disk partitions*. Partitions enable you to create a logical disk structure to organize hard drives. You can set up and format one or more disk partitions during installation. If you make an entire disk one partition, you cannot re-partition the disk later without either reinstalling the operating system or using a third-party disk utility. After you create a partition, you must format it to be able to store data on that partition.



**Figure 9–3: Disk partitioning in Windows 7.**

Partition information has traditionally been stored in a Master Boot Record (MBR). This technology has several limitations including the inability to work with disks over 2 TB or to have more than four primary partitions. The newer GUID Partition Table (GPT) enables you to work with drives greater than 2 TB and to have up to 128 partitions.

There are several types of partitions and disks used to create sections on a hard disk.

<b>Partition Type</b>	<b>Description</b>
Logical	A part of a physical disk drive that has been partitioned and allocated as an independent unit and functions as a separate drive.
Primary	A partition that contains only one file system or logical drive.
Extended	An extended partition can be subdivided into several file systems or logical disks/drives. Extended drives can be assigned a new drive letter.

<b>Disk Type</b>	<b>Description</b>
Basic	A basic disk contains a primary partition, logical drives, and possibly an extended partition. These partitions have been formatted with a file system and are used as a volume for storage. Up to four partitions can be made on a basic disk. Basic disks are the most commonly used storage type in a Windows environment.
Dynamic	A dynamic disk contains dynamic volumes, which are volumes that can span multiple disks. On a dynamic disk, up to 2,000 volumes can be created, though a maximum of 32 volumes is recommended.

## File System Types

During installation, you can choose to format the hard disk with the appropriate file system. There are several types of file systems you might encounter on different systems.

Type	Description
NTFS	For a typical Windows setup, it is recommended that you choose the NTFS file system. This file system is used in newer Windows operating systems and can handle partitions greater than 32 GB. Compared to FAT32, it is more efficient, provides better security controls, and offers file and folder compression.
FAT32	The FAT file system is a legacy formatting option that should only be used if running an older operating system such as Windows 95 or 98. The FAT file system is less secure and has a limit to size of partition it can support. If FAT32 is chosen, the size of the partition being formatted will determine the FAT file type used. If the partition is larger than 2 gigabytes, Windows automatically uses the FAT32 file system; smaller than 2 GB, FAT16 is used. If the partition is larger than 32 GB, FAT is not an option.
exFAT	exFAT is useful if you are sharing external drives between Windows and Mac computers. NTFS partitions are typically read-only on a Mac. When the drive is formatted on a Windows system with exFAT, it will be read/write when accessed from a Mac.
CDFS	<i>Compact Disc File System (CDFS)</i> CDFS is a very limited file system that was developed for optical disc media, typically for open source operating systems. Multiple operating systems support CDFS, including Windows, Apple® OS, and Unix-based systems. By supporting multiple platforms, CDFS allows for data and files to be exchanged without compatibility issues between the various operating systems.
ext2, ext3, ext4	The <i>ext2</i> file system used to be the native Linux filesystem of some of the previous releases. It is still supported in the current releases of Linux. <i>ext3</i> is an improved version of <i>ext2</i> . In case of an abrupt system shutdown, <i>ext3</i> is much faster in recovering data and better ensures data integrity. You can easily upgrade your filesystem from <i>ext2</i> to <i>ext3</i> . The newest default filesystem for Linux distributions is <i>ext4</i> . It is backwards-compatible with the <i>ext2</i> and <i>ext3</i> filesystems. Among <i>ext4</i> 's improvements over <i>ext3</i> are journaling, support of volumes of up to one exbibyte (EiB), and files up to 16 tebibytes (TiB) in size. <i>ext4</i> is the default filesystem for CentOS/RHEL 7 and Ubuntu installations.
NFS	NFS file systems are hosted on a server and enable the clients to access directories and files over the network as if they were stored locally.

## Quick and Full Format

Whether your needs are to support older operating systems with FAT, or newer systems with NTFS, there are two options available for formatting during setup: full format and quick format. During a full format, any existing files on the partition being formatted are removed and the disk is scanned for any potential bad sectors. This scan can be time consuming, which is why the quick format option is available. During a quick format, the existing files on the partition are removed, but the hard disk is not scanned for bad sectors. While the quick format may indeed be quicker, it is suggested that quick format is used only if the hard disk was previously formatted and you are sure there are no damaged sectors.

The quick format only removes entries from the index from the drive, and not all of the content on the drive. If there are no entries in the index, then the space is available for use in writing files. A full format replaces all of the content on the drive with zeros. This will clear the index on the drive as well, indicating that the drive space is available for writing files.



**Note:** Even though a full format replaces all of the content, with the right tools, data is still recoverable. So, if you need to make sure that the drive content is inaccessible, do a full format multiple times, or use a third-party disk wipe utility (or physically destroy the drive).

## Workgroups vs. Domains

A *workgroup* is a Microsoft peer-to-peer network model in which computers are grouped together with access to shared resources for organizational purposes. Members of a workgroup can access folders, files, printers, or other connections over the network. The computers that make up a workgroup appear together when you browse the list of networked devices in either the **Network** folder or **My Network Places**. Each computer in the workgroup maintains its own user account database. This means that if a user wants to log on at any computer within the workgroup, you must create an account for the user on each computer in the workgroup.

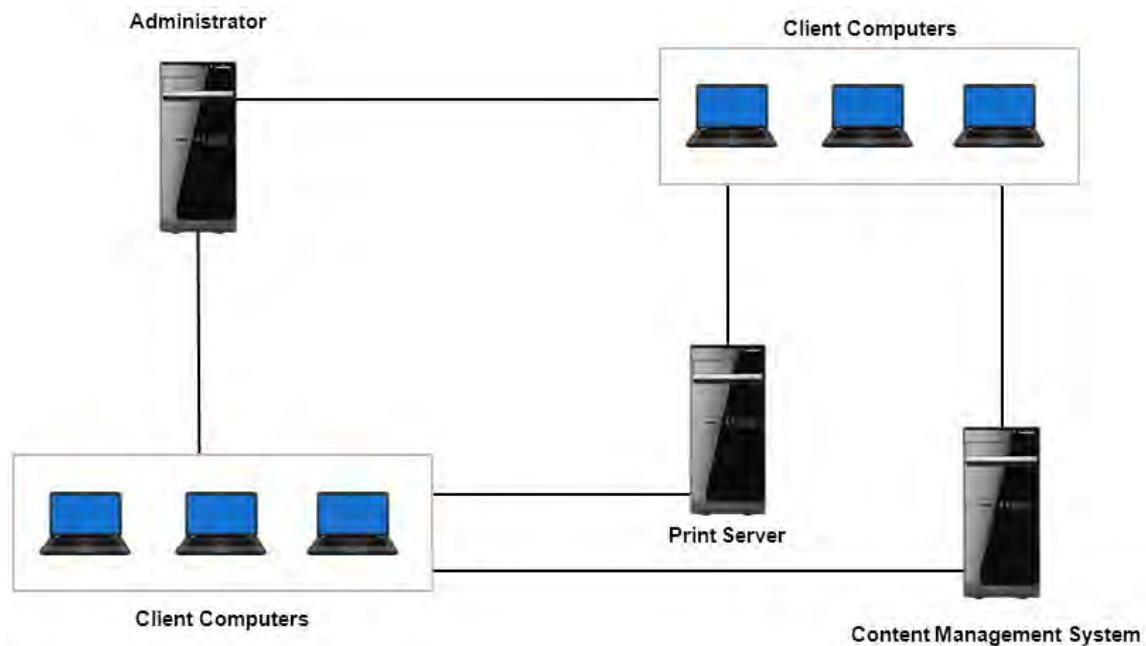


Figure 9–4: A workgroup.

A *domain* is a Microsoft client/server network model that groups computers together for security and to centralize administration. Computers that are members of a domain have access to a shared central user account database, which means that an individual can use a single user account to log on at any computer within the domain. Administration is centralized because you need to create the user accounts only once in the domain, not on each computer. Domains require a specially configured server computer called a *domain controller*, where the centralized user account database is stored. Like a workgroup, computers that are members of a domain appear together when you browse the network.

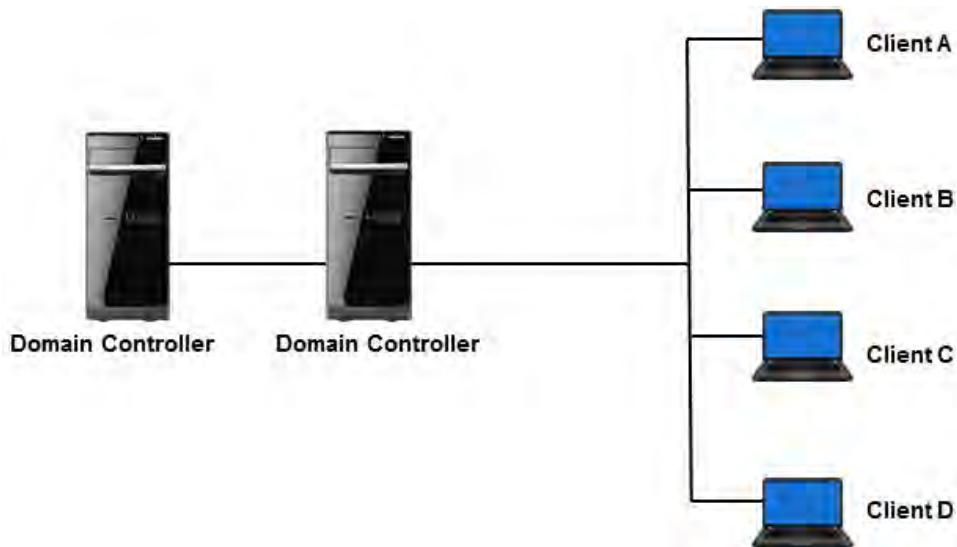


Figure 9–5: A domain.

## Homegroup vs. Workgroups

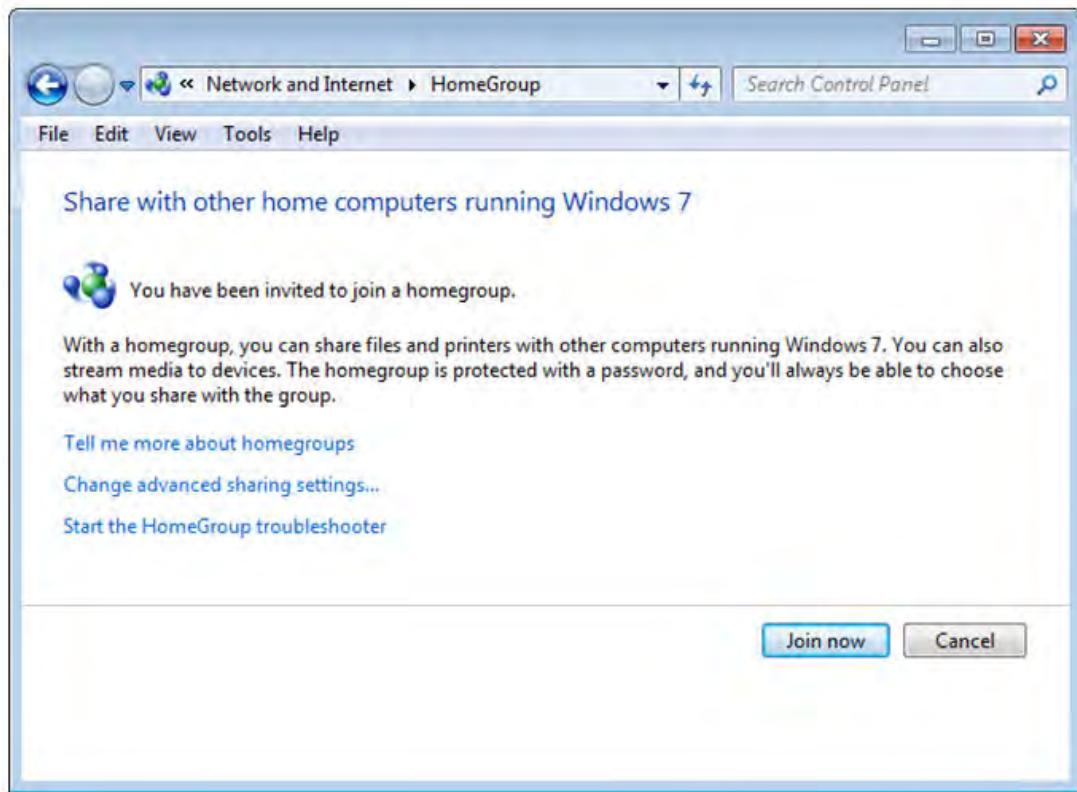
In Windows 7 and Windows 8, a homegroup is a peer-to-peer networking scheme where computers on a home network are grouped together for the purpose of sharing files and other resources such as printers. Computers on a home network must belong to a workgroup, but they can also belong to a homegroup.

When you install Windows 7, a homegroup is created automatically, if one does not already exist on your home network. The homegroup is automatically assigned a password by Windows. If you want to add computers to the homegroup, you will need to enter the password to join. Windows 8 does not automatically create a homegroup.

The homegroup provides easy resource sharing with security options such as:

- Excluding files and folders from being shared.
- Specifying whether or not others can change the files that you share.

The **HomeGroup Control Panel** contains options to manage your homegroup.



**Figure 9-6: The HomeGroup Control Panel.**

## Custom System Settings

There are several options that you can customize as you are installing a Windows operating system.

	<b>Note:</b> These options can be set during or after installation. They do not have to be configured during installation; if they are not set up during the installation, they can be changed at any time, typically through a Control Panel utility.
<b>Option</b> <b>Description</b>	
Regional and language settings	The default for a Windows system is the English language, with the location set to the United States. However, these settings can be customized to reflect region- or language-specific options. You can select the date and time for a specific location and choose appropriate regional settings, such as the manner in which numbers or currencies are displayed.
Computer name	During installation, you can provide the computer with a descriptive name and the organization to which you or the computer belongs.
Date and time	If you are within the United States and did not customize the regional and language settings, you can set the correct date and time, and choose the appropriate time zone for your region. If desired, you can choose to have Windows automatically adjust the time for Daylight Savings Time.
Network configuration	If Windows detects a network adapter during installation, you can decide how you want to configure networking settings for the computer. You can accept a Typical configuration or you can configure Custom settings that are appropriate to your environment. Otherwise, you can install your network adapter settings after the installation.

<b>Option</b>	<b>Description</b>
Workgroup vs. domain setup	During installation, you can decide if you want the computer to be a member of a domain or a member of a workgroup. If the computer is not on a network or on a network without a domain, you can select or create a workgroup for the computer to belong to. If the computer is part of a network with a domain, you can select the domain to which the computer will be added as a member.



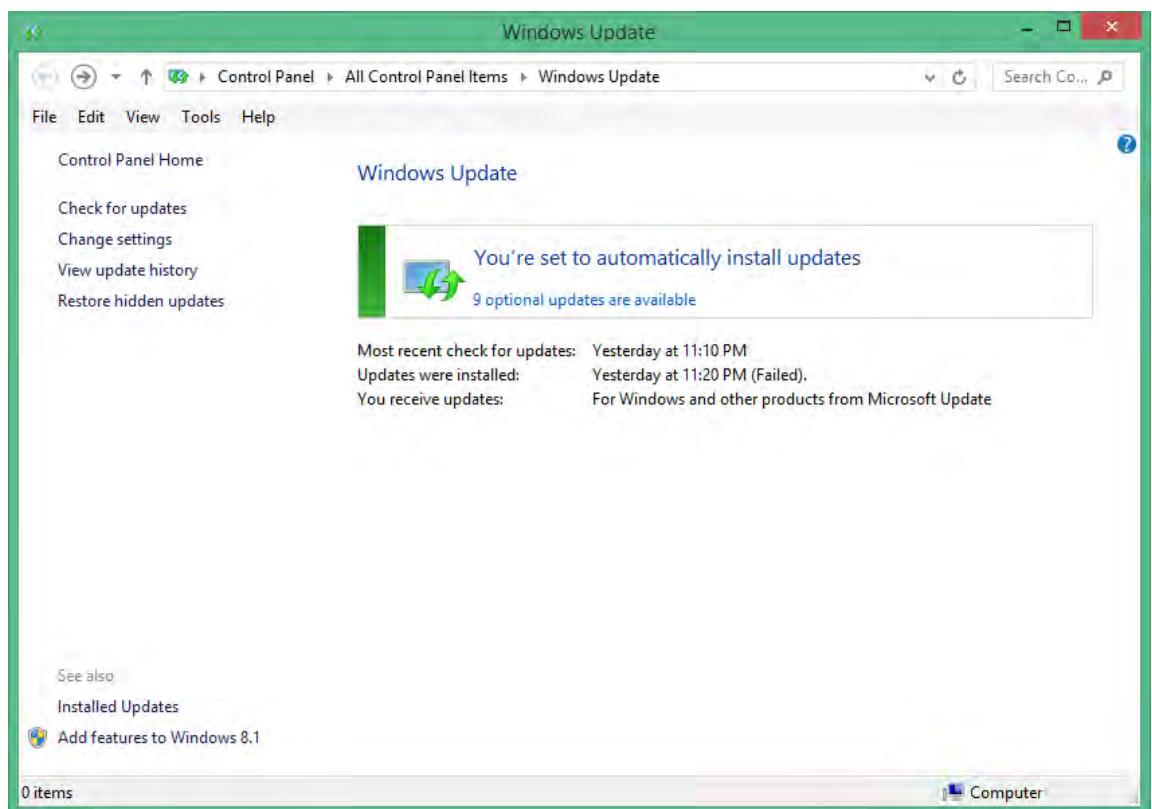
**Note:** If you are installing Windows 7 on a computer that is connected to a home network, the homegroup will be created when you configure the network settings.

## Software and Windows Updates

Both software applications and operating systems typically get updated on a regular basis. The updates might add new features, patch problems, or fix security holes. At a certain point in time, the application no longer receives updates after new versions of the applications or operating systems are released. It would be impractical for the software creator or manufacturer to continue to issue updates to old software.

As operating systems constantly evolve with the many changes in the technological world, there is always the possibility that you may need to update your operating system immediately after installing it. You will also need to maintain the system over time as changes and improvements are made. Updates fall into one of three categories: critical updates, including Service Packs and security-related system patches; optional software updates that provide new tools and functionality; and optional hardware updates such as new device drivers.

Updates to the Windows operating systems are available through the Windows Update Control Panel utility, a centralized location where you can check to see if your system is up to date and if there are any updates available, and configure the settings for updating your system. Regardless of the version you are running, the Microsoft Update website can provide updates for other Microsoft products that may have updates available.



**Figure 9–7: Windows Update Control Panel.**

## Cabinet Files

Windows updates are typically delivered as Cabinet (CAB) files. These files use compression technology to minimize space, and they can be embedded with security certificates to verify the integrity of the compressed files. You can use the EXPAND command to expand the files stored within CAB files.

## Service Packs and Patches

*Patches* are targeted operating system updates that Microsoft releases on an as-needed basis to provide enhancements to the operating system or to address security or performance issues. *Service Packs* are comprehensive updates that generally include all prior patches and updates, but which can also include important new features and functions. Windows XP SP2, for instance, included firewall changes; SP3 included support for Statements of Health and Digital Rights Management.

## Windows Genuine Advantage

Every time you access the Microsoft Update website, it goes through a process of validating your installation. If Microsoft deems the install to be invalid, you will not be able to proceed with updates and will be instructed to contact Microsoft.

## Microsoft Product Activation

Microsoft Product Activation or Volume Activation for Windows operating systems is an anti-piracy technology that verifies that software products are legitimately purchased. Product activation reduces a form of piracy known as casual copying. For example, you must activate the Windows operating systems within a given number of days after installation. After the grace period, users cannot access the system until they activate Windows. Volume Activation automates the activation process.



**Figure 9–8: Microsoft Product Activation.**

For individual installations of Windows, you can activate the installation over the Internet. If you do not have an Internet connection, you can activate over the phone, although this takes a little longer. If you wish, you can postpone product activation and activate later in the activation grace period.

In large organizations, you can use a Volume License Product Key, which eliminates the need to individually activate each installation of Windows. You can also activate Windows as part of an automated installation.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Install Microsoft Windows.

# ACTIVITY 9–3

## Installing Microsoft Windows 7

### Before You Begin

There is a VM named **Win7test##** installed on your computer that you can use to install Windows 7 Professional or Enterprise, and your instructor has provided you with installation DVDs or the instructions to use another installation method, as well as a valid product key (if needed).

### Scenario

One of the operating systems you support is Windows 7. You need a test environment in which you can test software and OS updates. You decide to install Windows 7 on the VM you set up previously.

1. Configure the VM to access the Windows 7 Professional setup program.
  - a) If you have a physical installation DVD, insert the Windows 7 Professional installation DVD into the optical drive of the computer.
  - b) In the **Virtual Machines** window, display the pop-up menu for **Win7test##** and select **Settings**.
  - c) In the left pane, select **DVD Drive**.  
The **DVD Drive** settings enable you to specify a physical drive, such as an optical drive, or you can browse for and select an ISO image to access.
  - d) If you have a physical installation DVD, verify that **Access a physical drive** is selected.
  - e) If you have an ISO image of the installation DVD, browse to the location of the ISO image and select **Open**.
  - f) Select **OK**.
2. Run the Windows 7 Professional setup program in the **Win7test##** VM.
  - a) Right-click the **Win7test##** VM and select **Start**.
  - b) In the **Actions** pane under **Win7test##** select **Connect**.
  - c) If you are prompted, press **Spacebar** to boot from the DVD drive or ISO image.  
The Setup program starts, and begins loading the files needed for setup.
3. Run the **Installation** wizard for Windows 7 Professional.
  - a) In the **Install Windows** dialog box, examine the selections for **Language to install**, **Time and currency format**, and **Keyboard or input method**. If necessary, adjust the selections for your locale. Select **Next**.
  - b) If prompted, click **OK** in the **Mouse pointer will be captured by the Virtual machine** dialog box.
  - c) Select **Next**.
  - d) Select **Install now**.
  - e) When the license terms are displayed, review them, check **I accept the license terms**, and select **Next**.
  - f) On the **Which type of installation do you want** screen, select **Custom (advanced)**.
  - g) On the **Where do you want to install Windows** screen, select **Drive options (advanced)**.
  - h) Select **Disk 0 Unallocated Space**, and select **Next**.  
The VM will automatically restart after a few minutes.
  - i) Observe as the VM restarts, Registry settings are updated, services are started, and the installation is completed.  
When the installation is completed, Windows restarts, prepares the computer for first use, and checks video performance.
4. Configure Windows.

- a) In the **Set Up Windows** dialog box, type **Admin###** for the user name and **VMWin7###** for the computer name. Select **Next**.  
You are prompted to set a password for the new account.
- b) Type and confirm **IPass1234** as the password and as the password hint, and then click **Next**.
- c) Type the product key provided by your instructor, and select **Next**.
- d) On the **Help protect your computer and improve Windows automatically** screen, select **Use recommended settings**.
- e) On the **Review your date and time settings** screen, select the correct **Time zone**, **Date**, and **Time** for your locale. Select **Next**.
- f) Select **Work network**.  
Windows prepares the desktop.

# TOPIC C

## Use Microsoft Windows

In the last topic, you installed the Windows operating system. In this topic, you will delve a bit deeper into using it. You will examine how you can use some of the common features. You will also use Task Manager to examine processes and performance of the operating system and applications.

### Common Windows Features

There have been a lot of versions and editions of Windows operating systems over the years. Many features are common between the OSs. Sometimes between versions, Microsoft changes the name of a feature slightly, but the functionality remains the same.

Feature	Description
File Explorer	Up until Windows 8, the utility used to access and manage files and folders was known as <b>Windows Explorer</b> . Windows 8 changed the name to <b>File Explorer</b> .
UAC	User Account Control (UAC) is an enhanced security feature of Windows Vista and later that limits the privileges of a standard user unless a computer administrator decides otherwise.
System restore	This feature enables you to either non-destructively restore the operating system without affecting files and applications, or to restore the system to the factory defaults.
Administrative tools	The <b>Administrative Tools</b> are grouped together under <b>Control Panel</b> → <b>System and Security</b> → <b>Administrative Tools</b> . In some installations, this is an entry from the <b>Start menu</b> . The tools include <b>Component Services</b> , <b>Computer Management</b> , <b>Data Sources</b> or <b>ODBC Data Sources</b> , <b>Disk Cleanup</b> , <b>Event Viewer</b> , <b>iSCSI Initiator</b> , <b>Performance Monitor</b> , <b>Resource Monitor</b> , <b>Services</b> , <b>System Configuration</b> , <b>Task Scheduler</b> , <b>Windows Firewall</b> , <b>Windows Memory Diagnostic</b> , and <b>Windows PowerShell</b> .
Windows Defender	 <b>Note:</b> More information about each of these Administrative Tools is covered where the tools are used throughout the course.
Windows Firewall	A <i>firewall</i> is a device or program that blocks unauthorized data transmissions and protects the computer from unauthorized access. <b>Windows Firewall</b> is a software-based firewall, included with almost all Windows installations, that protects the computer against attacks through the Internet or the network.

Feature	Description
Action Center and Security Center	<p>The <b>Action Center Control Panel</b> utility provides information about any security software currently deployed on or missing from the system, and provides access to helpful resources about current security threats, including a check for the latest Windows Update. <b>Action Center</b> also provides links to the <b>Backup and Restore</b>, <b>Windows Update</b>, and <b>Windows Program Compatibility Troubleshooter</b> utilities, where you can manage specific settings regarding system security and troubleshooting.</p>
	<p>In Windows Vista, the <b>Security Center Control Panel</b> included some of the same information as the <b>Action Center</b> does in Windows 7, but in the <b>Security Center</b>, links to the <b>Internet Options</b>, <b>Automatic Updates</b>, and <b>Windows Firewall Control Panels</b> are included.</p>
Event Viewer	<p>You can use the <i>Event Viewer</i> to view the contents of event logs, which contain information about significant incidents that occur on your computer. Examples of events that might be contained in an event log include a program starting or stopping and security errors.</p>
Control Panel	<p>The <b>Control Panel</b> is a graphical interface that provides access to utilities that you can use to configure the Windows OS or a computer's hardware. The specific <b>Control Panel</b> utilities that are available will vary depending on the version of Windows that you are using.</p>
	<p>Control Panel can be displayed in category view or classic view. As the name implies, category view groups the Control Panel utilities into categories. The classic view shows each utility separately as its own entry on the Control Panel window.</p>
	<p>In Windows 7, the <b>Control Panel</b> is available from the <b>Start</b> menu, and as a link in various <b>My Computer</b> views. You can open the <b>Control Panel</b> by selecting the <b>Open Control Panel</b> button located below the address bar of the <b>Computer</b> window.</p>
	<p>In Windows 8, you can access <b>Control Panel</b> through the Charms bar or by right-clicking the <b>Start</b> menu button from the Desktop.</p>
Gadgets	<p>The Desktop Gadget Gallery is a Windows Vista and Windows 7 feature that displays different gadgets, which are mini applications that perform different information-display tasks, including displaying the date and time, CPU usage, stock information, and user-selected news headlines.</p>

## File Structure and Paths

While not really a feature, all Windows versions also share a hierarchical organization of files and folders. However depending on the version and whether you are using the 32-bit or 64-bit version, the placement of files and folders might vary, as well as the paths you use to access those files and folders.

## Windows Vista Features

Windows Vista, released in 2007, introduced some new features. Many of the features have been carried into the more recent versions of Windows. Other features have been phased out due to security concerns or for sleeker, faster interfaces.

- Windows Aero® is a color scheme available in Windows Vista and Windows 7. Windows Aero introduced a glossy and transparent interface, Live Preview of taskbar buttons, and a Flip 3D view of open windows.
- The Desktop Gadget Gallery is available in Windows Vista and Windows 7, and it displays different gadgets or mini applications that can perform various information-display tasks.

Different editions offer different feature sets. For example, Vista Home Basic does not include advanced multimedia capabilities or support networking beyond a workgroup, while Home Premium adds Media Center, HDTV support, and the Windows Aero interface. Vista Business adds features such as Remote Desktop, the ability to encrypt the file system, and the ability to join a Windows domain. Windows Vista Enterprise and Ultimate add even more features such as UNIX application support, BitLocker, and multilingual user interfaces.

## Windows 7 Features

Many of the features of previous Windows versions were carried over into Windows 7, including Aero and gadgets.

- Support for multi-touch devices is added, as well as support for Virtual Hard Disk (VHD) file format.
- The default disk is partitioned into a partition that contains boot files, BitLocker files, and the Windows Recovery Environment (WinRE) environment files; a second partition is created for the operating system and for storing user created files.
- Action Center replaces the Windows Security Center.
- The snap feature allows you to drag a window to the edge of the screen and have it snap to take up half of the screen; snap another window to the other side of the screen to view the two windows side by side.
- Virtual XP mode is useful if you are still using applications written to take advantage of Windows XP features. Support for this feature has been discontinued, so if you use it, you are doing so at your own risk.
- Another feature you can use for older programs that don't run properly under Windows 7 is Compatibility Mode. You can configure settings to try to make the operating system appear, to the application, that it is running under the Windows OS version that it expects to run in.
- The Readyboost feature enables you to use a flash memory device to add RAM to your system. This feature was also available in Windows Vista, but you could only have up to 4 GB of additional RAM. The device must be at least 256 MB with at least 64 KB of free space. When the flash memory device is attached to the computer, Windows tests it to see whether it meets the requirements to use it for Readyboost.
- Shadow Copy is a feature that helps with making sure that files that are in use are backed up. A snapshot of the data at a particular point in time is created. The snapshot can then be included in your regular backup of the system.
- Easy Transfer is a utility to help migrate a user's email, data files, and settings from one computer to another. You will need to install the appropriate version of Easy Transfer on each system (Windows Vista or Windows 7) to create the backup, then using Easy Transfer on the Windows 7 computer, bring the email, data files, and settings onto the new computer.

Windows 7 is available in several different editions. Windows 7 Home Premium offers basic functions. Windows 7 Professional adds features that enable users to run programs in XP mode, connect to domains, and back up data to networks. Windows 7 Enterprise and Ultimate add even more features such as multilingual support, BitLocker, and compatibility with UNIX applications.

## Windows 8/8.1 Features

Windows 8 and 8.1 are the biggest change Microsoft has made to the look and feel of an OS in a long time.

- The **Start** screen uses tiles the user can select using touch, mouse, or keyboard to access applications.
- Applications can be traditional Windows-style applications or Windows Store apps. Windows Store apps are approved to meet specifications required to be included in the Windows Store. Apps and applications can be pinned to the **Start** screen, to the taskbar on the Desktop, or both. The computer can be configured to boot to the Desktop or to the **Start** screen. If users use

mostly Windows Store apps, it makes sense to boot to the **Start** screen, and if they use mostly traditional Windows applications, it makes sense to boot to the Desktop.



**Note:** You might see some literature and articles refer to the Windows 8 interface as the Metro UI. This is not an official Microsoft designation for the Windows 8 interface. You might also see it referred to as the modern interface and modern apps; these also are not official Microsoft terms.

- Like in Windows 7, you can snap windows side by side. Windows Store apps run in full screen, and those apps can also be positioned side by side. The Desktop can be side by side with a Windows Store app. All of the open apps and windows can be viewed as thumbnails down the left side of the screen. Drag one of the thumbnails onto the screen to either replace the current app you are viewing, or drag it so that a border appears between the windows and view them side by side. Depending on the size of the screen you are viewing Windows 8/8.1 on, you can have up to four apps side by side. Most screens accommodate two or three apps. Items running on the Desktop can also run side by side on the Desktop, then the Desktop can run side by side with a Windows Store app.
- Windows Store apps require that you are logged in using a Live ID sign in. This is any email address registered with Microsoft as your login credentials. Other benefits of using the Live sign in include being able to obtain updates from Microsoft as they are available. Also, OneDrive, the Microsoft cloud storage solution, uses your Live sign in. By default, you are given 5 GB of storage space on OneDrive.
- Booting the OS is faster than in previous versions of Windows. Only the required components are loaded into memory when the system is started; additional components are loaded when they are needed.
- The Charms bar is available on the right side of the **Start** screen or the Desktop. From the Charms bar, you can use the **Search** feature, access devices such as printers, share content through email or social media, or access **PC Settings**.
- If you are using multiple monitors, you can have the task bar display on both screens, or just on the main screen. In addition, you can show just the applications open on each screen on the task bar for that screen.

## Task Manager

**Windows Task Manager** is a basic system diagnostic and performance monitoring tool included with Windows Vista, Windows 7, and Windows 8. You can use **Task Manager** to monitor or terminate applications and processes, view current CPU and memory usage statistics, monitor network connection utilization, set the priority of various processes if programs share resources, and manage logged-on local users.

You can manage the following tasks in Windows Vista and Windows 7 Task Manager.

Task	Description and Purpose
Applications	Displays all of the applications currently running on the system and their status (running, not responding, etc.). Users can use the <b>Task Manager</b> to end an application that is running, switch to a different open application, or start a new application.
Processes	Displays all of the processes currently running on the system, including the CPU and memory usage for all processes. Users can choose to end a process from the <b>Task Manager</b> .
Performance	Displays the current CPU and physical memory usage statistics for the system in a graphical format and numerical format for an overall view of the current system performance.

<b>Task</b>	<b>Description and Purpose</b>
<b>Networking</b>	Displays the networks that the system is currently connected to, and graphically displays current connection utilization for all network connections.
<b>Users</b>	The <b>Users</b> tab was added in Windows Vista and is still available in Windows 7. It displays all of the users currently logged on to the system. Users can select another user's account and connect to that user's session, send them a message, or disconnect or log off the user via the <b>Task Manager</b> .

You can manage the following tasks in Windows 8 Task Manager.

<b>Task</b>	<b>Description and Purpose</b>
<b>Processes</b>	<p>Displays all of the apps currently running on the system and their status (running, not responding, etc.). Users can use the <b>Task Manager</b> to end an application that is running, switch to a different open application, or start a new application.</p> <p>Displays all of the background processes currently running on the system. Users can choose to end a process from the <b>Task Manager</b>.</p> <p>For both apps and background processes, the current status and the statistics are shown. The overall utilization as a percentage is shown at the top of each column. The table rows show the utilization of each app or background process.</p> <ul style="list-style-type: none"> <li>• CPU—total processor utilization across all cores as a percentage of the total CPU capacity.</li> <li>• Memory—total physical memory reserved by individual processes. The overall statistic is listed as a percentage of the available memory that is in use. Each process lists the number of MB of RAM it has reserved.</li> <li>• Disk—total utilization across all physical drives. The overall statistic is listed as a percentage of the total utilization. Each process lists the number of MB per second.</li> <li>• Network—total utilization on the current primary network. The overall statistic is listed as a percentage of the available bandwidth. Each process lists the number of Mbps.</li> </ul>
<b>Performance</b>	 <p><b>Note:</b> In previous versions of Task Manager, Network was listed on a separate tab.</p> <p>Displays the current CPU, physical memory, disk, and network usage statistics for the system in a graphical format and numerical format for an overall view of the current system performance.</p>
<b>App history</b>	<p>Displays resource usage for Windows Store apps for the current user account. Statistics for each app include:</p> <ul style="list-style-type: none"> <li>• CPU time—the amount of time the CPU spent processing instructions.</li> <li>• Network—the amount of network activity used by the app, including downloads and updates.</li> <li>• Metered network—the amount of network activity over a metered network connection.</li> <li>• Tile updates—total network usage for tile updates and notifications.</li> </ul>

Task	Description and Purpose
Startup	<p>The apps that run when the computer starts are listed on this tab. You can manage these apps by right-clicking an app and selecting one of the following choices:</p> <ul style="list-style-type: none"> <li>• Disable—toggle between enabling and disabling the app to run at startup.</li> <li>• Open file location—open File Explorer to the folder that contains the executable file for the app.</li> <li>• Search online—open the default browser to view results of a search for information about the app.</li> <li>• Properties—open the Windows Property dialog box for the executable file for the app.</li> </ul>
	 <b>Note:</b> In previous versions of Windows, the functionality found on the <b>Startup</b> tab was found in the <b>System Configuration</b> tool.
Users	<p>The <b>Users</b> tab displays all of the users currently logged on to the system.</p>
	<p>Users can select another user's account and connect to that user's session, send them a message, or disconnect or log off the user via the <b>Task Manager</b>.</p>
	<p>You can see which processes each user is running, which can be useful to identify whether a process is hogging resources.</p>
Details	<p>For all of the processes running on the computer, the following information is listed:</p>
	<ul style="list-style-type: none"> <li>• PID—the process ID for the file.</li> <li>• Status—the status, such as Running, for the process.</li> <li>• User name—the user that "owns" the process.</li> <li>• CPU usage—the percentage of CPU utilization used by the process.</li> <li>• Memory usage—the amount of memory reserved for the process.</li> <li>• Description—a short description to help you identify the process since it isn't always clear from the executable name which program the process is associated with.</li> </ul>
	<p>Right-clicking a process provides you with a range of actions you can take regarding the process. One of the most useful is setting the priority for the process, which can be used to reduce the priority of a CPU-hungry background process to give more CPU priority to foreground apps, making the foreground app function better.</p>
Services	<p>This is a duplicate of the services found in the <b>Control Panel Services</b>. This is just another way of accessing and managing those services.</p>

# ACTIVITY 9–4

## Using Task Manager

### Before You Begin

Perform this activity on your physical Windows 8.1 computer.

### Scenario

In this activity, you will use the **Task Manager** utility to examine your system's status.

1. Display the pop-up menu for the taskbar, and select **Start Task Manager**.
2. Examine the currently running processes.
  - a) Select **More details**.
  - b) Examine any apps and background processes listed on the **Processes** tab.
  - c) Select the various column headings to sort the list by each of the categories.  
Notice that the list changes order when various items are consuming more resources.
  - d) Select the **Details** tab.
  - e) Compare the information displayed on the **Details** tab with the information displayed on the **Processes** tab for the **Task Manager** process.
3. Use **Task Manager** to review the system's performance.
  - a) Select the **Performance** tab.
  - b) Observe the information displayed for the CPU.  
Information about the CPU utilization, speed, number of processes and threads, and uptime are displayed. Additional information about the CPU is also displayed including maximum speed, sockets, cores, and other details.
  - c) In the left pane, select **Memory**. Notice that the information displayed is now statistics regarding memory rather than CPU.
  - d) Select **Disk #** in the left pane to view statistics regarding the disk(s).
  - e) Select any network connection in the left pane to view statistics regarding the network(s).
4. Manage an application from within Task Manager
  - a) From the taskbar, select **Internet Explorer**.
  - b) Open a second tab in **Internet Explorer**.
  - c) In **Task Manager**, on the **Processes** tab, expand **Internet Explorer (2)**.  
A separate process for each of the open tabs is listed.
  - d) Right-click **New tab - Internet Explorer**.
  - e) Select **End task**. Notice that you are not prompted to confirm your selection.
  - f) Open another tab in **Internet Explorer**.
  - g) In **Task Manager**, right-click **Internet Explorer (2)** and select **End task**.
5. Select the **Services** tab, and examine the services that are running independently on the system.
6. Select the **Users** tab.  
This tab lets you see the other users who may be logged on to Windows 8. You can expand the tree under the user name to see what apps and processes are being used by this user.

**7. Close Task Manager.**



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Use Microsoft Windows Features.

# ACTIVITY 9–5

## Working with Microsoft Windows Features

### Before You Begin

You have a Windows 7 VM and a physical Windows 8.1 computer.

### Scenario

To be sure you know how to work with Windows features from both Windows 7 and Windows 8, you decide to try out some of the features you've read about.

1. Change from the Aero theme to a classic theme on Windows 7.
  - a) Log in to your Windows 7 computer.
  - b) Select the **Start menu**.
  - c) In the **Search** text box, type *aero*
  - d) In the results list, select **Change the theme**. The **Control Panel Personalization** window opens.
  - e) Observe the look of the **Start menu** and the window borders. The **Start menu** is a round button and the window borders are rounded with subtle shading.
  - f) Under **Change the visuals and sounds on your computer**, scroll down and under **Basic and High Contrast Themes**, select **Windows Classic**.
  - g) Observe that the **Start menu** is now a square button and that the window borders are square.
  - h) Under **Aero Themes**, select **Windows 7**.
  - i) Verify that the round **Start menu** and rounded window borders have been restored.
  - j) Close all open windows on the Windows 7 VM.
  
2. Add gadgets to the Windows 7 desktop.
  - a) Right-click the Windows 7 desktop and select **Gadgets**.
  - b) Drag the **Clock** gadget onto the right side of the desktop.
  - c) Drag another **Clock** gadget onto the right side of the desktop, below the first clock.
  - d) Close the window from which you selected the gadgets.
  - e) Point to the second clock, and from the toolbar that appears, select the **Options** button.
  - f) Using the right and left arrow buttons in the **Clock** dialog box, change the style of the clock to any other style.
  - g) In the **Clock name** text box, type *Houston*
  - h) From the **Time zone** drop-down list, select **(UTC-06:00) Central Time (US & Canada)**.
  - i) Select **OK**.
  - j) Set the other clock to **Eastern Time** time zone and label the clock **New York**
  
3. Place two Windows 7 windows side by side.
  - a) Open **Notepad**.
  - b) Drag the **Notepad** window to the right side of the screen until the window snaps to half the size of the screen.
  - c) Open **Word Pad** and drag the window to the left side of the screen until the window snaps to the left half of the screen.
  
4. Access the Windows 8 Charms bar.
  - a) Switch to your Windows 8.1 computer and verify that you are logged in with Live sign in. Your Live sign in is tied to the email address assigned to you for the class.

- b) Press the **Windows** key on your keyboard to switch to the **Start** screen. You can toggle back and forth between the Desktop and the **Start** screen by using the **Windows** key.
  - c) Move the mouse to the right side of the screen and move it up or down until the **Charms** bar is displayed.
  - d) Select **Search** and in the **Search** text box, type *notepad*
  - e) From the results list, select **Notepad**.  
Notepad opens on the Desktop because it is a traditional Windows style application.
  - f) Display the **Charms** bar again and select **Settings→Change PC settings→Personalization**.
  - g) Observe the theme choices. Notice that there are no longer Aero themes.
5. Open Windows Store apps and snap them side by side.
- a) Select the **Start** menu in the left corner of the taskbar to switch to the **Start** page.
  - b) Observe that some of the tiles change. These are live tiles that update based on available content.
  - c) Select the **Internet Explorer** tile.
  - d) Point to the lower-left corner of the screen until the **Windows Start** button appears, then select it.
  - e) Select the **Weather** tile.
  - f) Point to the upper-left corner of the screen, then drag down slightly to view the open windows.
  - g) Select one of the open windows and drag it right. A separator bar with three dots is displayed. Drop the selected window to the left of the currently displayed window.
  - h) Drag the bar to resize the windows.
  - i) Drag the bar until one of the windows closes.
  - j) Point to the upper-left corner to see that the window is still open, just not displayed.
  - k) Right-click the thumbnail of the window, and select **Close** to close the app.  
You can confirm that the app was closed by looking at the list of apps in Task Manager.
  - l) Close the Internet Explorer and Weather app windows.

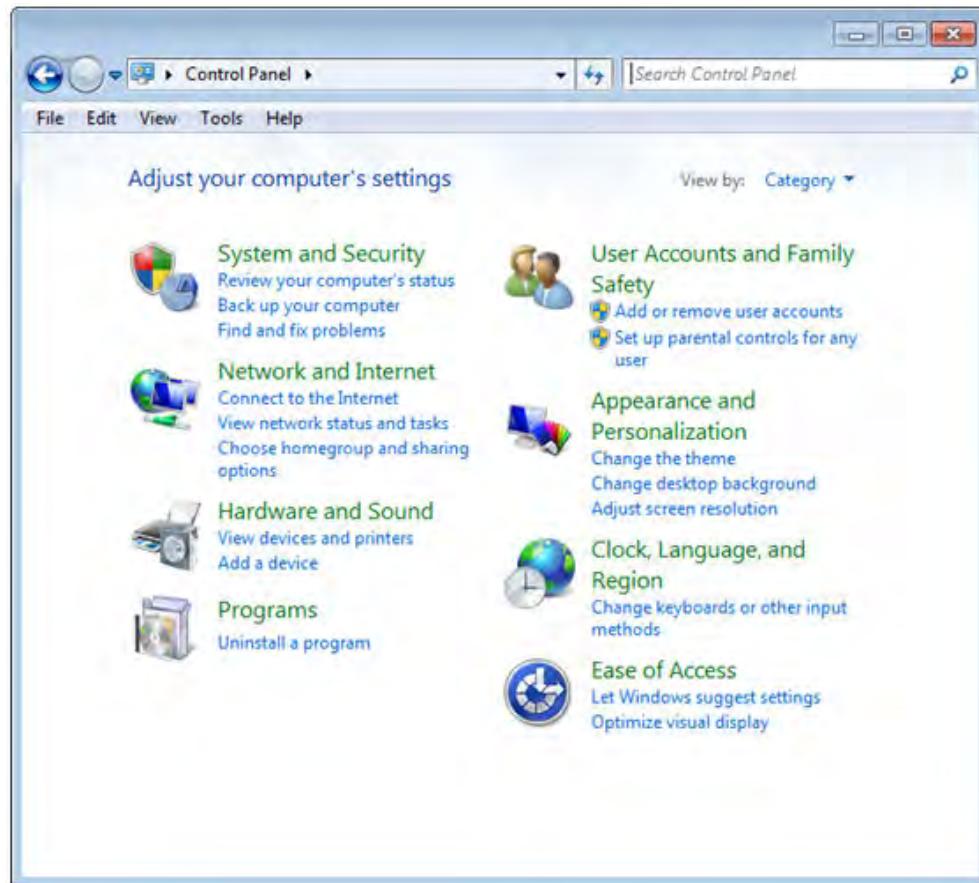
# TOPIC D

## Configure Microsoft Windows

There are many tools you will use to configure Windows. Some of these are GUI and some are command-line based. You have already seen a little bit of this in configuring display devices and other hardware where you used the Control Panel. In this topic, you will use the Control Panel as well as other GUI and command line tools to further configure the Windows operating system features and functions.

### Windows Control Panel

The **Control Panel** is a graphical interface that provides access to a number of utilities that you can use to configure the Windows operating system or a computer's hardware. The specific **Control Panel** utilities that are available will vary depending on the version of Windows that you are using.



*Figure 9-9: The Control Panel in Windows 7.*



**Note:** The **Control Panel** is available from the **Start** menu, and as a link in various **My Computer** views. In Windows 7, you can open the **Control Panel** by selecting the **Open Control Panel** button located below the address bar of the **Computer** window.

### Internet Options

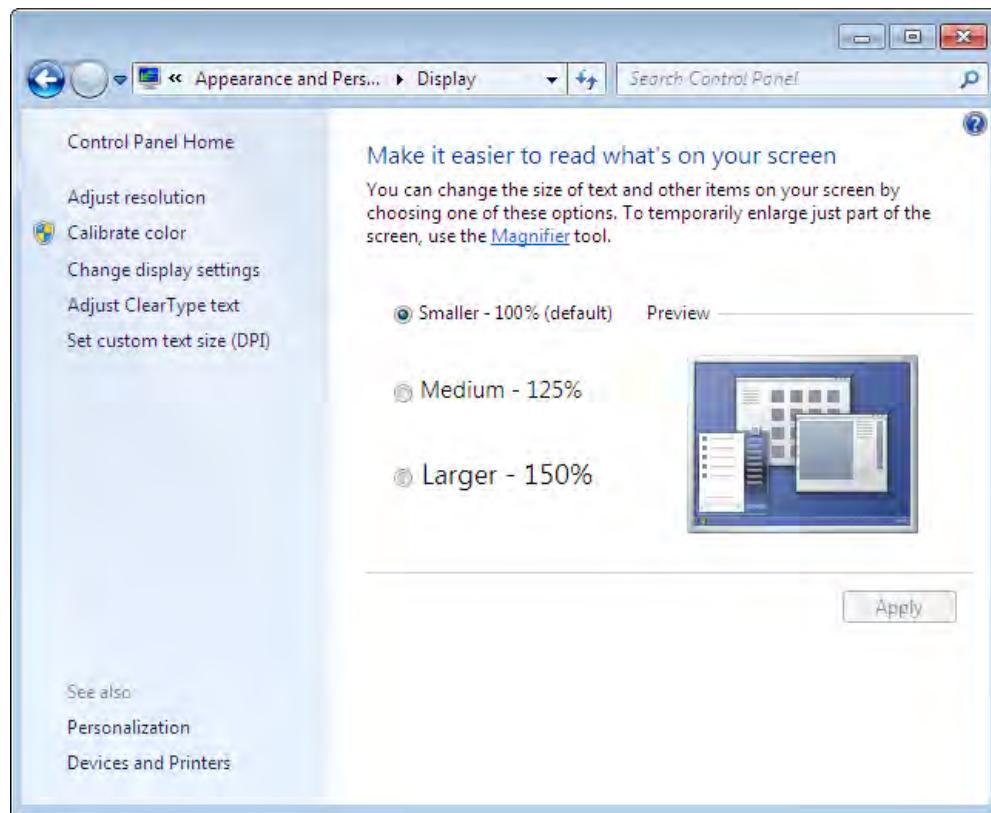
The **Internet Options Control Panel** utility has many settings that can be customized.

<b>Setting</b>	<b>Description</b>
<b>General</b>	<ul style="list-style-type: none"> <li><b>Home page:</b> Defines which web page the browser opens to by default.</li> <li><b>History:</b> Defines how many days the browser will keep a record of visited pages.</li> <li><b>Colors:</b> Defines the user's preferred colors for text, page backgrounds, and hyperlinks.</li> <li><b>Fonts:</b> Defines the user's preferred fonts for viewing pages.</li> <li><b>Languages:</b> Defines the user's preferred default language for viewing pages.</li> <li><b>Accessibility:</b> Defines settings that enable visually impaired or hearing-impaired users to access web pages.</li> </ul>
<b>Security</b>	Defines levels of security for different groups of websites, known as zones. By placing sites in zones and then configuring zone settings, users can enable or disable features such as the blocking or acceptance of web pages, or whether web scripts or controls can run automatically, based upon user preference.
<b>Privacy</b>	Defines the level of access that third-party cookies have to the browser.
<b>Content</b>	Contains various content-related configuration settings, including settings that relate to using content ratings on websites, implementing Internet security certificates, and the AutoComplete function in web-based forms.
<b>Connections</b>	Determines how Internet Explorer will use the computer's network connections to access Internet content.
<b>Programs</b>	Determines which programs Internet Explorer will launch by default when the user selects links that are associated with other types of Internet content, such as email or newsgroups.
<b>Advanced</b>	Defines a wide variety of settings, including how the browser handles external scripts, whether or not hyperlinks are always underlined, and whether or not videos can be played within web pages.

## Display and Display Settings

The **Display Control Panel** utility allows the user to configure the display properties for the system, including the physical appearance of the environment, such as the wallpaper, screen saver, color scheme, and font size used. The user can also configure the display settings for the monitor or monitors being used, including setting the primary monitor and the arrangement of additional monitors, extending the desktop onto another monitor, and determining the screen resolution and color quality for the monitors.

Common screen resolutions include 800 by 600, 1024 by 768, and 1280 by 1024, measured in pixels.



**Figure 9–10:** The Display utility in Windows 7.

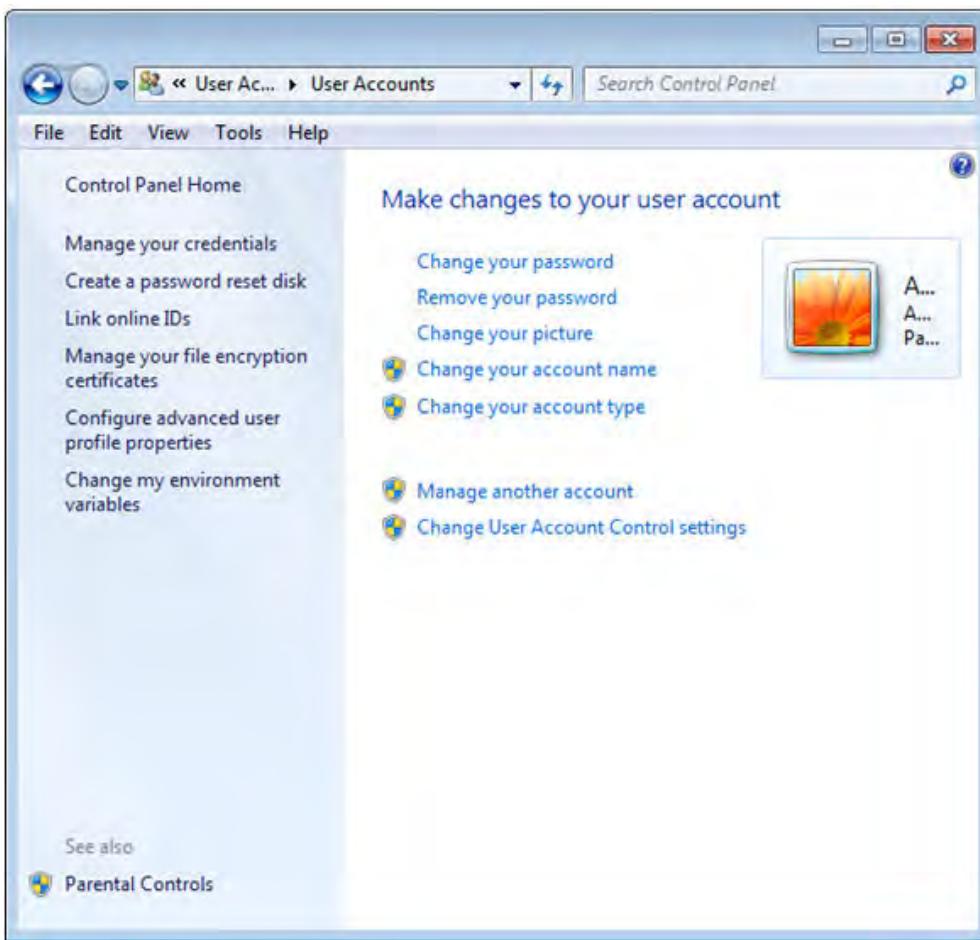
## User Accounts

A *user account* is a collection of credentials and important information about a person who has access to the system. Most importantly, it defines the rights and privileges assigned to the user, determining what kinds of actions they can perform on the system. There can be more than one user account added to a specific system. There may be users with the same permissions or different permissions assigned to the same computer.



**Note:** There will typically be at least two user accounts per system: the administrator and the user who owns or has been assigned the machine.

The **User Accounts Control Panel** utility lets you view and manage your own account, including changing your user name and password. If your account has been assigned administrator privileges, you may also be able to add, remove, or modify other user accounts to allow other users access to the system.



**Figure 9-11:** The User Accounts utility in Windows 7.

## Folder Options

The **Folder Options Control Panel** utility lets you configure settings for how files and folders are displayed when they are accessed. **Folder Options** also lets you configure more general settings such as whether new folders will open in a new window or the existing window, what the layout of folders opened in the navigation pane will be, what action is used to open a file in a folder, and which program is the default for opening specific file types.

Using **Folder Options**, you can also configure the **Advanced Settings** for files and folders, including:

- Whether simple file sharing, the feature in Windows that allows users to share files and folders with other computers on the network without permissions, is enabled or disabled. The default for the system is that simple file sharing is enabled.
- If you can view hidden files and folders, including protected operating system files. The default is that hidden files and folders, including the protected operating system files, are not displayed when accessing a folder that contains the files to protect them from being accidentally deleted or modified.
- Whether to hide or display extensions for known file types within the folder structure. The default is to hide file extensions for known file types.

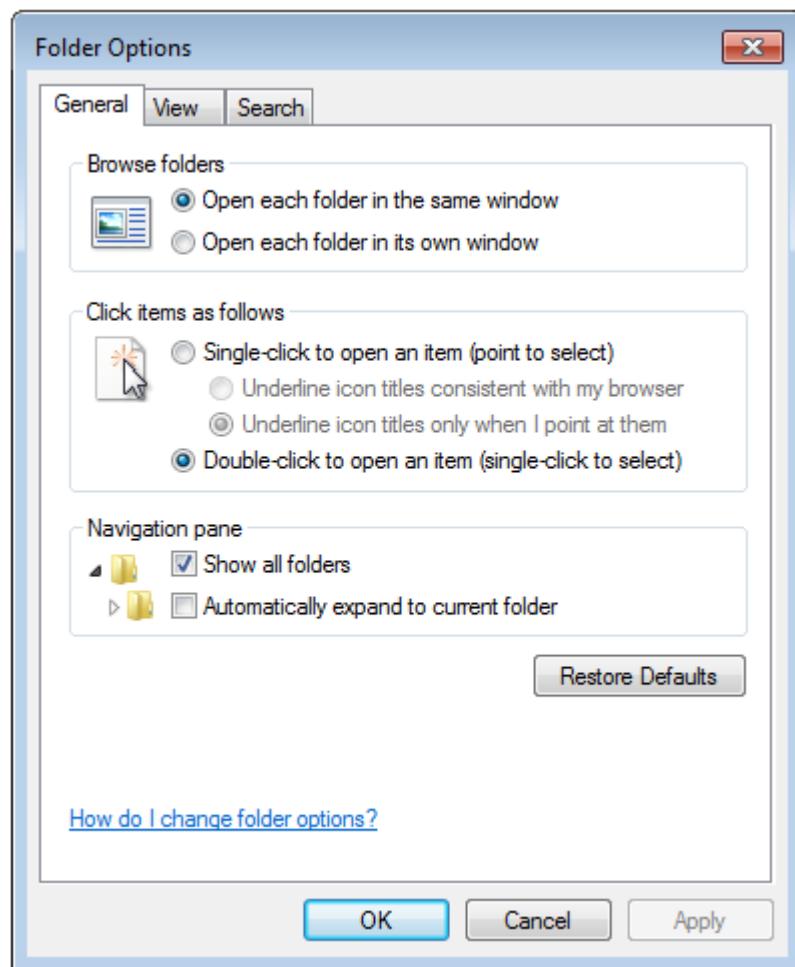
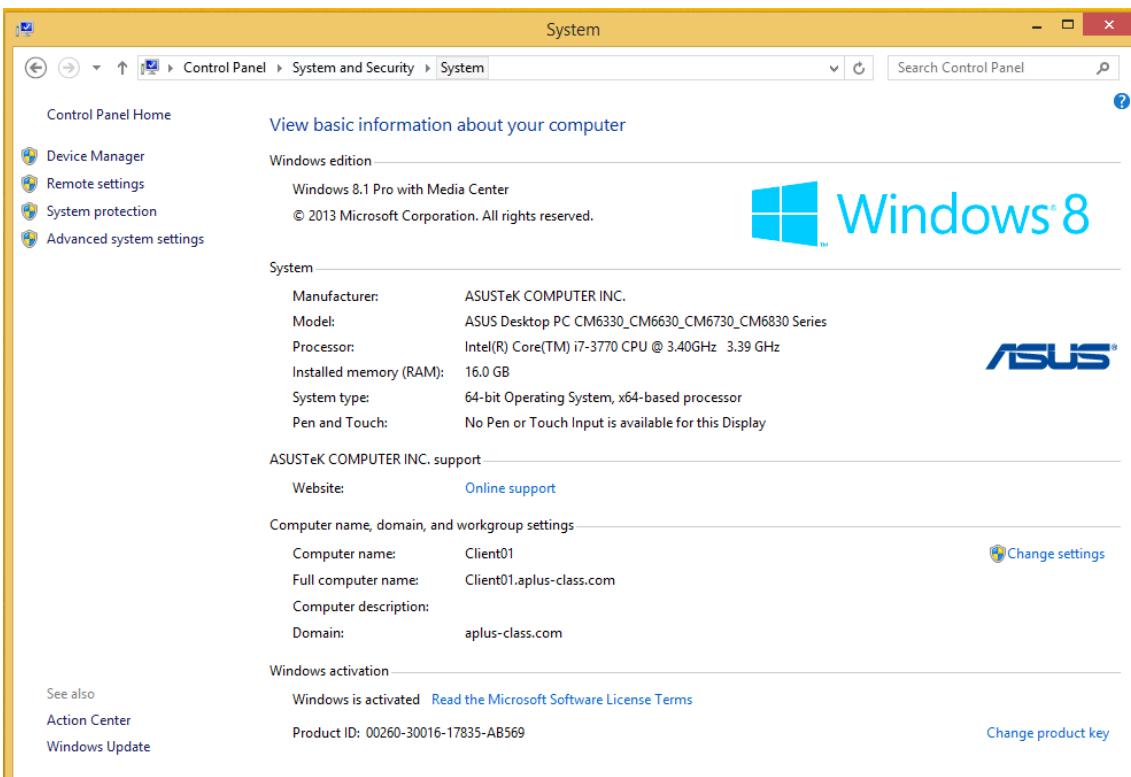


Figure 9–12: The Folder Options utility in Windows 7.

## System

The **System Control Panel** utility lets you view and configure settings for the system.



**Figure 9–13:** The System window.

System Section	Description
<b>Windows edition</b>	Identifies the edition of Windows installed on the system. If it is not the Pro or Enterprise edition, a <b>Get more features with a new edition of Windows</b> link is displayed. Select the link to purchase a license for another edition or enter the product key if you already purchased a new license.
<b>System</b>	Provides information about the system, including: <ul style="list-style-type: none"> <li>• Manufacturer</li> <li>• Model</li> <li>• Processor</li> <li>• Installed Memory (RAM)</li> <li>• System type</li> <li>• Pen and Touch</li> </ul>
<b>Support</b>	There might be a support section for the manufacturer, or that information might be provided through a link in the <b>System</b> section.
<b>Computer name, domain, and workgroup settings</b>	This section lists the current settings for <ul style="list-style-type: none"> <li>• Computer name</li> <li>• Full computer name</li> <li>• Optional Computer description</li> <li>• Workgroup or Domain name</li> </ul> The <b>Change settings</b> link in this section is used to change these settings.
<b>Windows activation</b>	Identifies whether Windows is activated and lists the Product ID. There are links to <b>Read the Microsoft Software License Terms</b> and to <b>Change product key</b> .

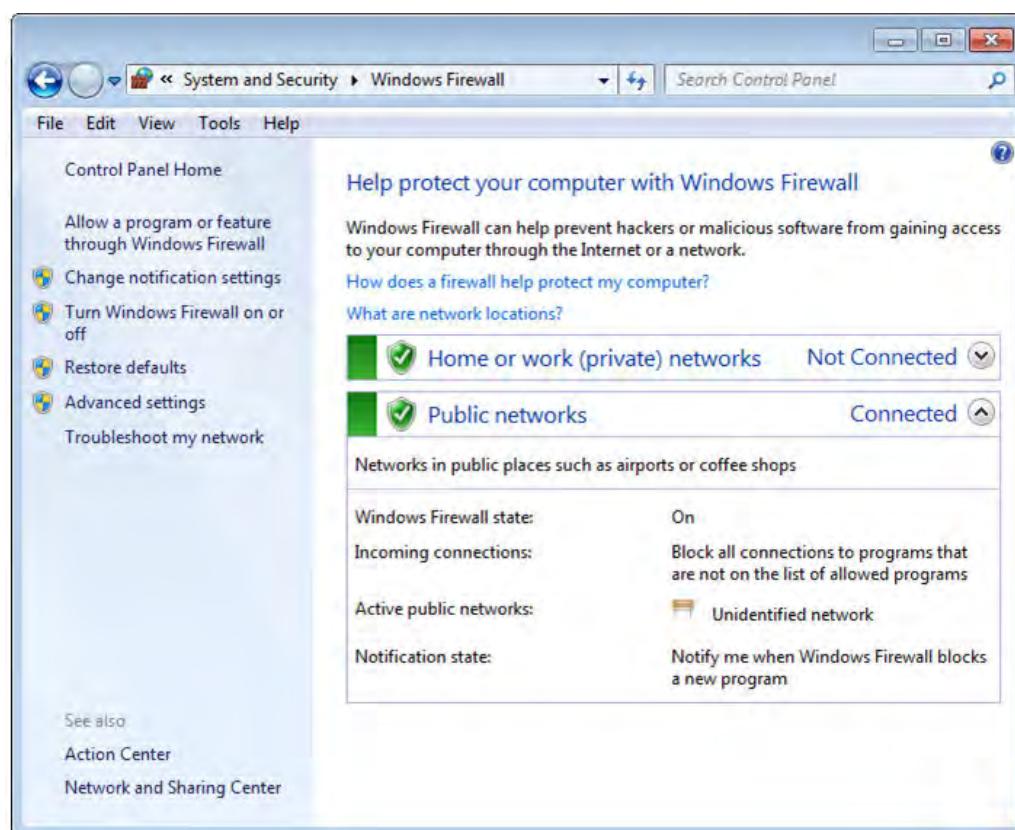
Links to other tools are also available in the left pane, including:

- Device Manager
- Remote settings
- System protection
- Advanced system settings
- Action Center
- Windows Update

## Windows Firewall

A firewall is a device or program that blocks unauthorized data transmissions and protects the computer from unauthorized access. **Windows Firewall** is a software-based firewall, included with almost all Windows installations, that protects the computer against attacks through the Internet or the network. The **Windows Firewall** utility enables you to:

- Enable or disable **Windows Firewall**.
- View active networks.
- Configure notifications concerning blocked activity.
- Open blocked ports.
- Add exceptions to blocking rules.
- Configure other firewall settings for both private (home or work) and public networks that the computer may access.



**Figure 9–14: The Windows Firewall utility in Windows 7.**



**Note:** In the corporate environment, this utility is usually not accessible to individual users, as the **Windows Firewall** settings are configured and controlled by an administrator in the IT department, or **Windows Firewall** is superseded by a dedicated enterprise-level firewall system.

## Power Options

Using the **Power Options Control Panel** utility, there are a number of power settings that can be configured for the computer.

<b>Power Option</b>	<b>Description</b>
<b>Hibernate</b>	In <i>Hibernate</i> mode, the computer will store whatever is currently in memory on the hard disk and shut down; when the computer comes out of hibernation, it will return to the state it was in upon hibernation.  In the <b>Power Options</b> utility, you can enable or disable hibernation, and you can view how much disk space is needed and available for hibernation. Once hibernation is enabled, you can configure the settings for when hibernation occurs using the <b>Power Plans</b> settings.
<b>Power Plans</b>	<b>Power Plans</b> are a set of built-in power configurations that you can use to manage how the computer uses power. For each <b>Power Plan</b> , there are default settings for when to turn off the monitor, when to turn off hard disks, and when to enter system standby, depending on whether the computer is plugged in or, if it is a laptop, is running on batteries. You can modify and save these settings for the selected power plan, or you can create and save a new power plan.
<b>Sleep/Suspend/ Standby</b>	The user can determine the amount of time of inactivity after which the computer is switched into sleep mode. In sleep mode, the computer conserves as much energy as possible by cutting off power to the parts of the machine that are not necessary to function, excluding RAM, which is needed to restore the system to its state once it is woken from sleep mode. These settings can be configured for when the computer is plugged in or, if it is a laptop, if it is running on batteries.  Depending on the operating system and version, sleep mode can be called a variety of things: <ul style="list-style-type: none"> <li>• <i>Sleep</i> mode in Windows Vista, Windows 7, Windows Server 2008, and Apple OSs.</li> <li>• <i>Suspend</i> mode in Linux.</li> </ul> <i>Standby</i> is another mode that uses less power. In standby mode, the computer reduces power to the hard drive and peripherals, while storing data in RAM. Because the data is in RAM, recovery from this mode is quicker than from sleep mode.

## Programs and Features

The **Programs and Features** utility enables you to enable or disable Windows features. You can also view installed updates or uninstall a previously installed program. In Windows 8, this utility only applies to traditional Windows applications and not to Windows Store apps; those are uninstalled from the **Start** screen tile associated with the app.



**Note:** Prior to Windows 7, to turn off a feature you had to uninstall it. In Windows 7 and beyond, the features remain stored on the hard disk, so you enable (and load) them or disable (and unload) them as needed. **Programs and Features** is where you would install IIS or uninstall features such as telnet, PowerShell, Internet Explorer, and media features.

The **Program Compatibility Troubleshooter** is also found in this utility, by selecting the link **Run programs made for previous versions of Windows**. This is a wizard-based tool that will attempt

to find and fix problems related to running older programs with the version of Windows that is installed.

## HomeGroup

Found in the **Network and Internet** category of Control Panel in Windows 7 and Windows 8/8.1, the **HomeGroup** utility is, as the name implies, designed to create a network between home computers. This is not recommended for corporate use. A peer-to-peer network is created as a homegroup on the network, through which users who join the homegroup can share files and printers, and stream media to networked devices.

## Devices and Printers

In the **Hardware and Sound** category of Control Panel, the **Devices and Printers** utility provides a single location where you can manage the external devices, and some internal devices such as SSD drives. Devices you typically find in this utility besides printers are monitors, external drives, wireless receivers for wireless mice and keyboards, network gateway device, smartphones that have been connected to the computer, other computers that might be available for sharing multimedia content, and Blue-ray disc players.

Depending on how the manufacturer wrote the drivers and software for the device, you might be able to manage all aspects of the device from this utility, or you might need to use separate utilities to manage some aspects of the device. At the very least, you can view the device's status, share it with other network users, change basic settings, and access troubleshooting tools.

## Sound

The **Sound** utility provides an interface for you to configure various sound related aspects of your system. There are four tabs in this utility.

<b>Tab</b>	<b>Description</b>
<b>Playback</b>	Configure the playback device, typically speakers, connected to the system. If there are multiple speaker sets available, you can specify which is the default.
<b>Recording</b>	Select the default recording device to use, and configure its settings and properties.
<b>Sounds</b>	Select a <b>Sound Scheme</b> to specify what sounds are created for Windows events and programs. You can select from preconfigured sound schemes, or modify the sounds associated with program events. You can also specify whether a sound is played when Windows starts up.
<b>Communications</b>	This is designed for automatically adjusting the volume of various Windows event sounds when the computer is used to make or receive phone calls. You can have it automatically reduce the volume of other sounds by 50 or 80 percent, do nothing, or mute all other sounds.

## Troubleshooting

The **Troubleshooting** utility is used to assist with identifying and automatically fixing common issues with programs, devices, network and Internet, and system and security.

## Device Manager

**Device Manager** displays all devices currently installed on the computer, and you can use it to modify the properties for these devices. You can use *Device Manager* to manage and configure hardware devices.

In Windows, there are several ways to access **Device Manager**:

- Select Start→Control Panel→System and Security→System→Device Manager.
- At a command prompt, enter the `mmc devmgmt.msc` command.
- In the navigation pane of Computer Management, select Device Manager.

In Windows 8, you can also access **Device Manager** from the Charms **Settings** option. It is found at the top of the Charms bar or, if viewing **PC settings**, it is at the bottom of the left pane.

You can use **Device Manager** to:

- View a list of all devices attached to the system.
- See the status of a device. An exclamation point means there is a problem with a device; a yellow question mark means the device has been detected but a driver is not installed, or there is a resource conflict.
- Enable or disable a device. A disabled device appears with a red X.
- Determine the device driver a device is using; upgrade a device driver; roll a device driver back to a previous version.
- Determine any system resources that the device is using, such as interrupt request lines (IRQs) or Direct Memory Access (DMA) ports.
- Uninstall or reinstall devices.

## Network and Sharing Center

Simple file sharing is disabled by default. To enable it, log on as a user with administrative privileges, open the **Control Panel**, and select **Network and File Sharing Center**. From the left pane, select the **Change advanced sharing settings** link, and then select **Turn on file and printer sharing** and **Turn off password protected sharing** and select **Save changes**.

The **Network and Sharing Center** is also where you can view active networks, access type (such as Internet), set up a new connection or network, troubleshoot network problems, change adapter settings, and configure or change advanced sharing settings.

## Windows Command Line Tools

You have already seen some of the command-line commands often used with Windows computers, including the CD, MD, RD, and DIR commands. These can be considered end-user commands. Some other commands are aimed more at administrative users.

The diagram shows a Windows Command Prompt window titled 'cmd C:\WINDOWS\system32\cmd.exe'. The window displays a command-line session. Annotations with arrows point to specific parts of the interface:

- Text-Based Commands:** Points to the command line area where commands like 'cd', 'dir', 'ren', and 'dir' are typed.
- Text-Input:** Points to the command line area where the command 'C:\>ren data documents' is being typed.
- Text-Output:** Points to the output area where the directory listing is displayed.

```

C:\>cd \
C:\>dir
Volume in drive C has no label.
Volume Serial Number is 1079-2CCB

Directory of C:\

09/12/2006  03:06 PM                0 AUTOEXEC.BAT
09/12/2006  03:06 PM                0 CONFIG.SYS
09/22/2006  11:48 AM            <DIR>          data
09/12/2006  03:17 PM            <DIR>          Documents and Settings
09/22/2006  11:43 AM            <DIR>          Program Files
09/22/2006  11:43 AM            <DIR>          WINDOWS
                           2 File(s)           0 bytes
                           4 Dir(s)        833,118,208 bytes free

C:\>ren data documents
C:\>dir
Volume in drive C has no label.
Volume Serial Number is 1079-2CCB

Directory of C:\

09/12/2006  03:06 PM                0 AUTOEXEC.BAT
09/12/2006  03:06 PM                0 CONFIG.SYS
09/22/2006  11:48 AM            <DIR>          documents
09/12/2006  03:17 PM            <DIR>          Documents and Settings
09/22/2006  11:43 AM            <DIR>          Program Files
09/22/2006  11:43 AM            <DIR>          WINDOWS
                           2 File(s)           0 bytes
                           4 Dir(s)        833,114,112 bytes free

```

Figure 9-15: The Windows command prompt.

	<b>Note:</b> The default path in Windows 7 for the prompt is the user profile folder for the current user (C:\Users\username). In Windows 8, the default path is the same as for Windows 7 unless you open Command Prompt (Admin), in which case the default path is C:\Windows\System32.
---	---

	<b>Note:</b> Because you can run DOS-type commands at the command prompt, it is sometimes casually called the "DOS prompt."
---	---

Some command-line commands complete their work in the text-based command window; others launch a GUI component. An example is MSCONFIG, which opens the System Configuration window in the GUI environment. You can run commands from the **Run** dialog box, but in some cases, the command prompt window closes as soon as the command finishes, so you don't see the results. In most cases, you will want to open an elevated **Command Prompt** window to run command-line commands.

<b>Command</b>	<b>Description</b>
<b>TASKKILL</b>	Typically used to end a task or process identified by PID or image name.
<b>BOOTREC</b>	If the <b>Startup Repair</b> option in <b>System Recovery Options</b> cannot repair system startup problems, use BOOTREC.exe to manually troubleshoot the problem. This command writes a new boot sector, compatible with the installed operating system, to the system partition.  In Windows 7, you can access bootrec through the System Recovery Options or the installation disk. In Windows 8/8.1, you will need to run bootrec at a Safe mode command prompt.
<b>SHUTDOWN</b>	This command is used to shut down, restart, log off, or hibernate a computer. Specify which state you would like to put the computer in by using options and parameters with the command. You can also use options to specify whether (and how long) to wait until the command does what you specified. For example, shutdown -r -t 0 specifies that you want to restart without waiting (restart 0 seconds from now).
<b>TASKLIST</b>	Creates a list of applications and services currently running on the local computer (or a specified remote computer). The image name, PID, session name and number, and memory usage are displayed in the task list.
<b>DISKPART</b>	The DISKPART command opens the DiskPart command interpreter. DiskPart can be used to manage computer drives including disks, partitions, volumes, and virtual hard disks.
<b>SFC</b>	The System File Checker (SFC.exe) scans for corrupted Windows system files and restores those files.
<b>CHKDSK</b>	Used to check disk integrity. Adding the /F option fixes any errors that are found on the disk.
<b>GPUPDATE</b>	Updates local and Active Directory group policy settings. Using the /Force option, you can specify that all policy settings, even those not changed, are reapplied. You can also specify that only User or Computer group policy settings are updated by using the /Target option.
<b>GPRESULT</b>	Displays group policy settings and Resultant Set of Policy (RSOP) for the specified user or computer. GPRESULT /R shows a summary of RSOP data for the current user on the local computer.
<b>EXIT</b>	Used to close the Command Prompt window. If you are running another command interpreter inside the Command Prompt window, it closes the command prompt interpreter and returns you to the command prompt.

## Command Interpreters

Windows provides several different command interpreters. The typical command prompt interface is the standard Windows command interpreter, available in Windows 7 and Windows 8. To access the command prompt interface, you can either run cmd.exe or select the **Command Prompt** shortcut from the **Accessories** menu in Windows 7. In Windows 8, from the Desktop, right-click the Start button and select **Command Prompt** or **Command Prompt (Admin)** if you need administrator access.

**PowerShell** is another command interpreter. It is designed as an administrative management and configuration environment. It is also used to create automated scripts. PowerShell uses cmdlets (pronounced as command lets). You can use the built-in cmdlets or create your own. PowerShell connects to the .NET Framework-connected environment, accepting and returning .NET Framework objects.

## Windows Administrative Tools

The **Administrative Tools** folder includes several tools that advanced users and system administrators can use to help manage the system. You can access the **Administrative Tools** folder by opening **Control Panel** and selecting **System and Maintenance** (Windows Vista and Windows 7) or **System and Security** (Windows 8/8.1).

Tool	Description
Computer Management	<i>Computer Management</i> is the primary administrative tool you will use to manage and configure a Windows computer. <b>Computer Management</b> combines several administrative utilities into a single console to provide easy access to the most common system tools, including <b>Event Viewer</b> , <b>Performance Monitor</b> , <b>Disk Management</b> , and more.
Local Users and Groups	You can use <i>Local Users and Groups</i> to create and manage user and group accounts on the local system. To access <b>Local Users and Groups</b> , open <b>Computer Management</b> , and expand <b>System Tools</b> .
Local Security Policy	You can use the <i>Local Security Policy</i> to view and edit the security settings for the local computer.
Performance Monitor	<i>Performance Monitor</i> is a software tool that monitors the state of services or daemons, processes, and resources on a system. <b>Performance Monitor</b> tracks one or more counters, which are individual statistics about the operation of different objects on the system, such as software processes or hardware components.
System Configuration	You can use <i>System Configuration</i> to identify and manage issues that may be causing the system to run improperly at startup.
Task Scheduler	You can use the <i>Task Scheduler</i> to create and manage certain system tasks that will be automatically carried out by your computer at predetermined times.
Component Services	<i>Component Services</i> is the GUI that developers and administrators can use to configure and administer Component Object Model (COM) components.
Data Sources	<i>Data Sources</i> uses Open Database Connectivity (ODBC) to move data between different databases on the system.
Print Management	You can use <i>Print Management</i> to view and manage all of the printers and print servers installed on a network.
Windows Memory Diagnostic	You can use the <i>Windows Memory Diagnostic</i> tool to check the RAM on the system and verify that it is functioning appropriately and efficiently.

Tool	Description
Windows Firewall with Advanced Security	You can use <i>Windows Firewall with Advanced Security</i> to manage advanced firewall settings for the computer and any remote computers that are connected to the network.

## Run Line Utilities

In Windows Vista and Windows 7, the **Search** function in the **Start** menu can be used in the same manner as the **Run** line, or the **Run** line can be added to the **Start** menu by customizing the properties. In Windows 8, from the Desktop, right-click the **Start** button and select **Run**. In all versions, you can also access the **Run** line via the keyboard shortcut **Windows key + R**.

You can use the **Run** line to access various system components and utilities by entering specific commands. These commands and their outcomes are the same for Windows Vista, Windows 7, and Windows 8.

Run Command	Description and function
command	Opens a new instance of the command interpreter/command prompt interface.
dxdiag	Opens and runs the <b>DirectX Diagnostic</b> tool, which displays hardware specifications and can be used to test that hardware's suitability for use with DirectX software, which handles multimedia tasks on Windows platforms. The report generated by running dxdiag can be used to view a list of all hardware, drivers, codecs, and system information for a computer, and can be a useful diagnostic tool.
explorer	Opens Windows Explorer in whatever the default view is for the system.
mmc	Opens the MMC.
[command].msc	Opens the management console for that entry (if one is available) when the .msc extension is added to the command. For example, diskmgmt.msc opens the <b>Disk Management</b> console, and services.msc opens the <b>Services Control Panel</b> .
msconfig	Opens the <b>System Configuration</b> utility.
msinfo32	Opens the <b>System Information</b> utility, which displays a summary of the hardware, software, and other system components in the environment.
mstsc	Opens the <b>Remote Desktop Connection</b> utility.
notepad	Opens an instance of Notepad.
regedit	Opens the <b>Registry Editor</b> , where the user can view or modify the contents of the Registry.
services.msc	Opens the <b>Services</b> console, where the user can manage all of the services and installed software on the system. Must be used with the .msc extension to open the management console.



**Note:** You can use the **Run** line to open programs, folders, documents, Internet resources, or any other system component if there is an appropriate command to use.

## .msc Extensions and the Run Line

There are several management consoles that you can access via the **Run** line by using the .msc extension. When you enter [command].msc in the **Run** line, it will open the management console for that utility if one is available. For example:

- devmgmt.msc opens the **Device Manager** console.
- diskmgmt.msc opens the **Disk Management** console.
- compmgmt.msc opens the **Computer Management** console.

## MSConfig

**MSConfig** is a system utility that is specifically used to troubleshoot issues that can arise during system startup. You can use it to view and manage which files or programs are processed on startup, including temporarily disabling and re-enabling software, programs, device drivers, or services that run automatically upon startup.



**Note:** **MSConfig.exe** is called **System Configuration** in Windows Vista and Windows 7, but was called the **Microsoft System Configuration Utility** in earlier versions.

Within the **MSConfig** utility, there are five areas that can be accessed and modified.

<b>Option</b>	<b>Description</b>
<b>General</b>	<p>Provides the options to choose from for startup configuration modes:</p> <ul style="list-style-type: none"> <li>• Normal startup. Windows will start in the normal manner. This is the default configuration or is selected once the other two modes have been used to troubleshoot an issue.</li> <li>• Diagnostic startup. Use this mode to troubleshoot issues by ruling out potential problem files. Windows will start running only basic services and drivers.</li> <li>• Selective startup. Use this mode to troubleshoot issues by running only the basic services and drivers at startup, but allowing the user to launch selected programs after startup. This enables you to begin to rule out each program as the potential cause of the problem.</li> </ul>

<i>Option</i>	<i>Description</i>
<b>Boot</b>	<p>Provides configuration settings for the boot process and advanced debugging configurations.</p> <p>Basic <b>Boot</b> options include:</p> <ul style="list-style-type: none"> <li>• Safe boot mode, including Minimal, Alternate shell, Active Directory repair, or Network modes.</li> <li>• No GUI boot.</li> <li>• Boot log.</li> <li>• Base video.</li> <li>• OS boot information.</li> <li>• Make all boot settings permanent.</li> </ul> <p>Advanced options include:</p> <ul style="list-style-type: none"> <li>• Number of processors.</li> <li>• Maximum memory.</li> <li>• PCI lock.</li> <li>• Debug.</li> <li>• Global debug settings.</li> <li>• Debug port.</li> <li>• Baud rate.</li> <li>• Channel.</li> <li>• USB target name.</li> </ul>
<b>Services</b>	<p>Displays all of the services that begin running at startup and their current status (running or stopped) and can be used to temporarily disable or re-enable specific programs or services to begin to determine which are potentially causing the problem at startup.</p>
<b>Startup</b>	<p>Displays all of the applications that begin running at startup, including the publisher of the application, the path to the .exe for the application, and the location of the shortcut or registry key for the application. You can temporarily disable or re-enable applications upon startup to begin to determine which application may be causing the startup issue.</p>
<b>Tools</b>	<p>Displays all of the diagnostic and advanced troubleshooting tools that are available on the system to help identify and fix the problem.</p>

The **MSConfig** tool is frequently used to test various configurations for diagnostic purposes, rather than to permanently make configuration changes. Following diagnostic testing, permanent changes would typically be made with more appropriate tools, such as **Services**, to change the startup settings of various system services.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Configure Microsoft Windows.

# ACTIVITY 9–6

## Configuring Microsoft Windows

### Before You Begin

You will perform this activity on your Windows 8.1 system.

### Scenario

In order to be more proficient in your role as a PC technician, you decide to practice using some of the configuration tools you recently learned about. It can be difficult to remember the names of commands to run, so you are excited to see that System Configuration, started by running MSCONFIG, provides access to many of the tools you will need as a technician.

1. Examine the system information with msinfo32.
  - a) Press **Windows + R**, and in the **Run** text box, enter ***msinfo32***
  - b) In the **System Information** dialog box, in the right pane, verify that the system is running Microsoft Windows 8.1 Enterprise (or Pro).
  - c) In the left pane, expand **Hardware Resources**.
  - d) To view the assigned interrupts, select **IRQs**.
  - e) Collapse **Hardware Resources**.
  - f) Expand **Components** and select **CD-ROM** to view information about your CD-ROM drive.



**Note:** If there is no CD-ROM drive, select another device.

- g) Collapse **Components**.
- h) Expand **Software Environment** and select **System Drivers** to view all the drivers installed on your computer.
- i) Select **File→Export** and save the file to the default location as ***my\_sys\_info***
- j) From the folder where you saved *my\_sys\_info.txt*, open the file in Notepad, review the information, then close Notepad.
- k) Collapse **Software Environment**.
- l) Close **System Information**.

2. Examine the system configuration settings with **MSConfig**.

- a) Press **Windows + R** and in the **Run** text box, enter ***msconfig*** and if prompted, select **Yes**.

**System Configuration** is a diagnostic and troubleshooting utility that can help automate routine troubleshooting steps. The **General** page controls overall startup behavior.

- b) Select the **Boot** tab.  
**System Configuration** provides another way to define how you want to boot the computer.
- c) Select the **Services** tab.

You can use **System Configuration** to enable or disable services that start when your computer boots.

- d) Select the **Startup** tab.  
On a Windows 7 system you can view and manage items that are configured to load at system startup. For Windows 8 you are provided with a link to **Task Manager**, which is where startup items are located for Windows 8.
- e) Select the **Tools** tab.
- f) Select each of the tools and observe the executable command associated with each tool.
- g) To close **System Configuration**, select **Cancel**.

# TOPIC E

## Upgrade Microsoft Windows

Previously, you installed Microsoft Windows on a PC. Upgrades are one method for installing Windows, but they are more commonly used to migrate from one version of Windows to a different or newer version. In this topic, you will perform a Windows upgrade.

Software vendors such as Microsoft are constantly coming out with new operating system versions, and it can sometimes be more economical to upgrade existing systems when possible, rather than to purchase new computer hardware with the new version pre-installed. Whether you are upgrading for an individual user or as part of a company-wide migration plan, the skills in this topic should help you upgrade from older versions of Windows to the current version successfully.

### In-Place Upgrades

An *in-place upgrade* is the process of installing a newer version of an operating system without first removing the existing operating system that is currently installed on the computer. In-place upgrades also eliminate the need to perform the most tedious tasks involved with a clean install of an operating system: saving or backing up data that has been saved on the computer, wiping the hard drive, migrating or transferring saved data back to the machine, and reinstalling any programs that had been added to the system. In essence, an in-place upgrade can overwrite the existing, older operating system with the new version without disruption to the end user's environment.

In-place upgrades have been known to cause problems when upgrading to a version of the operating system that is significantly different from the existing version. In-place upgrades are only recommended when moving between operating systems that are one version apart, such as from Windows Vista to Windows 7. When there is a larger gap in the differences between the systems, such as migrating from Windows Vista to Windows 8, a clean install is recommended instead of an in-place upgrade.

### Supported Upgrade Paths

Existing Windows operating systems that are installed on a machine can be upgraded to another version of Windows, but these upgrades can only follow specific and supported upgrade paths.

<i>Current Operating System</i>	<i>Can Be Upgraded To</i>
Windows Vista with SP1	<ul style="list-style-type: none"> <li>Any higher level of Windows Vista</li> <li>The same level of Windows 7 or higher</li> </ul>
Windows 7	<ul style="list-style-type: none"> <li>Any higher level of Windows 7</li> <li>Any level of Windows 8</li> <li>Any level of Windows 8.1</li> </ul>
Windows 8	<ul style="list-style-type: none"> <li>Any higher level of Windows 8</li> <li>Any level of Windows 8.1</li> </ul>
Windows 8.1	Any higher level of Windows 8.1

### Compatibility Tools

When upgrading to a different version of Windows, you will need to check to ensure that the existing hardware is compatible with the new operating system and that your existing software

applications will run properly on the new version of Windows. Applications written for earlier versions of Windows might not always work with your new OS version, but you may be able to select an appropriate application compatibility mode for the application after you have upgraded the operating system.



**Note:** To access the Upgrade Advisor to see if your system can run Windows 7, you can visit <http://windows.microsoft.com/en-US/windows/downloads/upgrade-advisor>.

For Windows 8 and Windows 8.1, download and run the Upgrade Assistant from <http://windows.microsoft.com/en-us/windows-8/upgrade-assistant-download-online-faq>. After the assistant analyzes the computer, a compatibility report lists the apps and devices that are compatible with Windows 8 or Windows 8.1, any items that need to be reviewed, and information about reinstalling compatible apps and devices.

## Application Compatibility Modes

The Windows 7 application compatibility modes are Windows 95, Windows 98/Windows Me, Windows NT 4.0 (Service Pack 5), Windows 2000, Windows XP (Service Pack 2), and Windows Server® 2003 (Service Pack 1). You can set the appropriate mode for a particular application by right-clicking the program's executable, choosing **Properties**, selecting the **Compatibility** tab, and then choosing the desired OS from the drop-down list.

In Windows 8, use the **Program Compatibility Assistant** to have Windows 8 automatically make the required changes to allow older applications to run under Windows 8/8.1. If the assistant is unable to allow the older application to run, you can try manually adjusting the settings. If that still doesn't work, you should upgrade the application to a current version that is compatible with Windows 8.



**Note:** The Windows Compatibility Center was a central location where you could find out if your hardware or software was compatible with the latest version of Windows. However, this feature has been retired and is no longer available on the Microsoft website.

## Migration Tools

There are some tools available through the Windows operating system to assist in migrating user information between systems, including files and settings.

Migration Tool	Description
User State Migration Tool	The <i>User State Migration Tool (USMT)</i> is a command line utility that copies files and settings from one Microsoft Windows computer to another, including user accounts, files, folders, Windows settings, email messages, and more. USMT can support the transfer of files and settings for Windows 2000, Windows XP, Windows Vista, Windows 7, and Windows 8. Not all versions of the USMT can support all source or destination operating systems.
Easy Transfer	<i>Easy Transfer</i> is a built-in data-migration utility in Windows Vista and above that helps transfer files, data, and settings from one personal computer to another. If the computer isn't running Windows 7 or Windows 8, the user will need to download and install a version of <b>Easy Transfer</b> for Windows Vista or Windows XP before beginning the migration process.
	<b>Easy Transfer</b> replaced the <b>Files and Settings Transfer Wizard</b> from Windows XP. It was upgraded with Windows 7 to include a file explorer for easy selection of files to transfer and provides a report of any files that were not migrated to the new system.

## Windows Upgrade OS Advisor

The Microsoft Windows 7 Upgrade Advisor can be a useful tool in determining whether a system meets the requirements for Windows 7. For single systems or for home computers, you can download and run the Windows 7 Upgrade Advisor, available at <http://windows.microsoft.com/en-us/windows/downloads/upgrade-advisor>. The Upgrade Advisor will scan your hardware and any connected devices to determine if you can upgrade to Windows 7 with your current hardware configuration. A similar tool was available for Windows Vista as well.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Perform a Windows Upgrade.

# ACTIVITY 9–7

## Upgrading a Windows System

### Before You Begin

You have Windows 7 installed in a VM that is capable of being upgraded to Windows 8.1.

Your instructor will provide you with installation media or the location of the Windows 8.1 ISO.

You will use the Microsoft Live ID email address you have been assigned for the class.

### Scenario

Your organization is no longer supporting Windows 7 systems. In preparation for upgrading those users still using Windows 7, you use your VM installation of Windows 7 to upgrade to Windows 8.1.

1. Verify that the Windows 7 system meets the requirements for Windows 8.1.
  - a) Log in to the Windows 7 system.
  - b) Open a web browser and access <http://go.microsoft.com/fwlink/p/?LinkId=261871>.
  - c) Select **Run** when prompted as to what action to take on the downloaded file.  
The Windows 8.1 Upgrade Assistant starts analyzing your system.
  - d) Review the information on the **Here's what we found** page and then select **Next**.
  - e) On the **Choose what to keep** page, examine the choices, and then, with **Windows settings, personal files, and apps** selected, select **Next**.
  - f) If **No compatible offers are available** is displayed, select **Back** and select **Just personal files** and select **Next**.
  - g) On the **Windows 8.1 is for you** page, select **Close**.  
You could purchase Windows 8.1 from this page.
  
2. Begin the Windows 8.1 upgrade.
  - a) Insert the media containing Windows 8.1 or point your system to the ISO location.
 

 **Note:** To insert the ISO file in Hyper-V, in the **Virtual Machine Connection** window, select **Media→DVD Drive→Insert Disk** then specify the path to the ISO image file.
  - b) From the DVD or ISO, run **setup.exe**.  
You might need to navigate a folder structure or perform additional steps to access the **setup.exe** file.
  - c) If prompted to **Get important updates** select **No, thanks** and then select **Next**.
  - d) If necessary, provide the product key and then select **Next**.
  - e) On the **License terms** page, check **I accept the license terms** and then select **Accept**.
  - f) Confirm what items to keep.
  - g) On the **Ready to install** page, select **Install**.  
The system will reboot several times as it is analyzed, files are copied, and the installation process begins.
  
3. Continue the installation
  - a) On the **Region and language** page, make any needed changes, then select **Next**.
  - b) On the **Personalize** page, select a color.
  - c) In the **PC name** text box, type **UpGrd##** where ## is your student number.
  - d) Select **Next**.

- e) If necessary, on the **Wireless** page, follow your instructor's directions to select and connect to an available wireless network, and then select **Next**.
  - f) On the **Settings** page, select **Use express settings**, and then select **Next**. You will configure Windows settings in upcoming activities, so you can accept the default settings for now.
  - g) On the **Sign in to your Microsoft Account** page, type the email address associated with your assigned Microsoft account, and then select **Next**.
  - h) On the **Help us protect your info** page, select **I can't do this right now**.
  - i) On the **OneDrive is your cloud storage** page, select **Next**. Windows uses your Microsoft account information to create a computer account and applies any personalized settings to that account.
  - j) When the system reboots, log in.
  - k) Observe the screen as Windows installs apps. Several messages are displayed that are intended to help you use the Windows 8.1 interface. When the Desktop screen is displayed, the Windows installation process is complete.
4. Update the name of the VM.
- a) In **Hyper-V Manager**, select the Windows 7 VM.
  - b) In the **Actions** pane, select **Rename**.
  - c) Rename the VM to **Upgrd##**
-

## Summary

In this lesson, you installed and configured operating systems. Whether you are upgrading, installing from scratch, or redeploying a system, you will need the skills that enable you to install, configure, and optimize computer operating systems to meet your business needs.

**Do you have experience installing operating systems? Do you feel you will be able to perform installations more efficiently as a result of the information presented in this lesson?**

**How often do you expect to be able to perform in-place upgrades instead of clean installs at your workplace?**



**Note:** Check your CHOICE Course screen for opportunities to interact with your classmates, peers, and the larger CHOICE online community about the topics covered in this course or other topics you are interested in. From the Course screen you can also access available resources for a more continuous learning experience.



10

# Optimizing and Maintaining Microsoft Windows

**Lesson Time:** 1 hour, 30 minutes

## Lesson Objectives

In this lesson, you will optimize and maintain Microsoft Windows. You will:

- Optimize the Windows operating system.
- Back up and restore system data.
- Perform disk maintenance tasks.
- Update operating system and other system software.

## Lesson Introduction

In the last lesson, you installed, configured, and upgraded Microsoft® Windows®. Once you have installed the OS, you need to maintain it on an ongoing basis and set up some basic preventive maintenance procedures to keep the device running. You will also want to make sure it is running the best it possibly can, so being able to optimize the OS is also important.

Maintaining an OS might not seem as exciting or interesting as performing a new installation or replacing a hard disk, but it is actually one of the most crucial tasks for a support technician. System maintenance is important for two reasons; first, proper maintenance can prevent system problems from arising. Second, proper maintenance of the system, including the creation of appropriate backups, can make recovery or troubleshooting operations much easier in the event that problems do arise. As an A+ technician, you can use the skills and information in this lesson to perform preventive maintenance as part of your ongoing job tasks.

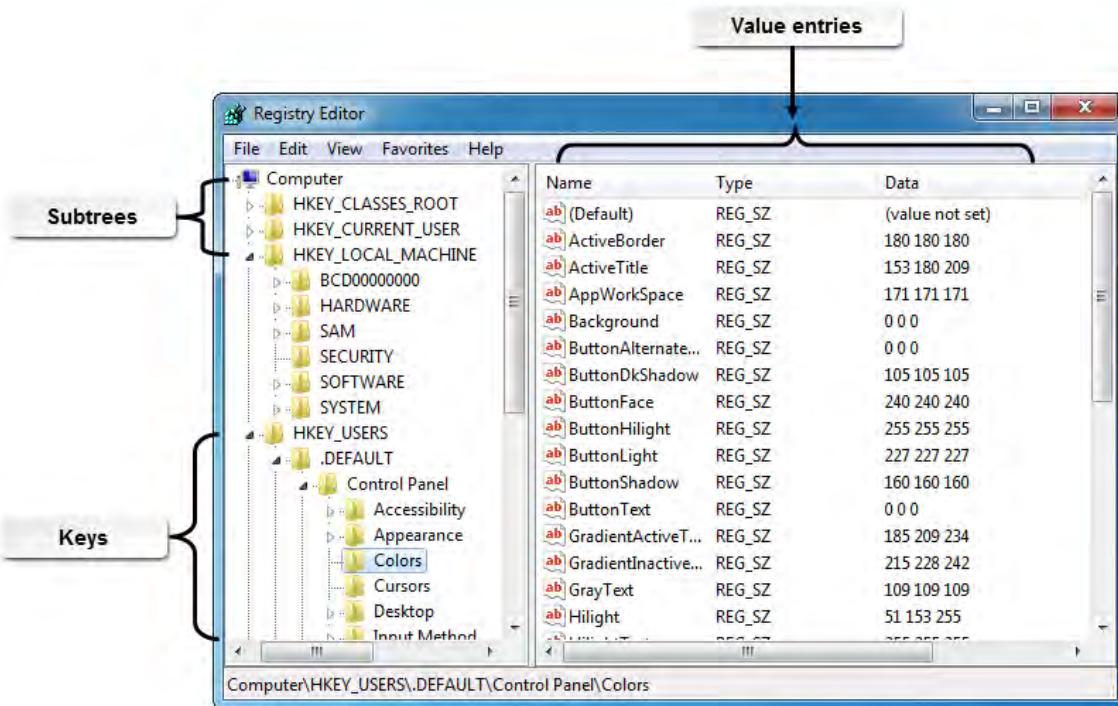
# TOPIC A

## Optimize Microsoft Windows

Once you've installed an OS and performed the initial configuration, you've provided a basic level of functionality. Over time, you might find that performance is lagging or that your specific requirements are not being met. Just installing and configuring is not the end of the job for an A+ technician. You will also want and need to optimize Windows so that you and your users can get the most out of the OS.

### The Registry

The *Registry* is the central configuration database where Windows stores and retrieves startup settings, hardware and software configuration information, and information for local user accounts. Logically, the Registry is divided into five sections called subtrees; each subtree is further divided into keys that contain individual data items called value entries. The Registry is stored on the disk as a group of files.



**Figure 10-1: The Registry.**

The Registry consists of five files stored in the \Windows\System32\Config folder: **Default**, **SAM**, **Security**, **Software**, and **System**. Plus, there is a Registry file named Ntuser.dat, which is unique for each user who logs on to the computer. This file is stored in each user's profile folder.

An individual Registry value entry consists of a name, a data type, and the actual data stored in the value. The data types can be various types of alphanumeric strings, binary data, or hexadecimal data.



**Note:** For additional information, check out the LearnTO **Use the Registry** presentation in the LearnTOs for this course on your CHOICE Course screen.

## Registry Subtrees

The Registry consists of five subtrees, which are sometimes called hives. Some of the subtrees are temporary pointers to information stored permanently in another Registry location. The following table lists and describes the subtrees.

	<b>Note:</b> HKEY is an abbreviation for "handle to Registry key."
<b>Subtree</b> <b>Contains</b>	
HKEY_CURRENT_USER	The user-specific configuration information for the user currently logged on to Windows. For example, information about the user's selected color scheme and wallpaper is stored in this subtree. These settings take precedence over the default settings for the local machine.
HKEY_USERS	User-specific configuration information for all the users who have ever logged onto Windows.
HKEY_LOCAL_MACHINE	All the configuration information for the computer's hardware. For example, this subtree contains information about any modems installed in the computer, any defined hardware profiles, and the networking configuration. These settings will be used when there are no settings specified in HKEY_CURRENT_USER.
HKEY_CURRENT_CONFIGURATION	Information about the current configuration of the computer's hardware. Windows operating systems support Plug and Play (PnP), a set of industry-standard device specifications, originally developed by Intel Corporation, which enables computers to automatically detect and install various types of devices without user intervention.
HKEY_CLASSES_ROOT	All the file association information. Windows uses this information to determine which application it should open whenever you double-click a file with a specific extension. For example, Windows automatically opens Notepad whenever you double-click a file with the extension .txt.  In Windows 95 and later, HKEY_CLASSES_ROOT displays merged information from other hives such as HKEY_LOCAL_MACHINE and HKEY_CURRENT_USER. To gain accurate configuration information, refer to those hives.

## Registry Editing

You can view and edit the contents of the Registry directly using the **Registry Editor** tool, regedit.exe. However, most changes to the Registry are made automatically by the system, by hardware devices, and by applications. It is rarely necessary to edit the Registry directly. If you ever need to do so, use extreme caution and back up the Registry files first, because incorrect changes can cause irrecoverable problems with Windows.

	Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to View and Edit the Registry.
---	---

# ACTIVITY 10-1

## Viewing and Editing the Registry

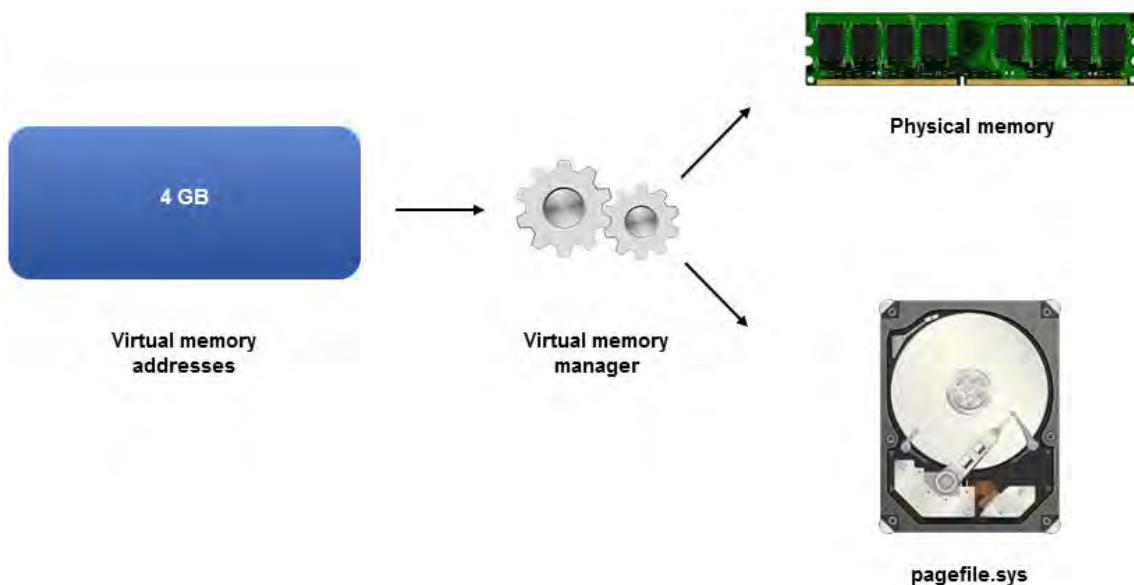
### Scenario

You have heard that making changes to settings on your computer changes values in the registry file. You want to experiment with making changes and see if the value changes in the registry.

1. View the current value for MouseTrails registry settings.
  - a) Open the **Run** dialog box and enter **regedit**
  - b) If prompted for Administrative access, select **Yes**.
  - c) In the **Registry Editor** window, select **Edit->Find**. In the **Find** dialog box, enter **mousetrails**
  - d) Observe the current value for **MouseTrails**. It should currently have a **0** in the **Data** column.
2. Back up the **Mouse** registry entry.
  - a) In the left pane, select **Mouse**.
  - b) Select **File->Export**.
  - c) In the **Export Registry File** dialog box, in the default location, save the file as **MouseBkup.reg**
3. Change the Mouse Trail setting in Control Panel.
  - a) Open **Control Panel**.
  - b) Select **Mouse**.
  - c) On the **Pointer Options** tab, check **Display pointer trails** and then select **OK**.
4. View the value in Registry Editor.
  - a) In the left pane of **Registry Editor**, collapse **Control Panel** then expand it again.
  - b) Select **Mouse**.
  - c) Observe the value for **MouseTrails**. The value has changed to **7**.
5. Set Mouse Trails to your preferred setting in Control Panel.

### Virtual Memory

Using *virtual memory* is a way for the computer to accomplish more than the limits of what its physical memory can perform. The computer system uses a portion of the hard disk as if it was physical RAM. When all physical memory is filled, the OS can transfer some of the least-recently used data from memory to a file on the hard disk called the *pagefile*, thereby freeing up an equivalent amount of space in main RAM for other purposes. When the original data is needed again, the next least-recently used data is moved out of RAM onto the hard drive to make room to reimport the needed data. In Windows systems, the *Virtual Memory Manager* (VMM) manages the memory mappings and assignments.



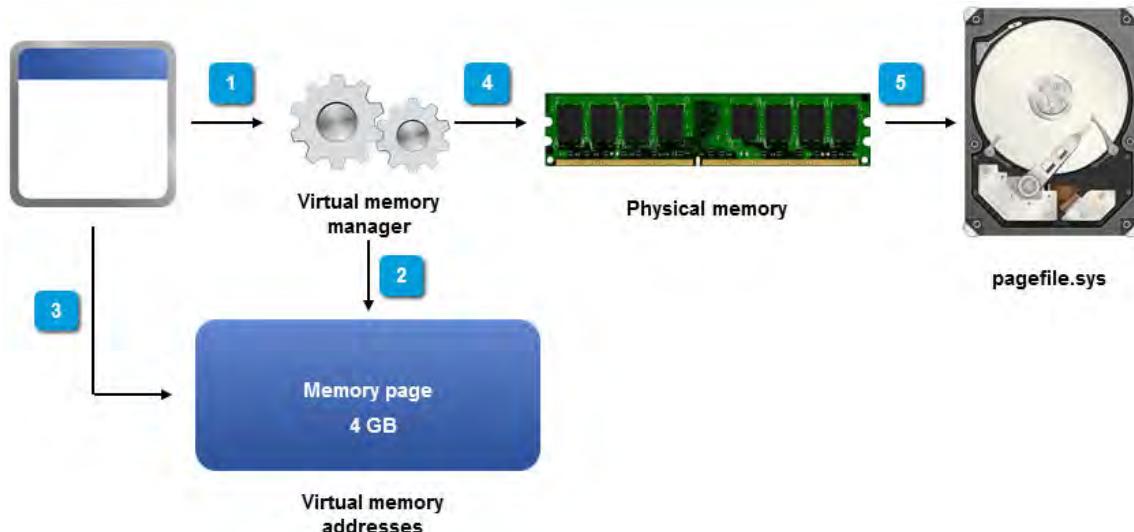
**Figure 10-2: Virtual memory.**

Virtual memory is not nearly as fast as actual memory. Modern SDRAM DIMMs read/write speeds are measured in nanoseconds, whereas hard drive seek, read, and write times are measured in milliseconds. If your computer is frequently exceeding its physical RAM and having to resort to using a pagefile on disk, adding more physical RAM may be the most economic way of effecting a noticeable change in performance.

## The Virtual Memory Process

When data is stored in virtual memory:

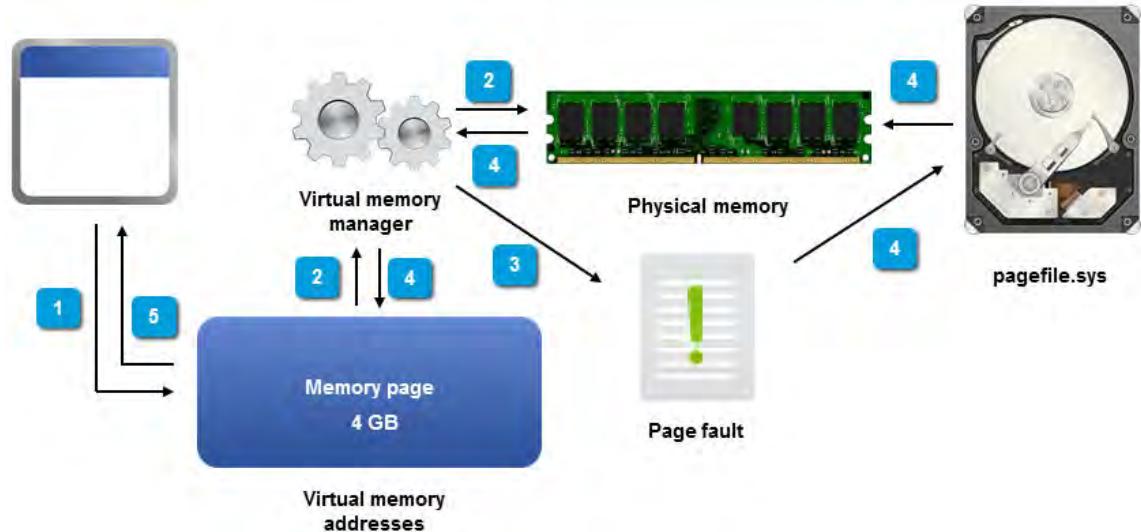
1. An application loads and requests memory from the system.
2. The VMM assigns it a *page* of memory addresses from within the virtual memory space.
3. The application stores information in one or more of the virtual memory locations.
4. The VMM maps the virtual address the application uses to a physical location in RAM.
5. As physical RAM becomes full, the VMM moves inactive data from memory to the pagefile in a process called *paging* or *swapping*.



**Figure 10-3: Storing virtual memory data.**

When data is retrieved from virtual memory:

1. An application requests data from its virtual memory location.
2. The VMM determines which physical RAM location was mapped to this virtual memory address.
3. If the VMM finds that the data is not present in the RAM location, it generates an interrupt called a *page fault*.
4. The VMM locates the data in the pagefile, retrieves the data from the hard disk, loads it back into RAM, and updates the virtual-to-physical address mapping for the application. If necessary, the VMM swaps other data out of RAM to release space.
5. The application retrieves the data from RAM.



**Figure 10-4: Retrieving data from virtual memory.**

### Pagefile Optimization

When you install Windows, the system automatically creates a pagefile named Pagefile.sys at the root of the drive. The size of the pagefile varies within a range determined by the pagefile's initial size value and maximum size value. The system sets the size values of the pagefile using an algorithm that takes into account the amount of physical memory and the space available on the disk. When the system starts, the pagefile is set to the initial size; if more virtual memory space is needed, the system adds it to the pagefile until it reaches the maximum size. An administrator can alter the initial and maximum size values to optimize the pagefile and virtual memory performance. In modern systems, there is rarely a severe shortage of either physical RAM or disk space, so optimizing the pagefile might not be an issue, but you can consider the following tips:

- Although Microsoft recommends an initial pagefile size of 1.5 times the amount of RAM, the more RAM you have, the smaller a pagefile you need.
- If the initial size of the pagefile is too low, the system will waste time as it adds more space to the pagefile. Adding space to the pagefile after startup also increases disk fragmentation. Consequently, it is often a good idea to set the initial size to the same value as the maximum size. If the initial size is too high, however, the pagefile will be mostly empty, which wastes disk space.
- If you get a lot of "low virtual memory" errors, increase the maximum size of the pagefile.
- If you have multiple drives, you can move the pagefile off the drive that contains the Windows system files, so that the computer can access system files and pagefile information simultaneously. Put the pagefile on the fastest drive that does not contain Windows.
- If there is not a noticeable speed difference between drives, create additional pagefiles on multiple drives. This speeds access time because the system can read and write from multiple

drives simultaneously. However, there is no performance advantage to putting the pagefile on different partitions on the same disk.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Optimize Virtual Memory.

# ACTIVITY 10-2

## Optimizing Virtual Memory

### Before You Begin

You have installed a second drive in your computer.

### Scenario

Some users have complained that their systems seem to frequently display messages that there is not enough memory available. You want to try adding a paging file to a second hard drive you recently installed to see if this might resolve the issue.

1. View the current Virtual Memory settings.
  - a) Open **Control Panel**, select **System**, and then in the left pane, select **Advanced system settings**.
  - b) On the **Advanced** tab, in the **Performance** section, select **Settings**.
  - c) In the **Performance Options** dialog box, select the **Advanced** tab.
  - d) In the **Virtual memory** section, select **Change** to open the **Virtual Memory** dialog box. You can see the current size of the pagefile in the **Currently Allocated** area at the bottom of the dialog box. By default, Windows automatically allocates the pagefile size for the primary C drive created at the time of installation.
2. Add a page file to the second hard drive.
  - a) Uncheck the **Automatically manage paging file size for all drives** check box to manually set the pagefile size.
  - b) Select Drive D.
  - c) Select **System managed size** and then select **Set**.
  - d) Select **OK** four times.
  - e) Select **Restart Now**.
  - f) Log in when the system has restarted.

# TOPIC B

## Back Up and Restore System Data

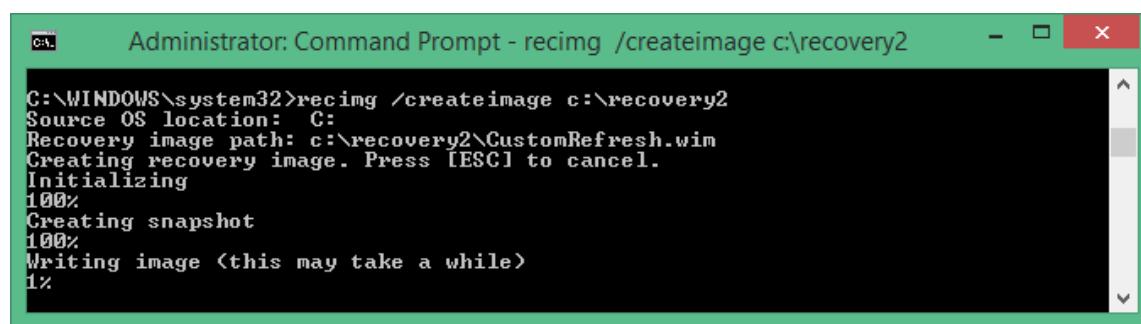
One of the important tasks you will need to perform as an A+ technician is making sure that users' data and system settings are being backed up in case things go awry. In this topic, you will examine some of the ways you can back up and restore system data.

### Data Backup and Restoration

*Data backup* is a system maintenance task that enables you to store copies of critical data for safekeeping. Backups protect against loss of data due to disasters such as file corruption or hardware failure. *Data restoration* is a system recovery task that enables you to access the backed-up data. Restored data does not include any changes made to the data after the backup operation. Data backups can be accomplished simply by copying individual files and folders to a local or network location or by using dedicated software and hardware to back up large amounts of data.

### Recovery Images

A *recovery image* is used when you request Windows to refresh your computer. Windows 8 and 8.1 computers come with a recovery image, but if you make changes and receive updates, refreshing the computer will eliminate those changes. You can create a custom recovery image using RECIMG.EXE from an elevated command prompt. This custom recovery image contains all of the desktop applications installed on the computer and the current state of Windows system files.



```
Administrator: Command Prompt - recimg /createimage c:\recovery2
C:\WINDOWS\system32>recimg /createimage c:\recovery2
Source OS location: C:
Recovery image path: c:\recovery2\CustomRefresh.wim
Creating recovery image. Press [ESC] to cancel.
Initializing
100%
Creating snapshot
100%
Writing image (this may take a while)
1%
```

Figure 10-5: Creating a custom recovery image in the C:\recovery2 folder.

The file created is named CustomRefresh.wim. When you create a custom recovery image, you specify which directory to store it in. If you have multiple custom recovery images, they all have the name CustomRefresh.wim, each under a different directory or folder.

Recovery images aren't used to store or refresh Windows Store apps, your documents, user profiles, or your personal settings. This information is preserved when you refresh your computer.

You can have multiple recovery images. When you are ready to refresh your computer, you can specify which custom recovery image to use as the active recovery image.

### System Restore

Windows Vista and Windows 7 use System Restore to assist in restoring system files on your computer to the way those files were at an earlier point in time. The system image is an exact duplicate of a drive. The system protection feature is used to create and save restore points that contain Registry settings and system information. A restore point represents a stored state of system

files. Windows creates restore points automatically each week or when a new driver or program is installed. You can also manually create restore points.

## System Image

A *system image* is a copy of Windows, applications, system settings, and data files that is stored in a separate location from where the originals of these items are stored. The system image can be used to restore your system if the hard disk or computer fails. The default when creating a system image is to only include the drives required to run Windows. A system image can only be created from drives formatted with the NTFS file system. Windows Backup can be used to create a backup of the files as well as the system image. Although backups can be saved to USB flash drives, CDs, DVDs, or hard drives, the system image can only be saved to a hard drive.

## Scheduled Tasks

Many of the preventive maintenance tools included with the Windows environment also provide you with the option of scheduling and automating the tasks they perform. Scheduling preventive maintenance tasks ensures that your data is safe and your computer is performing optimally.

Different organizations and even different administrators within an organization may have differing opinions on what preventive tasks should be performed automatically and how often. There are best practices for any organization or individual user when it comes to performing scheduled tasks.

Backups should be performed systematically and on a regular basis for the best protection against data loss. For large organizations that have important business data, scheduled backups are likely to be performed nightly for all users or for specific data housed in specific locations, and will be planned and scheduled by IT administrators. For smaller businesses or even individual users, backups can be scheduled to run automatically via the backup utility provided with the version of Windows. Users can choose what information will be saved, how it is saved (full or incremental), where it is saved to, and how often the backup will occur.

## Backup Schemes

Most large organizations will implement a structured backup scheme that includes a backup schedule and specifications for which files are backed up, where the backup is stored, and how it can be retrieved. The backup scheme will specify the backup *rotation method*, which determines how many backup tapes or other media sets are needed, and the sequence in which they are used and reused. Designated administrators will have the responsibility for designing and managing the backup scheme and for restoring data when needed.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Back Up and Restore System Data.

# ACTIVITY 10-3

## Scheduling System Backup

### Scenario

You do a lot of testing, and sometimes that testing can result in loss of data or in a system that doesn't work properly any more. You need to set up recurring system backups for your computer.

1. Turn on File History.
  - a) From the Charms bar, select **Settings**→**Change PC Settings**.
  - b) Select **Update and recovery**.
  - c) Select **File History** then select **On**.  
Backup should begin immediately.
2. Check the schedule for backups.
  - a) Open **Control Panel**.
  - b) Select **System and Security**→**File History** and then in the left pane, select **Advanced settings**.
  - c) Verify that the settings are configured to save copies of files every hour.
  - d) Close open windows, leaving only **Hyper-V Manager** and any VM windows open.

# TOPIC C

## Perform Disk Maintenance

In the last topic, you backed up system data to keep it safe. Another way to keep data safe is to ensure that a PC's disk drives are functioning properly. In this topic, you will perform disk maintenance tasks.

### Disk Maintenance

*Disk maintenance* is the process of monitoring and adjusting the configuration of HDDs and the file systems contained on those HDDs. Typically, disks work just fine without a great deal of maintenance. However, there are some actions and practices that can affect disk health and performance. By performing some relatively simple disk maintenance tasks, you can avoid or even solve problems such as:

- File system errors
- Bad sectors on the disk platters
- Corrupted files
- Disk fragmentation

### Disk Maintenance Tools

There are a number of tools within the Windows environment that can be used to perform preventive maintenance tasks.

<b>Maintenance Tool</b>	<b>Description</b>
Check Disk	<p>You can run a Check Disk (or <code>chkdsk</code> if using a command prompt) to scan the hard disk for any potential file system errors or bad sectors on the disk.</p> <p>Using Check Disk, you can:</p> <ul style="list-style-type: none"> <li>• Scan only for file system errors and view a report of any drive errors.</li> <li>• Scan for file system errors and attempt to automatically fix them.</li> <li>• Scan for bad sectors and attempt recovery of them.</li> <li>• Scan for both file system errors and bad sectors, and attempt to automatically fix both types of problems.</li> </ul> <p>In addition, Check Disk will run if the OS detects changes in the file system, storage configuration, or volume incompatibility in a multiboot configuration. See <a href="https://support.microsoft.com/en-us/kb/2854570">https://support.microsoft.com/en-us/kb/2854570</a> for more information.</p>
Disk Cleanup	<p>Disk Cleanup is a system utility available in all versions of Windows that frees up space on the hard disk that is being used to store unnecessary temporary files, such as Temporary Internet Files. Disk Cleanup scans the hard disk for these temporary files and will remove them with minimal user input.</p>

<b>Maintenance Tool</b>	<b>Description</b>
-------------------------	--------------------

Disk Defragmenter	<i>DEFRAG (Disk Defragmenter)</i> is a system utility available in all versions of Windows that scans and analyzes how file fragments are arranged and accessed on the hard disk. The tool arranges stored data on a disk into contiguous blocks to improve access speed, system startup, and overall system performance. Because individual files are stored on disks in multiple separate blocks, the used and empty storage areas on a disk can become fragmented and scattered. In Windows 8 and 8.1, this utility is called <b>Defragment and Optimize Drives</b> .
-------------------	--

## Scheduled Disk Maintenance

You can schedule to perform check disk and disk defragmentation on a regular basis.

<b>Scheduled Task</b>	<b>Description</b>
Scheduled check disk	Over time, the errors on the hard disk can build up and cause a computer to perform slowly or poorly. Scheduling a check disk to run regularly will keep these errors from accumulating on the hard disk. As with all scheduled tasks, you can choose when and how often the check disk will be performed, but it is recommended that you run the Check Disk utility weekly to scan and resolve any disk errors.
Scheduled disk defragmentation	Your computer automatically breaks large files into fragments and stores them in various locations, only piecing them together when the file is accessed. The more large files you access and are fragmented by Windows, the more fragments accumulate on the hard disk; the more fragments that accumulate on the hard disk, the slower your computer accesses files and processes commands. Scheduling Disk Defragmenter to run automatically and regularly can keep fragmenting to a minimum, optimize the space on the hard disk, and improve the overall performance of your computer. Like all scheduled tasks, you can choose when and how often to defragment the hard disk, but it is recommended that you schedule Disk Defragmenter to run once a week.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Perform Disk Maintenance.

# ACTIVITY 10-4

## Performing Disk Maintenance

### Scenario

Some computers in your organization are already configured with scheduled disk optimization. You want to verify that your computer has been configured to run disk optimization on a weekly basis. You also want to see if you can regain any disk space through Disk Cleanup.

1. Run **Disk Cleanup**.
  - a) From **Control Panel**→**System and Security**→**Administrative Tools**, select **Disk Cleanup**.
  - b) In the **Disk Cleanup: Drive Selection** dialog box, select your **C:** drive. Select **OK**.
  - c) Examine the list of **Files to delete** that is created.
  - d) Select **Temporary Internet Files** by clicking on the words, then select **View files**. A **File Explorer** window opens listing the temporary Internet files.
  - e) Close the **File Explorer** window.
  - f) Examine any other items that are checked.
  - g) Select **OK**.
  - h) When prompted **Are you sure you want to permanently delete these files?**, select **Delete Files**.
  - i) Close all open windows, leaving only **Hyper-V Manager** and any VM windows open.
2. Configure your system to perform **Defragment and Optimize Drives** tasks on a weekly basis.
  - a) Open **Control Panel** then navigate to **System and Security**→**Administrative Tools**→**Defragment and Optimize Drives**.
  - b) In the **Optimize Drives** dialog box, select **Change settings**.
  - c) Verify that **Run on a schedule (recommended)** is checked, and that the **Frequency** is set to **Weekly**.
  - d) Select the **Choose** button and verify that all drives are checked, then select **OK** or **Cancel** as needed.
  - e) Select **OK** or **Cancel** as needed.
  - f) Select any drive, then select **Analyze**. If any of the drives show greater than 10% fragmented, select **Optimize**.
  - g) Select **Close**.

# TOPIC D

## Update Software

Another facet of optimizing and maintaining your OS is to ensure that its software and any other software that it uses remains as up-to-date as possible. In this topic, you will update software.

### Patch Management

*Patch management* is the practice of monitoring for, obtaining, evaluating, testing, and deploying integral fixes and updates for programs or applications, known as *patches*. As the number of computer systems in use has grown over recent years, so has the volume of vulnerabilities and corresponding patches and updates intended to address those vulnerabilities. However, not every computer within an organization will necessarily be compatible with a certain patch, whether it be because of outdated hardware, different software versions, application dependencies, and so on. Because of the inconsistencies that may be present within the various systems, the task of managing and applying patches can become very time-consuming and inefficient without an organized patch management system. In typical patch management, software updates are evaluated for their applicability to an environment and then tested in a safe way on non-production systems. If the patch is validated on all possible configurations without causing more problems, only then will the valid patch be rolled out to all computers throughout the entire organization.

A patch management program might include:

- An individual responsible for subscribing to and reviewing vendor and security patches and updating newsletters.
- A review and triage of the updates into urgent, important, and non-critical categories.
- An offline patch-test environment where urgent and important patches can be installed and tested for functionality and impact.
- Immediate administrative push delivery of approved urgent patches.
- Weekly administrative push delivery of approved important patches.
- A periodic evaluation phase and full rollout for non-critical patches.

Many organizations have taken to creating official patch management policies that define the who, what, where, when, why, and how of patch management for that organization.

### Driver and Firmware Updates

Managing updates is an important part of preventive maintenance, to ensure that all computers under your care are up to date with the most current software or applications available. Having a plan in place for how you will manage updates will help to make sure that your computers are protected against all of the possible threats, vulnerabilities, and functionality issues that arise as the technologies evolve and change.

Driver and firmware manufacturers often develop updates to address known functionality issues. By updating device drivers and firmware, you can avoid many potential operational problems.

Most modern motherboards have a number of chips that contain the system firmware that runs the system BIOS or UEFI. This firmware may need an upgrade from time to time depending on the manufacturer. When the manufacturer issues an update, then the firmware will need to be updated. These updates contain security patches, updates to the performance, and updates to address any known issues. The updates can be installed in a number of ways, but most commonly can be downloaded from the manufacturer's website and then either burned to CD or copied to a flash drive.

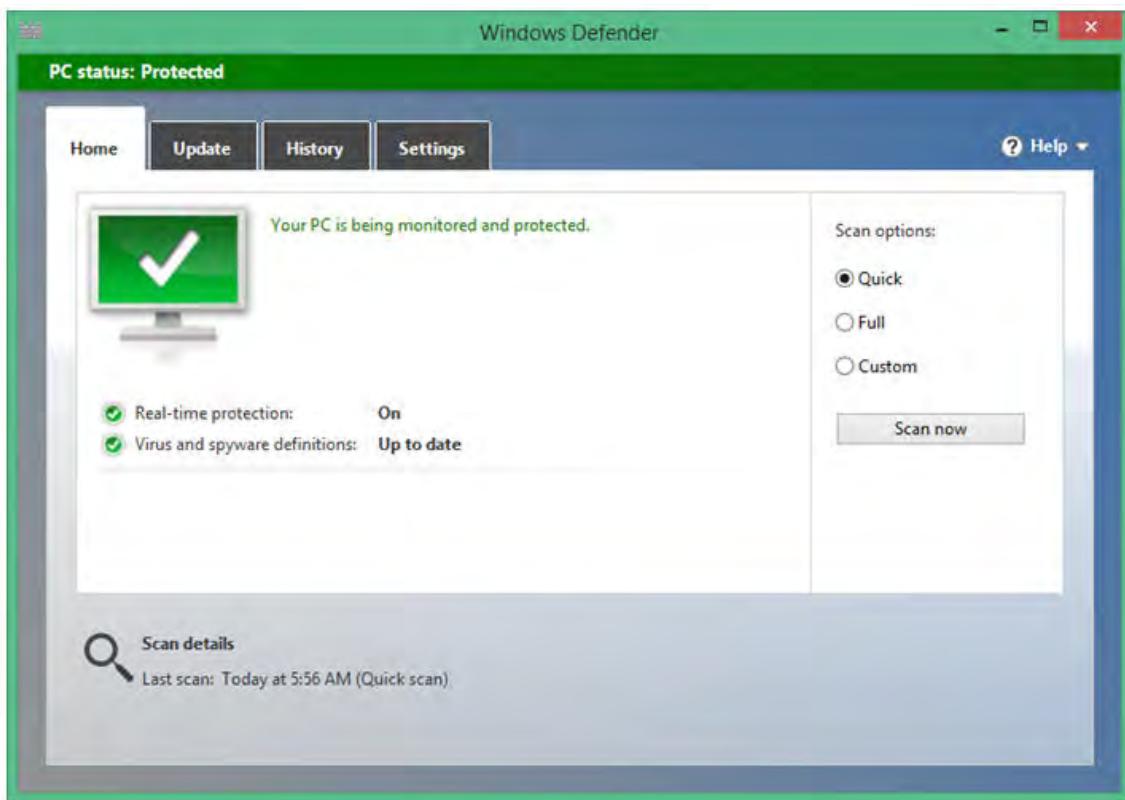
## Windows Updates

As you saw earlier in the course, the **Windows Update Control Panel** enables you to configure options for checking for and installing Windows updates. There are several types of updates Microsoft might offer you when your system is updated. You should always install Important updates as soon as possible. Other, optional updates can be installed if they seem like they would enhance or improve user experience and productivity.

<b>Update Type</b>	<b>Description</b>
Security updates	These important updates are installed automatically by default. Even if you have configured your system to not install updates automatically, you should test and install them as soon as possible to fix problems attackers might exploit. These are listed as <b>Important</b> updates in the Windows Update tool.
Optional updates	These recommended updates typically apply fixes to Windows features or add features. You can look through the list of updates listed as <b>Recommended</b> in the Windows Update tool and decide if they would make sense to be installed.
Service Packs	Service Packs roll up all of the above update types and are installed as a single update. The service packs bring the operating system fixes to a level playing field for everyone involved: from Microsoft to app developers to help desk and administrators to end users.
Language Packs	The optional language packs can be installed if you need to use the system in another language. Usually you won't want to install these as they take up time and space. You can hide them so you aren't continually prompted to install them.

## Antivirus and Antimalware Software

*Antivirus software* is an application that scans files for executable code that matches patterns, known as *signatures* or *definitions*, that are known to be common to viruses. The antivirus software also monitors systems for activity that is associated with viruses, such as accessing the boot sector. Antivirus software should be deployed on various network systems as well as on individual computers, and the signature database and program updates should be downloaded and installed on a regular basis as well as whenever a new threat is active.



**Figure 10-6: Windows Defender in Windows 8.1.**

Windows Defender is built into Windows 8/8.1. It contains an Antimalware Service Executable. Using the Administrative Tool, Task Scheduler, you can schedule when this runs. Other Microsoft tools to deal with malware include the Microsoft Safety Scanner and the Microsoft Malicious Software Removal Tool. These can be used to check your computer for specific malware and remove it from your system.

*Anti-spyware software* is specifically designed to protect systems against spyware attacks. Some antivirus software packages include protection against adware and spyware, but in most cases, it is necessary to maintain anti-spyware protection in addition to antivirus protection.



**Note:** If you install another antivirus or antimalware application on your computer, it might automatically turn off and disable Windows Defender. If no other antivirus or antimalware software has been installed, then Windows Defender should be running on your Windows computer.

## Antivirus and Antimalware Updates

Antivirus and antimalware updates must be managed as they are made available. Antivirus engine updates can include enhancements, bug fixes, or new features being added to the software engine, improving the manner in which the software operates. Updates can be implemented automatically or manually depending on the software. Automatic updating refers to software that periodically downloads and applies updates without any user intervention, whereas manual updating means that a user must be involved to either initiate the update, download the update, or at least approve installation of the update.

Microsoft antivirus and antimalware software updates are received as part of the Windows Update process. You can also download updates from the Download Center if you know updates are available, but have not yet received them on your computer.

## Guidelines for Managing Software Updates



**Note:** All of the Guidelines for this lesson are available as checklists from the **Checklist** tile on the CHOICE Course screen.

Follow these general guidelines to manage software updates:

- Consider developing a formal patch management process and identifying an update manager.
- Always test software updates before rolling them out to all users. If no test lab is available, select a few trusted users or use VMs as a sandbox. There are even cloud-based sandboxes you can use to test software updates.
- It's strongly recommended that you use another antimalware solution in addition to Windows Defender to provide adequate protection against malicious software.

# ACTIVITY 10-5

## Checking for Updates

### Before You Begin

This activity assumes you are using Windows Defender. If you are using a different antimalware application, your instructor will guide you through updating it.

### Scenario

You have received several help desk tickets related to a new virus infecting users' computers. You are using Windows Defender on most of the systems in your organization and want to make sure that the software has the latest updates.

1. Open Windows Defender.
  - a) Press **Windows+W** to open the **Search** tool.
  - b) Type **defender**
  - c) From the results, select **Scan for malware and other potentially unwanted software**.
  - d) If the scan starts automatically, select **Cancel scan**.
2. Check for updates.
  - a) In the **Windows Defender** window, select the **Update** tab.
  - b) Select the **Update** button.  
The latest virus and spyware definitions are downloaded and installed.
3. Verify the settings are performing real-time protection.
  - a) Select the **Settings** tab.
  - b) Verify that **Turn on real-time protection (recommended)** is checked.
  - c) In the left pane, select **Administrator**.
  - d) Verify that **Turn on this app** is checked.
4. Run a quick scan.
  - a) Select the **Home** tab.
  - b) Under **Scan options**, with **Quick** selected, select **Scan now**.
  - c) When the scan is completed, review the information shown, then close **Windows Defender**.

## Summary

In this lesson, you used various tools to optimize and maintain the Windows operating system. Ensuring that users' computers are working at optimum operating abilities will reduce the number of dissatisfied users and provide a more secure environment in which users can work.

**Which of the tools and concepts presented in this lesson have you used to optimize and maintain Windows operating systems? Which ones do you think you will use most often in the future?**

**Have you ever needed to restore settings from a restore point? If so, what happened that caused you to need to do a restore? Were you able to successfully restore the settings?**



**Note:** Check your CHOICE Course screen for opportunities to interact with your classmates, peers, and the larger CHOICE online community about the topics covered in this course or other topics you are interested in. From the Course screen you can also access available resources for a more continuous learning experience.

11

# Working With Other Operating Systems

**Lesson Time:** 2 hours

## Lesson Objectives

In this lesson, you will work with other operating systems. You will:

- Identify features and functions of the OS X operating system.
- Identify features and functions of the Linux operating system.

## Lesson Introduction

In the last two lessons, you worked with Microsoft Windows. As you know, an A+ technician will probably also be responsible for setting up, maintaining, and troubleshooting computers and devices that have other operating systems installed. Familiarity with OS X and Linux will enable you to support more of your user base.

# TOPIC A

## The OS X Operating System

Mac computers from Apple use the OS X operating system. Mac users tend to be found in art, music, graphic design, and education because OS X includes apps geared to those audiences. In this topic, you will examine some of the important features and functions of OS X.

### OS X

OS X® is the computer operating system developed by Apple® Inc. OS X is a Linux® derivative, and consists of UNIX-based operating systems and GUIs. This proprietary operating system is included on all Macintosh® computer systems.

El Capitan is the current Mac operating system as of fall 2015. If you need to upgrade from a previous version, the system requirements for El Capitan are:

- Mac hardware.
- 2 GB of RAM.
- At least 8 GB of available hard disk space.
- Snow Leopard version 10.6.8 or later and the Mac® App Store installed.
- An Apple ID.
- Internet access.
  - If you don't have Internet access, some features may be unavailable. You can have your Mac upgraded at an Apple Retail Store.



**Note:** If your Mac is running Leopard, you first need to upgrade to Snow Leopard, then update to its latest version. Then, you can upgrade to El Capitan.

OS X features include:

- Multiple user support.
- Integrated Mac, Windows, and UNIX server, file, and printer browsing in the Finder.
- The Safari® web browser.
- Native TCP/IP networking.
- Many file- and network-level security features.
- Comprehensive hardware device support with a unique Macintosh computer system design.

### Macintosh Hardware Compatibility

If your Macintosh® computer meets the minimum requirements for OS X installation, the hardware should all be compatible with the operating system. You can verify that your hardware is supported by examining the technical specifications, by product, at <http://support.apple.com/specs/>.



**Note:** You might hear the term "Hackintosh," which refers to installing OS X on non-Mac hardware, usually as a virtual machine.

### Macintosh Software Compatibility

Applications that ran in previous releases of Mac OS X should be supported when you upgrade to any current release.

If you need to use Mac OS 9 applications on a Mac OS X system, you can do so in the Classic environment in Mac OS X. To use the Classic environment, you must have a Mac OS 9 System Folder installed on your computer, either on the same hard disk as Mac OS X, or on another disk or

disk partition. For more information on Mac OS X technical specifications, see <http://support.apple.com/specs/macos>.

## OS X User Interface

The OS X GUI user interface is navigated using a mouse or trackpad. You can also use keyboard equivalences for many tasks. The one-button mouse that comes with a Mac can be configured to function as a two-button mouse. The trackpad on Mac laptops uses gestures to click, drag, scroll, zoom, open, and close items.

Some of the features you use to interact with the content on your Mac are the Finder, Dock, and Terminal.

<b>Feature</b>	<b>Description</b>
Finder	Finder is displayed when you turn on your Mac (or when you log in if log in is enabled). Through Finder, you manage the folders and files on your computer. Icons represent the computer, the folders, the files, and a trash can is available for throwing away files or ejecting disks. Some people refer to Finder as the desktop.
Dock	The row of icons at the bottom of most screens. All open windows and programs are represented by an icon in the dock. You can also secure items to the dock so that they are always available from the dock.
Terminal	Terminal is the command-line interpreter for OS X. From here, you can enter the Unix-like commands used in OS X at the command line.

## One-Button Mouse Configuration

The default one-button mouse that comes with a Mac can be configured to behave as if it has multiple buttons. From the **Apple** menu, select **System Preferences** and then **Keyboard & Mouse**. On the **Mouse** tab you can configure the **Secondary Button**. An alternative to configuring the secondary button is to use the **Control** button on the keyboard along with the mouse button to simulate "right-clicking" the mouse.

## Trackpad Gestures

The trackpad on a Mac laptop can do more than just help you click and drag items. Using multitouch gestures, you can do much more.

<b>Gesture</b>	<b>Description</b>
Tap to Click	When <b>Tap to Click</b> is enabled in the trackpad settings, this allows you to tap the trackpad rather than the button below the trackpad to click.
Dragging	Tap the trackpad twice, then right after the second tap, drag your finger. For longer dragging movements, slide your finger again after lifting it for no more than one second.
Drag Lock	When <b>Drag Lock</b> is enabled in the trackpad settings, this allows you to lift your finger for more than one second when dragging.
Secondary click	Specify where on the trackpad the secondary click is activated. Usually this is the lower right corner of the trackpad.  If you have a button below the trackpad, you can use two fingers on the trackpad and click the button.
Two finger scroll	Scrolls like you are using the scrollbar. You can also access the Scrolling Speed slider using this method.

<b>Gesture</b>	<b>Description</b>
Pinch Open/ Pinch Close	Using two fingers, spread them apart to enlarge the screen content. Using two fingers, bring them closer together to reduce the size of screen content.
Screen zoom	While pressing the Control key, drag two fingers on the track pad to zoom in the entire screen.
Three-finger swipe to navigate	Drag three fingers horizontally on the trackpad to move to the next or previous page.
Four finger swipe	<ul style="list-style-type: none"> <li>• Drag four fingers up to activate the <b>Show desktop</b> feature.</li> <li>• Drag four fingers down to activate the <b>Show all windows</b> feature.</li> <li>• Drag four fingers left or right to activate the <b>Program switcher</b> feature.</li> </ul>

## OS X Features

OS X includes features that make it an easy operating system to work with. Some features will be new to Windows users and might take a little while to get used to.

<b>Feature</b>	<b>Description</b>
<i>Mission Control</i>	<p>Mission Control enables you to see all open windows and spaces. The desktop area you see is referred to as a <i>space</i>. You can create multiple spaces, and switch between the spaces using Mission Control. All of the available spaces are shown at the top of the screen when you access Mission Control. You can access Mission Control by:</p> <ul style="list-style-type: none"> <li>• Using either three or four fingers, swipe up on the trackpad.</li> <li>• Double tap a Magic Mouse surface with two fingers.</li> <li>• From the Dock or Launchpad, select the <b>Mission Control</b> icon.</li> <li>• For Apple keyboards with a dedicated key, press the <b>Mission Control</b> key.</li> </ul> <p>Apps can be dragged from one space to another. Open the space containing the app you want to move, then in Mission Control, drag it to the desired space. Apps opened in Full Screen mode become their own space. You can switch between spaces by:</p> <ul style="list-style-type: none"> <li>• Selecting the space in the Mission Control window.</li> <li>• Using three or four fingers, swipe right or left on the trackpad to move to the next or previous space.</li> <li>• On the keyboard, press <b>Control+Left Arrow</b> or <b>Control+Right Arrow</b> to move to the previous or next space.</li> </ul> <p>You can create spaces through Mission Control. You can either point to the upper-right corner of the screen after opening Mission Control and select <b>Add Space</b> or drag the icon for an app to the <b>Add Space</b> button. If you want to close a space, press <b>Option</b> and select the <b>Close</b> button next to the space you want to close. If any windows are still in the space that is closed, they are moved to another open space.</p>



**Note:** Spaces is the same idea as virtual desktops in Linux.

<b>Feature</b>	<b>Description</b>
<i>Keychain</i>	<p>Keychain is a password management system built into OS X. It stores passwords and account information for users. When you access any password protected resource such as a website, email, or server, you are provided with the option to save the password. The password is saved in the keychain.</p>
	<p>Keychain Access is the app you use to manage your passwords and account information. It can also be used to manage digital certificates. You can export your keychain and import it on another Mac.</p>
<i>Spotlight</i>	<p>Spotlight is the OS X search feature. When you perform a search in Spotlight, the words you enter in the search are searched for in files, websites, app names, web content, and other locations. Select the magnifying glass icon to access Spotlight, then enter the words to search for. Spotlight uses auto-complete, so you don't have to type the full word or phrase if the desired results are found with the characters you already typed.</p>
<i>iCloud</i>	<p>iCloud is a cloud computing service offered by Apple. Mac and iOS users can use the iWork suite apps Pages, Numbers, and Keynote. Users of other operating systems can also use iCloud to store and share files, music, and photos. By default, users are provided with 5 GB of free storage. Additional storage can be purchased.</p>
	<p>To access iCloud, you need to sign up for an Apple ID. This is the same ID used to purchase items from iTunes, the App Store, and FaceTime.</p>
<i>Gestures</i>	<p>Multi-touch gestures can be performed on a Mac multi-touch trackpad, a Magic Trackpad, or a Magic Mouse. These gestures are performed using one or more fingers and tapping or swiping the surface of the input device. In the <b>System Preferences</b> Trackpad or Mouse pane, you can view animations for each of the available gestures.</p>
<i>Remote Disc</i>	<p>Not all Mac computers have an optical drive. This keeps the price as well as the weight of the device down. If you need to access a CD or DVD, you can do so using Remote Disc. On a Mac or PC that has an optical drive, configure it so that the Drive is set up to be shared. On the Mac without the optical drive, in the <b>Finder</b> sidebar, select the computer on which sharing of CDs and DVDs has been enabled and then select <b>Connect</b>. If the Mac you are using has an optical drive, <b>Remote Disc</b> will not appear in <b>Finder</b>.</p>
	<p>Not all CDs and DVDs can be shared. The following types of optical discs cannot be shared:</p>
	<ul style="list-style-type: none"> <li>• Audio CDs or DVDs</li> <li>• Movies on DVD or Blu-ray</li> <li>• Copy protected discs</li> <li>• Windows installation discs</li> </ul>
	 <p><b>Note:</b> If you are setting up Windows using Boot Camp on a Mac without an optical drive, create a disk image of the Windows installation disc and copy it to a flash drive.</p>
<i>Boot Camp</i>	<p>Boot Camp is a boot manager for OS X systems that enables users to install Microsoft Windows in a separate partition. The Boot Camp utility guides users through repartitioning the drive and installing Windows device drivers. At system boot, you can select whether to boot to OS X or Windows.</p>



**Note:** Remember, if an app is not responding, you can use **Force Quit** from the Apple menu to open the **Force Quit Applications** window, then select the non-responsive app and select the **Force Quit** button.

## OS X Management Tools

OS X includes several tools to help you manage backup and restoration of files, folders, and settings. It also includes tools for disk maintenance and screen sharing.

The following table includes some of the tools you will use most often.

Tool/Function	Description	Accessed From
Time Machine	A backup utility that backs files and folders up to a separate hard drive (not removable media) that has been formatted as a Mac file system. Files and folders can be restored from the Time Machine drive.	From the Apple menu, select <b>System Preferences</b> → <b>Time Machine</b> .
Snapshot	On Mac notebooks that don't currently have access to the Time Machine drive, local copies of files that are created, modified, or deleted are stored on the startup drive. They are copied to the Time Machine drive when it becomes available. Files and folders can be restored from the local snapshot.	From the Apple menu, select <b>System Preferences</b> → <b>Time Machine</b> . The timeline is displayed on the right side of the <b>Time Machine</b> window.
Image recovery	Using the <b>Disk Utility Restore</b> application or the <b>asr(8)</b> tool, you can create a pre-configured copy of OS X from a computer on which OS X has been installed and configured.	To access the Disk Utility, press <b>Command +Space</b> to open <b>Spotlight search</b> , type <b>Disk Utility</b> , and press <b>Return</b> . You can also select the <b>Launchpad</b> icon on your dock, select the <b>Other</b> folder, and select <b>Disk Utility</b> . Or, open a <b>Finder</b> window, select <b>Applications</b> in the sidebar, double-click the <b>Utilities</b> folder, and double-click <b>Disk Utility</b> . Once you are in the <b>Disk Utility</b> application, select the <b>Restore</b> tab.  For the <b>asr(8)</b> tool, open a Terminal window by selecting <b>Applications</b> → <b>Utilities</b> → <b>Terminal</b> , or from <b>Finder</b> , select <b>Finder</b> → <b>Services</b> → <b>New Terminal at Folder</b> or <b>New Terminal Tab at Folder</b> .

Tool/Function	Description	Accessed From
Disk maintenance utilities	The <b>Disk Utility</b> application can be used to verify or repair a disk. If you are unable to use this application, you can use the command line command <b>fsck</b> .	To access the Disk Utility, press <b>Command + Space</b> to open <b>Spotlight search</b> , type <b>Disk Utility</b> , and press <b>Return</b> . You can also select the <b>Launchpad</b> icon on your dock, select the <b>Other</b> folder, and select <b>Disk Utility</b> . Or, open a <b>Finder</b> window, select <b>Applications</b> in the sidebar, double-click the <b>Utilities</b> folder, and double-click <b>Disk Utility</b> .
Shell/Terminal	A Terminal window is where you can access the shell or command line in OS X.	For the <b>fsck</b> tool, open a Terminal window by selecting <b>Applications</b> → <b>Utilities</b> → <b>Terminal</b> , or from <b>Finder</b> , select <b>Finder</b> → <b>Services</b> → <b>New Terminal at Folder</b> or <b>New Terminal Tab at Folder</b> .
Screen sharing	You can share your screen or share the screen of another Mac.	You can open a Terminal window by selecting <b>Applications</b> → <b>Utilities</b> → <b>Terminal</b> , or from <b>Finder</b> , select <b>Finder</b> → <b>Services</b> → <b>New Terminal at Folder</b> or <b>New Terminal Tab at Folder</b> .
Force Quit	If an app is not responding, you can open the <b>Force Quit Applications</b> window, then select the non-responsive app and select the <b>Force Quit</b> button.	You can use iCloud to share your screen by selecting <b>Apple menu</b> → <b>System Preferences</b> → <b>Sharing</b> → <b>Screen Sharing</b> . You can also use <b>Finder</b> to connect to a remote Mac by selecting <b>Finder</b> → <b>Preferences</b> , then in the sidebar, in the <b>Shared</b> section, select <b>Back to My Mac</b> .  From the Apple menu, select <b>Force Quit</b> to open the <b>Force Quit Applications</b> window. You can also access this window by pressing <b>Command+Option+Esc</b> .

## Backup and Restore Tools

*Time Machine* is an application built into OS X that automatically performs backups of your files. The backup destination must be an external hard drive, an AirPort Time Capsule, or an OS X Server. The external drive can be connected using a USB, FireWire, or ThunderBolt port. When a blank external drive is connected to your Mac, you are prompted whether you would like to use it for backups. The drive must be formatted with the Mac OS X Extended (Journaled) file system; if another file system is currently in use, you are prompted to reformat the drive. By default, Time Machine maintains hourly backups for the past 24 hours. It also retains daily backups for the past month as well as weekly backups. If the drive to which you are backing up becomes full, the oldest backups are deleted.

If your computer isn't connected to your Time Machine drive, and you modify, delete, or create files, Time Machine creates copies of the files and stores the copies on the startup drive. These copies are referred to as local snapshots. The *local snapshot* is then copied to the Time Machine backup drive when it becomes available.

The Time Machine application displays a timeline. Backups are indicated on the timeline as color coded, dated tick marks.

- If you are using OS X Yosemite or later:

- Bright red tick marks indicate backups that can be restored right now from either the backup drive or a local snapshot.
- Dimmed red tick marks indicate backups that can be restored when the backup drive is available.
- If you are using OS X Mavericks or earlier:
  - Gray tick marks indicate backups that can be restored right now from a local snapshot.
  - Bright pink tick marks indicate backups that can be restored right now from your backup drive.
  - Dimmed pink tick marks indicate backups that can be restored when the backup drive is available.

## Disk Maintenance Utilities

The OS X built-in **Disk Utility** is a disk management tool and partition manager. There are several methods of accessing this disk maintenance utility:

- From Recovery Mode (press **Command+R** as the system boots).
- Using Spotlight Search and entering **Disk Utility**.
- From the docked Launchpad icon, select **Other** folder, then select **Disk Utility**
- In any **Finder** window, on the sidebar, select **Applications→Utilities→Disk Utility**.

Disk Utility includes many partition and disk management functions.

<b>Feature or Function</b>	<b>Description</b>
Partition drives and format partitions	You can create, rename, reformat, resize, and delete partitions on internal or external drives, and DMG image files that can be mounted and accessed as if they were drives.
First Aid	Assists with fixing disk problems. The <b>Verify Disk</b> button checks for problems and the <b>Repair Disk</b> button fixes the problems that are found. In addition, there are buttons to fix permissions issues—Verify Disk Permissions and Repair Disk Permissions.
Secure Erase	This feature should only be used on mechanical drives and can be used to erase an entire hard disk or partition, or just erase the free space. The <b>Fastest</b> option is the most secure and writes over the entire disk with zeroes one time.
<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;">  <b>Note:</b> Do not use Secure Erase on solid state drives as it just wears down the drive to no security purpose.         </div>	
Create and Manage Disk Images	Create a new blank disk image or create a disk image from a folder. This creates .DMG files, which can be mounted as drives. You can write files to the disk image file. The .DMG file can be encrypted and saved to cloud storage or a removable drive. You can also convert an image file from read/write to read-only. In addition, you can resize the disk image, making it larger or smaller as needed.
Restore	Enables you to copy a volume to another volume, a partition to another partition, or create a disk image as an exact duplicate of a partition. When you use a disk image to restore a partition, the contents of the partition are erased and the data from the disk image is copied on to the partition.
RAID	Enables creation of RAID 1 and RAID 0 drives. You can also use concatenation to combine RAID types to receive the benefits of each type of RAID.

## Screen Sharing

Screen sharing can be configured between Macs on the same network, between a Mac and a PC, or between Macs on two different networks. To share screens between two Macs on the same network, use the **Sharing** option from the **Apple→System Preferences** menu. Here, you can unselect **Remote Management** then check **Screen Sharing**. You can specify whether only specific users or all users can share your screen.

If you need to control a Mac from a PC, you need to join the Mac to the Windows workgroup. Request the name of the workgroup from the person with whom you will be sharing your screen.

To share a Mac from a remote location, use **Back to My Mac**. You need an iCloud Apple ID account in order to use this feature.

## Force Quit

Normally, to close an app, you just select **Quit** from the app menu. However, if the app is unresponsive, you might need to use **Force Quit**. There are several methods of accessing Force Quit:

- Press **Control+Option+Esc**.
- From the **Apple** menu, select **Force Quit**.

Finder is always open, so there isn't a **Quit** option for this app. If Finder becomes unresponsive, use **Force Quit** and select **Relaunch**.

## OS X Best Practices

There are several tasks you should perform on a regular basis to make sure that the OS X computers you support remain functional and working their best.

Task	Description
Scheduled backups	Using built-in features such as <b>Time Machine</b> , you can perform scheduled backups. You can also use third-party backup utilities to perform scheduled backups if your backup solution comes with its own applications for scheduling backups. Even if you have scheduled backups set up, you should manually perform a backup before making any big changes such as system OS updates or installing or removing apps.
Scheduled disk maintenance	Consider running <b>Disk Utility First Aid</b> monthly or bi-monthly if you often install or uninstall applications. Use the Repair Disk Permissions feature to make sure that permissions are set correctly. You should also run Repair Disk to check for bad blocks or a corrupted drive.
System updates	By default, Software update checks for updates once a week. Running <b>Software Update</b> manually from the <b>Apple</b> menu can be done at any time to check the App store for any updates.
Patch management	Checking for system updates is the first part of patch management. You should also check for updates for apps that you use. Updates might include bug and security fixes, and enhanced features. If you are supporting multiple users, be sure to test the patches first before deploying them to all users.
Driver and firmware updates	Drivers and firmware are typically updated when system updates are received. However, if you find that for some reason you need to update the drivers or firmware manually, you can access <b>System Information</b> to check the current information, including model Identifier, boot ROM version, and SMC version. If you try to install an update that isn't designed for your system, the software will not be installed and you will see an alert message.

<b>Task</b>	<b>Description</b>
Antivirus and antimalware updates	Mac systems aren't attacked as often as Windows systems, but you should still be running antivirus and antimalware on Macs. Be sure to configure the application to automatically check for updates as they become available. If the app isn't updated, you are not being fully protected.

# ACTIVITY 11-1

## Identifying Features and Functions of OS X

### Scenario

You are new to supporting Macs, but do have some experience supporting Windows systems. You want to identify the OS X equivalent of some of the Windows features and functions you are used to using.

1. What Windows and OS X features enable you to back up data and restore data from a backup?
  2. What Windows and OS X features enable you to manage storage devices?
  3. What Windows and OS X features enable you to identify which apps are running?
  4. What Windows and OS X features enable you to end the running of a non-responsive program?
  5. What Windows and OS X features provide you with cloud storage?
  6. What Windows and OS X features enable you to search for items?
-

## ACTIVITY 11-2

### Using OS X (Optional)

#### Before You Begin

If you have access to a Mac running OS X Leopard or newer, you can perform this activity.

#### Scenario

You want to try out some of the OS X features you recently learned about. You want to make sure that you can support any Mac users within your organization.

---

1. Examine Finder.
    - a) Locate the Dock.
    - b) Open an app.
    - c) Examine the file system.
  
  2. Examine Spotlight.
    - a) In Finder, select the magnifying glass icon.
    - b) Type **spot**  
Notice that the results auto-completes what it thinks you want to type next.
    - c) If necessary, continue typing until the results show **Spotlight**.
    - d) Observe the various locations and results of the search.
-

# TOPIC B

## The Linux Operating System

Operating systems vary greatly from manufacturer to manufacturer. Over the past few years, Linux has rapidly gained ground in the competitive operating system marketplace. For example, Linux is now widely preferred for web servers and Internet systems. Many individuals and organizations have accepted it as a desktop and server alternative because of its high security, low cost, and ease of licensing. In this topic, you will examine the basics of Linux, so that you can begin to understand and appreciate its benefits.

### Linux Distributions

*Linux* is a UNIX-like operating system originally developed by Linus Torvalds, starting in 1991 while he was a student at the University of Helsinki. Like all operating systems, Linux enables the most basic common system operations, such as file management, user account management, and so forth. It provides a means for users to interact with their computer's hardware and software.

Linux is perhaps most notable because it is free and open source. Programmers have made versions of Linux available for nearly every computer hardware platform in current use. Linux is available for:

- Network servers and enterprise-class computing environments.
- Desktop and end-user computers.
- "Non-computer" devices such as cell phones, automobile control systems, network routers, and alarm system controllers.

Linus Torvalds wrote the original Linux kernel. The kernel is the software component that provides the core set of operating system functions. These include features for managing system hardware and for communicating between software and hardware.

Since its creation, Linux has evolved into hundreds of distributions, also called *dists*, each tailored to their designers' needs. If you are a beginner, you will find it easier to choose one of the mainstream distributions depending on the installations. Some common distributions are:

- CentOS
- Red Hat® Enterprise Linux (RHEL)
- Fedora
- SUSE Linux Enterprise
- openSUSE
- Debian
- Ubuntu
- Mandriva
- Mint

### Internet Reference for Common Linux Distributions

You can refer to common Linux distributions in the following Internet sites:

- CentOS Linux: [www.centos.org](http://www.centos.org)
- Red Hat Enterprise Linux (RHEL): [www.redhat.com](http://www.redhat.com)
- Fedora: <http://fedoraproject.org>
- SUSE Linux Enterprise: [www.suse.com](http://www.suse.com)
- openSUSE: [www.opensuse.org](http://www.opensuse.org)
- Debian: [www.debian.org](http://www.debian.org)
- Ubuntu: [www.ubuntu.com](http://www.ubuntu.com)
- Mandriva: [www.mandriva.com](http://www.mandriva.com)

- Mint: [www.linuxmint.com](http://www.linuxmint.com)



**Note:** The site [linux.com](http://linux.com) has a yearly comparison of Linux distributions and commentary on what they feel are the best distributions to use for various purposes.

## The CentOS Linux Distribution

The CentOS Linux distribution is a stable, predictable, manageable, and reproducible platform derived from the sources of Red Hat Enterprise Linux (RHEL). CentOS is maintained by The CentOS Project, a community-driven free software effort that is modelled on the structure of the Apache Foundation and has its own governing board. CentOS benefits from Red Hat's ongoing contributions and investment.

This course uses CentOS Linux because it provides a free enterprise class computing platform that aims to be functionally compatible with the upstream product (RHEL) that it derives from. CentOS Linux does not contain Red Hat, Inc.'s product or certifications, although it is built from the same sources as the upstream enterprise products. More details about this may be found in the CentOS FAQ here: <http://wiki.centos.org/FAQ/General>.

For production environments, the licensed and fully supported Red Hat Enterprise Linux product is recommended.



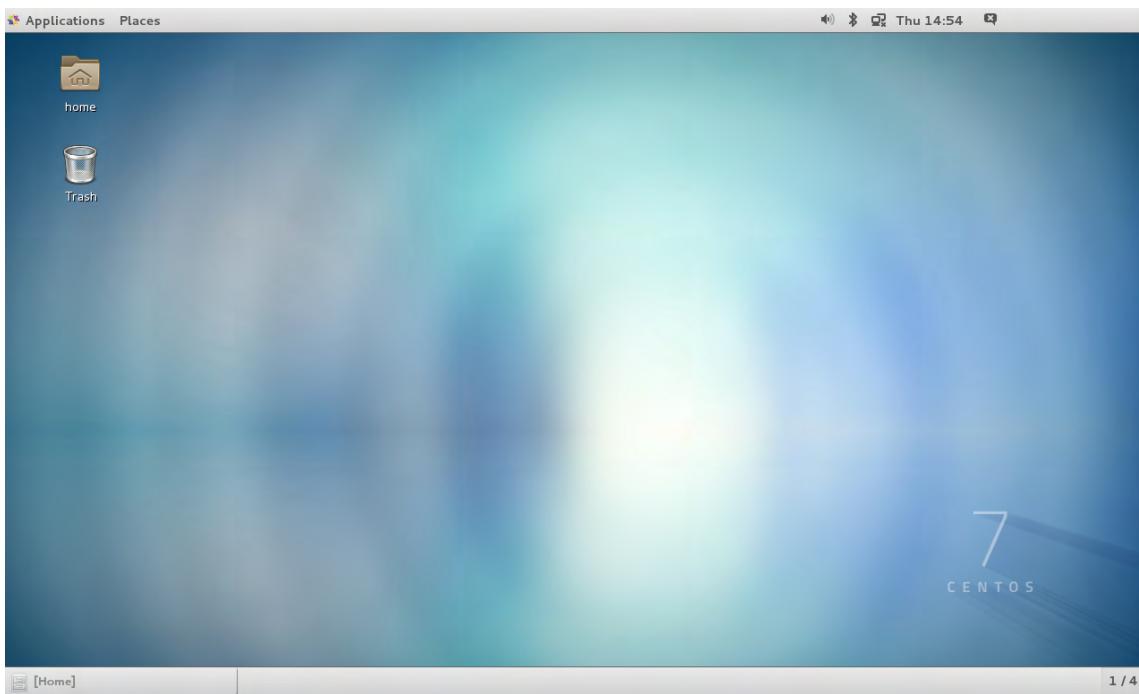
**Note:** To learn more, check out the LearnTO **Transition to Linux** presentation from the **LearnTO** tile on the CHOICE Course screen.

## Linux User Interfaces

There are a number of ways users interact with Linux. These include using a GUI interface or a shell interface. There are a variety of GUI interfaces that can be used with each of the Linux distributions. The shell interface, also referred to as the command line interface (CLI), is a plain text terminal that is used to enter commands. A variety of shells are available and can be used with each Linux distribution.

### GUI

The Linux *Graphical User Interface (GUI)* is a collection of icons, windows, and other screen graphical elements that help users interact with the operating system. The desktop menu provides access to the GUI applications available on the Linux desktop. There are different GUI implementations such as K Desktop Environment (KDE) and GNU Object Model Environment (GNOME).



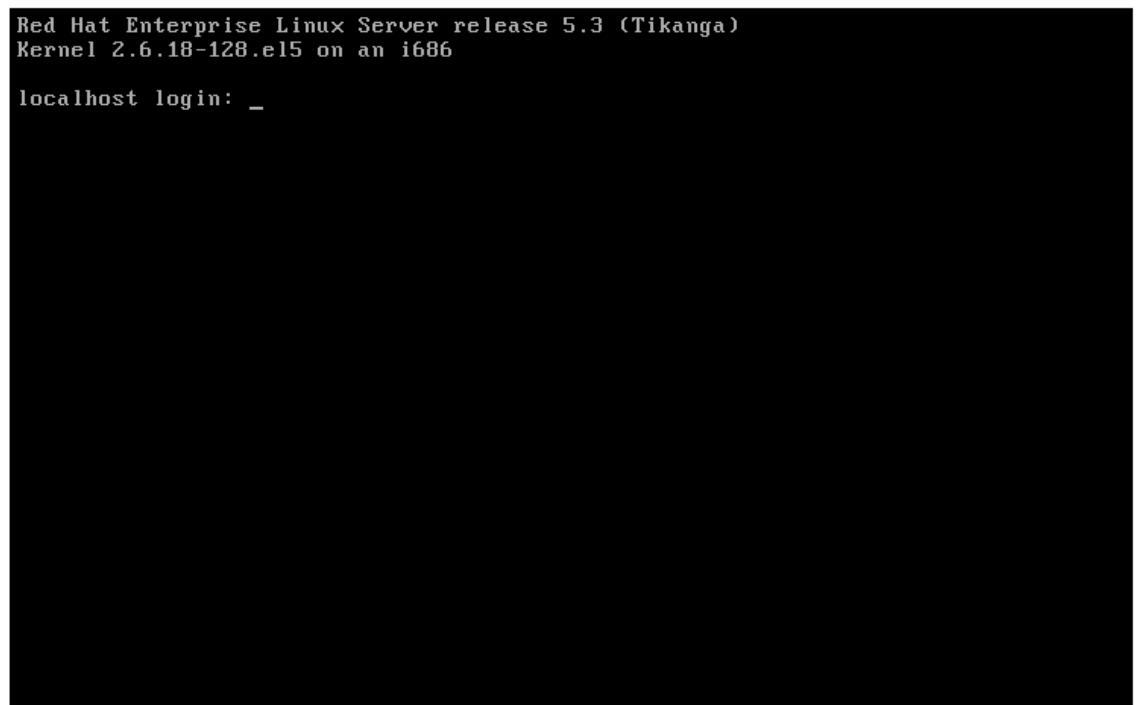
**Figure 11-1: A GNOME desktop in CentOS 7.**

The following table lists the uses of some common **Applications** menu categories in the GNOME GUI.

<b>Applications Menu Used To</b>	
<b>Category</b>	
Accessories	Access applications for performing work-related tasks such as creating text documents and presentations, or using a calculator.
Internet	Access applications for performing tasks on the Internet such as web browsers, email clients, instant messengers, or web editors.
Sound & Video	Access applications for viewing movies and listening to sound files or CDs.
System Tools	Access options for changing the settings on the Linux system.
Documentation	Access help on Linux.

## CLI

The *Command Line Interface (CLI)* is a text-based interface for the operating system, where a user typically enters commands at the *command prompt* to instruct the computer to perform a specific task. A *command line interpreter*, or command line shell, is a program that implements the commands entered in the text interface. The command line interpreter analyzes the input text provided by the user, interprets the text in the context given, and then provides the output.



```
Red Hat Enterprise Linux Server release 5.3 (Tikanga)
Kernel 2.6.18-128.el5 on an i686

localhost login: _
```

Figure 11-2: A CLI screen.

## Superuser

The **root** user, also known as the **superuser**, is the administrative account on a Linux system. This user can do anything on the system. You should only use this account when absolutely necessary. For most Linux distributions, you create a regular user when you are installing Linux. This is the user you should use. Even when you are performing administrative tasks, many of these can be performed as your regular user. For those instances where more power is needed, you can often use the **su** or **sudo** command to temporarily access the system with administrative privileges.

## Linux Features

There are several Linux features that make it appealing to a variety of users. Many websites and networks are based on a Linux server. End users who want to take advantage of the efficient use of resources can breathe life back into systems that Microsoft Windows can't run efficiently any longer by installing one of the Linux distributions. Linux systems can interact with both Windows and Mac computers on a network or through cloud services.

There is no specific Linux control panel for iCloud, but you can use the web-based access to iCloud from a Linux system. You can also configure your email client on Linux for an iCloud Mail account. Refer to the Apple support site for specific mail server settings.

Support for gestures such as those used on Windows touchscreen systems and Mac touchpads is available in some distributions of Linux. You can also install additional applications that provide support for touch devices on a Linux system. Refer to the online documentation for your distribution of Linux to see if gestures are supported.

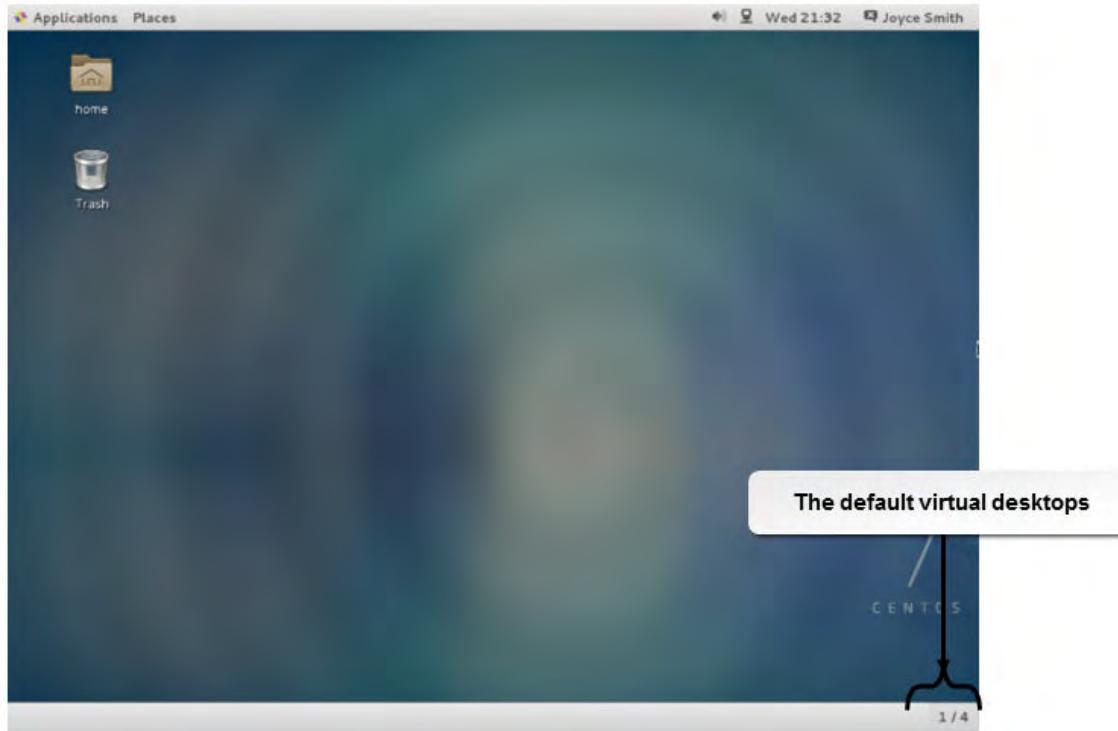
## Virtual Desktops

There will be times when a user needs to have multiple windows open on their desktop. Typically, to help manage the need to go between many different programs running simultaneously, users would do one of three things:

- Leave all windows open, which may result in a cluttered desktop.

- Minimize those windows that are not needed and use the taskbar or press **Alt+Tab** to switch between them. This approach could still be a bit confusing.
- Use virtual desktops.

Using multiple desktops helps keep a user's workspace organized and uncluttered. The default configuration provides two or four desktops depending on the distribution. For example, Ubuntu® provides two desktops by default and CentOS provides four. Users can switch between the virtual desktops by clicking one of the desktop buttons on the panel at the bottom of the desktop screen.



**Figure 11–3:** Virtual desktop buttons on the panel.

## GRUB

GRUB 2 is the newest version of the GRand Unified Bootloader (GRUB). The original version of GRUB is now referred to as GRUB Legacy and is no longer actively developed. Both versions are in use in Linux distributions. GRUB is the program that loads operating system kernels.

## Remote Access

Often, Linux administration is done from a computer other than the machine on which the network or web services are running. Remote access can be from another Linux computer, from a Windows computer, or from a Mac. Remote access is a type of screen sharing functionality. Depending on what you need to do and from which platform you are remotely accessing the Linux system, you use different tools.

- SSH
- OpenSSH*
- sftp
- rdesktop



**Note:** Refer to the man pages for the above commands for more details.

*X forwarding* is a mechanism by which programs are run on one machine and the X window output is displayed on another machine. X forwarding can be enabled or disabled by setting the `X11Forwarding` option to yes or no in the `/etc/ssh/sshd_config` file. This allows X11 tunnelling over an SSH connection.

*Virtual Network Computing (VNC)* is a platform-independent system through which a user can control a remote system. The virtual network is made up of the VNC client, the VNC server, and the VNC protocol. The client views the output that is displayed by the server through the VNC protocol. The user can run multiple VNC sessions at any given time. However, the display for each VNC client may differ from the display of the VNC server.

The `vncserver` command is used to start a system with VNC. The `$HOME/.vnc/xstartup` file allows a user to control applications running on a remote system. You can specify the display number that the VNC server will use when it is started.

The `vncviewer` command is used to view the VNC client. Various options are available for specifying `vncviewer` parameters.

# ACTIVITY 11–3

## Identifying Features and Functions of Linux

### Scenario

Your organization is considering moving some of the website and network services from Windows servers to Linux. You want to compare the features and functions of some Linux distributions to see which ones might best meet your needs. You also have some systems that are no longer capable of fully supporting the current Windows operating systems, but you have heard that Linux can possibly take advantage of these older systems and work well on minimal hardware resources.

1. Browse the web for comparisons of Linux distributions.
  - a) Open a web browser and go to your preferred search website.
  - b) Search for the phrase ***linux distribution comparison***
  - c) Briefly review the information you find.
2. Browse the web for comparison of Linux distribution features.
3. **Based on your research, which distribution would you recommend testing for use as a web and network services server?**
  
4. **Based on your research, which distribution would you recommend testing for use on older computers with limited resources?**

---

### Linux Installation

The hardware requirements for installing Linux will depend upon the distribution of Linux you choose. Linux is a portable operating system, which means it can run on a variety of hardware platforms. There are versions available for many different processor types, including Intel x86 and Pentium, Itanium, DEC Alpha, Sun Sparc, Motorola, and others. In general, a basic installation of Linux on a workstation might require as little as 16 or 32 MB of memory and 250 MB of disk space, but you might need several gigabytes of disk space for a complete installation, including all utilities.

### Installation Methods

There are several installation methods you can use to perform a Linux installation. These include:

- From a DVD or CD.
- Via a network.
- By accessing a network installation server.
- From boot media such as an ISO file or a boot USB device.

### Linux Hardware Compatibility

Because Linux is a portable operating system, it is compatible with a wide range of hardware. You will need to check with the vendor or provider of your Linux distribution to verify if your particular system hardware is supported by that distribution.

Some web resources you can use to research general Linux hardware support include:

- The Linux Hardware Compatibility HOWTO website at <http://tldp.org/HOWTO/Hardware-HOWTO/index.html>.
- The Linux Questions website's hardware compatibility list at [www.linuxquestions.org/hcl/](http://www.linuxquestions.org/hcl/).
- Linux hardware and driver support lists at [www.linux-drivers.org](http://www.linux-drivers.org).

## Linux Software Compatibility

Check your Linux vendor's website and read the technical documentation for the distribution of Linux you plan to install or upgrade to in order to determine if your existing applications will be supported under the new version. You can also check the resources at [www.linux.org/apps](http://www.linux.org/apps) for lists of Linux-compatible applications in various categories from a number of vendors. You can also register as a user at [www.linux.org/user](http://www.linux.org/user) and post questions about particular applications in the online user forums.

## Linux Filesystem Types

A *filesystem* is a method that is used by an operating system to store, retrieve, organize, and manage files and directories on mass storage devices. A filesystem maintains information, such as the date of creation and modification of individual files, their file size, file type, and permissions. It also provides a structured form for data storage. A filesystem by itself does not interpret the data contained in files because this task is handled by specific applications. Filesystems vary depending on several parameters, such as the purpose of the filesystems, the information they store about individual files, the way they store data, and data security.

Filesystem labels are assigned to filesystems for easy identification. The labels may be up to 16 characters long and can be displayed or changed using the `e2label` command.

Linux allows you to access other filesystems, such as NTFS and FAT, and mount them when required. However, you cannot install Linux on these filesystems.

Linux supports many common filesystem types. Some are described in the following table.

<i>Filesystem Type</i>	<i>Description</i>
<i>ext3</i>	This is an improved version of ext2, which was the native filesystem in many Linux releases. In case of an abrupt system shutdown, ext3 is much faster in recovering data and better ensures data integrity. You can easily upgrade your filesystem from ext2 to ext3.
<i>ext4</i>	The newest default filesystem for Linux distributions. It is backwards-compatible with the ext2 and ext3 filesystems. Among ext4's improvements over ext3 are journaling, support of volumes of up to one exbibyte (EiB), and files up to 16 TiB in size. Ext4 is the default filesystem for CentOS/RHEL 7 and Ubuntu installations.
<i>ReiserFS</i>	This filesystem can handle small files efficiently. It handles files smaller than 1K and is faster than ext2 and ext3. If appropriately configured, it can store more data than ext2.
<i>swap</i>	This is not a true filesystem, but rather is a portion of the hard disk that is used in situations when Linux runs out of physical memory and needs more of it. Linux pushes some of the unused files from RAM to swap to free up memory.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Install Linux.

# ACTIVITY 11–4

## Installing Linux

### Before You Begin

- Ensure you have the latest version of the CentOS Linux 7 x86\_64 Installation DVD or ISO file. (The ISO file must include the GUI.)
- You will install on the virtual machine you set up previously unless your instructor specifies otherwise.

### Scenario

A Linux system needs to be allocated for certain tasks. So, you'll install the latest version of the CentOS distribution and configure it so it's ready to be put to use.

1. Configure the Linux VM to boot from the CentOS7 installation source.
  - a) In **Hyper-V Manager**, configure the **Stu##-Linux** VM to access to CentOS7 DVD or ISO.
  - b) Configure the **Firmware** setting so that **Enable Secure Boot** is not checked.
  - c) Move **CD or DVD** to the top of the **Boot Order** list.
  - d) Select **OK** to save the settings.
  - e) Start and connect to the **Stu##-Linux** VM. The installation process should begin when the system starts.
2. Upon starting the installation process, the following CentOS 7 installation menu should appear. Press **Enter** to select the default option **Test this media & install CentOS 7** and continue with installation.



3. The CentOS Installer screen loads as follows and initiates a check of the installation media (DVD). To save time during this activity, you can press the **Esc** key to skip this step, although it is wise to check your media at least once when setting up production Linux servers.

```

- Press the <ENTER> key to begin the installation process.

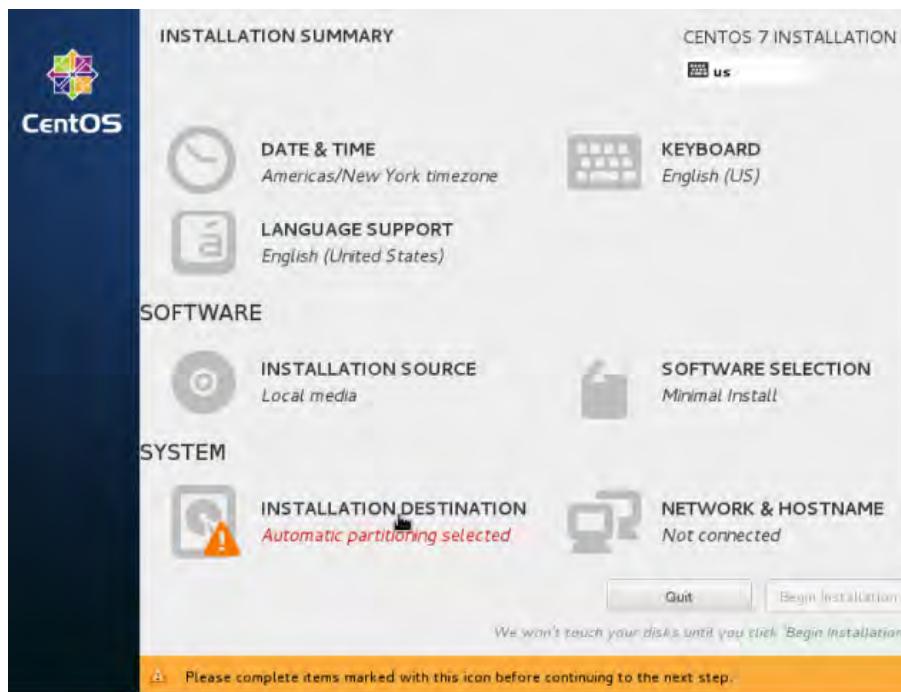
6.009001] sd 2:0:0:0: [sda] Assuming drive cache: write through
6.009923] sd 2:0:0:0: [sda] Assuming drive cache: write through
6.011186] sd 2:0:0:0: [sda] Assuming drive cache: write through
OK ] Started Show Plymouth Boot Screen.
OK ] Reached target Paths.
OK ] Reached target Basic System.
tracut-initqueue[840]: mount: /dev/sr0 is write-protected, mounting read-only
OK ] Started Show Plymouth Boot Screen.
OK ] Reached target Paths.
OK ] Reached target Basic System.
tracut-initqueue[840]: mount: /dev/sr0 is write-protected, mounting read-only
Starting Media check on /dev/sr0...
/dev/sr0: 8bfbb74bfbb488542bd7dffc2001a111
Fragment sums: f4f9fe5f9cc267c53231c9a25aecf5adac1e76a6ddd124f4f5bd5b976ffe
Fragment count: 20
Press [Esc] to abort check.
Checking: 035.3%_

```

- After the installer has run, a **Welcome** screen should appear. Select **English (United States)** as your **Language**, and select **Continue**.



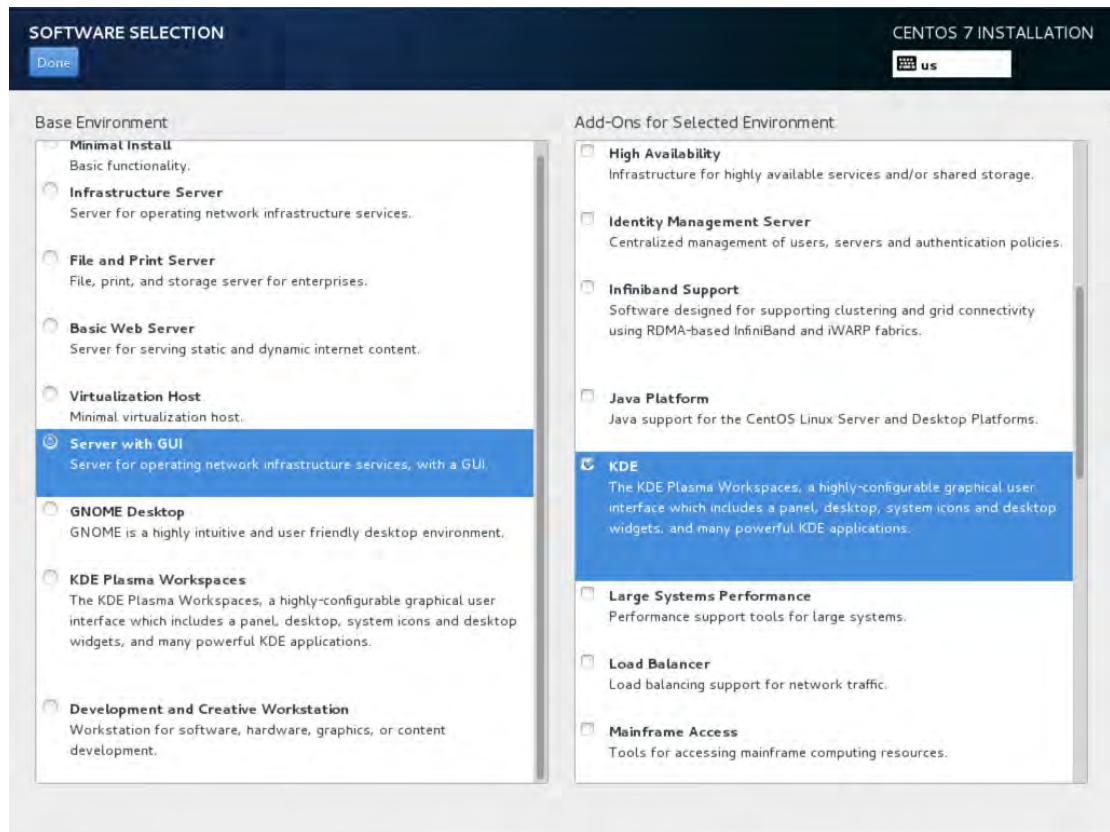
- The next screen prompt is **Installation Summary**, which contains many options to fully customize your system. Select **Date & Time** then change the settings to your local timezone. Select **Done** to close the **DATE & TIME** screen.



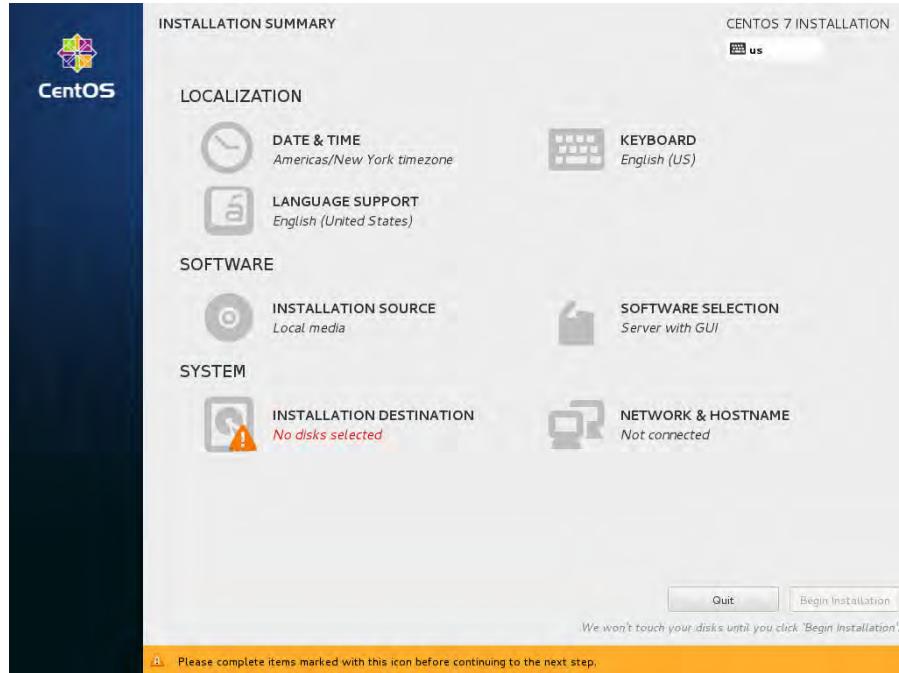
- Select **Software Selection** to choose which type of environment you want to set up.



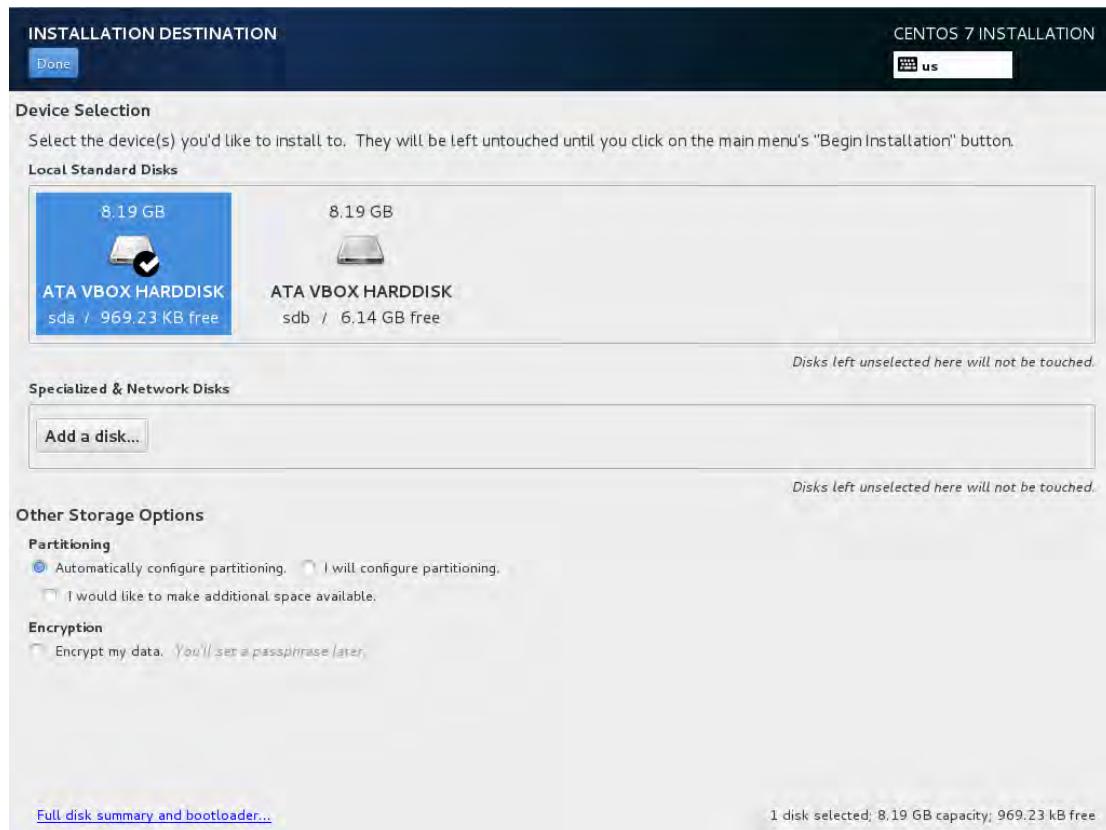
- Select **Server with GUI**, then in the **Add-Ons for Selected Environment** section, check the **KDE** option and select **Done**.



8. Select **Installation Destination** to choose where you want to install.



9. Select the first disk (**sda**), and select **Done**. Your installation disk options may differ, but appear similar to the following.



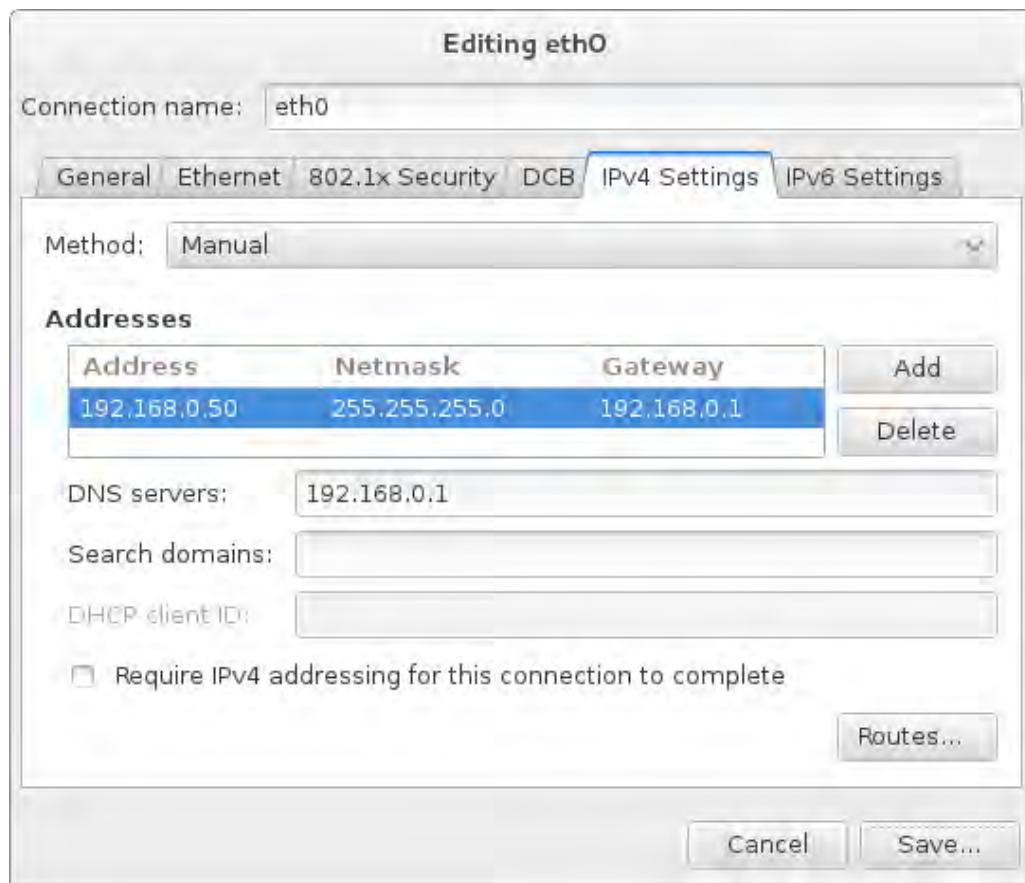
**10. To configure networking options, select **Network & Hostname**.**

- In the **Hostname** text box, type **srv##.aplusclass.com** where ## is the same student number you've used in prior lessons.
- If **Ethernet (eth0)** is set to **OFF**, click **OFF** to switch it to **ON**.
- To edit network settings, verify that the correct network device is selected and select **Configure**.
- On the **Editing eth0** screen, configure network parameters. On the **IPv4 Settings** tab, in the **Method** selector, select the **Manual** option.
- In the **IPv4 Settings** section, in the **Addresses** list, select the **Add** button.
- In the **IP Address** text box, type **192.168.0.##** (where ## is the same student number you've used in prior lessons). In the **Netmask** text box, type **255.255.255.0** and in the **Gateway** text box, type **192.168.0.1**



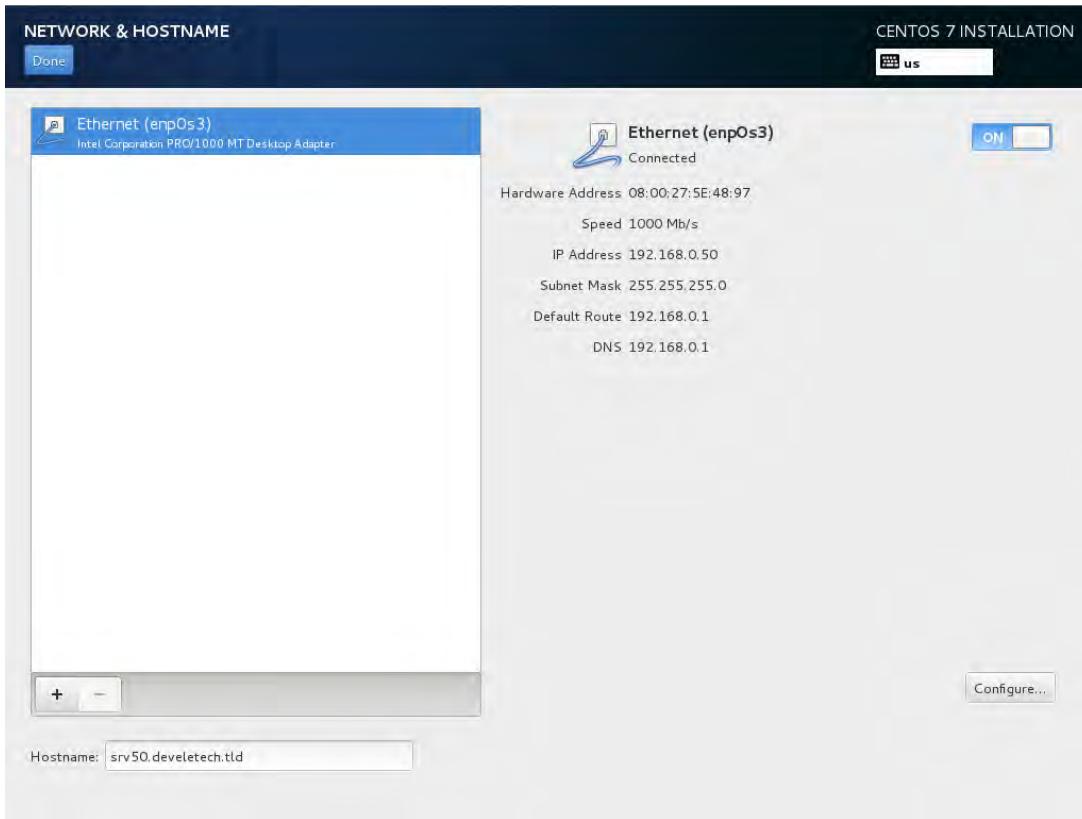
**Note:** Your instructor might provide you with different addresses than those listed in these steps.

- g) In the **DNS servers** text box, type **192.168.0.1** or enter the appropriate IP address for your classroom network DNS server. The resulting screen should look similar to the following.



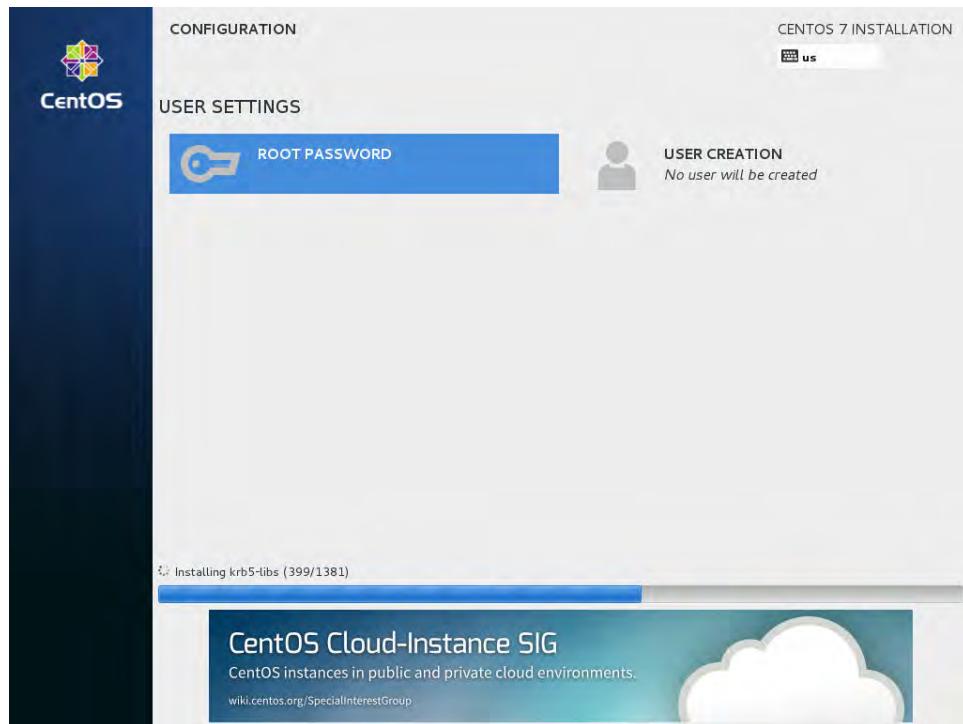
- h) To save your changes, select **Save**.

- i) In the upper-right corner, verify that the enabled switch is set to **ON**.

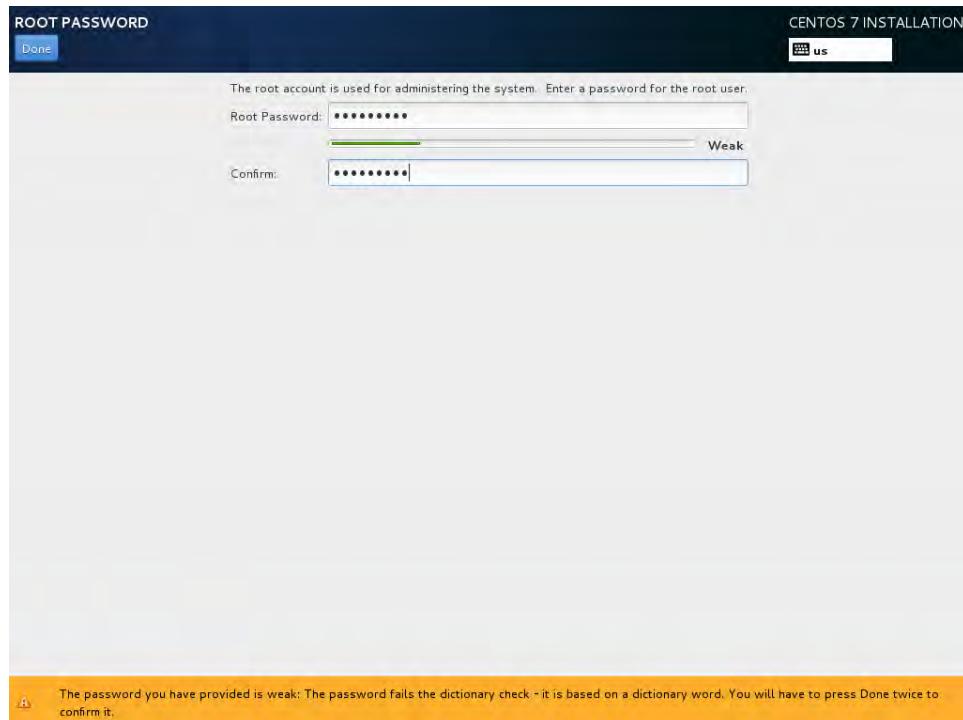


- j) Select the **Done** button to continue with the process.

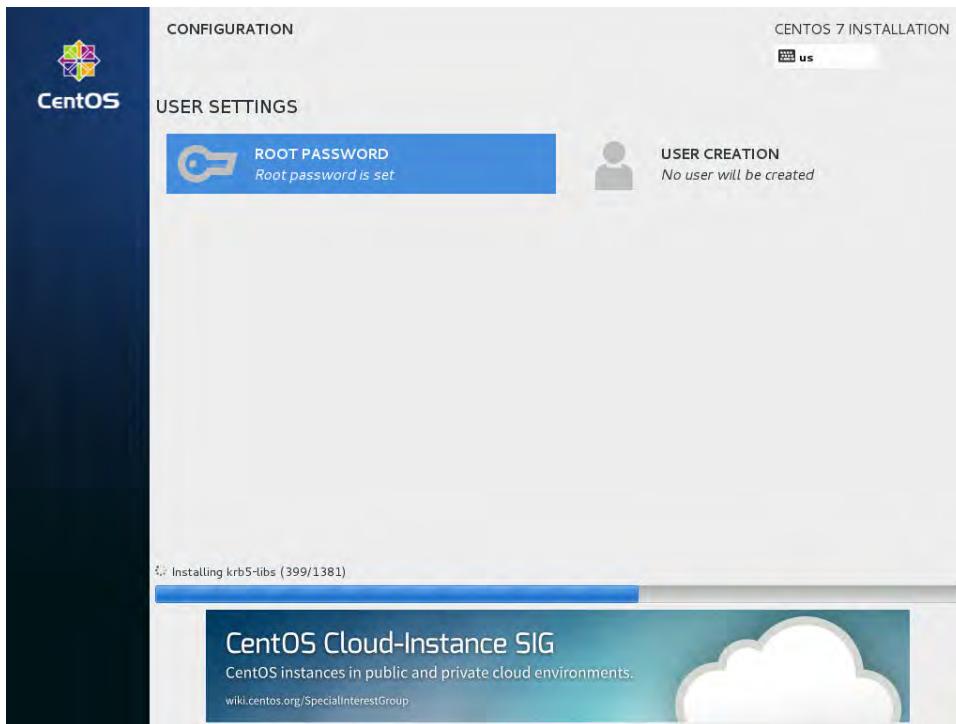
11. Select **Begin Installation** at the bottom of the prompt. While the installation proceeds in the background, select **Root Password**. On the **Root Password** page, in the **Root Password** text box, type **IPass1234** and press **Tab**.



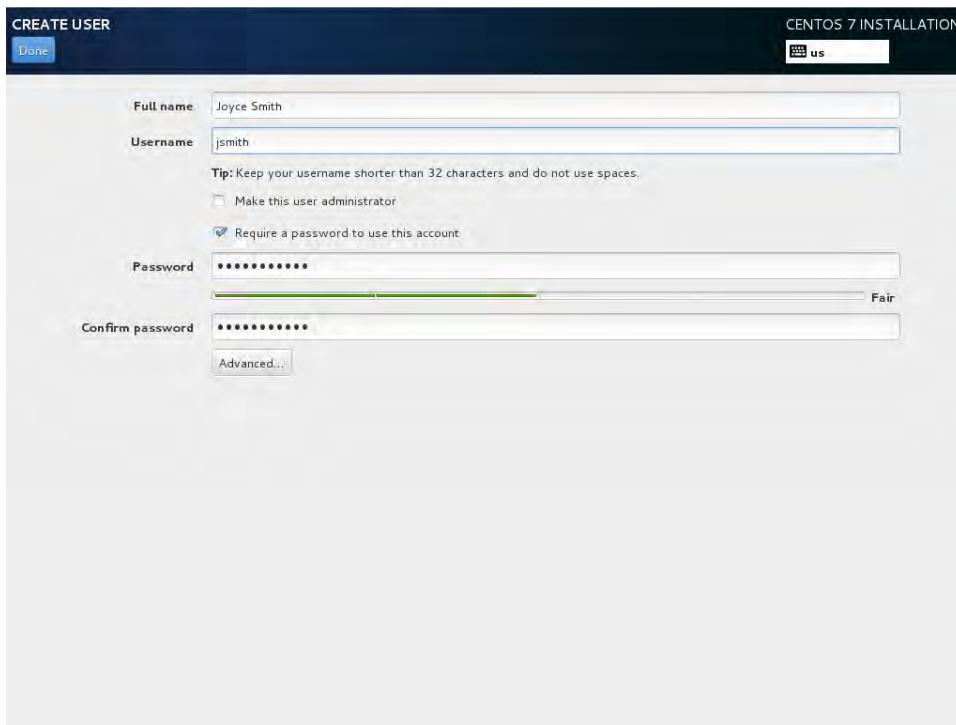
12. Enter and confirm **!Pass1234** as the root password, and select **Done**. Select **Done** a second time to confirm this password, acknowledging the warning that CentOS considers it a weak password.



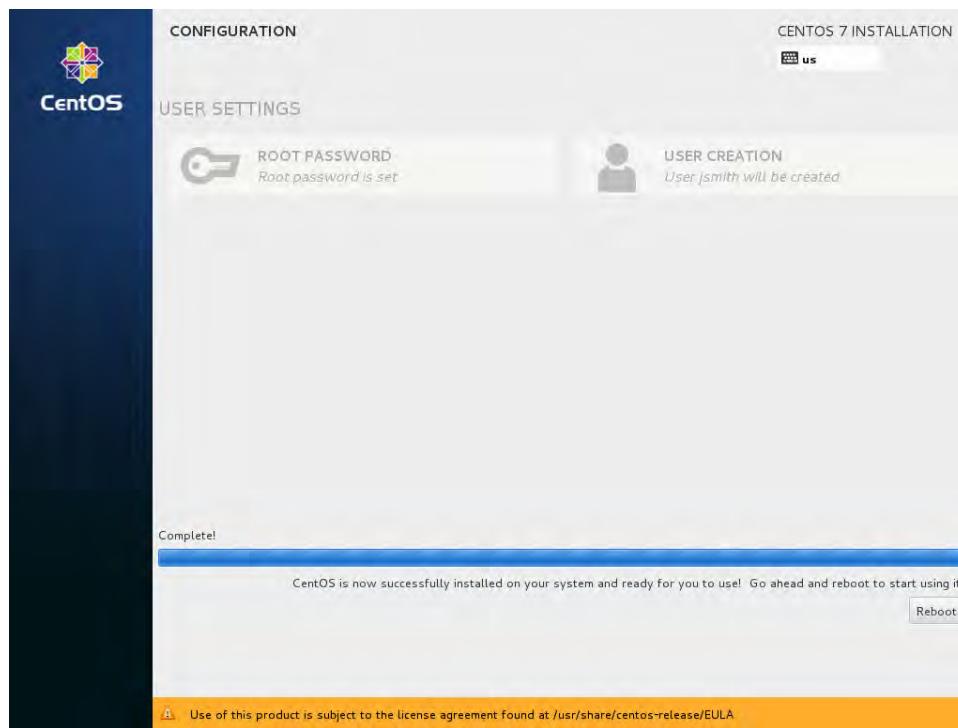
13. Next, select **User Creation** to create a new, non-root user for your system.



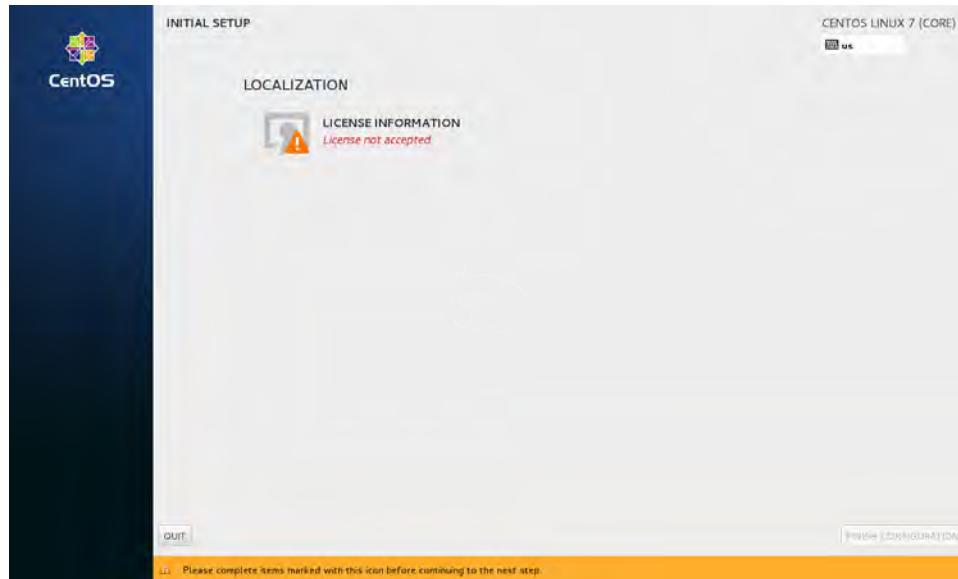
14. For the new user, in the **Full name** text box, type **Joyce Smith**. Verify that the **Username** **jsmith** is automatically filled in. Enter and confirm **my!Pass1234** as the password, and then select **Done**.



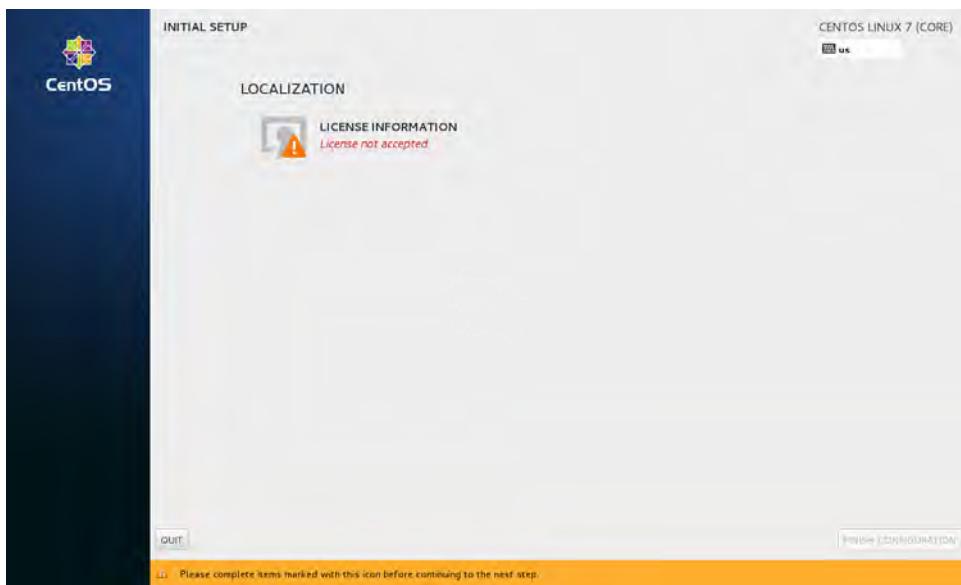
15. When installation has completed, the progress bar will be all blue and a **Complete** status will display (this may take 10-15 minutes). Select **Reboot** to reboot the Linux machine.



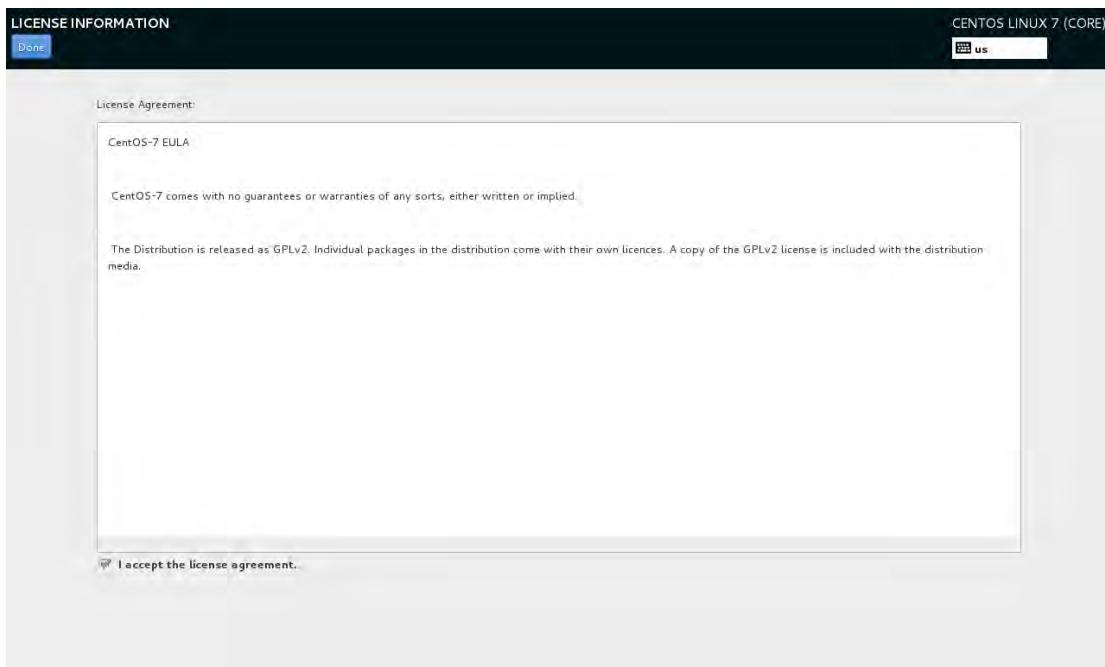
16. Verify that the following **Initial Setup** screen is displayed on boot.



17. Verify that the following **Initial Setup** screen is now displayed after your new installation completes the boot process. Select **License Information** to accept the license.



18. Under the License Agreement, check the check box labeled **I accept the license agreement** and select **Done**.



19. Select **Finish Configuration**.

## Linux Management Tools

There are a variety of Linux management tools, often many different tools that perform essentially the same function. By default, the Linux distribution you are using might have all, some, or none of the tools listed in this section. You can always install additional tools if the ones you have don't meet your needs or if you find a tool that would be more efficient to use in your environment.

The following table identifies some of the tools you are likely to use frequently.

<b>Tool/Function</b>	<b>Description</b>
Backup and Restore	There are several commands that are used for performing backup of files and directory structures.
Image recovery	Use dd to create a byte-level copy of a disk. You can then use a compression utility such as tar or gzip to compress the file for storage.
Disk maintenance utilities	The main tool you will use is <b>fsck</b> and its variants. Different Linux filesystems use different <b>fsck</b> commands.
Screen sharing	The main tools used in Linux for screen sharing are <b>vnc</b> and <b>ssh</b> . Your GUI might have additional tools and applications that can be used for screen sharing.
Force Quit	When an application stops responding, you can use the command-line command <b>kill -9</b> to force it to stop.

## Backup and Restore

Most Linux distributions include several utilities that can be used as part of an overall backup solution. For example, you can use utilities that are built into the operating system, or you can use a third-party solution such as Amanda, Afbackup, or Arkeia. Some of the built-in utilities you might use include:

- cpio
- rsync
- grsync
- dd
- dump
- restore
- tar
- gzip
- xz

## Image Recovery

Creating an image of a hard disk can be a time saver if you need to restore the full contents of a disk. You can use third-party utilities or the built-in dd command. An example of creating the image using dd is:

```
dd if=/dev/hda of=~/hdadisk.img
```

If something goes wrong with your disk, you can restore the disk using the .img file. Using the previous example, the dd command would be:

```
dd if=hdadisk.img of=/dev/hdb
```

This would restore the image to another hard disk (hdb).

## Disk Maintenance

If you are using a GUI Linux interface, there are often tools included for performing disk maintenance tasks. The tools vary based on the distribution of Linux you are using, the GUI you are working with, and what applications have been installed. Usually though, you can select the disk, and options for managing the disk are displayed. You might also be able to access them from an Applications menu or through system settings.

*Partition management* is the process of creating, destroying, and manipulating partitions to optimize system performance. Effective partition management enables you to keep track of the data in the

partitions and avoid data overflow. Various utilities, such as `sfdisk`, `GNU parted`, `gdisk`, and `partprobe`, are available for partition management.

If you are working from the command line, you will use several different disk maintenance commands depending on what you need to do.

- Depending on the partition type you need to manage, you will use different tools. Some files and commands for partition management include:

- `fdisk`
- `mkfs`
- `sfdisk`
- `GNU parted`
- `gdisk`



**Note:** Refer to the man page for command usage, including options, arguments, and complete syntax details.

- The `fstab` file is a configuration file that stores information about storage devices and partitions and where and how the partitions should be mounted. The `fstab` file is located in the `/etc` directory. It can be edited only by a root user. The `fstab` file consists of a number of lines—one for each filesystem.
- The `partprobe` program is used to update the kernel with changes in the partition tables. The program first checks the partition table, and if there are any changes, it automatically updates the kernel with the changes. The syntax of the `partprobe` utility is `partprobe [options] [device]`.
- In Linux, a filesystem cannot be accessed directly. It has to be associated with a directory to make it accessible to users. This association is brought about by loading, or mounting, the filesystem in a directory by using the `mount` command. After using the filesystem, it needs to be disassociated from the directory by unloading, or unmounting, the filesystem using the `umount` command.
- The `fsck` command is used to check the integrity of a filesystem. *Filesystem integrity* refers to the correctness and validity of a filesystem. Most systems automatically run the `fsck` command at boot time so that errors, if any, are detected and corrected before the system is used. Filesystem errors are usually caused by power failures, hardware failures, or improper shutdown of the system.



**Note:** The `fsck` command is similar in concept to the `chkdsk` and `scandisk` commands you may be familiar with from DOS and Windows-based systems.

- The `dump2fs` utility is used for managing ext2, ext3, and ext4 (extended) filesystems. It dumps the status of the extended filesystem onto the standard output device and prints the block group information for the selected device.
- The `debugfs` utility allows you to examine and modify ext2, ext3, and ext4 filesystems. When executed, the `debugfs` utility opens an interactive shell that can be used to examine and modify the extended filesystem.
- There are many xfs tools that allow you to work with the XFS filesystem.
  - `xfs_info`: Display details about the XFS filesystem.
  - `xfs_metadump`: Copy the metadata information of the XFS filesystem to a file.
  - `xfs_grow`: Expand the XFS filesystem to fill the disk size.
  - `xfs_repair`: Repair and recover a corrupt XFS filesystem.
  - `xfs_db`: Debug the XFS filesystem.

## Shells and Terminal Windows

A *shell* is a component that interacts directly with users. It also functions as the command interpreter for the Linux system. The shell accepts user commands and ensures that the kernel carries them out.

The shell also contains an interpretive programming language. A terminal window is a shell with a graphical user interface.

The various shells available in Linux are described in the following table.

<b>Shell</b>	<b>Description</b>
Bash	This is the default Linux shell. It provides the flexibility of the C shell in a Bourne shell-type environment. Use the command <code>bash</code> to open the Bash shell.
Bourne	This is the original UNIX shell developed by Steve Bourne at Bell Labs and is available on all Linux systems. Use the command <code>sh</code> to open the Bourne shell.
C shell	This was developed by Bill Joy at Berkeley and was designed to support C language development environments. It was also designed for more interactive use, providing several ways to reduce the amount of typing needed to complete a job. Use the command <code>csh</code> to open the C shell.
Korn	This shell is a combination of the C and Bourne shells. It uses the features of the C shell but the syntax of the Bourne shell. Use the command <code>ksh</code> to open the Korn shell.



**Note:** To learn more, check out the LearnTO **Select a Linux Shell** presentation from the **LearnTO** tile on the CHOICE Course screen.



**Figure 11–4: A blank shell prompt.**



**Figure 11-5:** The shell prompt in the GUI terminal window.

## Linux Commands

The generic format for a shell command is `command -option argument`. After typing your command, the shell responds by performing a specific action that is associated with that command. Linux is case sensitive, so you must enter commands in the required case.

```
[root@localhost ~]# ls -l /usr
total 236
drwxr-xr-x  2 root root 61440 May 25 13:04 bin
drwxr-xr-x  2 root root  4096 Aug  8 2008 etc
drwxr-xr-x  2 root root  4096 Aug  8 2008 games
drwxr-xr-x 123 root root 12288 May 25 11:42 include
drwxr-xr-x  6 root root  4096 Nov 25 2008 kerberos
drwxr-xr-x 108 root root 57344 May 25 13:04 lib
drwxr-xr-x  12 root root  4096 May 25 13:04 libexec
drwxr-xr-x  11 root root  4096 May 25 11:25 local
drwxr-xr-x  2 root root 16384 May 25 13:04 sbin
drwxr-xr-x 210 root root  4096 May 25 11:48 share
drwxr-xr-x  4 root root  4096 May 25 11:38 src
lrwxrwxrwx  1 root root    10 May 25 11:25 tmp -> /var/tmp
drwxr-xr-x  3 root root  4096 May 25 11:27 X11R6
[root@localhost ~]#
```

**Figure 11-6:** The `ls` command displays the list of files in the `/usr` directory.

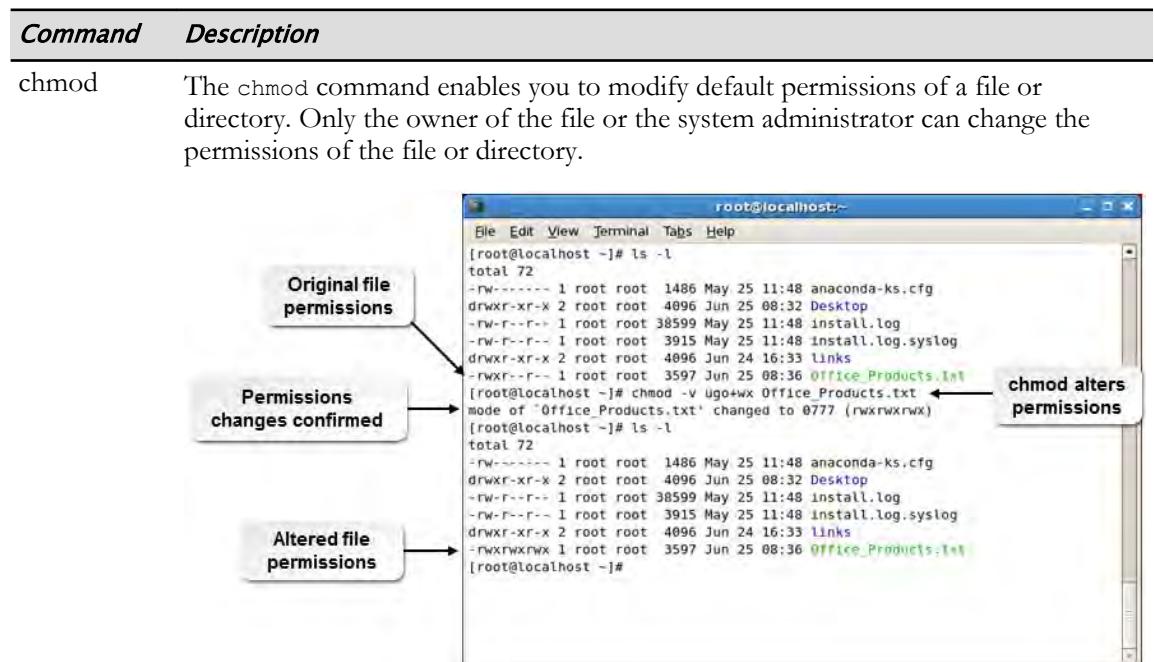
Some additional characteristics of shell commands include:

- An *argument*, also called command line argument, is usually a file name or directory name that indicates the files on which the command will operate. It is used as an input by some commands in Linux. Arguments can be files, directories, commands, or even a command switch. For example, `ls {file name}`, `ls {directory name}`, and `ls -l`.
- Sometimes commands can become quite long. You can access previously entered commands that are stored in the History file by using the **Up Arrow** and the **Down Arrow** keys.
- There are two ways of invoking a command located outside a path.
  - You can specify the path in which the command is located and then invoke the command. For example, assume that a command is located in the `/{{user-defined directory}}` directory. To invoke this command, you need to enter `/{{user-defined directory}}/{{command name}}`.
  - You can also navigate to the directory that contains the command and then invoke it. For example, assume that a command is located in the `/{{user-defined directory}}` directory. You need to change to that directory with the `cd /{{user-defined directory}}` command and then enter `./{{command name}}`.
- Some commands have long names containing version number information, weird spellings, or capitalizations. This can make it difficult to correctly enter the commands on the first try. In such a case, you can make use of the tab-completion feature. To use this feature, enter the first few characters of the command and then press **Tab**. If there is only one match, the rest of the file name is displayed. If you press the next letter of the file name you want and press **Tab** again, the complete file name should come up. If the system still cannot differentiate between the commands, it will beep again, and you have to enter additional characters or press **Tab** two times to view all available options.
- You can send or redirect the results of one command to another command. Pipes are used to combine Linux tools on a single command line, enabling you to use the output of one command as the input to another. The pipe symbol is a vertical bar (`|`), which you type between two commands. For example, `ls | more` enables you to look at a large directory listing one screen at a time.
- You can issue more than one command before pressing **Enter**. Place a semicolon (`;`) between the commands and they will be issued one after the other.
- If you enter a command, it runs as a child process to Bash, which is the parent process. If you enter `exec {{command}}`, the `exec` command will kill the parent processes and the bash process, and `{{command}}` starts to run as the parent process. For example, when a user has a limit applied on the number of process, the user can use the `exec` command to run an additional process by killing the parent process. Once the `exec {{command}}` is executed, you will be automatically logged out because the bash process has been terminated.

## Common Linux Commands

There are thousands of Linux commands that you might use, but the ones you should become familiar with and comfortable using for now are listed in the following table. As you continue to learn more about Linux, you will discover additional commands. You can always use the man pages to learn more about any command you encounter on a Linux system.

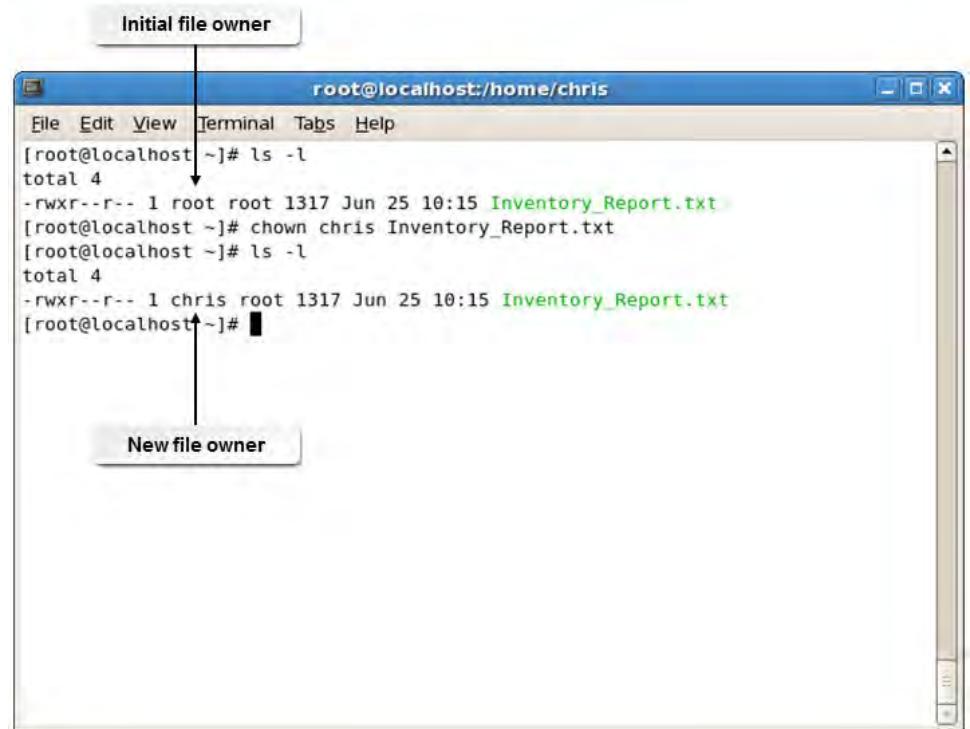
<b>Command</b>	<b>Description</b>
ls	Displays file listing. You can add options, preceding the list of options with the - character. Some of the options you will often use include: <ul style="list-style-type: none"> <li>• l for a long list format</li> <li>• a to include hidden files and directories</li> <li>• d to list directories in the current directory (rather than the content of the directories)</li> <li>• r to list entries in reverse order while sorting</li> <li>• R to list subdirectory content recursively</li> <li>• S to sort by file size</li> </ul>
cd	Changes the working directory to the specified directory.
pwd	Shows the name of the current directory.
passwd	Changes the password for the current user. When logged in with administrative access, you can also change the password for another user; for example, <code>passwd ralph</code> would change the password for the user ralph.
mv	Moves or renames files. When you specify the destination, if the path to the file is the same as the current directory (no path is included), then the file will remain in the current directory, just with a new name. If you specify a path in the destination, then the file will be moved to the new directory.
cp	Copies specified files and/or directories. You can copy a specific file to a specific destination, or you can copy multiple sources to a directory. There are many options for this command, but you should at least become familiar with the following: <ul style="list-style-type: none"> <li>• i to be prompted before overwriting the destination</li> <li>• l to link files rather than copy them</li> <li>• p to preserve attributes if possible</li> <li>• P to append the source path to the specified directory</li> <li>• r or R to recursively copy files and directories</li> <li>• u to copy only if the Source file is newer than the destination file</li> </ul>
mkdir	Creates the specified directory if it does not already exist.
rm	Removes the specified files. By default it does not remove directories, but if you use the -r or -R option, it will recursively remove directories and their contents, or the -d option to remove empty directories.

**Figure 11-7: Modifying permissions using the chmod command.**

The syntax of the chmod command is `chmod [options] {mode} {file name}`.

	<b>Note:</b> For more details on the chmod command, see <b>The chmod Command</b> section following this table.
--	--

chown  
The chown command can be used to change the owner, the group, or both for a file or directory.

**Figure 11-8: File ownership changed using the chown command.**

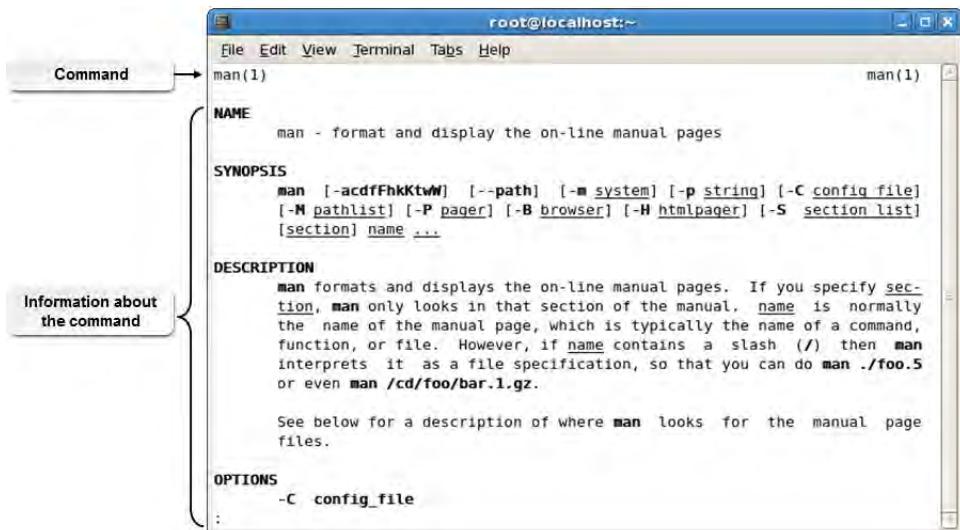
<b>Command</b>	<b>Description</b>
ifconfig and iwconfig	The <i>ifconfig</i> command is used for configuring network interfaces for Linux servers and workstations. It is also used to view the current TCP/IP configuration of a system, including the IP address and the netmask address.  The <i>iwconfig</i> command is used for configuring wireless network interfaces for Linux servers and workstations. It is similar to the <i>ifconfig</i> command, except that it is used to set up and view the parameters of wireless network interfaces.
ps	The <i>ps</i> command invokes the process table. When the command is run without any option, it displays the processes run by the current shell with details such as the PID, the terminal associated with the process, the accumulated CPU time, and the command that started the process. However, different options may be used along with the command to filter the displayed fields or processes.
q	The <i>q</i> command is used to exit from many commands including more, less, vi, and man.
su and sudo	The <i>su</i> command is used to change the ownership of a login session without logging out. It is generally used to switch ownership between an ordinary user and a root user, to change access permissions for administrative work.  The <i>super user do (sudo)</i> command allows users to run programs with the security privileges of the root user. It prompts you for your password and confirms your request to execute a command by checking the <b>/etc/sudoers</b> file, which is configured by the system administrator. The <i>sudo</i> command allows system administrators to give certain users or groups access to some or all commands without users knowing the root password. It also creates a log of all commands and arguments used, to maintain a record.
apt-get	The <i>apt-get</i> command is used to install or upgrade packages through the Internet or from the distribution CD on Debian, Ubuntu, or related Linux distribution. While installing or upgrading packages, the <i>apt-get</i> command accesses the website or the CD-ROM listed in the <b>/etc/apt/sources.list</b> file.
vi	The <i>vi</i> command invokes a text editor. Traditionally, this was simply the <i>vi</i> editor.  The <i>vim</i> command invokes the Vim editor. However, the <i>vi</i> command may also be used for this purpose because it automatically redirects the user to Vim. When entered without a file name as an argument, the <i>vim</i> command opens a welcome screen by default. To open a file, the syntax <i>vim {file name}</i> is used. If the file does not exist, Vim creates a file by the name specified and opens the file for editing. Vim supports multiple files being opened simultaneously.
dd	The <i>dd</i> command copies and converts files to enable them to be transferred from one type of media to another. The <i>dd</i> command has various options. <ul style="list-style-type: none"> <li>• <i>if={file name}</i> specifies the file from which data will be read.</li> <li>• <i>of={file name}</i> specifies the file to which data will be written.</li> <li>• <i>bs={number of bytes per block}</i> specifies the number of bytes at which data is read from an input file and written to an output file.</li> <li>• <i>count={number of blocks}</i> specifies the number of blocks to be written to the output file from the input file.</li> </ul>

<b>Command</b>	<b>Description</b>
shutdown	The command that is used to shutdown or restart a system. This closes files and performs other tasks necessary to safely shutdown a system.
grep	In its simplest form, grep is a search tool. It allows you to perform search actions, such as finding any instance you are searching for, in a file. For example, entering grep foo test returns all the lines that have a string matching “foo” in the file “test.” The grep command can also be used to search a directory for a certain file. The ls -l   grep audit command returns a long listing of any files in the current directory whose name contains “audit.”



**Note:** The term grep is derived from “Globally search a Regular Expression and Print”

man	The Linux <i>manual pages</i> , or man pages, contain the complete documentation that is specific to every Linux command; they are presented in simple ASCII text format. The man page for a specific command is displayed using the man command. The man pages are available on the system by default. They usually include information such as the name of the command, its syntax, a description of its purpose, the options it supports, examples of common usage of the command, and a list of related commands.
-----	---



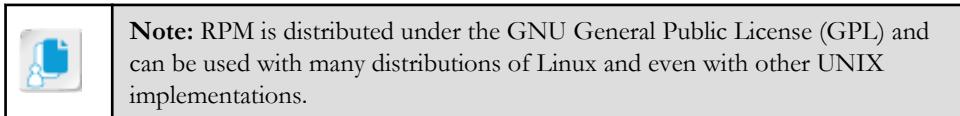
apropos	The apropos command is generally used when a user does not know which command to use to perform a certain action. It can be used with a keyword to display a list of the manual pages containing the keyword along with their man page sections. The apropos command searches a regularly updated database called the whatis database for the specified string and returns all matching entries.
date	The date command displays the current date and time set on a system. You can use the hyphen (-) or the colon (:) between the different fields of the date for a clear output.
whoami	The whoami command is used to display the user name with which you are currently logged in to the system. Sometimes, you may need to log in to a system and switch among different users, and you may not be sure with which user you are currently logged in. In such instances, you can use the whoami command to know your current user name.

Command	Description
rpm	The Red Hat Package Manager (RPM), developed by Red Hat®, is a tool for maintaining packages. By providing a standard software packaging format, RPM enables easy administration and maintenance of Linux systems and servers. RPM provides a standard installation mechanism, information about installed packages, and a method for uninstalling and upgrading existing packages.

```
[root@localhost ~]# rpm | more
RPM version 4.4.2.3
Copyright (C) 1998-2002 - Red Hat, Inc.
This program may be freely redistributed under the terms of the GNU GPL

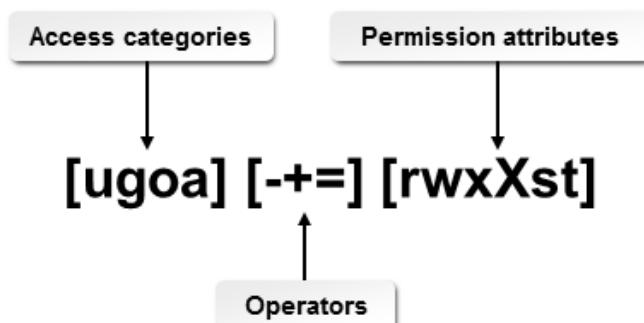
Usage: rpm [-aKfgpWHqV] [-aKfgpWHqVcdils] [-aKfgpWHqVcdilsaKfgpWHqV] [-aKfgpWHqV
cdilsaKfgpWHqV] [-aKfgpWHqVcdilsaKfgpWHqV] [-aKfgpWHqVcdilsaKfgpWHqVK] [-aKfgpWH
qVcdilsaKfgpWHqVK] [-aKfgpWHqVcdilsaKfgpWHqVKi] [-aKfgpWHqVcdilsaKfgpWHqVKiv] [-
aKfgpWHqVcdilsaKfgpWHqVKiv] [-aKfgpWHqVcdilsaKfgpWHqVKiv?] [-a|--all] [-f|--file
] [-g|--group]
      [-p|--package] [-W|--ftswalk] [--pkgid] [--hdrid] [--fileid]
      [--specfile] [--triggeredby] [--whatrequires] [--whatprovides]
      [--nomanifest] [-c|--configfiles] [-d|--docfiles] [--dump] [-l|--list]
      [--queryformat=QUERYFORMAT] [-s|--state] [--nomd5] [--nofiles]
      [--nodeps] [--noscript] [--comfollow] [--logical] [--nochdir]
      [--nostat] [--physical] [--seedot] [--xdev] [--whiteout]
      [--addsign] [-K|--checksig] [--delsign] [--import] [--resign]
      [--nodeigest] [--nosignature] [--initdb] [--rebuildddb] [--aid]
      [--allfiles] [--allmatches] [--badreloc] [-e|--erase <package>+]
      [--excludedocs] [--excludepath=<path>] [--fileconflicts] [--force]
      [-F|--freshen <packagefile>+] [-h|--hash] [--ignorearch] [--ignoreos]
      [--ignoresize] [-i|--install] [--justdb] [--nodeps] [--nomd5]
      [--nocontexts] [--noorder] [--nosuggest] [--noscripts]
      [--notriggers] [--oldpackage] [--percent] [--prefix=<dir>]
```

*Figure 11–9: Various options of the RPM tool are displayed.*



# The chmod Command

The `chmod` command supports two modes: the character mode and the numeric mode. The character mode allows you to set permissions using three components: access categories such as `u/g/o/a`; operators such as `+/-/=`; and permission attributes such as `r/w/x`. The numeric mode is represented by three-digit numbers.



*Figure 11-10: Components of the character mode.*

Operators decide whether a permission is to be granted or removed. Common operators associated with Linux permissions are listed in the following table.

<b>Operator</b>	<b>Description</b>
+	Grants permissions.
-	Denies permissions.
=	Causes the permissions assigned to overwrite other existing permissions. Assigns permissions similar to those of the reference file.

Permission attributes define exactly what a user is allowed to do with a particular file. The three permission attributes are listed in the table.

<b>Permission Attribute</b>	<b>Allows You To</b>
r (read)	View file content.
w (write)	Modify file content.
x (execute)	Run a file (if it is an executable program and is combined with the read attribute).

The permissions of a file or directory can be changed using the character method. The syntax of the `chmod` command when using this method is `chmod [options] {access categories} {operators} {permission levels} {file name or directory name}`.

Linux systems use octal (base-8) numbers to specify permissions. Each permission (r, w, and x) has an associated number.

<b>Octal Number</b>	<b>Attribute</b>	<b>Letter</b>
4	read	r
2	write	w
1	execute	x

By adding the octal numbers for the permissions you want to grant, you get the overall permission number to assign to a directory or file. Full permissions (read, write, and execute) are equivalent to  $4 + 2 + 1$ , or 7. Read and write permissions are equivalent to  $4 + 2$ , or 6. Complete permissions are expressed as a three-digit number, where each digit corresponds to the user, the group, and other permissions, respectively.

The syntax of the number method to change permissions is `chmod {number} {file name}`. Commonly used octal permission numbers are listed in the table.

<b>Octal Permission</b>	<b>Permission Attribute Equivalent</b>
755	<code>u=rwx, g=rx, o=rx</code>
700	<code>u=rwx, g=, o=</code>
644	<code>u=rw, g=r, o=r</code>
600	<code>u=rw, g=, o=</code>

## The Kill Command

The *process table* is a record that summarizes the current running processes on a system. It enables the administrator to keep track of all processes run by different users. Some of the details displayed in

the process table include the PID, the size of the program in memory, the name of the user who owns the process, and time.

Sometimes you might need to end one of the running processes. It might be because someone left a process running and you need to perform system maintenance or it might be because the process is no longer responding.

Different commands are used to send signals to processes to end or kill them.

<b>Command</b>	<b>Description</b>
kill	Sends any specified signal, or by default the termination signal, to one or more processes. The PID must be specified as the argument. The syntax of this command is <code>kill [options] {PID}</code> .
pkill	Signals processes based on the name and other identifiers as in the <code>pgrep</code> command. The syntax of this command is <code>pkill [options] {command}</code> .
killall	Kills all processes by the name specified. The syntax of this command is <code>killall [options] {command}</code> .



**Note:** The `kill` command accepts either the PID or the job number as an argument. So, this command can also be used as a job control tool.

You can either use the `kill` signal option or its corresponding numerical value to send a signal to terminate a process. The following table lists the most frequently used `kill` signal options and their description.

<b>Option</b>	<b>Used To</b>
SIGKILL or 9	Send the kill signal to a process.
SIGTERM or 15	Send the termination signal to a process.
SIGSTOP or 19	Stop a process.



**Note:** Sometimes, even after closing an X session, some of the X applications may not get terminated properly. In such cases, you need to use the `ps` command to identify the PID of that application and then kill the process.

You can use the `kill` command with the process table to end processes. By entering `kill` followed by the PID, you can terminate specific processes.

When you use the `kill` command with the jobs table, you are working only with the jobs that you started. However, the process table may display processes that do not belong to you. As a user, you can use the `kill` command only with processes that you own. As root, you can kill anyone's processes.

There are many options available with the `kill` command. These options are referred to as kill signals. Some processes cannot be eliminated by the `kill` command. To terminate these processes, use the `kill` command with the `-9` signal. This terminates the processes immediately.

## Linux Best Practices

Just like with other operating systems, there are a few things you should do on a regular basis to make sure that the system is running its best. Also, make sure that you have planned ahead so that if anything should go wrong with the system, you have the resources and ability to repair or restore functionality and services as quickly as possible.

Among the tasks you should include are:

- Scheduling regular backups. Using the backup method best suited to your organization, and on a schedule best suited to user and administrative needs, perform automated backups of data and system settings.
- Scheduling disk maintenance. On a regular basis, you should check the integrity of the hard drives. You also need to keep track of how much space is available, and who is using the space. If you have specific users that are hogging more than their fair share of disk space, consider instituting disk quotas and having those users move unneeded files to secondary storage such as DVD or tape.
- Using the app installation command for your Linux distribution, check for any available updates. This should be done at least weekly, if not more often depending on your organizational needs.
- Test all patches before deploying the patches throughout the organization.
- If devices are not performing as they should after an OS update, you might need to update drivers or firmware. Check documentation online to see if there is any indication that driver or firmware updates are warranted, and if so, download and install the appropriate files using the method used by your distribution of Linux.
- Linux systems are not often prone to virus or malware attacks, but you should be running some type of antivirus and antimalware application. Be sure that it is configured to check for updates as they become available.

# ACTIVITY 11–5

## Using Linux

### Before You Begin

You have installed Linux as a virtual machine.

### Scenario

You have just installed a Linux system. You want to try out some of the commands and features you have learned about recently.



**Note:** Whenever the instruction states “enter *command*”, you are required to type the command and press **Enter**. In Linux, commands, command-line options, and file names are case-sensitive.



**Note:** Activities may vary slightly if the software vendor has issued digital updates. Your instructor will notify you of any changes.

1. Log in to the GUI as **jsmith** and perform the initial system configuration since this is a new system.
  - a) To log in to the system, select user **Joyce Smith** on the GUI login screen.
  - b) In the **Password** text box, type **my!Pass1234** and press **Enter**.
  - c) On the **Welcome** screen, verify that **English (United States)** is selected, and select the **Next** button.
  - d) On the **Select input sources** screen, verify that **English (US)** is selected, and select the **Next** button.
  - e) On the **Connect to your existing data in the cloud** screen, select the **Next** button to continue.
  - f) On the **Thank You** screen, verify that the **Your computer is ready to use** message is displayed, and select the **Start using CentOS Linux** button to continue.
  - g) Note that the **GNOME Help** application is displayed by default, and select the **X** button in the upper-right corner to close the window.
2. Switch to the first CLI terminal (the second terminal) and log in as **jsmith**.
  - a) To switch to the second terminal, press **Ctrl+Alt+F2**.
  - b) To log in to the terminal, type **jsmith** at the **login** prompt and press **Enter**.
  - c) Type **my!Pass1234** when prompted for your **Password** and press **Enter**.
  - d) To view the current date and time of the system, at the command line, enter **date**  
Verify that the current date and time of the system is displayed.
3. Examine the directory structure.
  - a) Enter **pwd** to view the present working directory.
  - b) Enter **ls -la** to view the contents of the current directory, including all hidden files and details about those files and folders.
  - c) Enter **ls -laR / | more** to view all of the files and folders from the root of the system down through the directory structure. Piping it to the more command enables you to see one screen at a time.
  - d) Enter **q** to stop the more command and return to the command prompt.

## Summary

In this lesson, you examined some of the features and functions of the OS X and Linux operating systems. Being able to support these operating systems is as important in many organizations as being able to support Windows operating systems. Most of the features and functions in one operating system are available in the other operating systems, just with different names and sometimes implemented a little differently. With experience, these will become second nature as to where they are located and how to use them.

**Have you used OS X previously? If so, which edition? Does your organization use OS X?**

**Have you used Linux previously? If so, which distribution? Does your organization use Linux?**



**Note:** Check your CHOICE Course screen for opportunities to interact with your classmates, peers, and the larger CHOICE online community about the topics covered in this course or other topics you are interested in. From the Course screen you can also access available resources for a more continuous learning experience.

# 12

# Customized Client Environments

**Lesson Time:** 45 minutes

## Lesson Objectives

In this lesson, you will identify the hardware and software requirements for client environment configurations. You will:

- Define requirements for thick clients, thin clients, and virtualization clients.
- Define requirements for graphic and CAD/CAM design workstations, audio/video editing workstations, gaming PCs, home theater PCs, and home server PCs.

## Lesson Introduction

At this point in the course, you have identified the different components that make up a standard workstation, and the operating systems available for installation. With this information, you are ready to take a look at the hardware needs and requirements for different client configurations.

As an A+ technician, you must be knowledgeable in many different areas of information technology. This may include supporting a wide variety of client configurations, such as gaming or audio and video workstations. You must be prepared to fully support any type of environment, including more specialized hardware and software configurations based on job roles and tasks.

# TOPIC A

## Types of Common Business Clients

Now that you have identified the main components of a personal computer, you can start to take a look at what requirements are needed to install and configure a standard client. In this topic, you will identify the hardware and software needs to install a thin client, a thick client, or virtualization workstation.

When installing and configuring user workstations, it is important to identify what the specific needs are of the user that will be using the workstation to perform job tasks. Standard clients are a good starting point for any installation and must be examined to verify that they fit the requirements of the job function.

### Thick Clients

Standard business client computers are end-user computers that are administered and managed centrally by a server. Clients will typically include various hardware features and applications that suit the specific needs of the user. Client machines are generally referred to as either thin or thick, depending on the requirements. A *thick client*, also referred to as a fat client, performs most or all computing functions on its own.

Thick client requirements include:

- The computer must meet the standard requirements for running the selected operating system.
- Full application versions are installed and run directly from the client computer using its own resources. The applications are installed using traditional methods and are stored on the hard drive.
- If data is stored locally, then access to storage locations is required with a consistent pathway to data.
- If data is stored on the network, then a consistent path should be established to the storage location with proper security implementations.
- Hardware should be robust enough to run all required applications.

### Thin Clients

A *thin client* is a computer that relies heavily on another system, typically a server, to run most of its programs, processes, and services. Client setup requirements will be specific to a user's needs and will most likely be based on a job role.

The system requirements for thin clients include:

- The computer must meet the minimum requirements to run the selected operating system.
- The computer uses basic applications that can be accessed over the Internet. The applications do not get installed on the computer and do not use up any hard drive space. RAM is used to run the application from the server.
- The computer must have a fast network connection to access the server that is hosting the applications.
- The computer might require specialized software in order to access the applications hosted by the server.
- The computer may require a specific browser in order to run any web-based applications.

## Virtualization Workstations

A *virtualization workstation* is a computer that uses both hardware virtualization and client virtualization resources to provide a comprehensive virtual environment for users. The virtualized workstation is configured to use the system's hardware functions such as access to the graphics card, Random Access Memory (RAM), and Network Interface Cards (NICs), as well as run the software that provides multiple virtual machines (VMs). Organizations may use virtualization workstations to reduce the use and cost of hardware and to provide employees with a wide variety of OS specific applications from a single workstation. Virtualization provides users with a variety of applications and resources by offering multiple platforms within a single system.

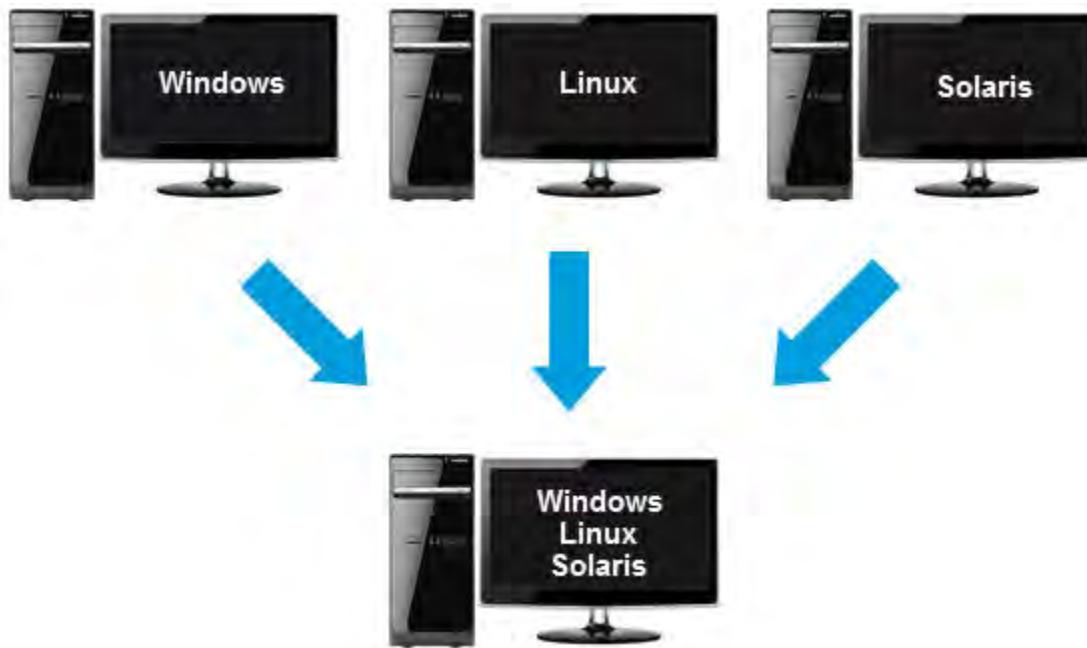


Figure 12-1: Virtualization workstations.

Common virtualization workstation software offerings include:

- VMWare®: <http://www.vmware.com>
- Oracle®'s VirtualBox: <https://www.virtualbox.org>
- Microsoft's Hyper-V® hypervisor (running on the server)

Virtualization software vendors will all have specific hardware and system requirements based on their actual software needs, but in most cases will require a virtualization workstation to have:

- The maximum RAM the motherboard can support.
- Maximum central processing unit (CPU) cores.
- Virtualization operating system (OS) if the local personal computer (PC) will be the VM host or virtualization client software installed on the PC if the VM is hosted on a server.
- Fast network connection for server-side VM hosting.

## ACTIVITY 12-1

### Selecting Components for Common Business Clients

#### Scenario

You have been asked by your manager to evaluate the hardware and software needs for all the clients within the Human Resources (HR) department of your organization. There was a recent reorganization of the department and some of the job roles and functions have changed. Based on the recent changes, you need to review the job functions and identify what type of client workstation will meet those needs.

1. A user needs to be able to access the central employee data repository to run reports, but does not need access to any local applications used to create, edit, and manage the employee data. The employee data is managed on a server that can be accessed with a log in. What type of client is best in this case?
  - Thin client
  - Virtualization workstation
  - Thick client
2. June has recently been put in charge of making updates to the Human Resource employee benefits website. She will be publishing a monthly newsletter and posting company wide announcements, among other small updates and changes, on a regular basis. All changes to the website must be tested on a number of platforms and web browsers to verify that the changes are correct regardless of the operating system and browser. What type of client setup would you suggest for her?
3. In order to properly support the HR employee benefits website, a new server running client VMs has been installed so that the environment that the application requires can be strictly administered by IT staff. Current PCs will be used to access the Client VM environment that is configured on the VM Server. What needs to be present at all PCs that will be accessing this new server and application?
  - Appropriately configured VM Client.
  - Fast network connection to server hosting the VM environment.
  - Upgrade to video cards.
4. True or False? The HR manager's client computer must meet the recommended requirements to run Windows 8.1 so that she can access and use all of the HR-related applications used by the organization. In this case, the best client option is a thick client.
  - True
  - False

# TOPIC B

## Custom Client Environments

The next logical step in examining custom computing environments is to take a closer look at some of the more specialized environments based on a specific function. In this topic, you will identify the hardware and software needs for various custom computing environments.

There are a wide variety of job functions within the job force, and you may find yourself having to support more specialized computer hardware and software installations. This may include media, audio, and even home entertainment systems. As an A+ technician, you must have the knowledge to provide support in any computing environment.

### Graphic Design and CAD/CAM Workstations

Media design workstations are configured to support the needs of graphic designers, engineers, architects, 3D media developers, and other design-driven job roles. The workstation's hardware and software needs will be dependent on the specific programs and computing tasks required by the job role.



**Figure 12-2: Graphic design and CAD/CAM workstations.**

Media design workstations require a specific set of requirements. Actual hardware and software requirements will depend on the user's specific job role and function, but most media design workstations will require a similar set of tools and components.

Common hardware components include:

- A multicore processor.
- A high-end video/graphics card with integrated *Graphics Processing Unit (GPU)*.
- Large flat panel display, or multiple monitors.
- Maximum RAM supported by the motherboard and CPU.

Common software applications include:

- Adobe's Creative Cloud.
- 3D Studio Max.
- Computer aided design (CAD) and manufacturing (CAM) programs.

### GPUs

The GPU (graphics processing unit) is an electronic circuitry unit that alters and controls the memory of a computer to meet the immediate needs of rapidly changing computer graphics and detailed visual images displayed on the display device. There are a number of ways GPUs are implemented within a computing device depending on the specific needs of the user and

applications. Most modern PCs, laptops, and some mobile devices come with a GPU already installed on either the motherboard or the CPU. The most powerful GPUs are considered to be high-end specialized units that come already installed on the video card and have various output methods and capturing devices.

## CAD Workstations

CAD workstations are unique in that they require both the hardware and the software on a system to meet certain requirements to produce complex 3D designs. CAD workstations require a high-end graphics card and monitor, and specialized input devices such as a digitizing tablet and light pen. Industries that use CAD created design specifications include automotive companies, aerospace, and architectural firms.

## CAM Workstations

Computer aided manufacturing workstations are a type of workstation that is set up with specific hardware and software that can control machine tools found in manufacturing environments. Specialized controller cards may be required as well as specialized connections and software. CAM machines may be installed in harsh environments—such as manufacturing buildings and automotive factories—so the workstations may need to be hardened machines that will not be adversely affected by their working environments.

## Audio/Video Editing Workstations

An audio/video editing workstation is a powerful computer setup that supports editing of audio and video recordings. These computers must be able to support the demanding editing programs that audio/video technicians use in post production editing functions. Most professional videos taken today include special effects and CGI (computer generated imagery) that is all applied after the digital video is taken. Common applications found on an audio/video editing workstation include:

- Sony's Vegas Pro.
- Apple's iMovie.
- WavePad.
- Corel's VideoStudio Pro X5.
- Adobe's Premiere Elements.
- AVS Audio Editor.
- MAGIX Movie Edit Pro and Music Maker.
- CyberLink's PowerDirector.
- Avid's ProTools and Motion Graphics



**Figure 12-3: An audio/video editing workstation.**

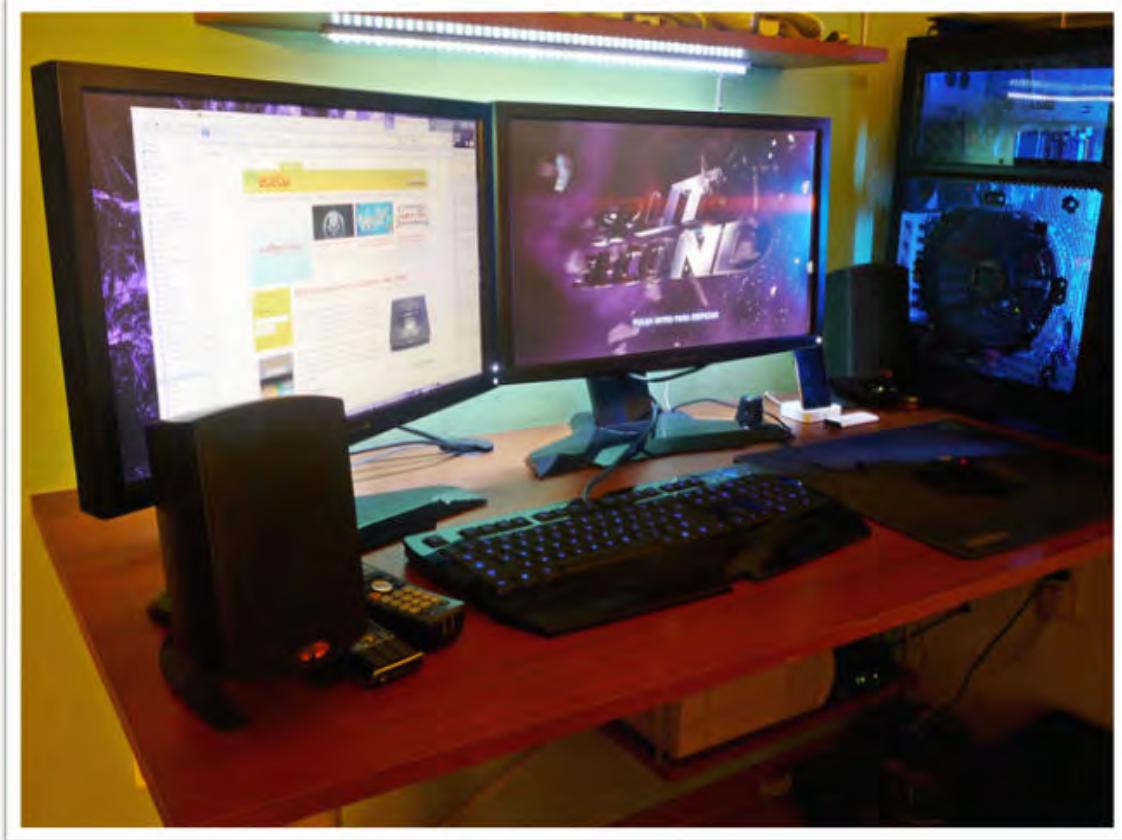
The hardware and software requirements for each individual audio/video editing workstation will differ depending on what specific tasks the job role will need to do. Most stations will require the following hardware components:

- A specialized audio and video card to support CGI and 3D post production effects.
- A large fast hard drive.
- A high-end GPU.
- Large flat panel or multiple displays.

## Gaming PCs

A *gaming PC* is a computer that comes equipped with powerful graphics capabilities, fast processing capabilities, and a large amount of memory. The main difference between a gaming PC and other consumer workstations is that they are specifically designed and built to support the demanding computing requirements by gaming software applications. All gaming PCs will require a high-end GPU to support the detailed 3D graphics and realistic imagery presented in PC games today.

Gaming platforms are also popular today and provide gamers with a number of application options, message boards, and file sharing via an online portal, such as Steam™ and Origin™.



**Figure 12–4: A gaming PC.**

Popular gaming software applications include:

- League of Legends.
- Diablo® III.
- World of Warcraft.
- StarCraft® II: Heart of the Swarm.
- Dota™ 2.
- Guild Wars® II.

There is such a wide variety of gaming software applications that each gaming PC will have specific requirements based on the needs of the user and the applications used. Gaming PCs require very specific components in order to support the demands of gaming software. Common requirements include:

- A multicore processor.
- A high-end video/specialized GPU unit.
- A high definition sound card.
- High-end cooling such as a water cooling system.
- Maximum RAM that is supported by the motherboard.
- Fast Internet connection for interactive gaming needs.
- Real-time video and audio input/output capabilities.
- In some cases, HDMI output.



**Note:** Game systems such as the Xbox One and PS4 are embedded systems, not PCs, but they do include many of the same components as listed above.

## Gaming Peripherals

There are many different peripherals used within the gaming world. The most common ones include the mouse and keyboard, but there are others that may be used depending on the type of game played:

- Gaming mice that are wireless and include many buttons and different ergonomic form factors.
- Customized keypads, with moveable keys.
- Steering wheels used for auto racing games.
- 3D glasses.
- Specialized gaming mouse pads.
- Specialized audio system.
- PC video camera.

## Home Theater PCs

A *home theater PC (HTPC)* is a computer system that is dedicated and configured to store and stream digital movies, either from the local hard drive or through an online subscription such as Netflix. Other capabilities include connecting and managing surround sound audio and speakers and DVR, or digital recording functions. The HTPC is usually equipped with specific entertainment software that can be used to manage the music and video files stored on the computer. The PCs are generally located near the TV and other home entertainment devices and have a HTPC form factor, which is aesthetically appealing and designed to look similar to other home entertainment devices. They are also designed to be less noisy than a traditional PC, with more compact quieter cooling methods and the addition of sound dampening foam or padding to limit excessive noise generated by the fan and hard drive.



**Figure 12-5: A home theater PC.**



**Note:** While you can purchase specialized home theater PCs, it is more likely that you will purchase a standard PC and add components such as a TV tuner card to make it into a home theater PC.

HTPCs are built specifically for home theater purposes, so most of the required elements are built right into the actual system. They generally include:

- A TV tuner card that allows the computer to display high-definition (HD) digital output and attach the cable provider's cable TV wire directly to the system.
- A cable card that provides authentication and encryption services to connect with the cable set top box provided by the cable company.
- Optical disc player that supports both DVD and Blu-ray.
- HDMI output for high-definition video and audio.
- Maximum RAM supported by the motherboard.
- Video card with both GPU and HD capabilities.
- Bluetooth® or wireless capabilities when using specialized remotes or input devices.

## Movie Players

There are a number of software applications available for playing HD movies on a HTPC, including:

- VLC media player.
- Cyberlink PowerDVD.
- Kodi (formerly known as XBMC).
- Windows Media Center for Windows Vista and Windows 7.

## Home Server PCs

A home server PC is a server for your house that is connected to multiple computing devices within the home to store videos, music, and pictures. It also provides central access to all stored files and is often used for file and print sharing with other computing devices in the home. The home setup generally includes a wireless network that all devices can connect to provided by a home wireless router. This allows any device to access the server within the home.

Each home server PC will have a variety of features and functions, but they all have common requirements for providing a home with necessary functions:

- Media streaming capabilities to access and play digital movies.
- File sharing for all home users to access the file system on the server.
- Print sharing.
- A gigabit NIC to provide the speeds necessary to perform large file transfers over the wireless network.
- Router that is compatible with the gigabit speed required by the NIC in the server.
- Redundant Array of Independent Disks (RAID) array to provide redundancy.

## ACTIVITY 12-2

### Selecting Components for Custom Client Systems

#### Scenario

You are a support technician for a local business that specializes in consulting, purchasing, and installing home computing solutions for consumers. You are responsible for fulfilling all the orders that have come in overnight through the business' website.

1. Customer 1 is using a desktop PC to play home movies and to set up slide shows to show his family their vacation photos and is having difficulty with the computer freezing during the movies. He is looking for a solution that will allow him to store and play his movies seamlessly through a computer. He also wants his wife to be able to access the pictures and movies from her laptop within the house. What type of computer setup would you suggest for this customer? What specific questions might you ask this customer about additional component needs?
2. Customer 2 is from a small real estate office who has recently hired a graphic designer to produce informational pamphlets and other marketing materials for the agency, such as property drop sheets and circular layout designs. The office manager has asked your company to determine the hardware and software needs for the designer's workstation so that it can be ordered and set up before their scheduled start date in two weeks. What hardware and software requirements would you suggest for the graphic designer's workstation?
3. Customer 3 is looking to make the switch from a traditional TV cable box and DVD player to a home theater PC, so that she can stream Netflix and record shows and movies from her TV. She already purchased a computer from a local home entertainment store but cannot figure out why she cannot connect the cable TV wire into the computer. What would you check for first?

## Summary

In this lesson, you identified all the different components needed to provide a custom computer setup that is based on specific user needs. There is a wide variety of job functions within the corporate world today, so identifying specific hardware and software needs based on a user's job role will only help you in providing the right level of support within your organization.

**Have you had any experience with any of the workstation or server setups presented in this lesson?**

**What types of custom client setups do you think you will encounter the most in your role as an A+ technician?**



**Note:** Check your CHOICE Course screen for opportunities to interact with your classmates, peers, and the larger CHOICE online community about the topics covered in this course or other topics you are interested in. From the Course screen you can also access available resources for a more continuous learning experience.

# 13

# Networking Technologies

**Lesson Time:** 2 hours, 30 minutes

## Lesson Objectives

In this lesson, you will identify network technologies. You will:

- Identify the physical network connections commonly used to connect PCs and mobile devices to networks.
- Identify the characteristics and properties of TCP/IP.
- Identify resources needed to connect client PCs and devices to the Internet.
- List ports and protocols commonly used in network communications.
- Identify tools commonly used to install, configure, and maintain networks.

## Lesson Introduction

In this course, you are learning to support a wide range of computing device features and functions. A key factor in device communication is how they are connected and how they transfer data to one another.

Just about every digital device on the planet today is connected to external resources via some kind of network, whether it is a small office/home office network, a corporate wide area network (WAN), or directly to the Internet itself. The ability to connect, share, and communicate using a network is crucial for running a business and staying connected to everything in the world, so as an A+ support technician, you will need to understand the technologies that underlie both local and global network communications to ensure that the organization you support stays connected.

# TOPIC A

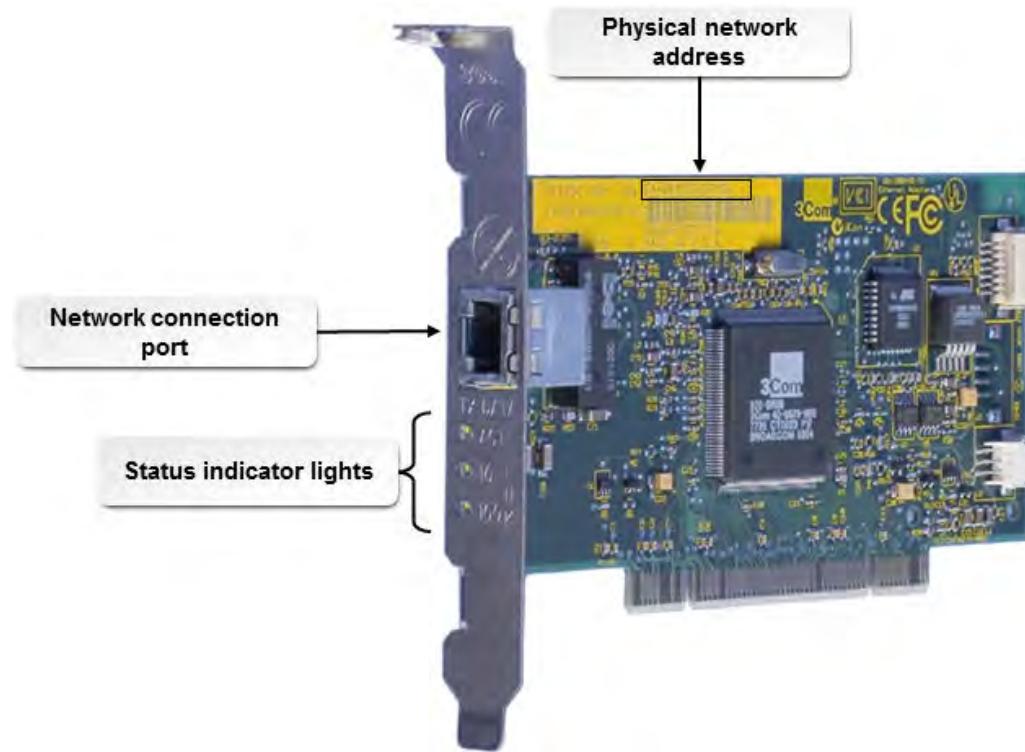
## TCP/IP Properties and Characteristics

In this lesson, you will identify various networking technologies. In order to do so, you will need to understand a few basic concepts and the connections used to implement computer networks and their components. In this topic, you will identify the physical network connections that make up most computer networks.

No matter what types of networks you support in your professional career, they will all share some fundamental characteristics as well as basic physical components. As a computer support technician, dealing with these components will need to be as natural to you as handling a scalpel is to a surgeon. The information in this topic will familiarize you with the physical network connections and components that you will deal with on a daily basis as a support technician.

### Network Interface Card Characteristics

Network interface cards have some special characteristics that distinguish them from other types of adapter cards.



**Figure 13-1: A network interface card.**

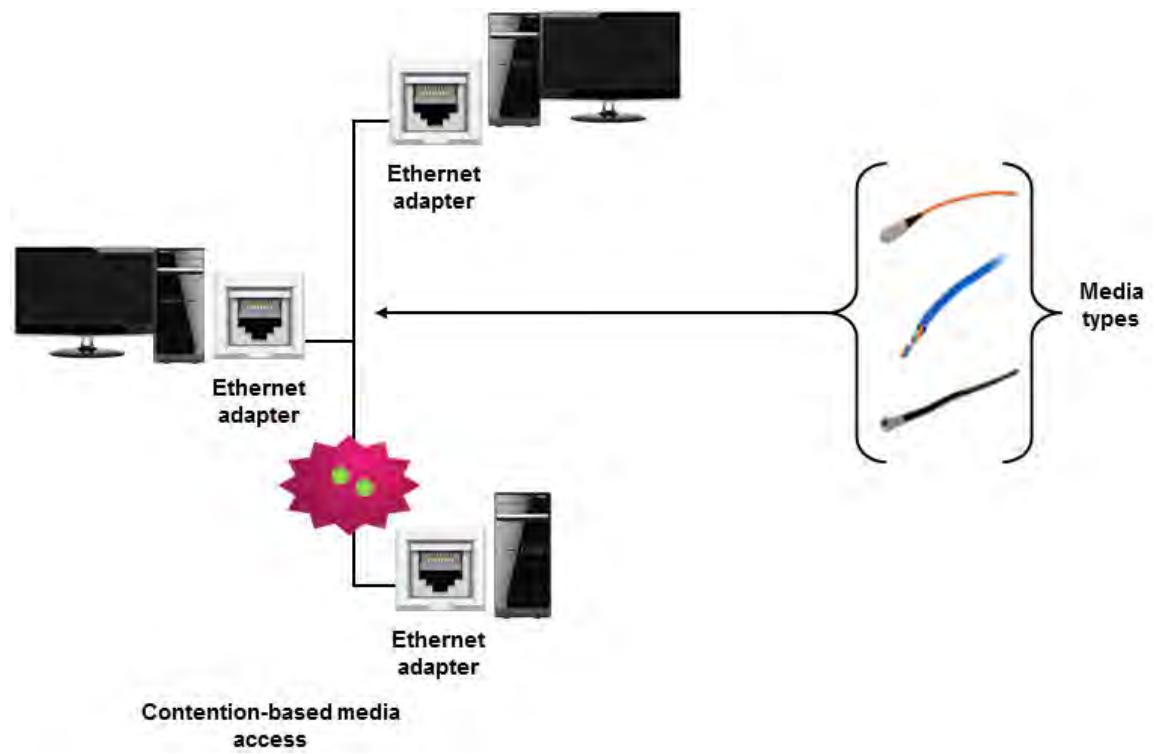
Network interface card characteristics are described in the following table.

Characteristic	Description
Network connection port	Network adapter cards will have one or more ports that are configured to connect specifically to a given type of network cable. Some older cards had several types of ports so that they could connect to several different types of network cable. Network connections today are standardized and almost all use one port type.

<b>Characteristic</b>	<b>Description</b>
Physical network address	<p>Each network adapter has a globally unique <i>physical address</i> burned onto the card by the card manufacturer. The physical address uniquely identifies every individual card that connects to the network cable or media. For this reason, the physical address is also called the <i>Media Access Control (MAC) address</i>. MAC addresses are six bytes long. A typical MAC address might appear as <b>00-00-86-47-F6-65</b>, where the first three bytes are the vendor's unique ID and the next three uniquely identify that card for its vendor.</p>
Status indicator lights	<p>Network adapters, including those built into most network devices, typically have one or more light emitting diode (LED) status lights that can provide information on the state of the network connection.</p> <ul style="list-style-type: none"> <li>• Most adapters have a <i>link light</i> that indicates if there is a signal from the network. If the link light is not lit, there is generally a problem with the cable or the physical connection.</li> <li>• Most adapters also have an <i>activity light</i> that flickers when packets are received or sent. If the light flickers constantly, the network might be overused or there might be a device generating network noise.</li> <li>• Some multi-speed adapters have a <i>speed light</i> to show whether the adapter is operating at 10 Mbps (Ethernet), 100 Mbps (Fast Ethernet), or 1000 Mbps (Gigabit Ethernet).</li> <li>• Some types of equipment combine the functions of more than one light into dual-color LEDs. For example, a green flickering light might indicate normal activity, while an orange flickering light indicates network traffic collisions.</li> </ul>

## Ethernet

An *Ethernet* network is a popular LAN implementation that uses Ethernet network adapters, contention-based media access, and twisted pair, coax, or fiber media. Xerox® corporation first developed Ethernet in the 1970s. Later, the IEEE used Ethernet as the basis of the 802.3 specification, which standardized Ethernet and expanded it to include a wide range of cable media. The 802.3 family of specifications also determines transmission speed (10 Mbps, 100 Mbps, or 1000 Mbps) and signal method (*baseband* or broadband).



**Figure 13-2: Ethernet.**

### Ethernet over Power Lines

The IEEE 1905-2013, more accurately, the IEEE 1905.1-2013 standard, provides a common interface for home networking technologies. The Standard for a Convergent Digital Home Network for Heterogeneous Technologies is designed to reduce network complexity for consumers and helps operators manage various networks throughout homes. There are various wired connections that can be used, but the most common under this standard are Ethernet over HDMI and Ethernet over power line. A device with built-in HDMI 1.4 capabilities allows audio, video, and data communication over an HDMI 1.4 cable. Devices that comply with the nVoy hybrid home networking standard can use Ethernet over power line.

Another name for Ethernet over power lines is Powerline. Powerline is a bridging technology used in home networks to provide network coverage in areas where wireless coverage is poor or non-existent. It's also used to connect older devices, such as TVs and game consoles that have an Ethernet port but no Wi-Fi connectivity. If you have a wireless hub or router, you can deploy a Powerline network solution. A Powerline kit contains two adapters and two Ethernet cables. To implement a Powerline kit:

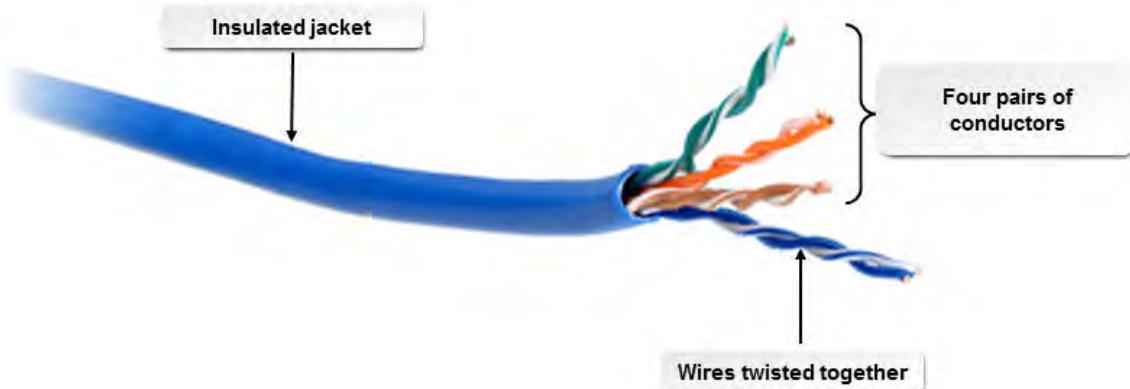
1. Connect one end of an Ethernet cable to your wireless router and the other end to the adapter, and then plug the adapter into the wall.
2. Connect the second Ethernet cable to the device and to the adapter, and plug the adapter into a wall socket.

The two adapters auto-detect, and packets can be sent from the router into the first adapter, across the electrical wiring in the walls, to the second adapter, out across the Ethernet cable to the device. There are kits that provide connection speeds faster than some 5 GHz Wi-Fi routers. Ethernet over Power networking kits typically provide security options such as encryption.

### Twisted Pair Cables

*Twisted pair* is a type of cable in which four pairs of insulated conductors are twisted around each other in pairs and clad in a protective and insulating outer jacket. There may be multiple pairs

depending on the type and size of cabling. Twisted pair cabling is typically less expensive and more flexible than other cable types, but it is susceptible to electromagnetic interference. Shielding can be added around the bundle of twisted pairs to reduce interference. Another transmission limitation of twisted pair cabling is that it has low bandwidth compared to other cabling types. Twisted pair is also susceptible to attenuation, or a reduction in signal strength. Attenuation may intensify when using a splitter to split the signal, potentially reducing signal quality.



**Figure 13-3: Twisted pair cable.**

### Types of Twisted Pair Cables

Twisted pair cable comes in two basic types: unshielded twisted pair (UTP) and shielded twisted pair (STP). As the name implies, STP encloses signal-carrying wires in a conducting shield to reduce the potential for electromagnetic interference. Some cables use a braided shield, which makes them heavier and more difficult to install than UTP. Other cables use an outer foil shield, known as screened twisted-pair cables.

UTP cable comes in different grades, called categories, which support different network speeds and technologies. A cable's category is typically printed on the cable itself, making identification easy.

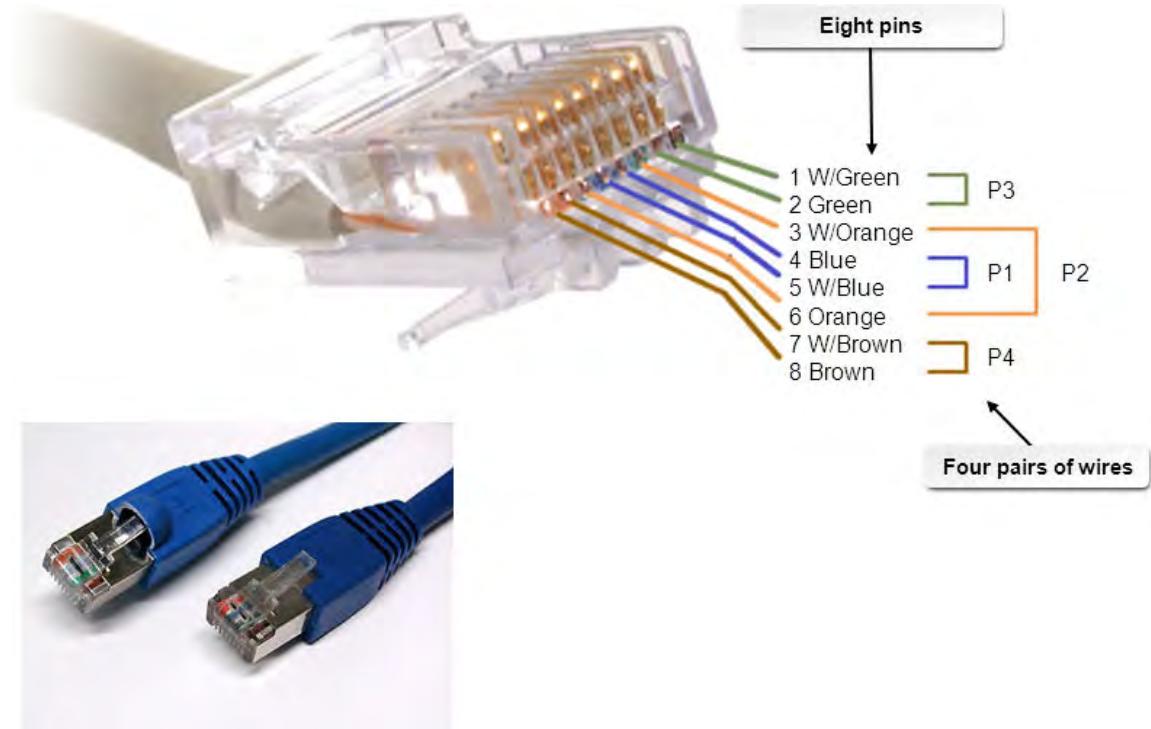
Category	Characteristics
CAT 3	<ul style="list-style-type: none"> <li>Network Type: Telephone or Ethernet</li> <li>Maximum speed: 10 Mbps</li> <li>Maximum frequency: 16 MHz</li> </ul> <p>CAT 3 is currently used for telephone wiring</p>
CAT 5	<ul style="list-style-type: none"> <li>Network Type: Fast Ethernet</li> <li>Maximum speed: Up to 100 Mbps</li> <li>Maximum frequency: 100 MHz</li> </ul> <p>CAT 5 has, for the most part, been replaced by CAT 5e.</p>
CAT 5e	<ul style="list-style-type: none"> <li>Network Type: Gigabit Ethernet</li> <li>Maximum speed: Up to 1 Gbps</li> <li>Maximum frequency: 100 MHz</li> </ul> <div style="border: 1px solid #ccc; padding: 5px;"> <span style="font-size: 2em; vertical-align: middle;">[Icon]</span> <b>Note:</b> CAT 5e is also available with a frequency of 350 MHz. When possible, it is recommended that you use the 350-MHz cable.         </div>

CAT 5e is the most common implementation of twisted pair cable today.

<b>Category</b>	<b>Characteristics</b>
CAT 6	<ul style="list-style-type: none"> <li>• Network Type: Gigabit Ethernet</li> <li>• Maximum speed: 10 Gbps</li> <li>• Maximum frequency: 250 MHz</li> </ul> <p>CAT 6 is commonly used for back-end, high capacity networking.</p> <p>Extended CAT 6 or CAT 6e cables perform better than CAT 6 when they are installed in an environment with high noise or RF interference.</p>
CAT 6a or CAT 6 Augmented	<ul style="list-style-type: none"> <li>• Network Type: Gigabit Ethernet</li> <li>• Maximum speed: 10 Gbps</li> <li>• Maximum frequency: 500 MHz</li> </ul> <p>CAT 6a is expected to replace HDMI for video transmission.</p>
CAT 7	<ul style="list-style-type: none"> <li>• Network Type: Gigabit Ethernet</li> <li>• Maximum speed: 10 Gbps+</li> <li>• Maximum frequency: 600 MHz</li> </ul> <p>CAT 7 supports 10GBASE-T Ethernet over a full 100 meters and offers improved crosstalk noise reduction.</p>

### Twisted Pair Connectors

The RJ-45 is an eight-pin connector used by twisted pair cables in networking. All four pairs of wires in the twisted pair cable use this connector.



**Figure 13-4: Twisted pair connectors**



**Note:** The RJ in RJ-11 and RJ-45 is an abbreviation for “registered jack.” An RJ-45 connector is also referred to as an 8P8C connector.

## PVC Cables and Plenum Cables

*Polyvinyl chloride (PVC)* is an inexpensive and flexible rubber-like plastic used to surround some twisted pair cabling. However, when PVC burns, it gives off noxious or poisonous gases.

*Plenum cable* jacketing does not give off noxious or poisonous gases when it burns. Fire codes require that you install this special grade cabling in the *plenum*, which is a building's air handling space between the structural ceiling and any suspended ceiling, under raised floors, and in firebreak walls.



Figure 13-5: PVC and plenum cables.

## Twisted Pair Wiring Standards

The *Telecommunications Industry Association (TIA)* and the *Electronic Industries Alliance (EIA)* developed the 568 Commercial Building Telecommunication Cabling standard. This standard defines the regulations on designing, building, and managing a cabling system that uses structured cabling according to specified performance characteristics to create a system of unified communications.

TIA/EIA releases recommendations for how network media may best be installed to optimize network performance:

- T568A is a legacy standard that was used in commercial buildings and cabling systems that support data networks, voice, and video. It further defines cable performance and technical requirements.
- T568B defines the standards for preferred cable types that provide the minimum acceptable performance levels for home-based networks, including:
  - 100-ohm twisted pair cable.
  - Shielded twisted pair cable.
  - Optical fiber cable.
- T568C is the latest standard released by TIA/EIA that is designed to be used in both home and commercial buildings and in multiple locations and to provide full support for all modern and future communications needs.

## Coaxial Cables

Coaxial cable, or *coax*, is a type of copper cable that features a central conductor surrounded by braided or foil shielding. An insulator separates the conductor and shield, and the entire package is wrapped in an insulating layer called a jacket. The data signal is transmitted over the central conductor. The outer shielding serves to reduce electromagnetic interference.

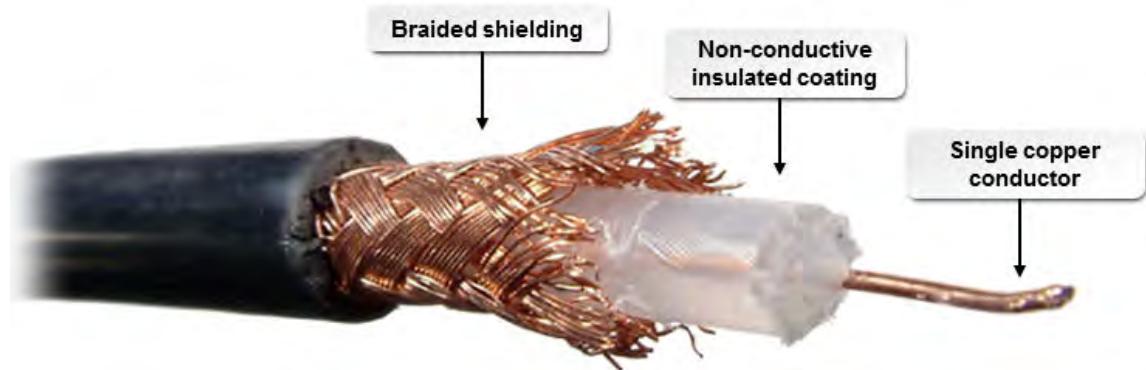


Figure 13-6: Coaxial cable.



**Note:** Coaxial cable is so named because the conductor and shield share the central COmmon AXis, or are co-axial. This arrangement helps prevent electromagnetic interference from reaching the conductor.

Like twisted pair cable, coax is susceptible to signal loss or degradation when splitters are used.

### Types of Coaxial Cables and Connectors

The different types of coaxial cable are described in the following table.

<b>Coaxial Cable Type</b>	<b>Description</b>
RG-58	<p>RG-58/U and RG-58A/U, also known as thinnet, are older types of media used for networking. The specifications include a maximum transmission speed of 10 Mbps using baseband transmission up to 185 meters in length.</p> <p>Thinnet connections are made with a twist-lock connector called a Bayonet Neill-Concelman (BNC) connector. Devices connect to the network with T-connectors. Each end of the cable must be terminated with a 50-ohm resistor.</p>  <p><b>BNC connector</b></p>
RG-59	<p>Another coax connector type is the <i>F-connector</i>, which is used to connect cable TV and FM antenna cables. Today, F-connectors are also used to connect cable modems to the CATV network.</p>  <p><b>F-connector</b></p>
RG-6	<p>RG-6 and RG-6/U has been replacing RG-59 in recent years as the preferred cable for CATV networks. Like RG-59, F-connectors are used to connect cable modems to the CATV network. Transmission distances are:</p> <ul style="list-style-type: none"> <li>• Up to 300 meters for 10 Mbps</li> <li>• Up to 200 meters for 100 Mbps</li> </ul>

<b>Coaxial Cable Type</b>	<b>Description</b>
RG-8	RG-8 is a thicker type of coaxial cable often referred to as thicknet. It is seldom seen today due to its expense and stiffness, but was popular at one time as a backbone cable in coaxial network installations. The specifications include a maximum transmission speed of 10 Mbps using baseband transmission up to 500 meters in length.



**RG8 connector**

Connections between Thicknet segments are made with a screw-type connector called an N-connector. Thicknet segments must be terminated with a 50-ohm resistor.

A legacy method used to quickly connect a computer to a thicknet wire is called a vampire tap.

## Termination

Coax network segments typically must be *terminated* to prevent signal reflections off the end of the cable. Cables are terminated by installing a resistor of an appropriate rating, typically 50 ohms, on the end of the cable.

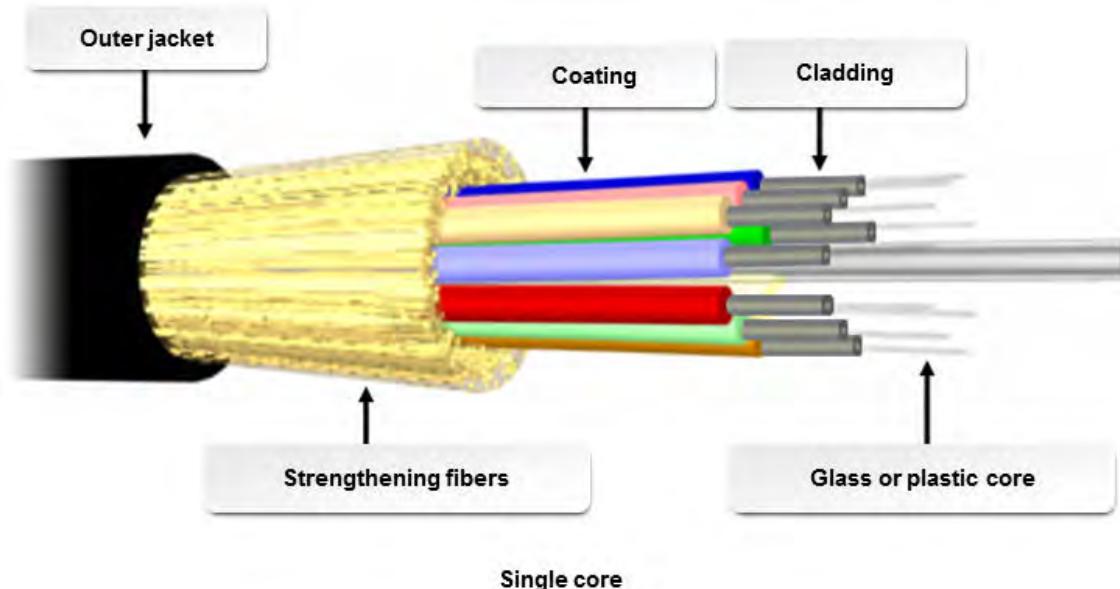
## Fiber Optic Cables

*Fiber optic cable* is a type of network cable in which the core is one or more glass or plastic strands. The core is between 5 and 100 microns thick and is surrounded by cladding, which reflects light back to the core in patterns determined by the transmission mode. A buffer, often made of plastic, surrounds the cladding and core. To add strength (or pull strength) to the cable, strands of Kevlar® surround the buffer. An outer jacket, sometimes called armor, wraps and protects the whole assembly. Light pulses from a laser or high-intensity light-emitting diodes (LEDs) are passed through the core to carry the signal. The cladding reflects the light back into the core, increasing the distance the signal can travel without being regenerated.

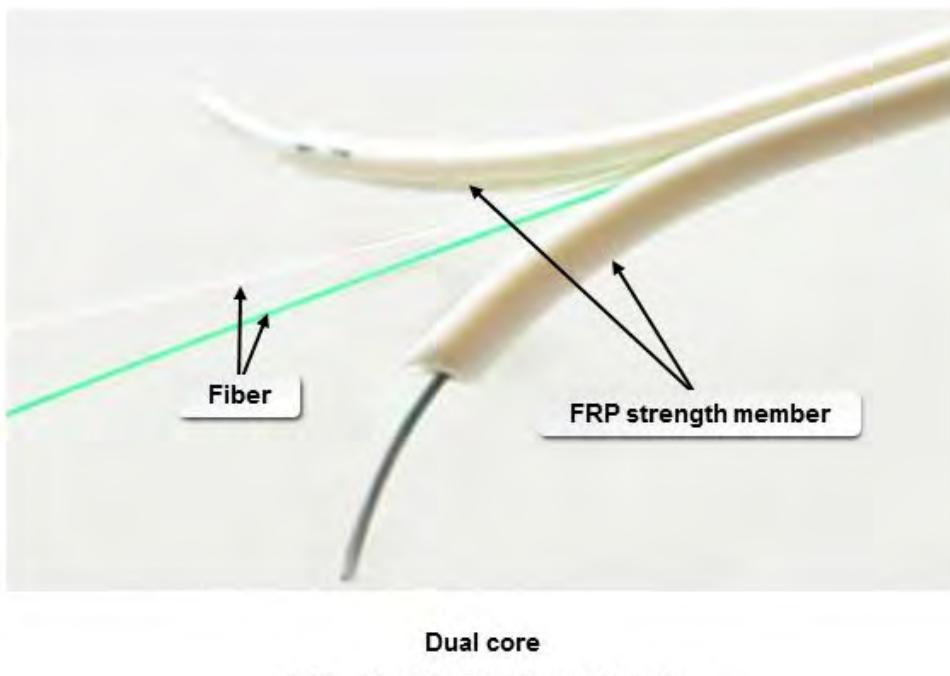
Fiber optic cables are expensive, fragile, and difficult to install. However, fiber optic transmissions are fast and reliable over extremely long distances, so they are used frequently in backbone wiring solutions. The theoretical throughput of fiber optic cables is in excess of 100 terabits per second, but more practical applications provide speeds of around 1 to 10 gigabits per second. Also, fiber optic cables are impervious to electromagnetic interference.

Despite their advantages, there are some transmission limitations of fiber optic cables. Many fiber optic cables, when bent, will start to leak some of their signal. This might enable an attacker to tamper with the signal. Fiber optic cables also need to be very well-shielded when installed outdoors in order to prevent extreme weather from causing damage.

Fiber optic cores are uni-directional. For this reason, they are installed in pairs, one for sending data and one for receiving data.



**Figure 13-7:** A single-core fiber optic cable.



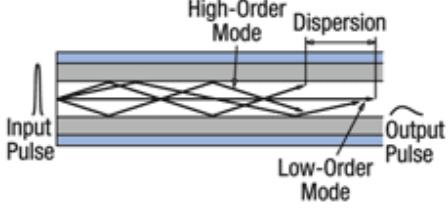
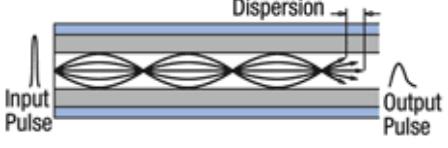
**Figure 13-8:** A dual-core fiber optic cable.

## Types of Fiber Optic Cables

There are two types of fiber optic cables: single-mode or multimode fiber.

- Single-mode has a small core that allows only one mode of light to propagate, so the number of light reflections created as it travels through the core decreases. This lowers attenuation and enables the signal to travel faster.

- Multimode has a large core that supports multiple modes of light to propagate. This allows the number of light reflections created as the light passes through the core to increase. More data can pass through. This cable is typically used for short distances.

<b>Mode Type</b>	<b>Description</b>
Single-mode fiber	Carries a single optical signal and has a small core that allows only a single beam of light to pass. A laser, usually operating in the infrared portion of the spectrum, is modulated in amplitude (intensity) to transmit the signal through the fiber.
	
Step index multimode fiber	Contains a core surrounded by cladding, each with its own uniform index of refraction. When light from the core enters the cladding, a step down occurs due to the difference in the refractive indices. Step-index fiber uses total internal reflection to trap light.
	
Graded index multimode fiber	Possesses variations in the core glass to compensate for mode path length differences. It provides up to 2 GHz of bandwidth, which is significantly more than step-index fiber.
	

## Fiber Optic Connectors

There are various connector types used with fiber optic cable.



**Note:** Connections are unidirectional, and each core has its own connector.

<b>Connector</b>	<b>Description</b>
<i>Straight Tip (ST)</i>	Used to connect multimode fiber, ST connectors look like BNC connectors. They have a straight, ceramic center pin and bayonet lug lockdown. They are often used in network patch panels. ST connectors are perhaps the most popular type of fiber connector.
	
<i>Subscriber Connector or Standard Connector (SC)</i>	Box-shaped connectors that snap into a receptacle. SC connectors are often used in a duplex configuration where two fibers are terminated into two SC connectors that are molded together. SC is used with single-mode fiber.
	
<i>Face Contact (FC)</i>	Similar to SMA connectors, FC connectors use a heavy duty ferrule in the center for more mechanical stability than SMA or ST connectors. These connectors are more popular in industrial settings where greater strength is required.
	
<i>Local Connector (LC)</i>	The LC is a small form factor ceramic ferrule connector for both single-mode and multimode fiber. It is about half the size of the SC or ST. The LC uses an RJ45-type latching and can be used to transition installations from twisted pair copper cabling to fiber.
	
<i>Sub Multi Assembly or Sub Miniature type A (SMA)</i>	Similar to ST connectors, SMA connectors use a threaded ferrule on the outside to lock the connector in place. These are typically used where water or other environmental factors necessitate a waterproof connection, which is not possible with a bayonet-style connector.
	

<b>Connector</b>	<b>Description</b>
<i>Mechanical Transfer Registered Jack (MT-RJ)</i>	The MT-RJ connector, sometimes called a Fiber Jack connector, is a compact snap-to-lock connector used with multimode fiber. The MT-RJ is easy to use and similar in size to the RJ45 connector. Two strands of fiber are attached with one connector.

## Wireless Connections

*Wireless connections* are network connections that transmit signals without using physical network media. Instead, signals are transmitted as electromagnetic energy, such as radio waves or satellite microwave. Most general office wireless implementations use radio. Wireless communication enables users to move around while remaining connected to the network.

	<b>Note:</b> Wireless communication permits connections between areas where it would be difficult or impossible to install wires, such as in hazardous areas, across long distances, or inside historic buildings. It is also extremely popular in standard business and home installations because of the mobility and flexibility it provides, as well as the simplicity of media-free installation.
---	--



**Radio waves**



**Satellite**

*Figure 13–9: Wireless connections.*

### Wireless Signal Strength

The ability to communicate via wireless network is highly dependent upon the local signal strength. Signal strength can vary in relation to a number of factors, including interference and distance from the Wireless Access Point (WAP). Most wireless devices will provide some kind of indicator regarding the strength of the current wireless signal. For example, in Windows, a wireless network card will display a message on screen when signal strength is low and connectivity is limited as a result.

### Wi-Fi

Wireless radio communications following the IEEE 802.11g Wi-Fi standard are the most common choice for ordinary wireless LAN connectivity for portable computers inside homes, offices, and, increasingly, public buildings. Choose Wi-Fi when you need to connect portable computer systems to a wired or wireless Ethernet LAN and enable users to move from place to place freely without a line of sight to the WAP. Wi-Fi provides good performance within the WAP coverage area, barring any signal interference.

## Other Network Connection Methods

In addition to coax, twisted pair, and fiber optic, you can use other types of cables and methods to make network connections, including USB, FireWire®, and RS-232 null-modem cable. You can also make wireless connections using radio, infrared, or satellite transmissions. Physical network cable connections are often referred to as a group as bounded media. Wireless connection types that transmit signals through the air without a cable are collectively called unbounded media.

### RS-232 Null-Modem Connections

RS-232 is a standard serial interface that was used to connect serial devices, particularly modems. These connections have been primarily replaced by the faster Ethernet, but can be found in some cases to connect devices for debugging and to connect devices in close proximity of one another. When you use an RS-232 null-modem cable to create network connections between computers, it mimics the presence of a modem connection between the two systems. There are some types of network connections, such as a dial-up Internet connection, that use telephone media. So, with an RS-232 null-modem cable connected to two computers' serial ports, you can, in effect, create a simulated dial-up connection directly between the two systems.

# ACTIVITY 13-1

## Identifying Network Cables and Connectors

### Scenario

You are working with the rest of the PC technicians team in cleaning up the storage bins and closets in your area. You have found a variety of cables and connectors thrown all together without any indication of what they are or what they are used for. You suggest to the team that the items be sorted and placed in labeled bins before storing in the closets.

1. Sort the connectors by type.
  - a) In one container, place all of the Ethernet twisted pair connectors.
  - b) In another container, place all of the fiber optic connectors.

You can break these down into specific fiber optic connector types if you have a large assortment.
  - c) Place other connectors in their own containers.
2. Sort the cables by type.
  - a) Place all of the Ethernet cable of the same category, for example Cat 5, in its own containers.

Be sure not to coil the cable too tightly so as not to break the wires.
  - b) Place all of the fiber optic cable in their own containers.
  - c) Place any other cable types in their own containers.
3. Look at the cables and connectors on the back of your computer, and identify what cables are used and what their purpose is.
4. **What type of cable is used to connect your computer to the network?**
5. **Are there any LED lights on the cable ports indicating activity?**

# TOPIC B

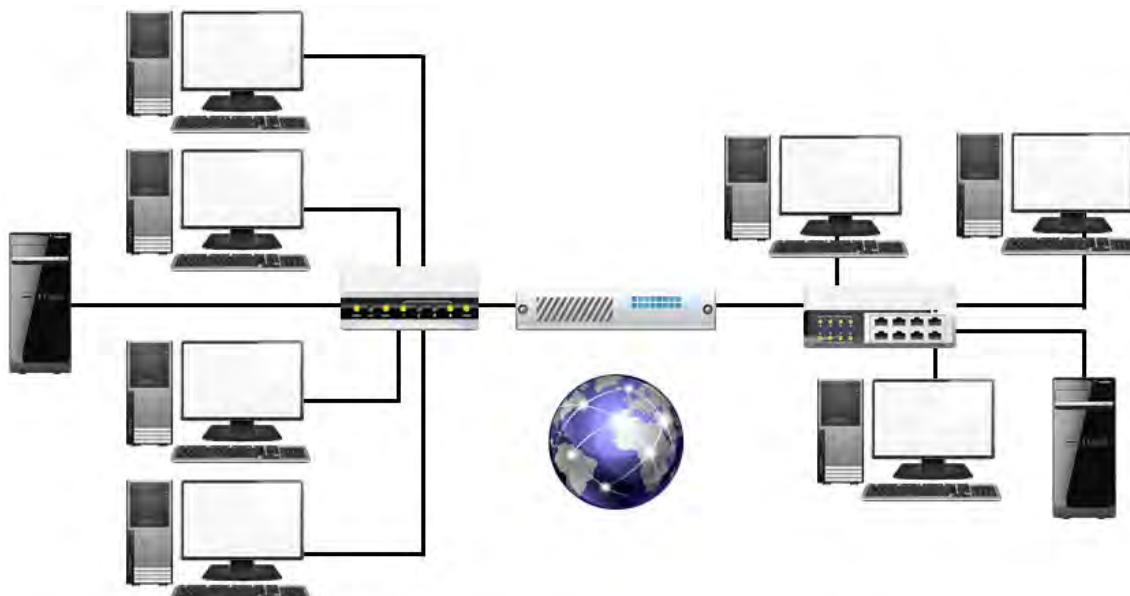
## TCP/IP

Now that you are familiar with the basic components that make up a network, you can start to take a closer look into how Transmission Control Protocol/Internet Protocol (TCP/IP) addressing and data delivery methods are used to implement TCP/IP on a network. In this lesson, you will identify the properties and characteristics of TCP/IP.

As an A+ technician, you must be able to identify the components of a system in order to provide the right level of support to your organization. Because all networks are different, you still need to be able to identify the components and how they are connected. Understanding how everything is connected and functioning within the network will allow you to properly support TCP/IP within the network.

## TCP/IP

*Transmission Control Protocol/Internet Protocol (TCP/IP)* is a non-proprietary, routable network protocol that enables computers to communicate over all types of networks. TCP/IP is the native protocol of the Internet and is required for Internet connectivity. TCP/IP is a suite of related protocols that work together to provide network addressing and naming, and data delivery. In this suite, IP provides addressing, TCP provides connection-oriented message transmission, and User Datagram Protocol (UDP) provides connectionless, best-effort message transmission.



TCP/IP enables communication across different network types.

Figure 13-10: TCP/IP.



**Note:** For additional information, check out the LearnTO **Interpret an IP Address** presentation in the LearnTOs for this course on your CHOICE Course screen.

## Non-proprietary, Routable Protocols

Non-proprietary means that no one group or organization owns or controls the protocol. You do not have to purchase software from a particular vendor or pay any kind of licensing fee to use TCP/IP.

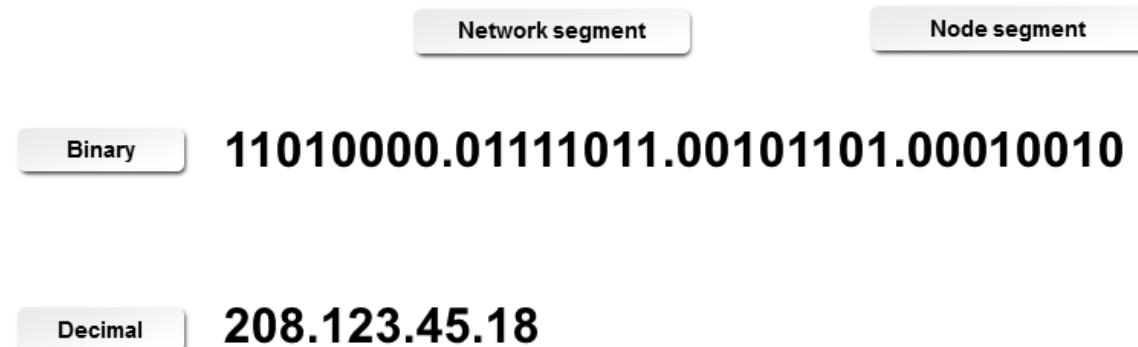
Routable means the protocol can be used to communicate between different network sections. Thus, TCP/IP communications are not confined to a single network segment. To be routable, a protocol must provide addresses that identify individual network segments as well as network *hosts*.

## Broadcast, Unicast, and Multicast

Broadcasts are network communications that are sent to all the computers on the network at once. Compare this to unicast transmissions, which are sent to a specific address, or multicast transmissions, which use a single address to transmit to a group of systems.

## IPv4 Addresses

An *IPv4 address* is a 32-bit number assigned to a computer on a TCP/IP network. Some of the bits in the address represent the network segment; the other bits represent the computer, or node, itself. For readability, the 32-bit IPv4 address is separated into four 8-bit octets, and each octet is converted to a single decimal value. Each decimal number can range from 0 to 255, but the first number cannot be 0. In addition, all four numbers in a host address cannot be 0 (0.0.0.0) or 255 (255.255.255.255).



**Figure 13-11: An IPv4 address.**

## Network Names

Systems on a network are typically assigned a host name, in addition to the numeric address. The host name is the descriptive name you see assigned to computers on the Internet, but systems on local networks have them as well. On the Internet, these host names appear to the left of the domain name. Host names can be up to 63 characters long.

## Binary and Dotted Decimal Notation

TCP/IP uses binary numbering. Binary is a base 2 numbering system in which any bit in the number is either a zero or one. An IP address might appear in binary as 11001011.01111011.00101101.00010010.

Although the underlying IPv4 addresses are binary numbers, for readability, TCP/IP addresses are usually displayed in dotted decimal notation. Dotted decimal notation consists of four decimal numbers separated by three dots. Each decimal number is called an octet because it represents eight binary bits. When pronouncing a dotted decimal number, include the separator dots. For example, the IPv4 address 192.168.1.18 is pronounced one ninety-two dot one sixty-eight dot one dot eighteen.

## Subnet Masks

A *subnet mask* is a 32-bit number that is assigned to each system to divide the 32-bit binary IP address into network and node portions. This makes TCP/IP routable. A subnet mask uses a binary operation to remove the node ID from the IP address, leaving just the network portion. Subnet masks use the value of eight 1s in binary, or 255 in decimal, to mask an entire octet of the IP address.

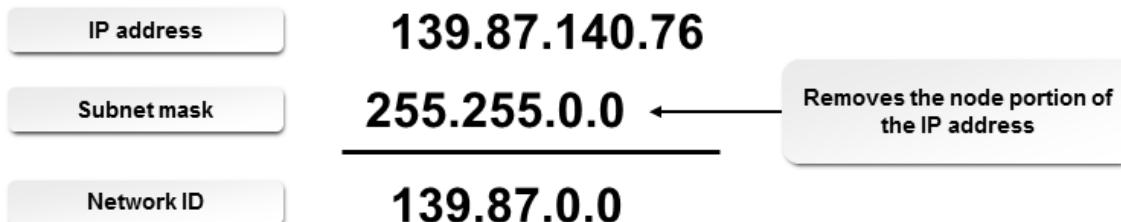


Figure 13–12: The subnet mask.

## Gateways and the Default Gateway

A *gateway* is a device, software, or a system that has the ability to convert data between incompatible systems or devices. Gateways can translate data between different operating systems, or email formats, or between totally different networks. A gateway can be implemented as hardware, software, or both. You can also install gateways as software within a router, allowing the router to act as a gateway when required, and eliminating the need for separate hardware.

When TCP/IP communications need to be routed to systems on other networks, the protocol directs the packets to a special address known as the *default gateway*. The default gateway is different from a typical gateway in that the address is typically that of a network router that connects the local network to other external networks. A default gateway address is not a required component of a TCP/IP address assignment, but without a default gateway, the computer will only be able to communicate on the local network segment.

## IP Address Classes and Classless Addressing

The designers of the TCP/IP suite defined five ranges of addresses, called address classes, for specific network uses and sizes. Changes in the Internet since the early 90s have rendered classful addresses all but obsolete. One of the final remnants of classful addressing is the use of the terms "Class A," "Class B," and "Class C" to describe common subnet masks.

Class and Subnet Mask	Description
Class A 255.0.0.0	<p>Class A subnet masks provide a small number of network addresses for networks with a large number of nodes per network:</p> <ul style="list-style-type: none"> <li>Number of nodes per network: 16,777,214</li> <li>Network ID portion: First octet</li> <li>Node ID portion: Last three octets</li> </ul> <p>Used only by extremely large networks, Class A addresses are far too big for most companies. Large telephone companies and ISPs leased most Class A network addresses early in the development of the Internet.</p>

<b>Class and Subnet Mask</b>	<b>Description</b>
Class B 255.255.0.0	<p>Class B subnet masks offer a larger number of network addresses, each with fewer nodes per network:</p> <ul style="list-style-type: none"> <li>Number of nodes per network: 65,534</li> <li>Network ID portion: First two octets</li> <li>Node ID portion: Last two octets</li> </ul> <p>Most companies leased Class B addresses for use on Internet-connected networks. In the beginning, there were plenty of Class B addresses to go around, but soon they were depleted.</p>
Class C 255.255.255.0	<p>Class C subnet masks offer a large number of network addresses for networks with a small number of nodes per network:</p> <ul style="list-style-type: none"> <li>Number of nodes per network: 254</li> <li>Network ID portion: First three octets</li> <li>Node ID portion: Last octet</li> </ul> <p>Because there can be more Class C networks than any other type, they are the only addresses still generally available.</p>

## Classless Addressing and CIDR

Because the traditional IP address classes have limitations on the number of available addresses in each class, there are now various implementations that utilize classless addressing. In these schemes, there is no strict dividing line between groups of addresses, and the network address/node address division is determined entirely by the number of 1 bits in the subnet mask.

*Classless inter-domain routing (CIDR)* is a classless addressing method that considers a custom subnet mask as a 32-bit binary word. Mask bits can move in one-bit increments to provide the exact number of nodes and networks required. The CIDR notation combines a network address with a number to represent the number of 1 bits in the mask. With CIDR, multiple class-based networks can be represented as a single block.

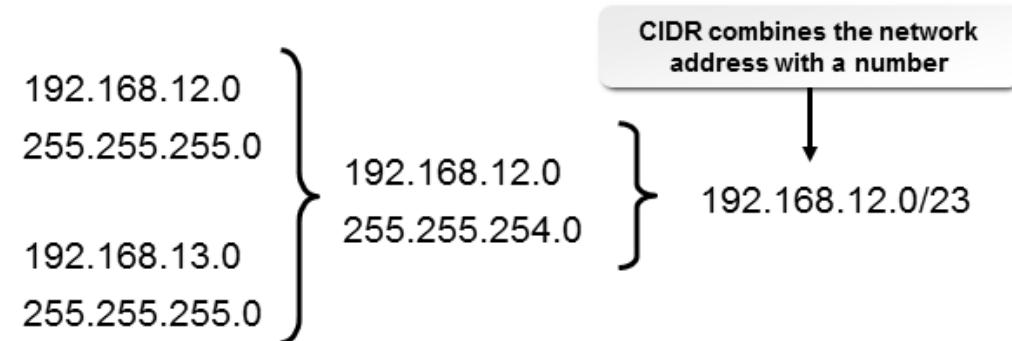


Figure 13-13: CIDR.



**Note:** CIDR can also be referred to as classless routing or supernetting. Because of its efficiencies, CIDR has been rapidly adopted, and the Internet today is largely a classless address space.

## CIDR Subnet Mask Values

There are different values possible for each CIDR subnet mask. The /24, /16, and /8 CIDR masks correspond with the classful ranges of Class C, Class B, and Class A, respectively.

## IPv6 Addresses

*IP version 6*, or *IPv6*, is an Internet standard that increases the available pool of IP addresses by implementing a 128-bit binary address space. IPv6 also includes new efficiency features, such as simplified address headers, hierarchical addressing, support for time-sensitive network traffic, and a new structure for unicast addressing. One of the goals of IPv6 is to keep the IP headers as small as possible to make access to the address more efficient and quicker. Non-essential information in IPv6 headers is moved to optional extension headers. In IPv6, address blocks are automatically assigned hierarchically by routers. Top-level routers have top-level address blocks, which are automatically divided and assigned as routers and segments are added. This divides the address space logically instead of randomly, making it easier to manage.

IPv6 is not compatible with IPv4, so now, it is narrowly deployed on a limited number of test and production networks. Full adoption of the IPv6 standard will require a general conversion of IP routers to support interoperability. IPv6 makes use of an Institute of Electrical and Electronics Engineers (IEEE) standard called Extended Unique Identifier (EUI). A host computer implemented with EUI-64 can assign itself a 64-bit IPv6 interface identifier automatically.



**Note:** For more information on IPv6, see the IETF's IP Version 6 Working Group charter at [www.ietf.org/html.charters/ipv6-charter.html](http://www.ietf.org/html.charters/ipv6-charter.html).

### IPv6 Address Format

An *IPv6 address* has 128 bits or 16 bytes and is denoted as eight hexadecimal blocks separated by colons. The byte on the left has the highest order, and the byte on the right has the lowest order.

**2001:0DB8:AC10:FE01:0056:0000:0000:0000**

Hexadecimal format

**0010 0000 0000 0001:0000 1101 1011 1000:1010 1100 0001 0000:1111 1110 0000 0001:  
0000 0000 0101 0110:0000 0000 0000:0000 0000 0000 0000:0000 0000 0000 0000**

128-bit binary format

**Figure 13-14: An IPv6 address.**

To make the representation easier, some abbreviation techniques are used. For example, one abbreviation technique used replaces all zero hexadecimal values with a single zero and removes the leading zeros of all nonzero values.

For example, in the IPv6 address **2001:DB8:0000:0056:ABCD:EF12:1234**, the third, fourth, and fifth bytes contain consecutive zeros and, therefore, they can also be represented as **2001:DB8:0:56:0:ABCD:EF12:1234** without the unnecessary zeros.

Another technique used replaces all consecutive zero values or consecutive leading zeros with a double colon. However, the double colon can be used only once in an address. This is because when a computer comes across a simplified address, it replaces the double colon symbol with as many zeros as required to make it 128 bits long. If an address contains more than one double colon, the computer cannot determine the number of zeros for each place.

For example, the IPv6 address **2001:DB8:0000:0056:0000:ABCD:EF12:1234** can also be represented as **2001:DB8::56:0:ABCD:EF12:1234** or **2001:DB8:0:56::ABCD:EF12:1234** after replacing any one of the consecutive zeros with a double colon.

## Comparison of IPv4 and IPv6

IPv4 addresses use 32 bits as opposed to the 128 bits used in IPv6 addressing. While implementing IPv4 addresses, IPSec is optional. However, the IPSec security feature is not optional in IPv6 addresses. The header information structure is different between IPv4 and IPv6 addresses. IPv6 is not compatible with IPv4, so now, it is narrowly deployed on a limited number of test and production networks. Full adoption of the IPv6 standard will require a general conversion of IP routers to support interoperability.



**Note:** IPSec will be covered in greater detail later in the course.

## Addressing Schemes

When assigning addresses to hosts on your network, you must assign an address in the appropriate scheme based on the type of network and access is given to that host.

<i>Scheme</i>	<i>Description</i>
Private	<i>Private IP addresses</i> are addresses that organizations use for nodes requiring IP connectivity within enterprise networks, but not requiring external connections to the global Internet. IP addresses in each of the Classes A, B, and C are reserved as private IPv4 addresses. Because they are not routable, private IP addresses do not cause duplicate IP address conflicts on the Internet.  In IPv6, these are referred to as site-local addresses.
Public	<i>Public IP addresses</i> are addresses that get shared on the Internet. To ensure the uniqueness of each public address, they are distributed in blocks by ICANN.
APIPA/Link Local	<i>Automatic Private IP Addressing (APIPA)</i> is a feature of Windows that enables a DHCP client computer to configure itself automatically with a random IPv4 address in the range of 169.254.0.1 to 169.254.255.254 if there is no DHCP server available. A computer with an APIPA-range address is usually nothing more than a symptom, to the technician, of a DHCP problem that requires resolution.  In IPv6, link local addresses are required, and always begin with FE80.
Loopback address block	The block of addresses in the IPv4 127.0.0.0/8 or IPv6 ::1 range are reserved for loopback. Information sent out from the device is routed back to the source without any processing or change. This is designed mainly to use for testing purposes.

## Static and Dynamic Addressing

On a TCP/IP network, you can assign IP address information statically to nodes by manually entering IP addressing information on each individual network node. Or, *dynamic addressing* can be used to assign IP addresses using the Dynamic Host Configuration Protocol (DHCP) service.

*Static addressing* involves configuring TCP/IP statically on a network and requires that an administrator visit each node to manually enter IP address information for that node. If the node moves to a different subnet, the administrator must manually reconfigure the node's TCP/IP information for its new network location. In a large network, configuring TCP/IP statically on each node can be very time consuming and prone to errors that can potentially disrupt communication on the network. Static addresses are typically only assigned to systems with a dedicated functionality, such as router interfaces, network-attached printers, or servers that host applications on a network.

## DHCP

*Dynamic Host Configuration Protocol (DHCP)* is a network service that provides automatic assignment of IP addresses and other TCP/IP configuration information on network systems that are configured as DHCP clients. DHCP requires a DHCP server computer configured with at least one active DHCP scope. The scope contains a range of IP addresses and a subnet mask, and can contain other options, such as a default gateway address or *Domain Name Server (DNS)* server address. When the service is enabled, it automatically leases TCP/IP configuration information to DHCP clients for a defined lease period.

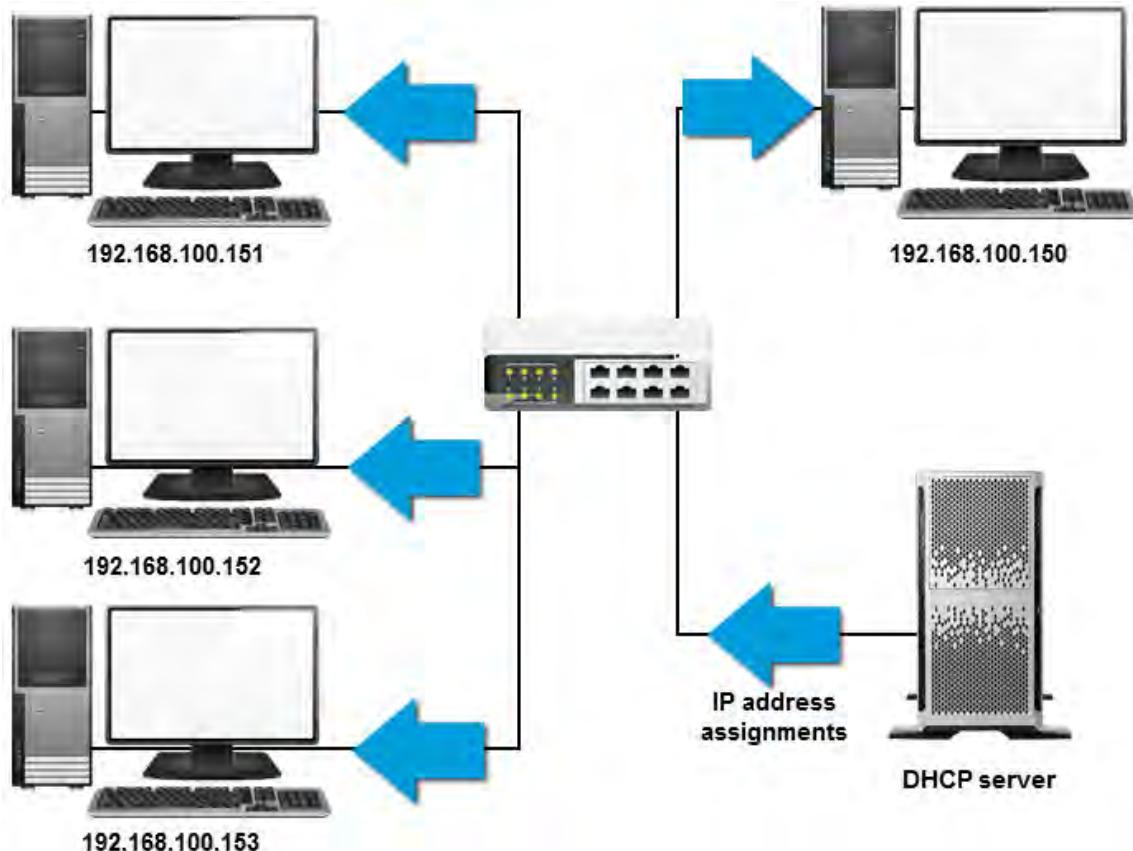
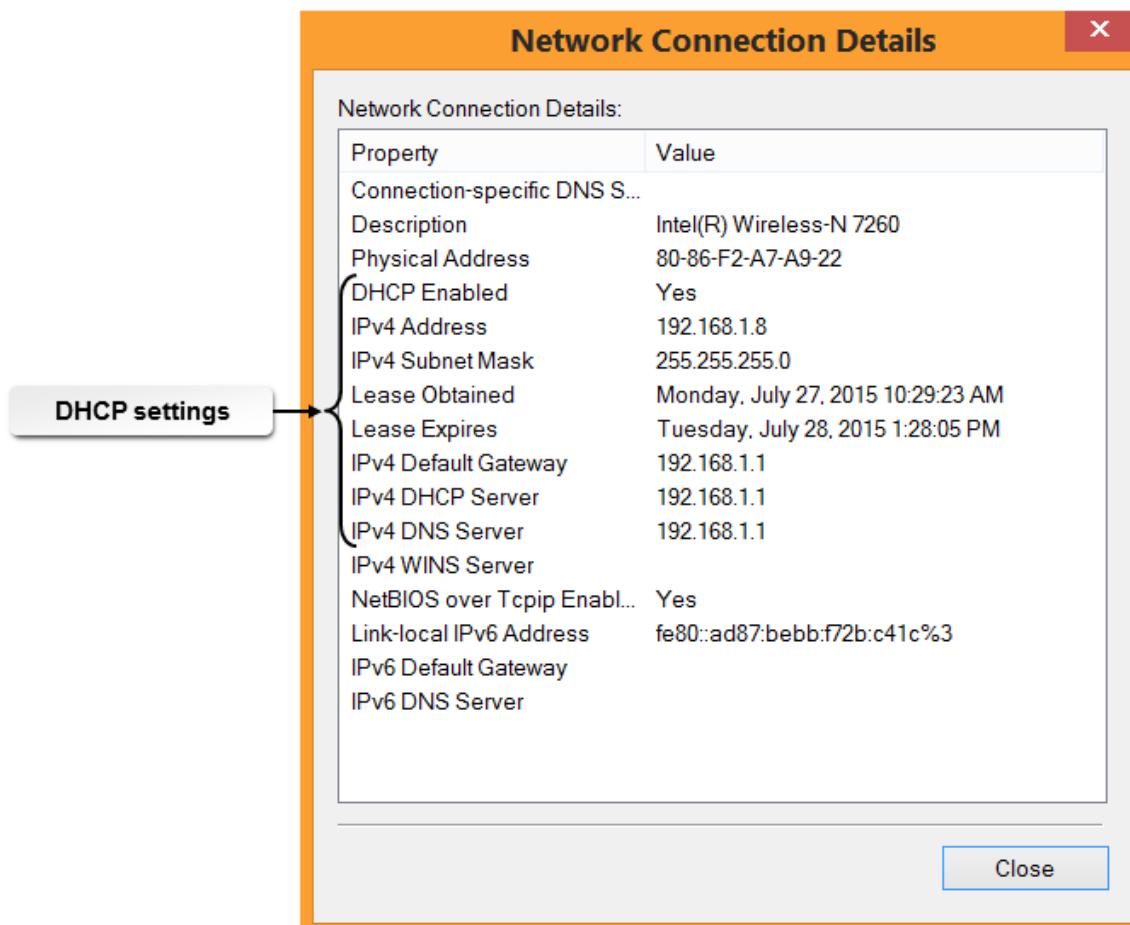


Figure 13-15: DHCP.

## Client-Side DHCP Settings

If you need to use a static IP address, you will need to specify the address, the subnet mask, the default gateway, and at least one DNS server. If you decide to get the IP address automatically from a DHCP server, those values will be provided for you when you lease the IP address.



**Figure 13-16:** The IPv4 DHCP network connection details.

## DNS

Computers on TCP/IP networks are assigned both a host name and an IP address. Users generally access systems by their descriptive names, and the network needs to translate, or resolve, those names into the relevant systems' IP addresses. The *Domain Name System (DNS)* is the primary name resolution service on the Internet as well as private IP networks.

DNS is a hierarchical system of databases that map computer names to their associated IP addresses. DNS servers store, maintain, and update the databases and respond to DNS client name resolution requests to translate host names to IP addresses. The DNS servers on the Internet work together to provide global name resolution for all Internet hosts. For example, the IP address 209.85.165.99 might map to [www.google.com](http://www.google.com).

## Client-Side DNS

Client-side DNS can be implemented by running a DNS service on a client computer. The client can quickly use the client resolver cache to lookup host names for resolution. This enables the client to perform basic DNS lookups without having to connect to a DNS server. In cases where the lookup is out of scope for the client resolver, the DNS servers that store, maintain, and update databases will respond to any resolution requests that may be out of scope for client-side DNS services to handle. In this case, the client-side DNS service will communicate directly with multiple DNS servers to resolve name requests made from the client machine.

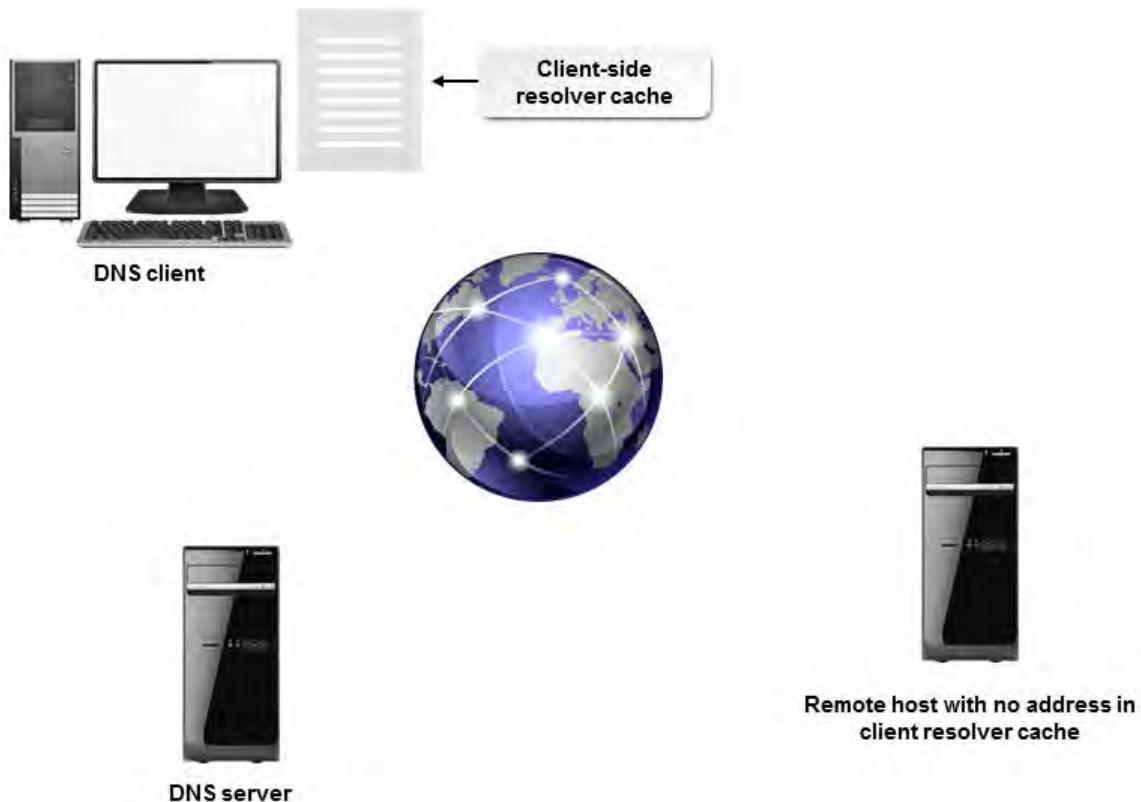


Figure 13-17: Client-side DNS.

# ACTIVITY 13-2

## Examining TCP/IP Information

### Scenario

In this activity, you will examine the configuration settings on your host computer that enables it to connect to the network.

1. Determine the protocol in use on your Windows 8.1 host computer.
  - a) Open **Control Panel**. In the **Search Control Panel** text box, type **network connections**.
  - b) Under **Network and Sharing Center**, select **View network connections**.
  - c) Examine the contents of the **Network Connections** window.  
One of the connections that is displayed in this window is the connection to the class network.
  - d) Display the pop-up menu for the network connection, and select **Properties**.
  - e) In the **This connection uses the following items** list, verify that **Internet Protocol Version 4 (TCP/IPv4)** is listed.
  - f) Close the **Properties** dialog box without making any changes.
2. View the TCP/IP information assigned to your network adapter.
  - a) Display the pop-up menu for the network connection, and select **Status**.
  - b) Select **Details**.
  - c) In the **Network Connection Details** dialog box, examine the information for the IPv4 address, subnet mask, and default gateway.
3. In the **Network Connection Details** dialog box, examine the information for DHCP.
4. If DHCP is enabled on your computer, when does the lease expire?
5. In the **Network Connection Details** dialog box, examine the information for DNS.
6. How many DNS servers are listed?
7. Return to the network connection properties, and examine the **Internet Protocol Version 4 (TCP/IPv4)** properties.
  - a) Select **Close**.
  - b) Select **Properties** to return to the network connection properties.
  - c) In the **This connection uses the following items** list, select **Internet Protocol Version 4 (TCP/IPv4)**, and then select **Properties**.
  - d) Select **Advanced**.
  - e) Select the **DNS** tab.
  - f) Select **Cancel** three times, and then select **Close**.
  - g) Close the **Network Connections** window.

# TOPIC C

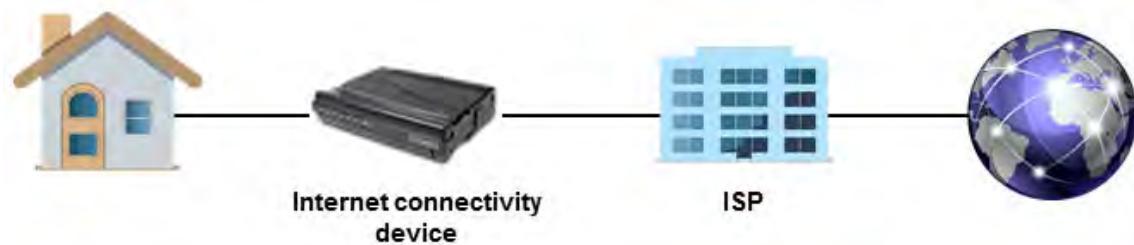
## Internet Connections

In the previous topics, you identified network communication technologies and the components of TCP/IP. To complete your understanding of network concepts, you will need to examine the technologies that connect multiple nodes and networks together. In this topic, you will identify network connectivity technologies.

Putting together a network is like putting together a huge puzzle. There are physical pieces, such as network adapters and network clients, and conceptual pieces, such as protocols and addresses. However, to understand how the pieces all fit together you need to be able to see the overall picture. Examining the large structures and techniques that provide network connectivity between and within network locations will help you see the big picture of network implementation and support.

### ISPs

An *Internet Service Provider (ISP)* is a company that provides Internet access to individuals and to businesses. Most ISPs charge a fee for this connection. Customers receive logon information, access to servers that provide name resolution and email services, dynamic or static IP configurations, and a method for connecting to the ISP. Once connected to the ISP, the customer can access the Internet.



**Figure 13–18: An ISP.**

## Internet Connection Types and Features

Internet connections can be accomplished in a wide variety of ways today. Each method has unique connection technology that is used to connect computing devices to the Internet.

Method	Description
Cable	<p><i>Cable</i> or <i>cable modem</i> transmissions use a cable television connection and a specialized interface device known as a cable modem to provide high-speed Internet access to homes and small businesses. Cable access arranges users in groups around nodes that split the television and data signals at the cable provider's end.</p> <p>The speed of the network varies depending on how populated the group on each node is. Download speeds can vary by more than 1 Mbps in different areas. Most cable companies try to guarantee at least a 768-Kbps download speed; however, speeds of 3.0 to 7.0 Mbps are common, and speeds of 20 Mbps or more are possible.</p>

<b>Method</b>	<b>Description</b>
DSL	<i>Digital Subscriber Line (DSL)</i> transmits digital signals over existing phone lines. It has become a popular way to connect small businesses and households to the Internet because it is affordable and provides a relatively high download speed—a typical maximum is 1.5 Mbps for basic DSL and 7 Mbps for high-end DSL. However, distance from the phone company's switching station and the quality of the lines affect the total bandwidth available to a customer.
Dial-up	<i>Dial-up lines</i> are local loop <i>Public Switched Telephone Network (PSTN)</i> connections that use modems, existing phone lines, and existing long-distance carrier services to provide low cost, low bandwidth WAN connectivity, and remote network access. Dial-up lines are generally limited to 56 Kbps and are sometimes used as backups for higher bandwidth WAN services.
Fiber	<i>Fiber</i> is a method used to connect devices to the Internet using fiber optic cable. Fiber is mostly used in smaller areas to connect computing devices to a router. It provides a fast data exchange rate over distances of several kilometers.
Satellite	Geostationary <i>satellites</i> orbit 22,236 miles above the Earth's equator, or zero latitude. They orbit in the same direction the Earth rotates (west to east) at the same speed of the rotation.. One orbit takes 24 hours, the same length of time the Earth rotates once on its axis, so the satellite appears stationary. This positioning eliminates the need for satellite antennas, or dishes, to track satellites, which simplifies data exchange and reduces costs. Set up the satellite dish once, and barring extreme weather conditions, the dish maintains constant contact with the satellite. Satellites are used for a variety of purposes, such as television broadcasts, radio communication, mapping, weather forecasting, telecommunication, Internet access in rural and remote regions not serviced by cable broadband or DSL and wide area network connections.  Older satellite Internet providers required people to have a telephone line to use the Internet. Data downloads were sent through the satellite to a receiver dish, However, requests for data such as web page, were transmitted over telephone wires. Most providers now provide the ability to send and receive data using a satellite Internet dish. Unlike a TV dish that only receives data, an Internet dish contains a transmitter so it also can send data. A satellite Internet connection requires a satellite receiver/transmitter dish, a satellite modem and coaxial cable that connects the modem to the dish. Satellite Internet access speeds depend on the service package purchased
ISDN	<i>Integrated Services Digital Network (ISDN)</i> is a digital transmission technology that carries both voice and data over digital phone lines or PSTN wires. Connections are made on demand by dialing another ISDN circuit's telephone number.  ISDN and DSL are very similar technologies because they both use existing phone lines to transmit digital signals. However, ISDN technology predates DSL and has largely been superseded by DSL for the home and small business market. ISDN requires a specialized client adapter called a Terminal Adapter, which DSL does not. ISDN is also slower than DSL, being limited to a data rate of approximately 128 Kbps for basic rate ISDN, and thus barely qualifies as high-speed. (Primary rate ISDN, which was commonly used for network backbone communications before fiber optic cable, provides more bandwidth and has higher speeds.)

<b>Method</b>	<b>Description</b>
Cellular	<p><i>Cellular</i> technology uses radio signals to transmit network data over the cellular telephone system. Cellular-enabled computers have a cellular radio built in. Coverage can be regional, national, or global, depending on the service chosen and the capabilities of the cellular service provider. Signal fidelity will vary depending on interference and the distance from a cell tower.</p> <p>Some of the cellular transmission technologies and standards in use include Code-Division Multiple Access (CDMA) and the Global System for Mobile Communications (GSM). CDMA is a spread-spectrum implementation that uses the full frequency spectrum for each channel rather than assigning specific frequencies to particular users. It separates the calls using digital encoding. GSM uses time-division multiplexing (TDM), which transmits multiple calls on the same frequency by dividing each call into separate time slices.</p> <p>Use a cellular <i>Wireless WAN (WWAN)</i> when you have users that have no other way to connect to the Internet, your company's VPN, or both. Cellular WWANs are typically more expensive than Ethernet WANs. You can also turn mobile devices into cellular hotspots, or tether them to other devices, in order to propagate network access.</p>
LOS	<p>Line of sight is a wireless connection method in which endpoints can transmit signals to one another as long as they are unobstructed by physical objects. A wireless antenna at one endpoint is directly pointed at a wireless endpoint farther away, without trees, buildings, or other tall structures interfering with the signal. The antennas themselves are typically affixed to the top of tall buildings in order to reduce this interference. A line of sight service can cover great distances that typical wireless signals cannot, while at the same time saving the service provider from having to install cabling infrastructure. Additionally, the connection in an LOS service is often low latency.</p> <p>A disadvantage of LOS is that the actual unobstructed sight line can be difficult to maintain, especially if the area between the two endpoints is not owned by the client or the provider. Likewise, LOS services are usually more expensive than other methods.</p>

## ACTIVITY 13-3

### Discussing Internet Connections

#### Scenario

You are moving to a new neighborhood which is closer to your new job. You need to be able to connect to the Internet from your new home. The real estate agent who is helping you locate your new home has provided you with information on the available providers and the types of Internet connections they offer. You want to make sure to select one within your budget that is fast enough to watch streaming movies and manage your email, among other online activities.

1. Which communication method uses existing telephone lines to transmit digital signals?
  - Cable modem
  - DSL
  - ISDN
  - Fiber
  - Satellite
2. Which communication method uses the same physical media to provide high-speed transmission of data and television signals?
  - Cable modem
  - DSL
  - ISDN
  - Fiber
  - Satellite
3. Which communication method uses light to carry signals?
  - Cable modem
  - DSL
  - ISDN
  - Fiber
  - Satellite
4. If you have remote employees that need to connect to the corporate network but they are located in a remote area with no access to high-speed Internet service, what do you think is the best Internet connection method to use in this situation?

# TOPIC D

## Ports and Protocols

In the previous topics, you explored different network connections, including high-speed Internet connections. Now you are ready to examine the various ports and protocols that are used to ensure data transmission is successful and secure. In this topic, you will examine common TCP and UDP ports and protocols.

Properly configuring the ports of a network device and selecting the right protocol will ensure that data gets transmitted over the network. As an A+ technician, you must understand how ports and protocols are implemented within a network and how they function to provide the right level of data transmission while keeping data secure.

### TCP and UDP

The TCP/IP protocol suite includes two protocols: *Transmission Control Protocol (TCP)* and *User Datagram Protocol (UDP)*. TCP is a connection-oriented, guaranteed-delivery protocol used to send data packets between computers over a network such as the Internet. It is part of the Internet protocol suite along with the *Internet Protocol (IP)*. TCP is responsible for breaking up data into datagrams, reassembling them at the other end, resending data lost in transit, and resequencing data. It sends data, waits for an acknowledgement, and fixes erroneous data. IP is responsible for routing individual datagrams and addressing.

The User Datagram Protocol (UDP), also known as the Universal Datagram Protocol, is a connectionless protocol in the Internet protocol suite. A connectionless, best-effort delivery protocol, UDP is used with IP like TCP. It transmits data and ensures data integrity as TCP does. UDP, however, lacks reliability, flow-control, and error-recovery functions. It is less complex than TCP, and since it is a connectionless protocol, it provides faster service.

### Network Ports

In TCP/IP networks, a *port* is the endpoint of a logical connection. Client computers connect to specific server programs through a designated port. All ports are assigned a number in a range from 0 to 65,535. An international agency, the *Internet Assigned Numbers Authority (IANA)*, separates port numbers into three blocks:

- Well-known ports, which are preassigned to system processes by the IANA.
- Registered ports, which are available to user processes and are listed as a convenience by the IANA.
- Dynamic ports, which are assigned by a client operating system as needed when there is a request for service.

### Port Ranges

There are three recognized blocks of port numbers.

<b>Block</b>	<b>Range</b>	<b>Description</b>
Well-known ports	Port range: 0 to 1,023.	Well-known ports are pre-assigned for use by common, or well-known, services. Often the services that run on these ports must be started by a privileged user. Services in this range include HTTP on TCP port 80, IMAP on TCP port 143, and DNS on UDP port 53.

<b>Block</b>	<b>Range</b>	<b>Description</b>
Registered ports	Port range: 1,024 to 49,151.	These ports are registered by software makers for use by specific applications and services that are not as well known as the services in the well-known range. Services in the registered port range include SOCKS proxy on TCP port 1080, QuickTime® Streaming Server administration on TCP port 1220, and Xbox® Live on TCP and UDP port 3074.
Dynamic or private ports	Port range: 49,152 to 65,535.	These ports are set aside for use by unregistered services and by services needing a temporary connection.

## Common Ports

This table lists some of the most common well-known TCP and UDP port numbers. Additional well-known ports and other port number assignments are available online at [www.iana.org/assignments/port-numbers](http://www.iana.org/assignments/port-numbers).

<b>Port</b>	<b>Type</b>	<b>Service Name</b>	<b>Purpose</b>
21	TCP	FTP	File transfers
22	TCP/UDP	SSH	Secure shell for secure data transmission
23	TCP/UDP	TELNET	Telnet services
25	TCP	SMTP	Simple mail transfers
53	TCP/UDP	DNS	Domain name system
80	TCP	HTTP	Hypertext transfer protocol
110	TCP	POP3	Post office protocol
137	UDP	SMB NetBIOS	Server Message Block (SMB) Network Basic Input/Output System (NetBIOS) naming service
138	UDP	SMB NetBIOS	Server Message Block (SMB) NetBIOS datagram distribution service
139	TCP	SMB NetBIOS	Server Message Block (SMB) NetBIOS session service
143	TCP/UDP	IMAP	Internet message access protocol
427	TCP/UDP	SLP	Service Location Protocol used by svrloc service in network browser.
443	TCP	HTTPS	HTTP secure combines HTTP with SSL/TLS protocols.
445	TCP TCP/UDP	SMB CIFS	Server Message Block (SMB) Common Internet File System (CIFS)
548	TCP	AFP	Apple Filing Protocol over TCP used by AppleShare, Personal File Sharing, Apple File Service

<b>Port</b>	<b>Type</b>	<b>Service Name</b>	<b>Purpose</b>
3389	TCP/UDP	RDP	Remote desktop protocol

## LDAP

*Lightweight Directory Access Protocol (LDAP)* is a directory service protocol that defines how a client can access information, perform operations, and share directory data on a directory server. It was designed for use specifically over TCP/IP networks and on the Internet in particular. In most implementations, LDAP relies on the DNS service. First, DNS enables clients to find the servers that host the LDAP directory, and then the LDAP servers enable clients to find directory objects. Most common network directories are LDAP-compliant.



**Note:** LDAP uses port 389.

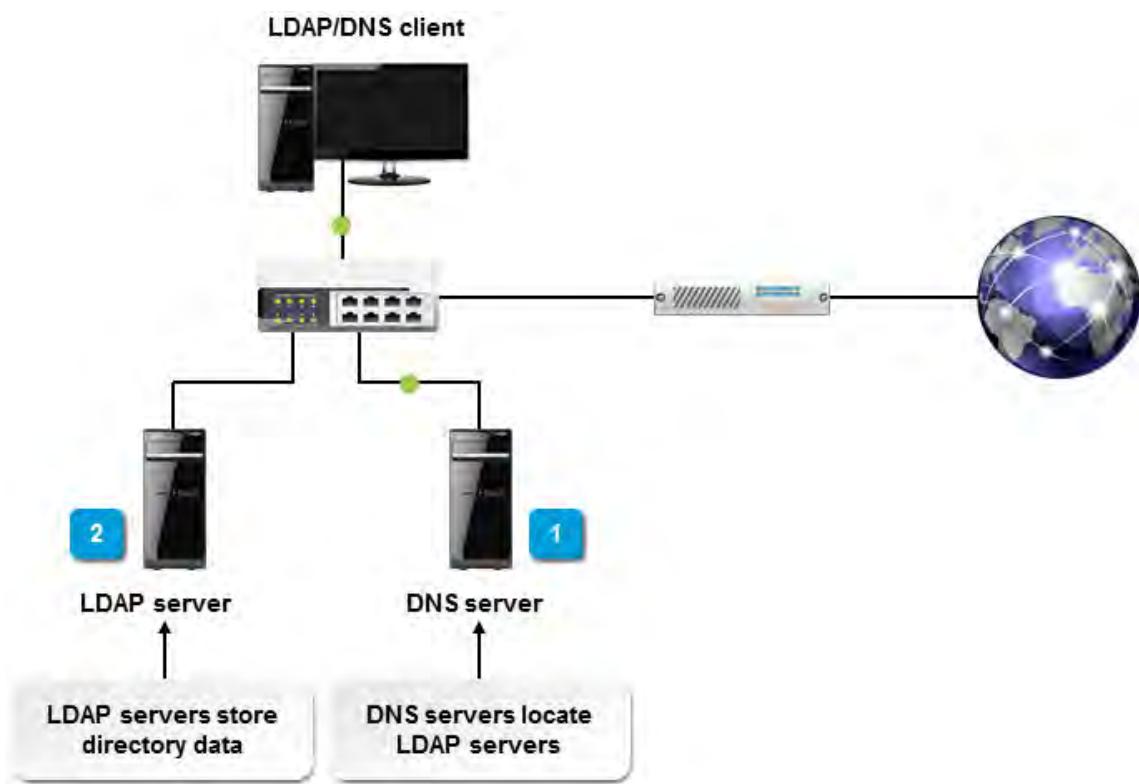


Figure 13-19: LDAP.

## SNMP

*Simple Network Management Protocol (SNMP)* is a protocol used to collect information from network devices for diagnostic and maintenance purposes. SNMP includes two components, management systems and agent software, which are installed on network devices such as servers, routers, and printers. The agents send information to an SNMP manager. The SNMP manager can then notify an administrator of problems, run a corrective program or script, store the information for later review, or query the agent about a specific network device.



**Note:** SNMP uses ports 161 and 162.

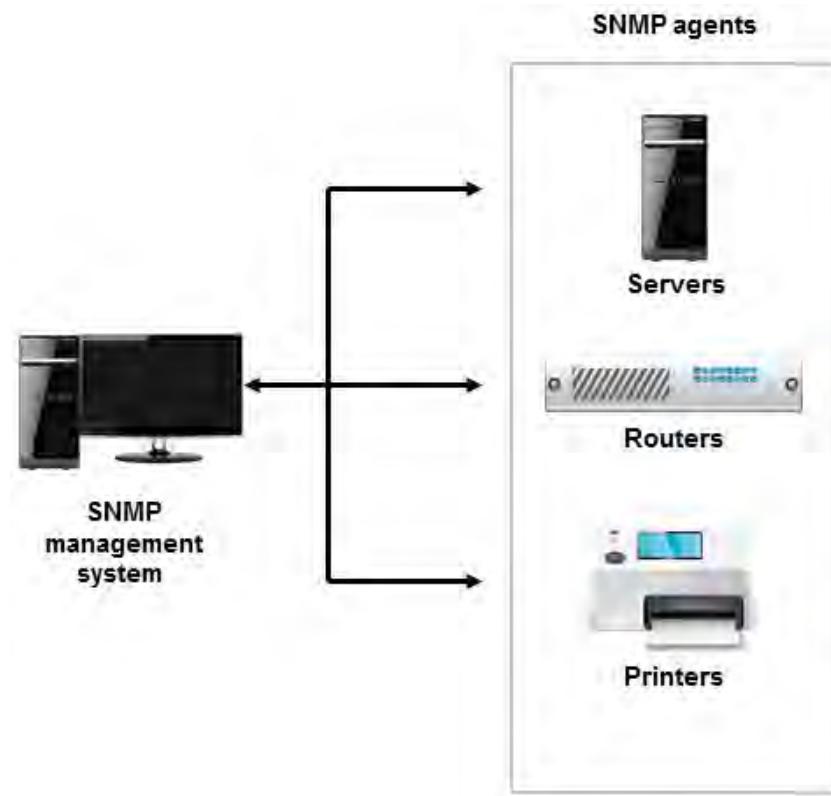


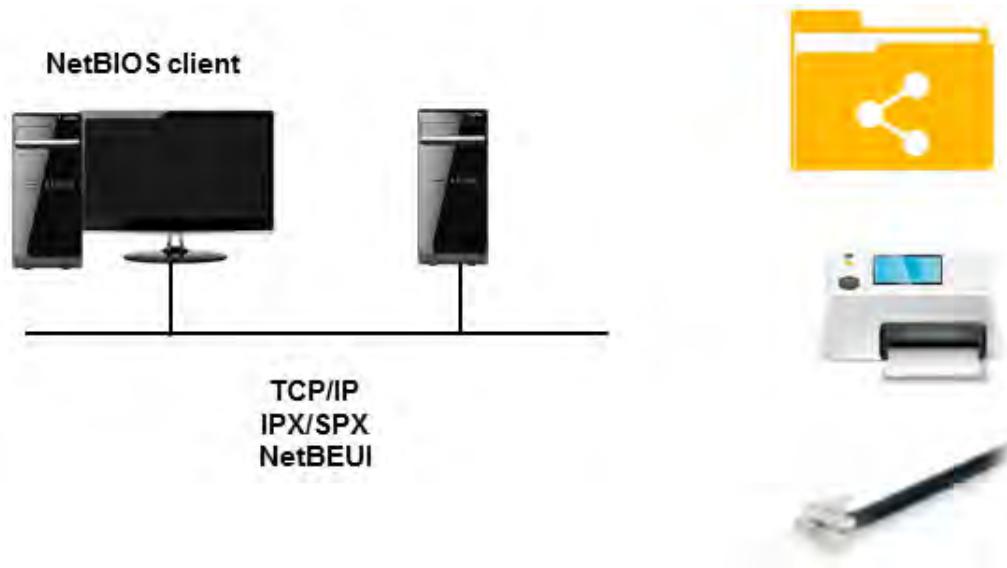
Figure 13-20: SNMP collects information from network devices for diagnostic purposes.

## SMB

The *Server Message Block (SMB)* is a protocol that helps share resources such as files, printers, and serial ports among computers. In a TCP/IP network, NetBIOS clients, such as Windows systems, use NetBIOS over TCP/IP to connect to servers, and then issue SMB commands to complete tasks such as accessing shared files and printers.



**Note:** SMB uses port 445.



**Figure 13–21:** Resource sharing using SMB.

## CIFS

The *Common Internet File System (CIFS)* protocol enables users on various computing platforms to share files without the need to install additional software to do so. CIFS replaces the SMB protocol to provide Windows users with file and printer access. Using CIFS enables users to open and share files over the Internet in native applications rather than just in web browsers. If a user changes a file opened through CIFS, the changes are saved to both the server and client side simultaneously.



**Note:** CIFS uses port 445 or 3020.

Microsoft revised CIFS and named the revision SMB 2.0 or SMB2. SMB2 was introduced with Windows Vista and has been further revised and enhanced since then.

## SSH

*Secure Shell (SSH)* is a UNIX/Linux-based protocol that enables a user or application to log on to another computer over a network, execute commands, and manage files. It provides strong authentication methods and secure communications over insecure channels. It is a more secure version of remote connection programs that transmit passwords unencrypted, such as Telnet. With the SSH `slogin` command, the entire login session, including the password, is encrypted and protected against attack.



**Note:** SSH uses port 22.



Figure 13-22: SSH.

## AFP

The Apple File Protocol (AFP) has been around since the 1980s when it was introduced as part of the original AppleTalk network system. For Macs communicating with other Macs, this is still often used.

Starting with OS X Mavericks, Apple began the migration from AFP to SMB2 to make cross-platform file sharing easier, faster, and more secure. Macs running OS X 10.9 Mavericks automatically default to SMB2 when talking to each other. (AFP is used as a fallback when sharing files with older Macs.)

When communicating with other systems such as Windows systems, Mac users will use SMB2.



**Note:** AFP uses port 548.

# ACTIVITY 13–4

## Identifying Network Ports and Protocols

### Scenario

You want to learn more about the ports and protocols you recently learned about. You also want to see which ports and protocols are in use on your computer when you perform different tasks.

1. Examine which ports are in use by which applications.
  - a) Open an administrative command prompt.
  - b) At the command prompt, enter **netstat -o**
  - c) Observe the list of processes that are running. The number after the colon is the port number for the running process.
  - d) Open a web browser and then resize the browser so it is next to the command prompt window.
  - e) At the command prompt, enter **netstat -o** again.
  - f) In the web browser, open **google.com**.
  - g) At the command prompt, enter **netstat -o** and then record one of the PID numbers for a process.
  - h) Press **q** to stop the list.
  - i) Enter **tasklist /fi "pid eq ####" /fo list /v** where ##### is the PID number you recorded.
  - j) Observe the ports that are in use.
2. Select one of the ports from this topic, and using your preferred search site, find out more information about where, when, and why the protocol is used.  
Share your results with the class.
  - a) Using the **google.com** search page you opened in the browser, locate and briefly review the RFC for the port.
  - b) Determine which apps use the port.
  - c) Review any security concerns regarding the port.

# TOPIC E

## Networking Tools

Now that you have covered network connection methods, ports, and protocols, you are ready to take a closer look at tools used to properly install, configure, and maintain all parts of a network.

Working with networks can be challenging depending on the size, location, and environment. In order to properly and safely work with networking components, you must understand how networking tools are used and how they can be used to fix common issues found in networks.

### Cable Testers

A *cable tester*, also called a *media tester*, is an electrical instrument that verifies if a signal is present on a network cable. A simple cable tester will determine whether a cable has an end-to-end connection and can detect shorts or opens, but it cannot certify the cable for transmission quality.



Figure 13-23: A cable tester.

### Cable Strippers

A *cable stripper*, also called a *wire stripper*, is often part of a wire crimper, allowing the user to strip wires of their protective coating, and then use the crimping tool to attach a media connector.



Figure 13-24: A cable stripper.

## Crimpers

A *wire crimper* is a tool that attaches media connectors to the ends of cables. You can use it if you need to make your own network cables or trim the end of a cable. There are different crimpers for different types of connectors, so select the one that is appropriate for the type of network media you are working with. A *wire stripper* is often part of a wire crimper, allowing the user to strip wires of their protective coating, and then use the crimping tool to attach a media connector.



Figure 13-25: A wire crimper.

## Multimeters

A *multimeter* is an electronic instrument used to measure voltage, current, and resistance. It usually has two probes with leads, one red and one black, that are plugged into two sockets on the meter. To switch between measuring volts, ohms, and amps, the leads can be moved to different sockets, or there may be a selector switch. Digital meters have a screen that displays the numeric value of what you are measuring. Analog meters have a thin needle that swings in an arc and indicates the value of what you are measuring. Many meters also have specific settings for testing circuit continuity, diodes, or battery charges. Multimeters are sometimes called volt-ohm meters.



**Note:** Use a digital multimeter whenever possible. It is much more difficult to read and interpret an analog multimeter accurately.

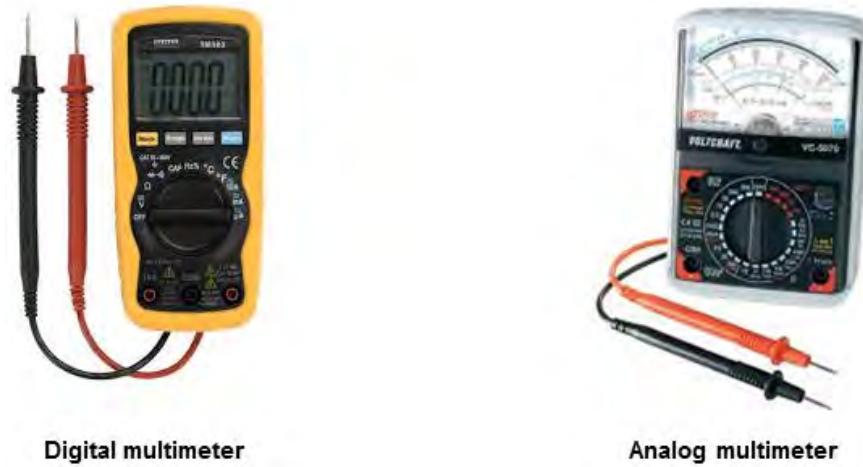


Figure 13-26: Multimeters.

## Tone Generators and Probes

A *tone generator* is a device that sends an electrical signal through one pair of UTP wires. A *tone locator* or a *tone probe* is a device that emits an audible tone when it detects a signal in a pair of wires. Tone generators and tone locators are most commonly used on telephone systems to trace wire pairs. A digital toner and toner probe trace and locate voice, audio, and video cabling on a network. In addition to confirming the cable location, a toner and probe can verify continuity and detect faults.



Figure 13-27: A tone generator and a tone locator.



**Note:** The combination of a tone generator and tone locator is frequently referred to as “fox and hound.”

Do not confuse tone generators and tone locators with cable testers. Tone generators and tone locators can only help you differentiate between different UTP cables.

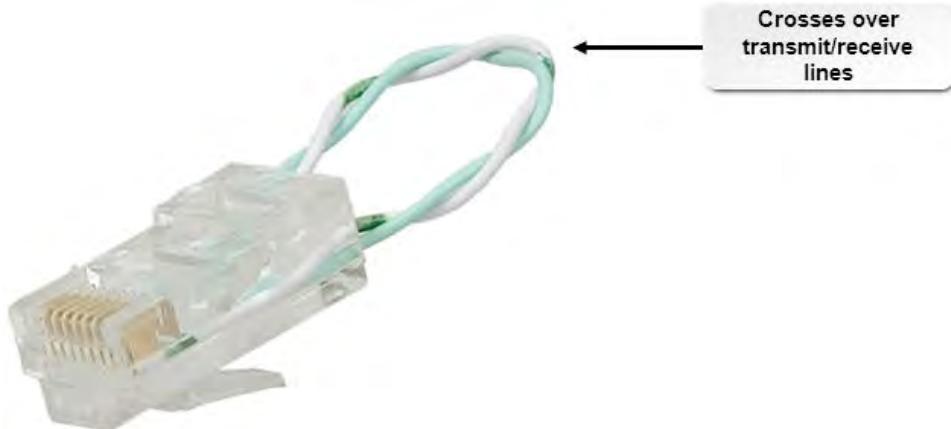
To locate a cable in a group of cables, connect the tone generator to the copper ends of the wires; then move the tone locator over the group of cables. A soft beeping tone indicates that you are close to the correct wire set; when the beeping is loudest, you have found the cable.



**Caution:** Do not connect a tone generator to a cable that is connected to a NIC. The signal sent by the tone generator can destroy network equipment.

## Loopback Plugs

A *loopback plug* is any tool that causes the device to transmit a signal back to itself. It is typically used for diagnosing transmission problems that redirect electrical signals back to the transmitting system. It typically plugs into a port and crosses over the transmit line to the receive line. Many times technicians will construct their own device based on their specific needs, but it can be used to test Ethernet network interface cards (NICs).



**Figure 13–28:** A loopback plug.

## Punch Down Tools

A *punch down tool* is used in a wiring closet to connect cable wires directly to a patch panel. The tool strips the insulation from the end of the wire and embeds the wire into the connection at the back of the panel. The punch down tool makes connecting wires to a patch panel easier than it would be to connect them by hand. Without the punch down tool, you would have to strip the wire manually and connect it by twisting it or tightening it around a connection pole or screw.



**Note:** The technical name for a punch down tool is an Insulation Displacement Connector (IDC).



**Figure 13–29:** A punch down tool.

## Wi-Fi Analyzers

A spectrum analyzer is an instrument that displays the variation of signal strength against the frequency.

A *wireless tester*, *wireless locator*, or a *Wi-Fi analyzer*, is a Wi-Fi spectrum analyzer used to detect devices and points of interference, as well as analyze and troubleshoot network issues on a WLAN or other wireless networks. Like network analyzers, wireless testers give an overview of the health of a WLAN in one central location, enabling technicians to troubleshoot problems efficiently.

When a wireless network is detected, the Wi-Fi analyzer displays information such as the SSID, average signal quality, MAC address, and channel frequency. You can then use this information to help optimize your wireless network.

## Networking Utilities

Microsoft includes a variety of tools in its Windows operating systems that you can use to troubleshoot TCP/IP.

Tool	Use To
ipconfig	Verify the configuration of TCP/IP and to release or renew DHCP IP address leases. (Other operating systems use different commands instead of ipconfig. For example, Linux uses ifconfig.)
ping	Test TCP/IP communications. With the -t switch, you can ping the indicated host until the request gets interrupted; with the -l [number] switch, you can send a ping of a specified buffer size.
tracert	Determine and test all points along the route the computer uses to send a packet to a destination. If tracert is unsuccessful, you can use the results generated to determine at what point communications are failing. (Linux uses traceroute.)
nslookup	Verify that the computer can connect to a DNS server and successfully find an IP address for a given computer name.
netstat	Show the status of each active network connection; netstat will display statistics for both TCP and UDP, including protocol, local address, foreign address, and the TCP connection state. Because UDP is connectionless, no connection information will be shown for UDP packets.
net	Manage Microsoft network resources from a command line. With the use option, you can connect or disconnect the computer from a shared resource. You can also retrieve information about current network connections. To see all of the available commands in this suite, type net /? at a command line.
Device connection status	Depending on whether you are using a wired or wireless network connection, the connection status might be called something like <i>Local Area Connection</i> or <i>Wireless Network Connection</i> . Verify that the device is connected to the network and able to send and receive data.
Network troubleshooters	Walk you through the resolutions to various common network problems. There are several network-related troubleshooters in the <b>Help and Support Center</b> that can help.

### ipconfig Options

The ipconfig command provides several options that are helpful for network maintenance and troubleshooting.

Command	Enables You To
ipconfig /all	View the computer's host name, DNS domain name, and for each network interface, the physical (MAC) address, the IPv4 and IPv6 addresses, subnet mask and link-local address, default gateway, and DNS server(s). In addition, you can use this display to determine whether the computer was configured through DHCP or APIPA. If the computer obtained its addressing through DHCP, you will also see information about the DHCP lease and the IP address of the DHCP server.
ipconfig /release	Release the IP addressing information assigned to the computer by the DHCP server or APIPA.

<b>Command</b>	<b>Enables You To</b>
ipconfig /renew	Lease IP addressing information from a DHCP server or APIPA. If the computer already has a good IP address leased, it will not renew unless you release the address first.
ipconfig /flushdns	Clear DNS information on the client so that client updates with new configuration information more quickly. This command is also used for troubleshooting in situations where the client has incorrect information in its DNS cache.
ipconfig /registerdns	Register the client with its DNS server.

# ACTIVITY 13-5

## Identifying Networking Tools

### Scenario

You recently learned about some of the more powerful and popular networking tools you will encounter as a PC technician. You decide to try them out to see how they work.

1. You need to determine if a cable is carrying a signal. Which networking tools might help you?
  - Crimpers
  - Cable testers
  - Multimeters
  - Punch down tool
2. You need to connect cable wires to a patch panel. Which networking tool might help you?
  - Crimpers
  - Loopback plug
  - Punch down tool
  - Toner probe
3. Open a command prompt.
  - a) Press **Windows Key+R** to open the **Run** dialog box.
  - b) In the **Open** text box, enter **cmd**
4. Display and examine the TCP/IP configuration information for your computer.
  - a) Enter **ipconfig /all**
  - b) Scroll through the results of the command as your instructor describes the information that is displayed.
5. Verify network connectivity with the **APLUS-DC** server.
  - a) Ping the classroom server by IP address or name.
  - b) Examine the results. Were you able to reach the target computer?
6. Examine the status of network connections on your computer.
  - a) Enter **netstat**
  - b) Examine the results as your instructor describes them.
7. View help for the **net** command.
  - a) Enter **net /?**
  - b) Enter **net help**
  - c) Examine the results as your instructor describes them.
  - d) Select at least one of the **net help** commands (such as **net help view**) and display detailed help information. Share your findings with the rest of the class.
8. Close the command prompt.

## Summary

In this lesson, you identified many different network technologies. Networking is at the heart of any type of business. Without it, a business simply cannot function in today's world. It is your job to ensure that the networks behind the business are running properly and managed correctly.

**What do you think are the most important network concepts covered in this lesson?**

**What experience do you have with any of the technologies discussed in this lesson?**



**Note:** Check your CHOICE Course screen for opportunities to interact with your classmates, peers, and the larger CHOICE online community about the topics covered in this course or other topics you are interested in. From the Course screen you can also access available resources for a more continuous learning experience.



14

# Installing and Configuring Networking Capabilities

**Lesson Time:** 2 hours, 30 minutes

## Lesson Objectives

In this lesson, you will install and configure networking capabilities. You will:

- Configure basic Windows networking.
- Configure Windows proxy and firewall settings.
- Use selected Windows networking features.
- Install and configure SOHO networks.

## Lesson Introduction

In the last lesson, you identified networking technologies. With that knowledge, you are now prepared to implement those technologies. In this lesson, you will install and configure networking capabilities.

As an A+ technician, your duties might include setting up and configuring PCs so that they can connect to a network. By installing and configuring networking capabilities, you will be able to provide users with the connectivity they need to be able to perform their job duties.

# TOPIC A

## Configure Basic Windows Networking

In the previous lesson, you focused on the network infrastructure and how it all works together. Now you can take a look at how the operating system is configured to run on the hardware. In this topic, you will configure Windows networking.

Once all the hardware and connections are made in a networking environment, you will need to make sure that the operating system is configured to use the hardware successfully. It is important to fully understand not only the hardware and the connections within a network, but also how Windows will need to be setup and configured to accomplish connectivity with the resources of a network.

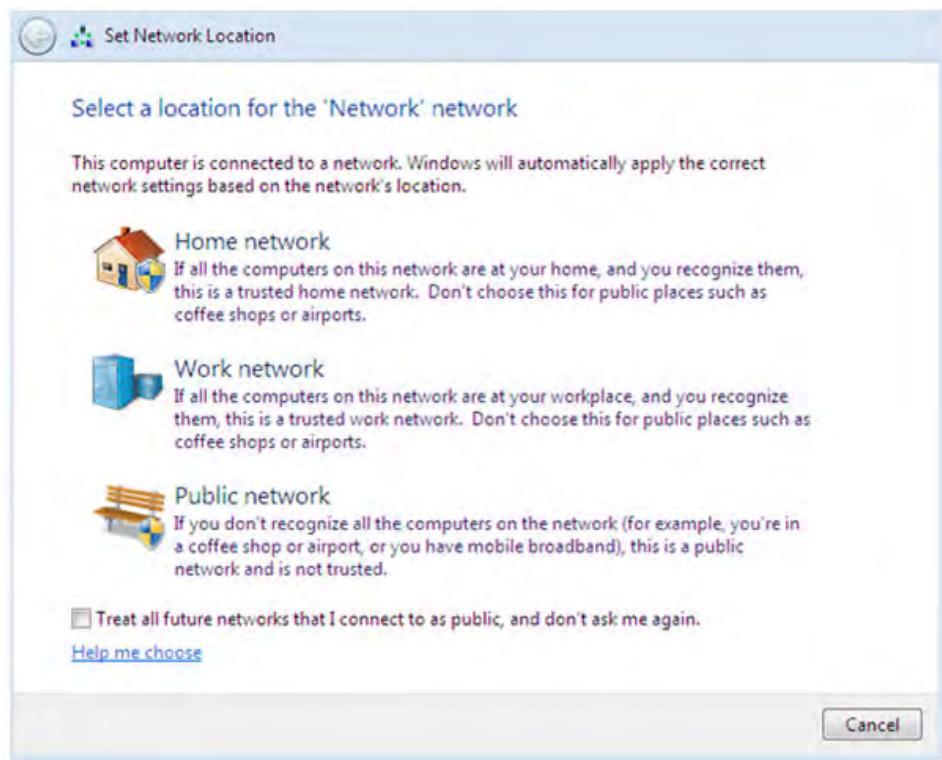
### Network Connection Types

You can connect devices to a network in several ways. How those devices communicate with one another is determined by the connection method:

- Virtually, using a virtual private network (VPN) connection.
- Using a dial-up connection.
- Wirelessly, through a wireless access point (WAP).
- Wired, using Ethernet cabling.
- Using a WWAN cellular connection.

### Network Location Settings

Windows is configured to recognize three different network locations depending on what type of network you are connecting to. Network settings can be determined during the Windows 7 installation, or they will be set the first time the device is connected to a network.



**Figure 14-1: Network settings in Windows.**

The following table describes each of the network location settings.

Location	Description
Home	The Home network setting is used for small home networks where devices are trusted. All devices connected in a home network must be part of a workgroup or part of a homegroup. This allows all devices to recognize and see one another within the network using the network discovery function.
Work	The Work network setting is used for small private business networks. In this configuration all devices are part of a workgroup and can see one another as peers, but cannot join as a homegroup.
Public	The Public setting is used when devices connect to a network in a public space. This setting automatically applies security settings for that location and protects your device from unauthorized access via the public network.

## Network Card Properties

A computing device's network card can be configured for optimal performance and specific network requirements. For integrated NICs, many of the following properties can be configured in the system BIOS.

<b>Property</b>	<b>Description</b>
Speed and duplex settings	<p>The speed and duplex of the NIC can determine how efficiently data transmissions are sent. The speed can range from 10 MB/s to 1,000 MB/s and can run in three different modes:</p> <ul style="list-style-type: none"> <li>• <i>Half duplex</i> permits two-way communication, but only in one direction at a time.</li> <li>• <i>Full duplex</i> permits simultaneous two-way communication.</li> <li>• <i>Auto negotiation</i> is used to negotiate a speed and duplex method that is compatible with the network router or switch. In this process the NIC can respond quickly with a speed that meets the requirements of the network device.</li> </ul>
	 <p><b>Note:</b> In most cases, this will be set to Auto negotiation and this is the value you will want.</p>
Wake-on-LAN	<p><i>Wake-on-LAN (WOL)</i> is a networking capability that is built into a device's NIC circuitry that allows a device to turn on, or power up, when a network message is received by another computing device. You can check if your NIC has this functionality by booting up the system BIOS and checking the NIC card properties.</p>
PoE	<p><i>Power over Ethernet (PoE)</i> is a technology standard that enables both power and data to be transmitted over an Ethernet cable. NICs that are PoE compliant will allow both power and data to be sent as long as the device itself is also PoE compliant. PoE is commonly used to power and transmit data for APs that are installed in locations where AC outlets are not available.</p>
QoS	<p><i>Quality of service (QoS)</i> allows NICs to prioritize and manage data traffic in order to fully support the networking needs for all devices connected.</p>



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Configure Network Card Properties.

# ACTIVITY 14-1

## Configuring Network Card Properties

### Scenario

In your test lab, you want to see at what speed your VMs are connecting to the network. You also want to verify that the VMs are configured to use full duplex communication.

1. View the connection speed of your Windows 8.1 VM.
  - a) Open **Control Panel**.
  - b) Select **Network and Internet**.
  - c) Open **Network and Sharing Center**.
  - d) From the **Network and Sharing Center**, select **Change adapter settings**.
  - e) Right-click the NIC and select **Status**.
  - f) In the status dialog box, observe the **Speed**. Is the speed what you expected it to be? If not, is it higher or lower than you expected? Consider reasons for the discrepancy, if any are found.
  - g) Select **Close**.
2. View the speed and duplex settings for your NIC.
  - a) Right-click the network card and select **Properties**.
  - b) Select **Configure**.
  - c) Select the **Advanced** tab.
  - d) From the **Property** list, select **Speed & Duplex**.



**Note:** In most cases, you will leave this at Auto negotiate.

- e) Examine the options under **Value**.
- f) If the value is acceptable, select **Cancel**. If necessary, change the value and select **OK**.
3. Record IP address and related settings.
  - a) Display the **Properties** for the network card.
  - b) On the **Networking** tab, select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.
  - c) Use the following table to record the IP address and related settings.

Parameter	Value
Static IP address	
Subnet mask	
Default gateway	
DNS server address	

It's a good practice to record these values in case you have issues with connectivity in the future.

- d) Select **OK**.
- e) Close the network card properties dialog box.

## Alternate IP Address Configurations

In some cases you may need to configure an alternative IP address for your client computer. By configuring a static backup addressing scheme, you can ensure connectivity when DHCP is unavailable. Make sure to assign an appropriate IP address, subnet mask, and gateway, as well as at least one DNS server address.

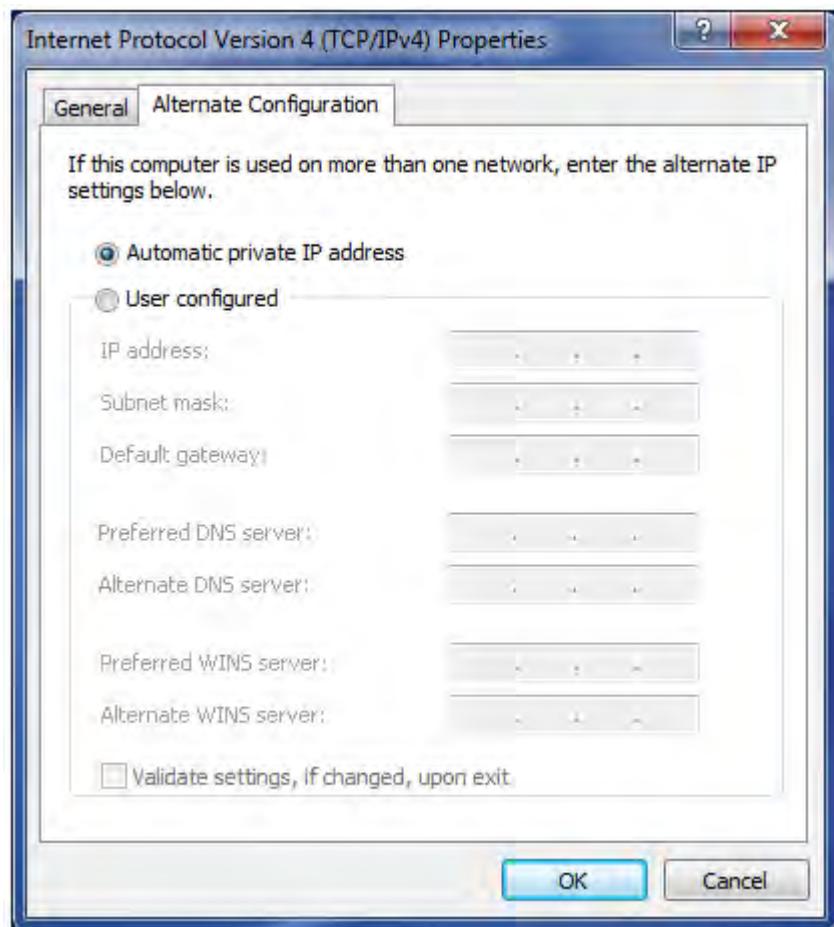


Figure 14-2: Alternate IP address settings.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Configure Alternate IP Addresses.

# ACTIVITY 14-2

## Configuring Alternate IP Addresses

### Scenario

A technician recently configured some network cards to use static IP addresses for several users. These users also need to be able to communicate with the Linux users whose computers are on another network, without additional configuration on their parts.

1. Open the properties for the network adapter and IPv4.
  - a) If necessary, open **Network Connections**, select the network card, and open the properties dialog box for the network card.
  - b) In the properties dialog box, select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.
2. Set up the alternate configuration.
  - a) Select the **Alternate Configuration** tab.
  - b) Select **User configured**.
  - c) For the **IP address**, type **192.168.0.a**, where **a** is your student number plus 200.
  - d) For the **Subnet mask**, type **255.255.255.0**.
  - e) For the **Default gateway**, type the value provided by your instructor.
  - f) For the **Preferred DNS server**, type the value provided by your instructor.
  - g) Select **OK** twice.
  - h) Close all open windows and dialog boxes.
  - i) If prompted, restart your computer.

## Windows Networking Options

There are three networking options available in Windows:

- Homegroups
- Workgroups
- Domains

Homegroups, workgroups, and domains are different organizational and security models for Windows networking.

- Homegroups provide easy file and printer sharing, but are available only for Windows 7, 8, and 8.1 computers.
- Workgroups are unstructured collections of individual named computers and are usually deployed in homes and small offices.
- Domains require a specially configured Windows Server computer called a domain controller and are most often used in corporate environments with centralized administration.

### Effects of Domain Membership

Domain controllers run the Microsoft Active Directory® directory service. To fully participate in the benefits of an Active Directory domain, client computers must become members of the domain.

Domain membership means:

- The computer has a computer account object within the directory database.
- Computer users can log on to the domain with domain user accounts.

- The computer and its users are subject to centralized domain security, configuration, and policy settings.
- Certain domain accounts automatically become members of local groups on the computer.

## Prestaging Computer Accounts

In Windows Server 2012, as well as other versions of Windows Server, you can create the computer accounts in Active Directory before you join the computer to the domain. This process is called *prestaging*, and requires administrative privileges to add Active Directory objects.

## Directory Services

A *network directory*, or *directory service*, is a centralized database that includes objects such as servers, clients, computers, user names, and passwords. The directory is stored on one or more servers and is available throughout the enterprise. The directory provides centralized administration and centralized authentication.

	<b>Note:</b> There are many directory services available from different network vendors. Some directory services include Microsoft's Active Directory Domain Services, Open LDAP, and Novell's eDirectory, although eDirectory is now less common.
---	--

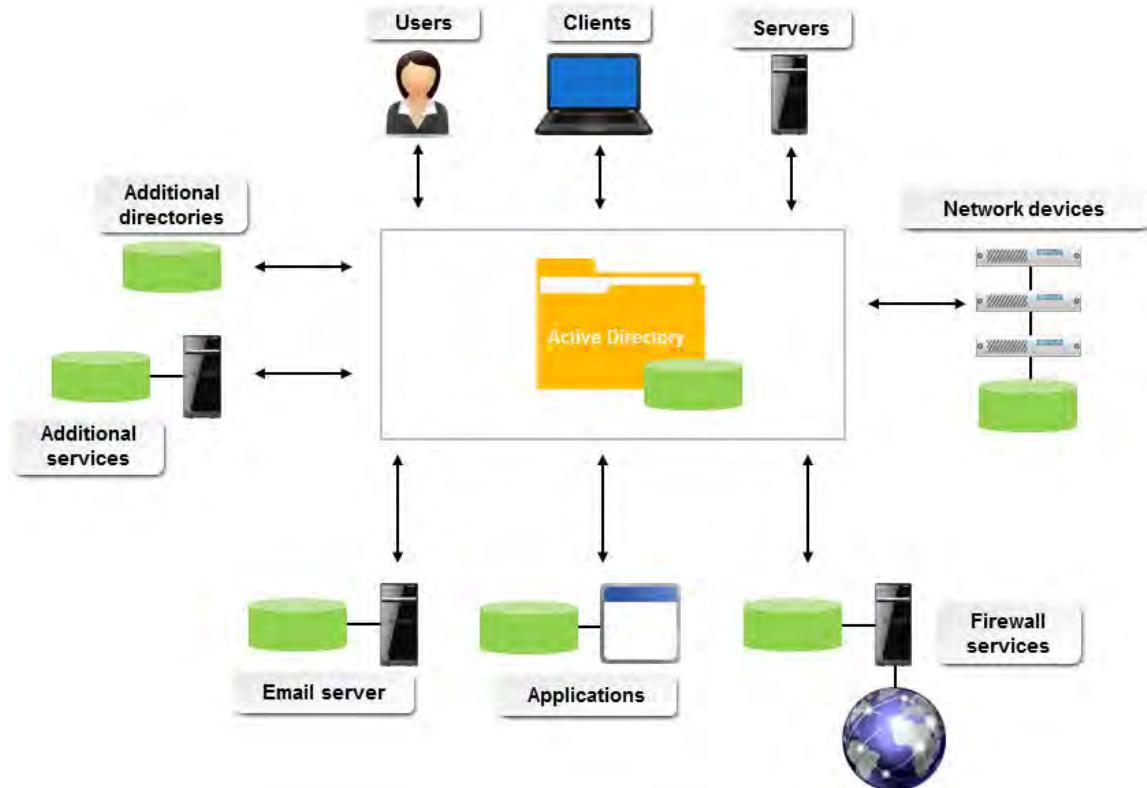


Figure 14-3: A network directory.

	Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Join a Computer to a Domain.
---	--

# ACTIVITY 14-3

## Joining a Computer to a Domain

### Before You Begin

A domain controller named APLUS-CLASS has been created and configured as part of the course setup.

### Scenario

In this activity, you will examine the current networking configuration for your computer and for the VM you created. Then, you will join your computer to the **APLUS-CLASS** domain, and re-examine the networking configuration settings to see how they changed.

1. Determine the network configuration for your host computer.
  - a) Open **Control Panel** to **System**.
  - b) In the **Computer name, domain, and workgroup settings** section, observe the **Computer name**, **Full computer name**, and **Workgroup** settings for the computer.
  - c) Minimize the **System Control Panel**.
2. Determine the network configuration for the **Upgrd##** virtual machine.
  - a) Switch to the **Upgrd##** VM.
  - b) Determine the **Computer name**, **Full computer name**, and **Workgroup** settings for the **Upgrd##** VM.
  - c) Close the **System Control Panel** within the VM.
3. Join your host computer to the **APLUS-CLASS** domain.
  - a) Switch back to the **System** window for the host computer.
  - b) Select **Change settings**.
  - c) In the **System Properties** dialog box, on the **Computer Name** tab, select **Change**.
  - d) Select the **Domain** radio button, type **APLUS-CLASS** and select **OK**.
  - e) In the **Windows Security** dialog box, for **User name**, type **Admin##** and for **Password**, type **!Pass1234** and then select **OK**.
  - f) Acknowledge the welcome message, and then restart the computer when you are prompted to do so.
  - g) When the computer restarts, press any key, select **Switch User** and select **Other User**. For **User name**, type **aplus-class\admin##** and for **Password**, type **/Pass1234** and select **Enter** to log on to the **APLUS-CLASS** domain.
4. Examine the changes to the networking configuration.
  - a) On the host computer, open the **System Control Panel**.
  - b) In the **Computer name, domain, and workgroup settings** section, examine the **Computer name**, **Full computer name**, and **Workgroup** settings for the computer.  
The settings should reflect a change to the **Full computer name**, where the name should resemble **Client##.aplus-class.com** and the **Workgroup** setting should have been replaced with the **Domain** setting, where the **Domain** is **aplus-class.com**.
  - c) Close the **System Control Panel**.

# TOPIC B

## Configure Network Perimeters

Through the use of features such as proxy servers and firewalls, you can help prevent unauthorized access to systems. In this topic, you will examine and configure settings for using proxy servers and Windows Firewall.

### Proxy Settings

In computer networking, a *proxy* is a system that acts as an intermediary for requests for resources.

Client proxy software can be installed on any client machine to add an additional level of security between the client machine and the proxy server. Data requests sent from the client get routed from the client side proxy through a back channel directly to the proxy server. The key part of this relationship is the additional metadata attached to the request by the client proxy that aids with identification once it hits the proxy server. So in essence the client proxy and the server proxy work together to provide quick identification and access to resources.

When configuring a client computer, use the following settings:

- Set the proxy server settings to the correct IP address.
- Exceptions can be set to include ranges (for example, you can bypass a proxy server if you access anything in the 192.168.x.y scope).
- Proxy settings can be set so that all HTTP or FTP connections use a proxy server, but no other connections.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Configure Proxy Settings.

## ACTIVITY 14-4

### Configuring Proxy Settings

#### Scenario

You don't currently have a proxy server on the network, but there are plans to put one in place soon. You want to make sure you know how to configure Internet Explorer to take advantage of the proxy server once it is up and running.

1. Access Internet Explorer options.
  - a) Open **Internet Explorer**.
  - b) Select the **Tools** button.
2. Configure proxy settings.
  - a) Select the **Connections** tab.
  - b) Select **LAN settings**.
  - c) Check **Use a proxy server for your LAN**.
  - d) Observe the **Address** text box. This is where you would enter the address of the proxy server.
  - e) Check **Bypass proxy server for local addresses**.
  - f) Select **Advanced**. Notice that you can specify proxy address and port numbers for various protocols, or use the same proxy server for all protocols. You can also configure a list of exceptions for which you do not want to use the proxy server.
  - g) Select **Cancel** until all dialog boxes are closed.
  - h) Close **Internet Explorer**.

## Windows Firewall Settings

Windows client firewalls can be configured for networking to ensure that they are secure against unauthorized access attempts and attacks. Consider the following settings when setting up the firewall:

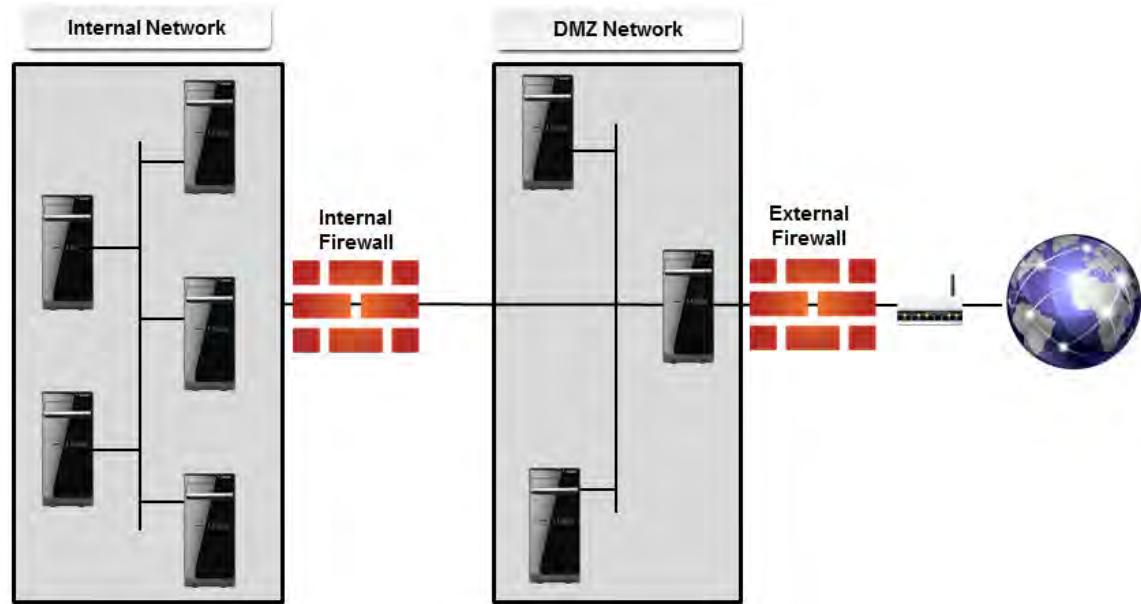
- Enabling or disabling port security on certain ports.
- Inbound and outbound filtering. The user can set up rules or exceptions in the firewall settings to limit access to the web.
- Reporting and logging activity.
- Malware and spyware protection.
- Pop-up blocking.
- Port assigning, forwarding, and triggering.
- Enabling or disabling the Windows Firewall when necessary.

Windows Firewall is a software-based firewall that is included with all currently supported versions of Windows operating systems. Once an operating system is installed, Windows Firewall is automatically installed and enabled. By default, the firewall blocks unsolicited incoming traffic on all ports. You can open blocked ports and configure other firewall settings by using the Windows Firewall program in the **Control Panel** or through Windows Security Policy Settings. Windows Firewall offers many security options and can be configured to drop outgoing traffic as well as incoming traffic.

## DMZs

A *demilitarized zone (DMZ)* is a small section of a private network that is located between two firewalls and made available for public access. A DMZ enables external clients to access data on private systems, such as web servers, without compromising the security of the internal network as a whole. The external firewall enables public clients to access the service whereas the internal firewall prevents them from connecting to protected internal hosts.

In small offices, DMZs are commonly used to protect any client-facing web servers. This security method prevents any hackers from seeing the private internal IP scheme.



**Figure 14-4: A section of a private network available for public access.**

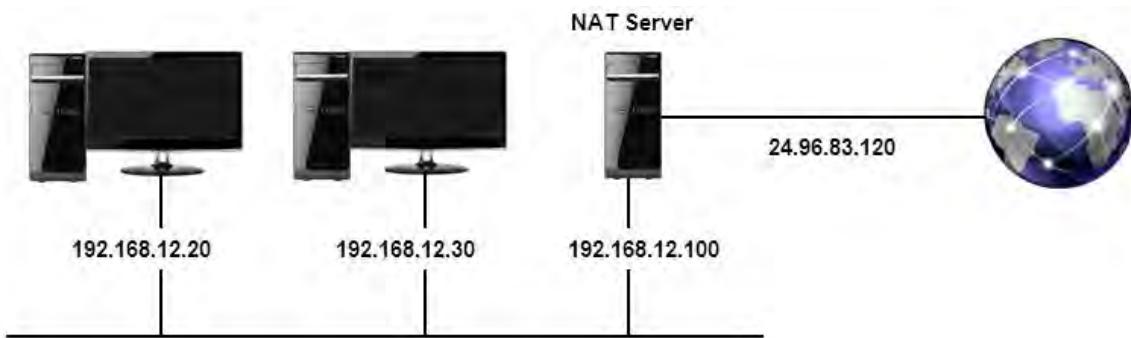
DMZs might also be referred to as perimeter networks or screened subnets.

## NAT Implementations

In order to keep internal addresses private, *Network Address Translation (NAT)* is used to conceal internal private IP addresses from external networks. A router is configured with a single public IP address on its external interface and a private address on its internal interface. A NAT service running on the router or on another system translates between the two addressing schemes. Packets sent to the Internet from internal hosts all appear as if they came from a single IP address, thus preventing external hosts from identifying and connecting directly to internal systems.



**Note:** A vast internal network can be configured with a single public address, which makes NAT both secure and cost-efficient.

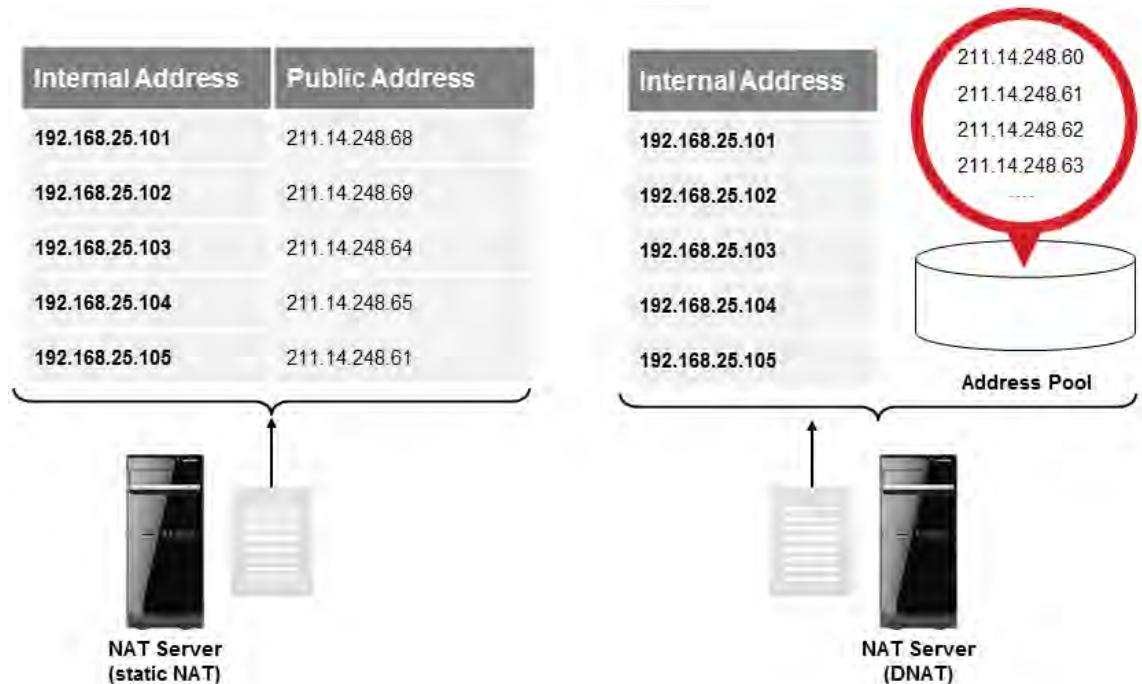


**Figure 14-5: NAT Implementation.**

NAT can be implemented as software on a variety of systems or as hardware in a dedicated device such as a router. Internet Connection Sharing (ICS) in Windows systems includes a simple software-based NAT implementation, but requires a separate device, such as a modem, to provide actual Internet connectivity. Hardware-based NAT devices, such as cable modems and DSL routers, often have extended functionality and can double as Internet access devices.

## DNAT

In static NAT, each internal address is mapped to a single specific public address. In dynamic NAT (DNAT), there is not a one-to-one ratio of internal to external addresses; any number of internal addresses can share a pool of external addresses.



**Figure 14-6: DNAT.**



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Configure Windows Firewall Settings.

# ACTIVITY 14-5

## Configuring Windows Firewall Settings

### Scenario

Some users have been having problems getting to online sites and intranet sites. You want to make sure that the Windows Firewall settings are not causing the issue. Also, you recently attended a security seminar where you learned about using Windows Firewall to prevent users from accessing systems that are not up-to-date.

1. Access Windows Firewall settings.
  - a) Open **Control Panel**.
  - b) Select **System and Security** if you are using Categories.
  - c) Select **Internet Options**.
  - d) Select **Windows Firewall**.
  - e) Observe the current configuration.
2. Examine the firewall settings options for Private and Public networks.
  - a) In the left pane, select **Turn Windows Firewall on or Off**.  
All of the settings should be enabled.
  - b) Select the **Back** button next to the address bar.
3. Examine the firewall rules.
  - a) In the left pane, select **Advanced Settings**.
  - b) Scroll through and observe settings for **Inbound Rules** and then for **Outbound Rules**.
4. Configure Connection Security Rules.
  - a) Right-click **Connection Security Rules** and then select **New Rule**.  
You might need to select Connection Security Rules and then right-click it.
  - b) Examine the types of connection security rules you can create. The wizard guides you through configuring each type of rule.
  - c) With **Isolation** selected, select **Next**.
  - d) Examine the settings for when authentication occurs, then select **Next**.
  - e) Examine the available authentication methods, then select **Next**.
  - f) Verify all boxes are checked so that the rule applies to **Domain**, **Public**, and **Private** network connections, then select **Next**.
  - g) In the **Name** text box, type **Isolation Rule** and then select **Finish**.
5. Disable the rule and close Windows Firewall windows.
  - a) Select **Isolation Rule** and observe the configuration information displayed.
  - b) Right-click **Isolation Rule** and select **Disable Rule**.
  - c) Close all open windows.

# TOPIC C

## Using Windows Networking Features

So far, you have configured Windows networking, including configuring IP addresses, proxy settings, and firewall settings. Now it's time to test the configuration. In this topic, you will use some of the most popular features offered on Windows networks.

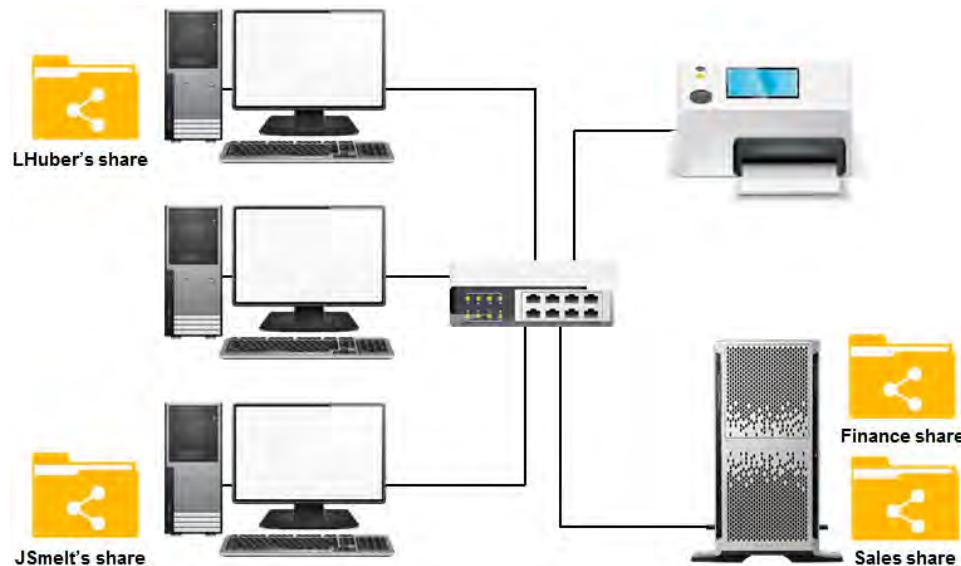
As an A+ technician, your duties might include supporting users with some basic networking tasks, as well as helping troubleshoot their PCs' configurations. By configuring and using common Windows features such as network shares and Remote Desktop, you'll be well-equipped to support the users in your organization.

### Windows Network Shares

On Windows systems, you can share folders by modifying the folders' properties. When you share a folder, you assign it a share name that can be different from the underlying folder name. You can share the folder more than once using different names.

Users can connect to the shared folder by browsing to the computer in **Network**, or by selecting **Start→Run** and entering the Universal Naming Convention (UNC) path to the folder, in the form `\computername\sharename`. Be aware that a shared folder has two sets of permissions: the NTFS permissions (which are on the **Security** tab of that folder's **Properties**) and the share permissions (which are on the **Shared** tab of that folder's **Properties**). The security permissions do not automatically change once a folder is designated as a share, and there is no propagation between the two.

Users can also map a network share as a drive on their computer. This assigns the network share a letter (e.g., F:), just as if it were a local drive. Windows and running applications can more easily interface with mapped network drives. You can map a network share as a drive by opening the **Map Network Drive** wizard and providing the drive letter and network path to the share.



**Figure 14-7: Windows network shares.**

## File Sharing with OS X

When you use OS X, you can share files in the **Public** folder for your user account with up to 10 other network users. (Sharing with more users requires OS X Server.) You will need to make the AppleTalk® service active, assign a network name to your computer, and start the file sharing service. Other OS X users on your local network can then connect to your system by selecting **Connect To Server** from the **Go** menu and browsing for your computer's name. They can access files in your **Public** folder, and place files in your **Drop Box** folder.

For more information about file sharing in OS X, including information on how to make other folders public, share files with remote users on the Internet, and share with computers running different operating systems, see the technical document "Mac 101: File sharing" on the Apple Computer website at <http://support.apple.com/kb/HT1549>.

## File Sharing with UNIX or Linux

UNIX and Linux are typically used as centralized network file servers, rather than for ad hoc peer-to-peer resource sharing. These systems generally use the Network File System (NFS) protocol to share files with other UNIX and Linux systems. NFS enables clients to see the files on the shared system as if they were part of the client's own local file system.

The specific steps for implementing file sharing with NFS will vary depending on your operating system version and also depending on whether you use shell commands or your system's Graphical User Interface (GUI) to configure the service. This is also true for the commands or steps the clients will need to use to mount the file systems that NFS exports.

## Windows Administrative Shares

Certain folders are shared by default on every Windows system. These administrative shares can be deleted, but by default, the system will re-create them every time it restarts (unlike local shares, which do not get re-created if they are deleted). The administrative shares are hidden shares, which means that they have a dollar sign (\$) appended to the share name. (You can create your own hidden shares by doing the same thing.) You can connect to hidden shares by entering a Universal Naming Convention (UNC) path, but otherwise, the shares are not visible on the network.

You can see all shares on a system, including administrative shares, by opening **Computer Management**, expanding **Shared Folders**, and selecting the **Shares** node. You should see the following administrative shares on every Windows system:

- The root of each drive on the system is shared with its drive letter. Thus, the C drive is shared administratively as C\$, the D drive is shared as D\$, and so on.
- The folder where Windows is installed, usually the C:\Windows folder, is shared as ADMIN\$.
- An InterProcess Communication (IPC) network object is created and shared as IPC\$. This does not represent a local folder, but enables computers to establish network sessions.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on **How to Create a Network Share**.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on **How to Map a Network Share**.

# ACTIVITY 14-6

## Creating a Network Share

### Scenario

You have a group of users that need to share some files in a folder on the department server. Before you set it up for the users, you want to try out network shares on a test folder to make sure you know how it works.

1. Navigate to the C: drive and create a folder named **Share#** with the # being your student number.
2. Share the **Share#** folder with **Everyone**, and grant **Read/Write** share permissions.
  - a) Select the folder, display its pop-up menu, and select **Share with**.
  - b) Select **Specific people** to open the **File Sharing** wizard.
  - c) On the **Choose people to share with** page, select the down arrow next to the text box and select **Find people**. In the **Select Users or Groups** dialog box, type **everyone**. Select **Check Names** and then select **OK**.
  - d) In the list, select **Everyone**, and then select the down arrow under **Permission Level**. Select **Read/Write**.
  - e) Select **Share**.
  - f) In the **User Account Control** dialog box, in the user name text box, type **APLUS-CLASS/Administrator##**.
  - g) In the **Password** text box, type **!Pass1234** and select **Yes**.
  - h) Select **Done**.

### Remote Desktop

*Remote Desktop* is used to operate a Windows computer from a remote location as if you were in front of it. Depending on the permissions you define, you will have full access to all resources, including printers, storage devices, and the network to which the machine is attached. You are even capable of accessing multiple machines at once or hopping to multiple machines in a chain, by running Remote Desktop on each machine on the daisy chain. In other words, Computer01 has a Remote Desktop connection to Computer02, and Computer02 has a Remote Desktop connection to Computer03. Computer01 has access to Computer03 through the open window that displays Computer02's desktop.

The biggest limitation of Remote Desktop on Windows is that only one person can be logged in to the machine at once, so once you log in using Remote Desktop, the monitor at the local computer will go to the login screen. If a local user logs in, the remote user will be disconnected. Remote Desktop is not really a remote diagnostic and troubleshooting tool as much as a management tool.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Configure Remote Desktop.

# ACTIVITY 14-7

## Configuring and Using Remote Desktop

### Before You Begin

You will work with a partner for this activity.

### Scenario

Members of the PC Technician team take turns being on call after hours and weekends. One of the ways to be efficient at doing this support is to have access to your work computer from home so that you have access to the information and tools on your work computer. You decide to try using Remote Desktop Connection to do this.

1. Set up your computer so that it allows remote connections.
  - a) Open **Control Panel** and select **System**.
  - b) Select **Remote settings**.
  - c) If prompted, enter your admin## password.
  - d) In **System Properties** dialog box, in the **Remote Desktop** section, select **Allow remote connections to this computer**.
  - e) Acknowledge the message regarding sleep and hibernation settings.
  - f) Select **Select Users**.
  - g) In the **Remote Desktop Users** dialog box, select **Add**.
  - h) In the **Select Users or Groups** dialog box, enter your user name, then select **OK**.
  
2. Connect to your PC using Remote Desktop.
  - a) Switch computers with your partner.
  - b) Using the **Search** charm, search for and select **remote desktop connection**
  - c) In the **Remote Desktop Connection** dialog box, type the name of the PC that you allowed remote connections to.
  - d) Select **Connect**.
  - e) When prompted for your password, enter it.
  
3. Perform tasks on the remote computer.
  - a) From the Remote Desktop Connection bar at the top of the window, select the **Remote Commands** arrow on the left, then select **Charms**.
 


**Note:** If the Remote Desktop Connection window is not full screen, the commands are not visible. Right-click the top of the Remote Desktop Connection window to display a pop-up menu, then select **Remote Commands** to see the options including Charms.
  - b) Select **Settings→PC Info** and verify that it is showing information about the remote computer.
  - c) Open a command prompt window on the remote PC and enter **ipconfig** to verify that you are viewing the IP settings for your remote PC.
  - d) Close the command prompt window.
  - e) From the **Remote Commands** menu, select **Start** to switch between the **Start** screen and the **Desktop**.
  - f) With the **Start** screen displayed, from the **Remote Commands** menu, select **App Commands** to display the customization options.
  - g) Select **App Commands** again. Notice that a box appears around the first tile on the **Start** screen. You can now use the arrow keys to move between tiles on the **Start** screen.

4. End the remote session.
    - a) At the top center of the Remote Connection window, select the **Close** button.
    - b) When prompted that your remote session will be disconnected, select **OK**.
-

# TOPIC D

## Install and Configure SOHO Networks

Previously in this course, you covered basic networking concepts, the Transmission Control Protocol/Internet Protocol (TCP/IP) addressing scheme, and how networks are connected. In this topic, you will use that knowledge to install and configure a SOHO network.

SOHO networks are much like the larger corporate networks, just on a much smaller scale. No matter what the size or location of the network, you are still responsible for understanding how it is structured and configured. A+ technicians must understand the needs and complexities of SOHO wired and wireless networks.

### SOHO Networks

A *SOHO network* is a network that provides connectivity and resource sharing for a small office or home office. Generally limited to fewer than 20 computers or nodes, a SOHO network often facilitates sharing of files and printers, as well as services such as email, faxing, and so forth. A SOHO network can contain a combination of wired and wireless computer connections, and all of the computing devices in a SOHO network usually share the same physical location.



*Figure 14-8: A SOHO Network.*

### How Small is Small?

SOHO networks can range in size, and there is no real consensus as to the maximum number of nodes that can be in a SOHO network. Some sources cite the maximum as 10 nodes, while others say that four or five nodes is the maximum.

### Infrastructure Mode and Ad Hoc Mode

In *infrastructure mode*, wireless devices communicate with other devices by first going through an access point (AP). In infrastructure mode, wireless devices can communicate with each other or can communicate with a wired network.

*Ad hoc mode* is a method for wireless devices to communicate directly with each other without the use of an AP. Operating in ad hoc mode allows all wireless devices within range of each other to discover and communicate in peer-to-peer fashion without involving central access points (including those built in to broadband wireless routers). An ad hoc network tends to feature a small group of devices in very close proximity to each other.

## Basic QoS

The amount of data being transmitted over networks is rising every day. Also, the type of data being transferred is changing. Traditional applications such as File Transfer Protocol (FTP) and Telnet are now outnumbered by real-time multimedia applications such as IP telephony, multimedia applications, and videoconferencing. FTP and Telnet are very sensitive to packet loss but are tolerant to delays in data delivery. The reverse is applicable to multimedia applications; they can compensate for some amount of packet loss, but are very sensitive toward delays in data delivery. Therefore, an optimum usage of bandwidth becomes very critical while dealing with multimedia applications. Low bandwidth may result in a bad quality transmission of real-time applications, leading to dropouts or hangs. In small offices, this issue can be a major problem due to the small network and need to access the Internet. To avoid this, certain parameters were developed to prioritize bandwidth allocation for real-time applications on networks such as the Internet and guarantee a specific quality of service (QoS).

QoS parameters include the maximum amount of delay, signal loss, and noise that can be accommodated for a particular type of network traffic; bandwidth priority; and CPU usage for a specific stream of data. These parameters are agreed upon by the transmitter and the receiver, the transmitter being the ISP and the receiver being the subscriber. Both the transmitter and receiver enter into an agreement known as the *Service Level Agreement (SLA)*. In addition to defining QoS parameters, the SLA describes remedial measures or penalties to be incurred by an ISP in the event that the ISP fails to provide the QoS promised in the SLA.

### Relevance for SOHO Networks

In SOHO networks, network performance degradation can occur when several users are running multiple applications or processes (such as downloads) that consume a lot of network bandwidth. Often, the effects of this are markedly slow Internet connections or connectivity issues with Voice over IP (VoIP) phones. By implementing basic QoS to prioritize services such as VoIP over file downloads and Internet surfing, you can ensure that the services that you decide to prioritize are getting the bandwidth they need.

## 802.11 Wireless Standards

The *802.11* standard is a family of specifications developed by the *IEEE* for wireless LAN technology. 802.11 is also called *Wi-Fi*, short for "wireless fidelity."



**Note:** The speed and ranges listed in the table are theoretical values set by the IEEE. The speed and range vary in actual use.

### 802.11 Standard Description

802.11a	802.11a is an approved specification for a fast, secure, but relatively expensive wireless protocol. 802.11a supports speeds up to 54 Mbps in the 5 GHz frequency band. Unfortunately, that speed has a limited range of only 60 feet, which, depending on how you arrange your access points, could severely limit user mobility.
802.11b	802.11b is the least expensive wireless network protocol. 802.11b provides for an 11 Mbps transfer rate in the 2.4 GHz frequency. Some vendors have increased the rate on their devices. 802.11b has a range up to 1,000 feet in an open area, and a range of 200 to 400 feet in an enclosed space (where walls might degrade the signal). It is not compatible with 802.11a. This standard supports up to 14 channels, but the available channels depend on local regulations. For instance, in areas where the FCC governs, the available channels are channel 1 through channel 11.

### 802.11 Standard Description

- 802.11g      *802.11g* is a specification for wireless data throughput at the rate of up to 54 Mbps in the 2.4 GHz band. It is compatible with 802.11b, and is replacing it due to its faster speed.
- 802.11n      *802.11n* increased speeds dramatically with data throughput up to 600 Mbps in the 2.4 GHz or 5 GHz ranges.
- 802.11ac      *802.11ac* is a wireless standard that is often described as a "souped up 802.11n." Speeds have increased again with the lowest being 433 Mbps, and some working at as much as 1.3 Gbps. One way the speed has been increased is that 802.11ac only works in the 5 GHz band. (First-generation 802.11ac routers are concurrent dual-band routers that support 802.11n clients on the 2.4 GHz frequency band and 802.11ac clients on 5 GHz band.)  
It also uses *beamforming* which transmits radio signals directly at a specific device using smart antennas.



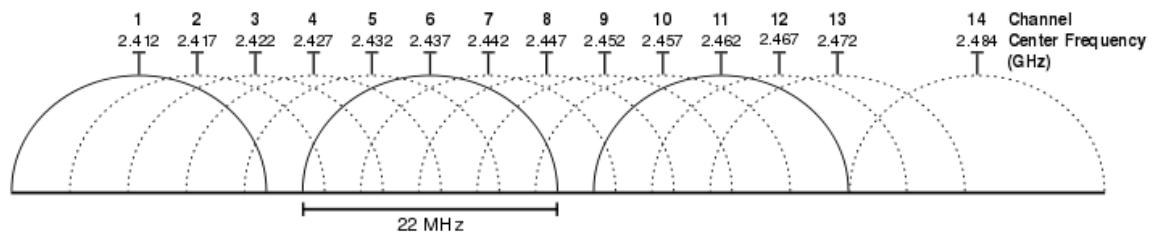
**Note:** 802.11ac, Bluetooth, and smart devices are tied to the "Internet of Things."



**Note:** Home-based Wi-Fi networks are often susceptible to interference from microwave ovens, which also operate in the 2.4 GHz frequency range.

## Channels

The 802.11b, g, and n specifications define 14 channels within the Industrial, Scientific, and Medical (ISM) 2.4 GHz band. Each channel is composed of a range of frequencies transmitting at low power, rather than a single frequency transmitting at high power. The data from a single transmitting node is spread across all frequencies in the channel. Because the overall frequency range of the ISM band is limited, the channels have been implemented with substantial overlap. Special codes embedded in the signal give each transmitting node a distinguishing pattern, so that several nodes can share the same channel at once. At some point, however, the channel becomes saturated with too many nodes sharing not only the frequencies from their own channel, but also portions of adjacent channels.



**Figure 14-9: Frequencies and overlap of wireless channels.**

The only three channels that have no overlap with each other are 1, 6, and 11. Nonetheless, they still have overlap with the other channels. In addition, most wireless access points come configured out of the box with one of these channels. Because of their popularity, these channels may in practice be busier than some of the others. You should use a wireless spectrum analyzer such as InSSIDer to find which channels in your area are actually the least busy. Newer access points will auto-negotiate their channel.

You can use a Wi-Fi analyzer to see the available channels. Depending on the app you use, you might see which channels are in use near you, the signal quality of the channel, or other information. One example for Android devices is the Wi-Fi Analyzer app. On a Linux system, you can use the command `sudo iwlist wlan0 scan | grep \Channel` to identify channels that are

experiencing congestion. On Mac systems, hold **Option** while selecting the **Wi-Fi** icon on the menu bar and selecting **Open Wireless Diagnostics** then **Utilities** to see the best 2.4 and 5 GHz channels that are available. Then, configure your wireless router to use a different channel to optimize the wireless signal.

## Wireless Encryption

*Encryption* is the process of converting data into a form that is not easily recognized or understood by anyone who is not authorized to access the data. Only authorized parties with the necessary decryption information can decode and read the data. Encryption can be one-way, which means the encryption is designed to hide only the cleartext and is never decrypted, or it can be two-way, in which the encryption can be decrypted back to cleartext and read.

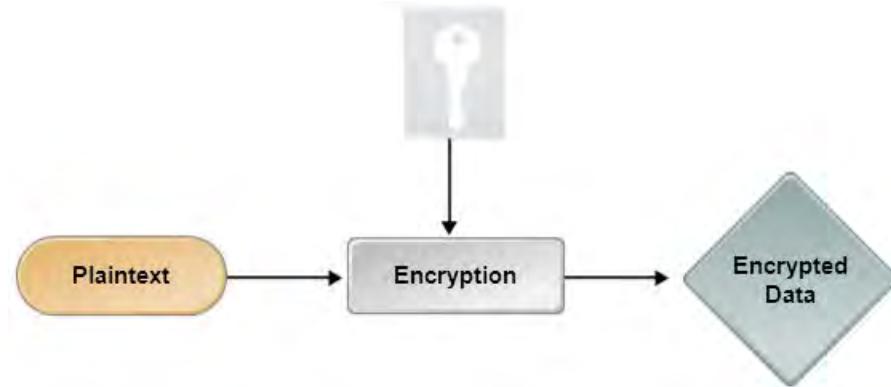


Figure 14-10: Encryption.

The use of wireless computing devices is rapidly increasing every day. This also increases the risk of wireless security attacks on devices to gain access to secure data and resources. *Wireless encryption* conceals and protects data during transmission so that if the data were accessed during transmission it cannot be read. There are a number of encryption types available to provide encryption over wireless data transmissions.

Wireless Encryption Type	Description
WEP	<i>Wired Equivalent Privacy (WEP)</i> provides 64-bit, 128-bit, and 256-bit encryption for wireless communication that uses the 802.11a and 802.11b protocols. While WEP might sound like a good solution at first, it ironically is not as secure as it should be. The problem stems from the way WEP produces the keys that are used to encrypt data. Because of a flaw in the method, attackers could easily generate their own keys by using a wireless network capture tool to capture and analyze network data and crack WEP in a short period of time.
WPA	<i>Wi-Fi Protected Access (WPA)</i> is a security protocol that was introduced to address some of the shortcomings in the WEP protocol during the pending development of the 802.11i IEEE standard. It uses strong authentication and data encryption mechanisms. WPA2 provides improved data encryption through the <i>Temporal Key Integrity Protocol (TKIP)</i> , which is a security protocol created by the IEEE 802.11i task group to replace WEP. It is combined with the existing WEP encryption to provide a 128-bit encryption key that fixes the key length issues of WEP.

Wireless Encryption Type	Description
WPA2 or 802.11i	<p><i>802.11i</i> is a complete wireless standard that adds strong encryption and authentication security to 802.11 and relies on 802.1x as the authentication mechanism. 802.11i is sometimes referred to as <i>WPA2</i>.</p> <p>In addition to TKIP, WPA2 adds <i>Advanced Encryption Standard (AES)</i> cipher-based Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) encryption for even greater security and to replace TKIP. It provides a 128-bit encryption key.</p>

## WAPs

A *Wireless Access Point (WAP)* is a device that provides connection between wireless devices and enables wireless networks to connect to wired networks. A WAP is sometimes called just an AP or a WLAN-AP. WAPs have a network interface to connect to the wired network and a radio antenna or infrared receiver to receive the wireless signals. Many include security features that enable you to specify which wireless devices can make connections to the wired network.

	<b>Note:</b> These are also referred to as an access point or wireless router.
---	--

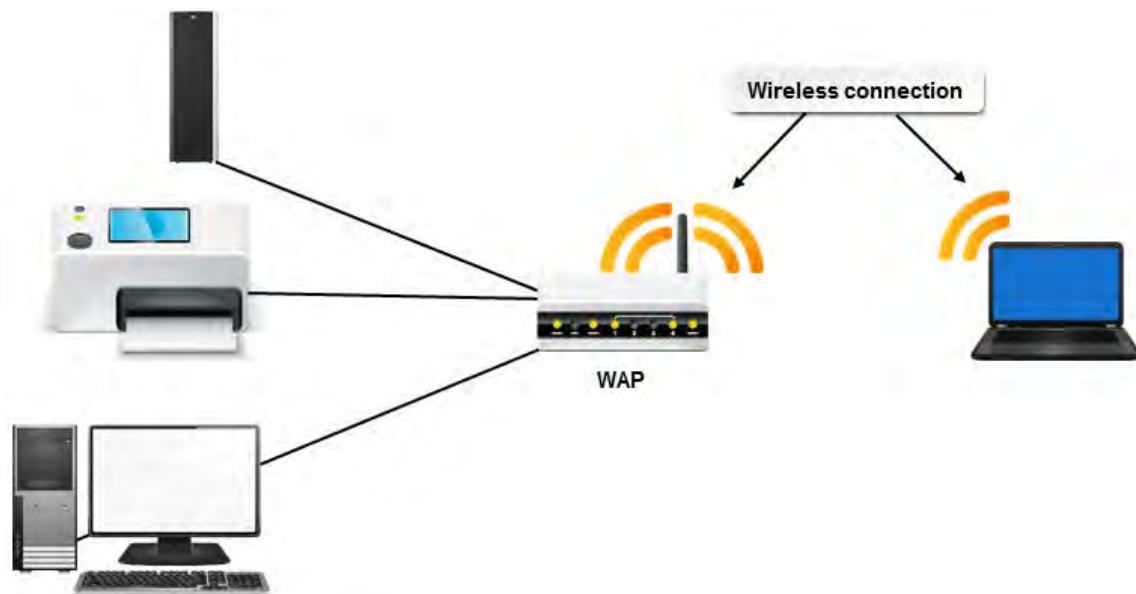


Figure 14-11: A WAP connecting to a wired network.

## SSIDs

The *Service Set Identifier (SSID)* is a 32-bit alphanumeric string that identifies a WAP and all devices that connect to it. Since a wireless client device must provide the SSID in order to connect to the WAP, the SSID functions as a sort of password for the wireless network. However, because the WAP typically broadcasts the SSID in plain text, it does not provide any security. It is more realistic to think of the SSID as a network name that is applied to the grouping of the WAP and the devices currently connected to it. The administrator can accept a device's default SSID or specify an SSID manually to more clearly identify the device.

	<b>Note:</b> SSIDs are case-sensitive.
---	--

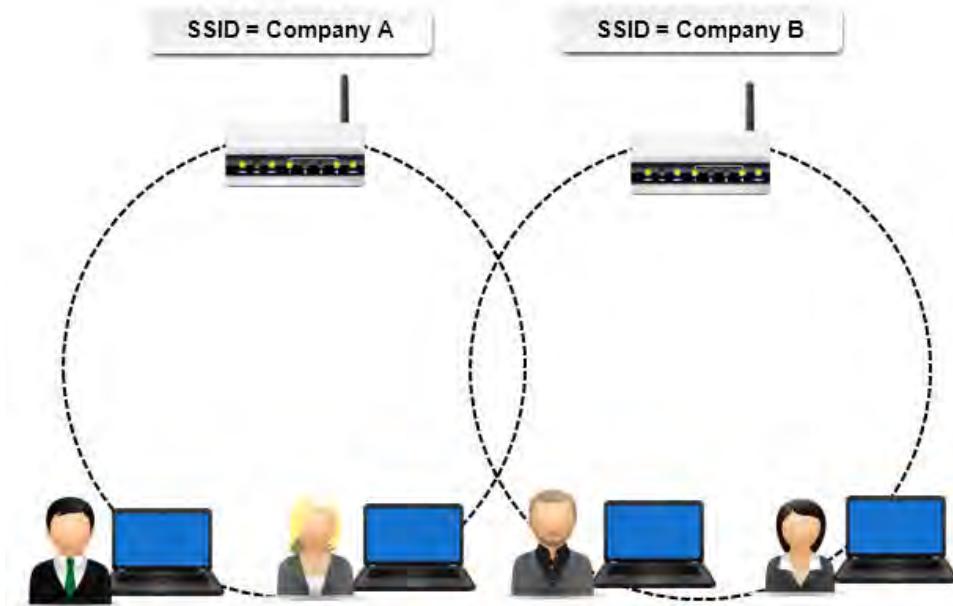


Figure 14-12: SSID.

## Port Triggering and Forwarding

If your router has NAT, then you can also configure port forwarding, which forwards a network port from one network node to another, and port triggering, which automates port forwarding by specifying ports (triggering ports) to automatically and dynamically forward inbound traffic to.



Figure 14-13: Port triggering and forwarding.

## Router Settings

Most routers available today can be configured for wired and wireless networks. Depending on the router installation, there are a number of settings that can be configured to ensure connectivity, security, and access.

<b>Setting</b>	<b>Description</b>
Basics	Basic settings apply to both wired and wireless routers and can include the ability to: <ul style="list-style-type: none"> <li>Secure your router or access point administration interface.</li> <li>Change default administrator passwords and user names used to access the router administration page.</li> <li>Disable remote administration.</li> <li>Secure/disable the reset switch/function.</li> <li>Change the default SNMP parameter.</li> <li>Regularly upgrade the Wi-Fi router firmware to ensure you have the latest security patches and critical fixes.</li> </ul>
SSID	When installing a wireless router, change the default Service Set Identifier (SSID) and verify that you are not broadcasting out to the network.
MAC filtering	Apply MAC address filtering to both wired and wireless routers. By configuring a wireless access point (WAP) to filter MAC addresses, you can control which wireless clients may join your network.
Channels	Change the default channel on wireless routers. By changing the router channel, you can optimize data transmission and reduce interference with other routers in close proximity. If your router is dual channel, then you can easily change from the default channel to the other channel available. To help determine what channel is not being used, there are utilities available that can scan the local area and display used channels. This can be very helpful in choosing a different less-used channel for your router.
DHCP	Depending on the needs of your network, turn on DHCP on both wired and wireless routers to automatically connect and assign an IP address, or turn it off and enter a static IP address.

## Router Firmware

As with other devices, you might need to update the firmware in your wireless router or WAP. This might be to take advantage of new features, fix security holes, or patch problems.

Another upgrade to the firmware that some people do is to upgrade to a firmware that is not provided by the wireless router manufacturer. These are firmware modifications created by groups that change the functionality of the wireless router. The OpenWrt open source firmware is customizable, or you can download one of the firmware implementations that are already packaged and ready to install. One example of firmware based on OpenWrt that is ready to use is DD-WRT. This works well with Linksys wireless routers.



**Note:** For more information about DD-WRT, visit <https://www.dd-wrt.com/site>.

## UPnP

*Universal Plug and Play (UPnP)* is built into many wireless routers to enable computers, printers, and other Wi-Fi-enabled devices to be easily discoverable by the router. While this might make connection easy for your users, it also makes it easy for hackers to discover and take advantage of UPnP discoverability features as well. The hackers might disable devices or even take over your

devices and network. You should strongly consider disabling UPnP on your routers or make it available only inside your LAN and not outside of your network.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Install and Configure SOHO Networks.

# ACTIVITY 14-8

## Installing and Configuring a SOHO Network

### Before You Begin

In this activity, you will use a simulation so the changes you make in the activity do not affect any devices on your physical network.

### Scenario

You will be helping to set up several SOHO networks for satellite locations. Before you go out into the various locations, you want to practice configuring the wireless router. You found a simulator online that uses the same model wireless router you will be installing in the satellite offices.

1. Connect to the wireless router's configuration interface.
  - a) Open **Internet Explorer**.
  - b) In the **Address** bar, enter <http://ui.linksys.com>
  - c) From the list of routers, select the **E1200** link.
  - d) Select the **2.0.04/** link.
  - e) In the **Warning** message box, check the **Do not show me this again** check box and select **OK**.



**Note:** This website emulates a common router configuration interface. When working with a real device, you will typically connect to http://192.168.1.1 and be prompted to enter a user name and password. For a list of default user names and passwords by router, navigate to <http://www.routerpasswords.com>.
2. Set an SSID for your wireless network.
  - a) On the menu bar at the top of the page, select the **Wireless** tab.
  - b) If necessary, select **Manual**.
  - c) In the **Network Name (SSID)** text box, double-click and type **ap##**



**Note:** Because you are using an emulator, you can use all lowercase letters in the **Network Name (SSID)** text box.

  - d) Select **Save Settings** and, in the **Message from webpage** message box, select **OK**.
  - e) Select **Save Settings** again, and then select **Continue**.
3. Set WPA2 encryption with a passphrase.
  - a) Under the **Wireless** tab on the menu bar, select the **Wireless Security** link.
  - b) From the **Security Mode** drop-down list, select **WPA2 Personal**.
  - c) In the **Passphrase** text box, type **/Pass1234**
  - d) Select **Save Settings**, and then select **Continue**.
4. Configure the router's administration settings.
  - a) On the menu bar, select the **Administration** tab.
  - b) In the **Router Password** text box, double-click the existing password (represented by asterisks) and type **P@ssw0rd**
  - c) In the **Re-Enter to Confirm** text box, type the same password.
  - d) In the **Local Management Access** section, clear the **HTTP** check box and check the **HTTPS** check box.
  - e) In the **Local Management Access** section, for the **Access via Wireless** option, select **Disabled**.

- f) In the **Remote Management Access** section, verify that **Remote Management** is disabled.
  - g) At the bottom of the web page, select **Save Settings**.
  - h) On the **Your settings have been successfully saved** page, select **Continue**.
  - i) Close **Internet Explorer**.
-

## Summary

In this lesson, you identified many different network technologies. Networking is at the heart of any type of business. Without it, a business simply cannot function in today's world. It is your job to ensure that the networks behind the business are running properly and managed correctly.

**What experiences do you have in working with any of the networking technologies discussed in this lesson?**

**Do you have any experience working with SOHO networks? What do you expect to support in future job functions?**



**Note:** Check your CHOICE Course screen for opportunities to interact with your classmates, peers, and the larger CHOICE online community about the topics covered in this course or other topics you are interested in. From the Course screen you can also access available resources for a more continuous learning experience.

# 15

# Supporting Mobile Digital Devices

**Lesson Time:** 1 hour, 15 minutes

## Lesson Objectives

In this lesson, you will support mobile digital devices. You will:

- Install and configure exterior laptop components.
- Install and configure interior laptop components.
- Explain characteristics of various types of other mobile devices.
- Compare and contrast accessories and ports of other mobile devices.
- Install and configure basic mobile device network connectivity and email.
- Identify methods and best practices for synchronizing mobile devices.
- Troubleshoot and repair common mobile device hardware issues.

## Lesson Introduction

In the previous lessons, the focus has been on installing hardware components, operating systems, and establishing network connectivity. As an A+ technician, you will also require a robust knowledge of portable computing principles. In this lesson, the focus will be on laptop, tablet, and smartphone devices and how they differ from desktop systems.

Mobile devices are everywhere today. Because of their portability and powerful computing capabilities they are prominent in most workplaces. So, as a certified A+ technician, you will be expected to configure, maintain, and troubleshoot mobile computing devices. With the proper information and the right skills, you will be ready to support these devices as efficiently as you support their desktop counterparts.

# TOPIC A

## Install and Configure Exterior Laptop Components

In this lesson, you will support mobile digital devices. One of the most prevalent mobile devices in today's workplaces has to be the laptop computer. As an A+ technician, you will be asked to configure and maintain laptops for yourself and other users. In this topic, you will install and configure exterior laptop components.

### Laptops

A *laptop* is a complete computer system that is small, compact, lightweight, and portable. All laptops have specialized hardware designed especially for use in a smaller portable system, use standard operating systems, can run on battery or AC power, and can connect to other devices. Laptops and their components can vary by the following factors:

- Size of the device. Smaller models are referred to as notebooks or sub-notebooks and typically have fewer features.
- Display size, quality, and technology.
- Keyboard size, number of keys, and additional options.
- Pointing device used.
- Power supply type.
- Battery type used.
- Length of battery support time.
- How long it takes to recharge the battery.
- Power cord connection and power source options.
- Docking solutions.
- Connections for external peripherals.
- The power button can be located inside or outside of the closed case. It is more often located inside so that it is not accidentally turned on when it is in the user's briefcase or being transported in some other bag.
- Bays or connections for additional drives such as optical drives.



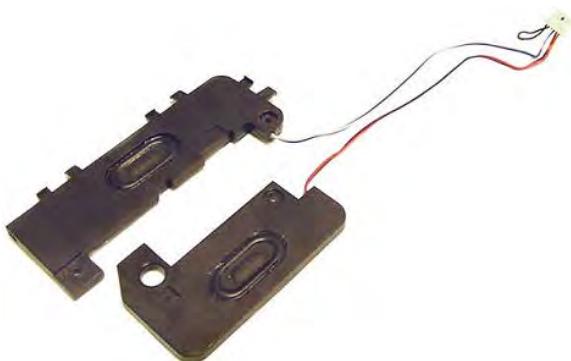
**Figure 15–1:** A laptop.

## Laptop Hardware Components

A laptop has many different hardware components that each have unique characteristics and features.

Component	Description
Keyboard	The keyboard is an integrated component on a laptop. Laptop keyboards often have fewer keys than external keyboards, with some keys used in combination with an <b>Fn</b> key to access additional functions. Some laptop keyboards can be removed or turned around to make the laptop function as a tablet.



<b>Component</b>	<b>Description</b>
Touchpad	A touchpad is a small, touch-sensitive pad where you run your finger across the surface to send electronic signals to the computer to control the pointer on the screen. Touchpads can have buttons like a mouse or trackball, or the touchpad can be configured to detect finger taps on its surface and process those signals like a mouse button.
	
Frames	The <i>plastics</i> or aluminum frames are the hard surfaces that cover the internal components of the laptop. They are typically secured together using small screws or pressure tabs.
	
Speaker	The speakers are located in a number of locations depending on the style and manufacturer of the laptop. Newer model laptop speakers are just as powerful as the desktop versions.
	

<b>Component</b>	<b>Description</b>
Battery	<p>The battery designed for laptops is rechargeable and can easily be removed or replaced. Most batteries will last between one and six hours per charge while extended life batteries have a wide range of limitations based on the manufacturer and what the user is doing with the laptop. Programs that require more computing power and screen updates such as multimedia applications are likely to deplete the battery faster than working on simple word processing documents. Some laptops offer extra battery packs that can be inserted in place of other removable devices, such as optical drives, allowing users to easily reconfigure their laptops for various travel and working situations. Rechargeable batteries are used in most portable computing devices. They are usually packaged in a battery pack.</p> <p>Before replacing a laptop battery you should verify what the system requirements are. New batteries must be compatible with the system.</p>



DC jack	The direct current (DC) jack on a laptop provides power through the power cord. Most laptop DC jacks are specific to the manufacturer and even the laptop model, so make sure to check the documentation for power requirements and compatible power cords.
---------	---



<b>Component</b>	<b>Description</b>
Screen	The screen is the visual display of a laptop and is typically hinged at the bottom and swings down to form the cover for the laptop. It latches to the body of the computer to secure it for transport.
 <p>Some laptops have touch screens, allowing users to control onscreen objects and use onscreen keyboards.</p>	



**Note:** For additional information, check out the LearnTO Replace a Laptop Battery presentation in the LearnTOs for this course on your CHOICE Course screen.

## Guidelines for General Laptop Support



**Note:** All of the Guidelines for this lesson are available as checklists from the **Checklist** tile on the CHOICE Course screen.

There are some general guidelines that can be helpful when supporting laptops within the workplace. With the increased use of smaller laptop devices, you should be aware of the issues and best practices applied when working with the hardware components:

- Verify that there are adequate cooling methods installed and used. Overheating is a serious issue when operating laptops.
- Be aware of the device's warranty restrictions and guidelines. You never want to break a warranty by opening the case or replacing an integrated component that may have been fully covered by a warranty.
- Be careful of the wires that pass through the hinges of a laptop. They can be easily damaged when replacing a display or screen.

## External Laptop Expansion Options

External laptop expansion is provided by ports on the laptop and adapters connected to those ports. The ports usually found on laptops are:

- USB
  - Usually 2 USB ports
  - Some include eSATA in combination with USB
- Thunderbolt
  - Typically found on Mac laptops
- Ethernet
- An external monitor port

- DisplayPort
- HDMI

Many laptops no longer include an optical drive, so users will need to either connect through a network to a shared optical drive, or use an external optical drive that connects to the USB port, commonly known as a USB optical drive. In addition to connecting USB devices, the USB port can be used with adapters to enable connection to other features that aren't built into a particular laptop. Adapters include:

- USB to RJ-45 *dongle*
- USB to Wi-Fi dongle
- USB to Bluetooth

## Express Cards

*ExpressCards* are mobile expansion cards designed by the PCMCIA to replace traditional PC Cards. The ExpressCard slot on mobile devices provides PCI Express and USB connectivity. The two form factors available for the ExpressCard are the ExpressCard/34 (34 mm wide) and ExpressCard/54 (54 mm wide).

ExpressCard slots are a bit smaller than the PC Card slots and are usually located on the side of the laptop. ExpressCards can be used to provide many additional functions such as wireless network access, USB ports, and others.

The ExpressCard technology has many advantages over the PC Card, including reduced voltage usage, increased bandwidth, and a maximum throughput of 2.0 Gbps through PCI Express and 480 Mbps through USB. Some manufacturers are providing both PC Card slots along with ExpressCard slots to comply with both standards.

## Special Function Keys

Laptops are all so different and the features can vary based on the manufacturer. A common feature included in most devices are the special function keys. The specific keys available will depend on the size, shape, and overall design of the laptop but most systems will provide the basic keys. The special keys are typically positioned horizontally along the top length of the keyboard and allow users to launch operating system commands, and manage laptop settings from their keyboard in many ways:

- Switching between single and dual displays.
- Turning the wireless on and off.
- Changing the volume of the speakers.
- Managing the screen brightness.
- Turning the Bluetooth® on and off.
- Configuring the keyboard backlight.
- Turning the cellular function on and off.
- Turning the touch pad on and off.
- Changing the screen orientation.
- Enabling and disabling GPS.
- Accessing media options such as fast forward and rewind.
- Turning airplane mode on and off.



**Note:** The function keys vary between laptops. Not every laptop will have all of these special functions and other laptops might have additional special functions. The feature on the key printed in white is the default feature.



*Figure 15-2: Special function keys.*

## Laptop Docking Solutions

One of the most attractive features of laptops is that they are so portable. They can be docked and undocked quickly for transport. Docking solutions provide users with a power source and full size peripherals with a similar feel to a full size desktop computer. There are a few different docking options depending on the specific needs of the user.

Docking Solution	Description
Docking station	<p>For laptops, a <i>docking station</i> is used when a laptop computer replaces a desktop computer. This technology is rarely used today and is considered to be legacy hardware. The laptop is connected to the docking station through a docking port located on the back or bottom of the laptop. Docking stations typically extend the capabilities of the laptop by providing additional interfaces for the laptop. In addition, there are often slots for desktop PCI or ISA expansion cards, drive bays for additional mass storage devices, and possibly additional ports and connectors, such as extra USB or wireless connections.</p> <p>For other mobile devices such as tablets, docking stations are experiencing a resurgence. These docking stations can include HD ports, Gigabit Ethernet ports, USB 3.0 ports, audio out, and mini-display ports.</p>
Port replicator	<p>A <i>port replicator</i> is a scaled-down version of a docking station that presents the interfaces that the laptop already has. It contains connections for the standard ports, such as power, keyboard, mouse, and display, but it generally does not support additional expansion cards or drive bays, although some port replicators will contain extra USB or wireless connections.</p>
Media/accessory bay	<p>Some portable computing devices offer media/accessory bays to allow a user to expand the functionality of the device. Such bays often accept optical drives, secondary hard drives, or secondary batteries. These bays are typically proprietary and the accessories for the bays must be ordered directly from the device manufacturer. Most laptops today will utilize wireless peripherals and USB attached drives, so USB hubs and media bays are not used as much anymore.</p>

## Laptop Locks

Because laptops are so portable, they are easily lost or stolen. Another feature of laptops is the ability to attach a physical laptop lock or a cable lock. A physical cable lock attaches to the laptop using one of the compatible slots. The cable is then secured around a permanent object. The lock is usually accessed using a combination or a key. Depending on the lock, it may attach to the VGA or printer port. The locks come with special screws that secure the lock in place. The Kensington lock is a cable lock that inserts into a specifically designed port on the laptop. After the Kensington cable was released, laptop manufacturers named the special port the Kensington lock port.



Figure 15–3: Kensington laptop locks.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Install and Configure External Laptop Components.

# ACTIVITY 15-1

## Working with Exterior Laptop Components

### Scenario

In this activity, you will examine a laptop and identify its components.

1. Examine a laptop and identify the external components such as the keyboard, display, track point, or touch pad.
2. What special function keys does the laptop have?  
Try out the various special function keys. Some are used in combination with an **Fn** key.
3. Connect the laptop to a suitable stationary object using a cable lock.
4. What expansion options are available on the laptop?  
If your instructor has expansion cards available, install one in the appropriate expansion slot.
5. If the laptop has a media card reader slot, insert an appropriate media card and read data from or write data to the media card.
6. Connect external peripherals.
  - a) Connect an external mouse and keyboard to the laptop.



**Note:** Users often use wireless mouse and keyboard with a receiver plugged into USB ports on the laptop.

- b) Connect an external display to the laptop.

Depending on the port available on the laptop and the connection options on the monitor, you might need to use a cable with different connectors on each end, such as a DVI to HDMI or VGA to DVI cable.

- c) Verify that the peripherals work properly.
- d) Press **Windows+P** and try out the various **Project** options.



**Note:** An alternative to pressing **Windows+P** is from the **Charms** bar, select **Devices→Project** to display the **Project** pane.

# TOPIC B

## Install and Configure Interior Laptop Components

In the last topic, you installed and configured external laptop components. There will be situations where dealing with external components won't completely address the issues or problems a user is having with his or her laptop. In this topic, you will install and configure interior laptop components.

### Interior Laptop Components

The internal components of a laptop are similar to full size desktop computers except that they are much smaller and more compact to fit inside the case.

<b>Component</b>	<b>Description</b>
Motherboard	<p>From a technical viewpoint, a laptop system board is very similar to the system boards found in desktop systems. The main difference is that the components are often compressed to squeeze into a smaller space. Other major differences include reduced power consumption and more common integration of items such as video, sound, USB/FireWire®, wired and wireless network connections, and so on. Laptop system boards often contain power management and throttling options to help in preserving battery life. These features allow for the machine to adjust the power to the processor and other components as necessary.</p> <p>The integration of all the features on the motherboard limits customization options and necessitates replacement of the entire board when one of the integrated features fails. However, you may be able to use an alternative slot or port and add an adapter card or an external device to substitute for the failed integrated component.</p>
CPU	<p>Laptop CPUs are designed to use less power and to generate less heat than desktop CPUs, and often are designed to be used without a CPU fan, which, again, saves on size and weight, as well as reducing power consumption to maximize battery life. CPUs can be surface-mounted devices, soldered directly to the motherboard, or attached via a socket on the motherboard. CPUs that are soldered onto the motherboard are not replaceable. It is best to determine how a laptop CPU is attached before trying to replace it.</p>

Component	Description
Storage drive	<p>Portable computer drives are specially designed to fit in portable computers. Drives can be unique to a manufacturer and sometimes even to the computer model. All laptop computers have an internal storage drive.</p> <ul style="list-style-type: none"> <li>• Hard drives come in three main form factors: 1.8 inch, 2.5 inch, and 3.5 inch. The 3.5 inch HDD tends to be too big for laptops, so in most laptops the hard drives are 1.8 or 2.5 inches. The smaller size drives tend to run at slower speeds than the 3.5 inch desktop HDDs.</li> <li>• Newer laptops come with SSDs and hybrid drives, typically with the same form factor as HDD but cooler, faster, and better able to handle rough movement.</li> <li>• Laptops may also include a combination of two or three of these different drive types.</li> </ul> <p>Some internal drives are difficult to remove and require dismantling of the computer. Others have a slide lock to unlock them from the case, so that you can slide the drive out. If it is too difficult to remove the internal drive from the notebook you are working on, then you might consider using alternate storage drive solutions such as USB or FireWire drives that can be connected externally.</p>
Memory	<p>Portable devices use memory that was specifically designed for those devices. Since it is not produced in as high quantities as desktop memory, it tends to be more expensive. While some laptops use <i>Small Outline Dual In-line Memory Modules (SODIMMs)</i>, which are about half the size of standard desktop DIMMs, or <i>MicroDIMMs</i>, many require non-standard proprietary memory that must be ordered from the manufacturer. Other portable computing devices and some notebooks use flash memory modules rather than regular RAM.</p> <p>Be sure to check the documentation for your device so that you purchase the correct type of memory. Before you replace the memory in a laptop, you must verify that it is compatible with the system. Always check the manufacturer's documentation or website to verify the form factor and types of compatible memory.</p>
	 <p><b>Note:</b> Several memory websites provide a small program you can install that will tell you the type of memory running in a laptop. You also can find the correct memory by providing information about the manufacturer and model number at websites like <a href="http://www.crucial.com">www.crucial.com</a>.</p>
Optical drive	<p>Optical drives in laptops are similar in function to the full size desktop models except that they are small and more compact. When replacing a drive, the first thing to do is check with the manufacturer to verify that it can be replaced and with what type of drive. You need to make sure that the drive you install is compatible with the laptop.</p>
Wireless card	<p>In some laptops, the wireless card and video card can be upgraded to improve performance. However, replacement is dependent on whether the card is an integrated component of the mobile system board. In this case, you cannot upgrade or replace the card. If the card is independent of the system board, then you should refer to the manufacturer's documentation to verify what components can be replaced and upgraded. Some components may be covered under a system's warranty, so refer to the manufacturer's policies to determine what can be upgraded without breaking the warranty guidelines.</p>

<b>Component</b>	<b>Description</b>
Webcam	Webcams can usually create still images as well as video. Some cameras have 1080p high definition resolution. External cameras are often connected via USB. Whether they are internal or external, webcams include software that provides options to manipulate the image/video stream.
Microphone	Microphones enable you to participate in Internet-based conversations such as webinars and Skype. Some mics are part of a headset unit while others may be inserted in the audio output port (the microphone extends up from the port and can flex for best position). Also, some mics have a noise-cancelling feature.

	<b>Caution:</b> Only open a laptop to access internal components if it is no longer under warranty or if you are an authorized technician for the laptop brand.
	<b>Note:</b> For additional information, check out the LearnTO <b>Install RAM in a Laptop</b> and LearnTO <b>Replace a Laptop Battery</b> presentations in the LearnTOs for this course on your CHOICE Course screen.

## Laptop Memory Package Specifications

The following table lists some of the technical specifications for laptop memory packages.

<b>Memory Package</b>	<b>Description</b>
SODIMM	<p>Small Outline Dual Inline Memory Module.</p> <p>Used in some notebook systems and Apple® iMac® systems.</p> <p>Measures about 2 inches by 1 inch and has 144 pins.</p> <p>Capacity ranges from 16 to 256 MB per module.</p>
MicroDIMM	<p>Micro Dual Inline Memory Module.</p> <p>Used in small, sub-compact notebooks.</p> <p>Measures about 1.5 inches long and has 144 pins.</p> <p>Capacity ranges from 512 MB to 1 GB.</p>

## Types of Laptop Displays

Most laptops use *TFT (Thin Film Transistor)* displays. These are usually either TN (Twisted Nematic) or IPS (In-Plane Switching) displays. These all fall under the category of LCD displays. Some newer laptops leverage the OLED display technology to provide higher quality images.

Some laptops have removable screens or screens that can be rotated. This allows the laptop to also function as a tablet. These screens typically are also touch screens so that when they are being used as a tablet, because the keyboard and touch pad are not available, the user needs a method of interacting with the displayed content.

## Laptop Display Components

Within the display unit of a laptop, there are several specialized components with unique functions.

Component	Description
Inverter	An <i>inverter</i> is used to convert DC power to AC power for the display. When an inverter fails, depending on the laptop model, it may be appropriate to simply replace the display rather than replace the inverter. Replacement of the inverter requires an exact match, both electrically and mechanically (connectors, size/shape, and mounting).
Backlight	The liquid crystals in the display are unlit and require a light source to make them visible. This can be edge lighting, but more likely, a backlight is used. The backlight is typically provided by fluorescent or LED lighting. A <i>backlight</i> is the typical form of illumination used in a full-sized LCD display. Backlights differ from frontlights because they illuminate the LCD from the side or back, where frontlights are in front of the LCD. <i>Frontlights</i> are used in small displays such as on MP3 players to increase readability in low light conditions. Edge lighting is another common method of lighting the LCD display.
Wi-Fi antenna	The Wi-Fi antenna is typically placed inside the display section of the laptop. The cables are run along the sides of the display unit and connect to the network card inside the main unit of the laptop. It sends and receives wireless signals and transmissions to the WAP.
Webcam	Most laptops have a built-in webcam, built into the plastics above the display.
Microphone	Most laptops also have a built-in microphone. The location of the microphone varies between laptops, but is usually located somewhere in the plastics around the display, often next to the webcam.
Digitizer	When a laptop, smartphone, or tablet has a touchscreen display, it uses a digitizer. The <i>digitizer</i> is sandwiched between a layer of glass and the LCD display. Analog signals are created when you tap or swipe the surface of the display. The digitizer is connected to the laptop with a flexible digitizer cable. A grid of sensors is activated when you tap or swipe the screen. The information from the sensors is sent through the digitizer cable to a circuit that converts the analog signal to a digital signal.



**Note:** On screen keyboards and any other touch action uses the digitizer.

## Mini-PCIe Cards

Laptop systems offer many different options to expand system functionality.

Some portable systems include a PCI Express Mini Card (Mini-PCIe) slot. A *Mini-PCIe* card is an extremely small expansion card, often just a few centimeters in length. Unlike PC Cards, Mini-PCIe cards are internal and are installed by the computer manufacturer. Mini-PCIe cards are most often used to increase communication abilities by providing network adapters or modems and support various connections and buses:

- USB.
- Diagnostic wiring that provides LED for wireless network connectivity.
- System management Bus (SmBus).

## Laptop Power Supplies and Batteries

Laptops can use either AC power sources (alternating current from an electrical outlet) or DC power sources (direct current from a battery). While the laptop is in its portable state, it uses

batteries. When the device is used as a desktop computer or peripheral, it can use either batteries or AC power.

AC power connectors vary from device to device. It is important that a laptop not be used with a power cord other than the one provided by the manufacturer. When the laptop is not being used as a portable device, it is usually plugged in using the AC power cord that matches the computer. The battery is also recharged through this connection.

## Auto-Switching and Fixed Input Power Supplies

Power supplies with voltage selector switches are called fixed-input power supplies. The voltage selector switches generally have two settings—for example, 220 and 110—depending on the manufacturer. If you set the switch to a higher voltage than supplied by the power source, the system will not receive enough power and will not function properly. However, if you set the switch to a lower setting than supplied by the power source—for example, if you set the switch to 110V while connected to a 220V outlet—you run the risk of burning out the power supply, damaging system components, or more seriously, creating a fire or electrocution hazard.

Auto-switching power supplies do not have a manual voltage switch, but detect the voltage level supplied by the outlet and set themselves to the correct voltage automatically. This can be convenient and safe for people who travel to various countries with portable computers.

## Laptop Cooling Considerations

Heat can be a considerable problem with laptops due to their compact size and integrated design. The components are all within close proximity and can generate a lot of heat. There are a number of cooling methods and considerations used to keep the devices within a safe heat range for operation:

- Laptop CPUs are engineered to draw less power and thus run cooler than their similarly rated desktop counterparts.
- Fans are used to move the hot air out from the inside of the laptop case.
- Limit the use of the laptop battery as much as possible. The battery itself can be a heat source.
- Laptop cooling pads are accessories that are designed to sit under the laptop to protect a user from getting a burn from a device overheating. The cooler is placed underneath the laptop to move the air away from the device.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Install and Configure Interior Laptop Components.

## ACTIVITY 15-2

### Installing Interior Laptop Components (Optional)

#### Scenario

You have a spare laptop in your work area that is the same model as the laptops you support for the users in your organization. In order to make sure you know how to access internal laptop components, you decide to locate, remove, and replace various internal components on the laptop.

---

1. Remove and replace the memory module.
    - a) Locate the memory module in the laptop.
    - b) Remove the cover from over the memory.
    - c) Remove the memory.
    - d) Reinstall the memory.
    - e) Replace the cover over the memory.
  2. Remove and replace the hard drive.
    - a) Locate the hard drive in the laptop.
    - b) Remove the cover from over the hard drive.
    - c) If necessary, release any locking clips and remove any screws.  
Some laptops locate the hard disk inside a drive attachment bracket or cage.
    - d) Disconnect the cable from the hard drive.
    - e) Carefully remove the hard drive.
    - f) Reinstall the hard drive.
    - g) Replace the cover over the hard drive.
  3. Following the manufacturer's instructions or your instructor's guidance, remove the outer case from the laptop.
  4. Remove and replace the fans.
  5. Disconnect and reconnect the keyboard connector.
  6. Disconnect and reconnect the touch pad connector.
  7. Reassemble the laptop.
-

# TOPIC C

## Other Mobile Devices

Up until this point in the course, your primary focus has been on the more traditional system hardware components and laptop technologies. In this topic, you will dive into the mobile computing realm and will take a closer look at the capabilities and technologies that they employ to provide optimal performance.

Not only has mobile technology reached a new level of performance and portability, but also the use of these devices is on the rise every day. As a certified A+ technician, you will be expected to understand how these devices work and how they should be deployed within the workplace.

### Tablets

Mobile devices that fall into the tablet PC category range from larger tablets that look like a traditional laptop but have a touch screen to small notebook-sized mobile devices that operate similarly to a smartphone, but are a bit larger and have more computing power. Operating systems found on tablets include:

- iOS
- Android
- Windows 7
- Windows 8
- Windows 8.1
- Windows 8.1 RT
- Windows 10
- Blackberry OS

### Tablets vs. Laptops

Laptops and tablets both offer a wide variety of hardware features that allow for better portability and ease of use, but there are also some major differences that should be considered.

<i>Characteristic</i>	<i>Laptops</i>	<i>Tablets</i>
Repairs	The hardware components of a laptop can be fixed and replaced when issues arise. This is still fairly common with newer laptops as well.	There are few field-serviceable parts in a tablet. What makes it difficult to repair a tablet is that the parts are soldered and not socketed. When something breaks, in most cases, the entire tablet needs to be replaced.
Upgrades	The hard drive and central processing unit (CPU) can be upgraded, if needed, to meet OS requirements or to add more functionality to the laptop.	Tablets are not typically upgradeable, unless it is software-related. The storage components cannot be upgraded. What makes it difficult to upgrade a tablet is that the parts are soldered and not socketed.

<b>Characteristic</b>	<b>Laptops</b>	<b>Tablets</b>
Touch interface	Many laptops do not come with a touch interface component. You can purchase specific laptops that have the feature, but it is not a feature of all laptops.	All tablets come with touch interface technology. The touch technology allows the user to interact with the tablet. It is also the primary input method used for tablets. Tablets utilize a touch interface that allows interaction between the user and the OS.  <i>Multitouch</i> is the technology used on the surface of the touch screen on tablets and other mobile devices. The technology can recognize more than one contact on the surface at one time. This allows users to pinch and zoom the screen to make images or text larger and smaller.
Storage	Many laptops have a mobile version of a traditional mechanical hard drive that has a higher storage capacity than solid state drives (SSDs). However, as the price of SSD drives has come down, SSD drives are starting to show up in more laptops.	Most tablets will come equipped with SSDs. Because of the space limitations and the portability of the tablet computers, SSDs make sense. They have no moving parts to maintain and provides a more stable mechanical design. The SSDs are made up of a number of flash chips that can retrieve data much faster than a standard hard drive that needs to start a motor and move the arm to read data.
OS	Laptops can run a number of different operating systems including versions from Microsoft, Linux, and UNIX.	Tablets can generally only run the OS that the device was manufactured to run. The actual OS will depend on the specific tablet due to the CPU architecture versus the ARM architecture.



**Note:** For additional information, check out the LearnTO **Identify Laptops vs. Tablets** presentation in the LearnTOs for this course on your CHOICE Course screen.

## Smartphones

New smartphones are emerging almost every day. The market is expanding and demand for powerful mobile devices has never been higher. While Android and iOS dominate the smartphone device marketplace, there are many other technologies and devices available. The most popular devices used in the marketplace include:

- iPhones®.
- Android smartphones such as Samsung™ Galaxy S® 6 Edge, MOTOROLA® DROID Turbo, and HTC One™ M9.
- Windows smartphones.

## Wearable Devices

A variety of wearable devices have been created that work with smartphones or as standalone devices. These take mobility one step further than smartphones and tablets by being hands-free devices.

<b>Wearable Device</b>	<b>Description</b>
Smart watches	<p>Smart watches look like large wrist watches. In addition to showing the time like a traditional wrist watch, they sync with your smartphone or tablet to let you know when you receive a phone call or text message, alert you with meeting reminders, and have apps designed for the smart watch. The smart watch connects to your mobile device using a Bluetooth connection, so must be within range of the phone or tablet.</p> <p>The screen is created from strengthened glass that enables it to stand up to dust and physical contact of every day wear and use. The display might use OLED, AMOLED, LCD, or black and white screens using E-Ink or E-Paper making them more visible in bright sunlight. Typically, the smart watch uses a touch screen, but will probably also have physical buttons.</p> <p>Some smart watches include features such as:</p> <ul style="list-style-type: none"> <li>• A remote shutter control for the camera on the phone or tablet.</li> <li>• Apps to access the music stored on the smartphone, or enough internal memory to store music without access to your smart phone.</li> <li>• An alert when you are out of Bluetooth range with your smartphone or tablet.</li> <li>• Voice commands that enable you to search the Internet, perform hands-free phone calls, create and send or receive text messages, and more.</li> <li>• Fitness monitor capabilities.</li> </ul>
Fitness monitors	<p>Fitness monitors are wearable devices that enable the user to track activity and monitor health and fitness measurements. Fitness monitors might be worn on the wrist or ankle, or be attached to the user's clothing.</p> <p>Features of fitness monitors might include:</p> <ul style="list-style-type: none"> <li>• Pedometer to count the steps taken during a specified period of time.</li> <li>• Accelerometer to measure the intensity of the workout.</li> <li>• A heart rate monitor.</li> <li>• A blood pressure monitor.</li> <li>• A calculation of the number of calories burned.</li> </ul>
Glasses and headsets	<p>Glasses that connect to smartphones or tablets via Bluetooth connections offer many of the same features as smart watches. Some of these also include the ability to take and store still and video images within the glasses device.</p> <p>Smartphone headsets enable a user to make and receive hands-free phone calls. This is important when driving, as many states fine drivers for the dangerous practice of using a cell phone while driving. These might connect to the smartphone through the headphone jack, but more often they connect using Bluetooth connectivity.</p>

## Phablets

A phablet is a cross between a smartphone and a tablet. It is usually simply a very large smartphone.

## e-Readers

An e-reader is essentially a tablet device, often with many of the same features as a tablet. The touchscreens are sized to mimic the size of a standard paperback or hardcover book. The screen is often optimized for reading in bright light. It has internal storage to store book content, and often allows you to store other files and even games. It connects to networks using Wi-Fi so you can download additional content. Like most tablets and smartphones, it uses a USB cable to charge the device. The battery in the device is designed to allow the user to read for several hours before needing to charge the device again.

Many e-readers also include a web browser, games, and PDF reader. Some also include the ability to connect to the Internet over a cellular connection.

Users can purchase content from retailers such as Amazon. Many libraries also have eBooks available to lend to users.

## Smart Cameras

A smart camera is any camera that includes Wi-Fi, NFC, and GPS capabilities. By having Wi-Fi built into the camera, the user can easily share the photos with social media sites or upload photos to another device such as a computer or smartphone. The GPS feature adds digital data to the image, tagging the image with the coordinates of the location where the photo was taken.

Other features of smart cameras can include built-in processors to improve the image quality and select the appropriate camera settings automatically based on lighting and other factors in the scene. Images are typically saved to a memory card, but also might be saved to internal memory built into the camera.

## GPS

GPS (Global Positioning System) devices use multiple satellites to pinpoint the user's exact location. Different GPS devices are designed for different functions. Some are designed for use in cars, and include maps that only allow the user to see roads. Others are designed for hikers, runners, and even dogs, who are often not on roads.

Smartphones include GPS functionality. This allows the user to use the phone as a navigation device. It also allows users to use apps on other devices to find a lost phone, or for law enforcement to try to locate a missing person who is carrying a GPS equipped phone.

For car GPS units, the maps are typically stored in the GPS unit so that you don't need a cellular connection to the device. Most GPS devices now include lifetime updates to the maps. Newer GPS units receive current information about road incidents such as construction or accidents so that users might elect to choose another route to avoid the incident. Older GPS devices came with the maps stored in the device. The maps could only be updated with corrections and new roads by purchasing new maps.



**Note:** When using a GPS to navigate while driving, make sure to also use common sense and not just go where the GPS indicates. Some maps might be out-of-date or poorly created, and send you into a body of water or over train tracks where there is no crossing.

# ACTIVITY 15-3

## Identifying Mobile Devices and Features

### Before You Begin

Your instructor might ask you to share any mobile devices you have with your classmates.

### Scenario

The sales team is a very mobile population in your organization. You want to be prepared to assist those users with the vast array of mobile devices they use. You want to examine how these devices work in order to identify what each device is capable of doing.

1. Examine an iOS device, and examine an Android device.
2. Compare the interfaces and settings, and share your findings with the rest of the class.
3. Examine a GPS device. This might be a portable device, one designed for a car, or a smartphone app.
4. Examine an e-Reader device. This might be a portable device or a smartphone app.
5. Examine a tablet and identify the features of the tablet. The tablet might run the Windows, Android, or iOS operating system.
6. Examine a wearable device and identify the features and functions of the device.

# TOPIC D

## Mobile Device Accessories and Ports

Mobile devices gain much of their functionality by being able to connect to the user's regular computer. By making the files available on the mobile device, they can continue working on the files from a mobile device. Being able to connect the mobile device back to the computer might require additional accessories. In this topic, you will examine the connection types and accessories used for mobile devices.

### Connection Types

Mobile devices have a variety of connection types. Some are physical ports and some are logical ports. Some of the connection types you might encounter on mobile devices include:

- NFC (near field communication).
- Proprietary, vendor-specific ports for power and communication between the mobile device and other computers and mobile devices.
- Micro USB or Mini USB ports.
- Lightning port on Apple products.
- Bluetooth connections.
- Infrared connections.
- Hotspot or tethering to enable devices to connect to the Internet through another cellphone's or other mobile device's Internet connection.

### Accessories

Mobile device accessories often take up a larger space in retail stores than the mobile devices themselves. The following table includes some of the accessories users like to use with their mobile devices.

<b>Accessory</b>	<b>Description</b>
Headsets	Mobile device headsets can be simple earphones with a microphone boom, or they might be Bluetooth enabled devices that clip to one ear. The headset usually has a method of answering calls for mobile phones built into the headset.
Speakers	Speakers for mobile devices might use a headphone jack built into the device, or they might use Bluetooth connections.
Game pads	Game pads that can connect wirelessly to the mobile device might be used to play games or navigate through apps.
Docking stations	Mobile devices need to have their batteries charged. Many users use a docking station that also has speakers built into it and acts as a music player and an alarm clock. Some docking stations also enable a mobile device to connect to a home theater system, so music and movies stored on the mobile device can be displayed on a large screen and heard through the home theater speakers. This device is usually specific to the mobile device, such as an iPod dock.

<b>Accessory</b>	<b>Description</b>
Extra battery packs and chargers	Mobile devices often have battery life of several hours of use, but if you are traveling, you might end up using your mobile device more than you usually would. Having an extra battery pack that has been charged enables the user to switch out the depleted battery pack with the fully charged battery pack. When the user reaches a destination where the depleted battery pack can be recharged, it can be plugged in to the charger and begin re-energizing.
Protective covers and water proofing	Many smartphone users like to personalize their phone by placing it in a protective cover. These might be simple plastic cases for looks only, or they might be cases with extra thick padding. Some covers also provide water proof protection for the device. Screen protectors applied directly to the surface of the device help prevent scratches and might improve readability of the device in bright sunlight.
Credit card readers	For devices with the appropriate port, a credit card reader can be added to a tablet or smartphone. This enables mobile vendors, such as those at festivals or street vendors, to take credit card payments without having a network cable or phone line connected to the credit card reader.
Flash memory cards	Flash memory cards such as MicroSD cards are often paired with smartphones, tablets, and other mobile devices to store and transfer digital photos, videos, and movies.

## ACTIVITY 15-4

### Comparing Mobile Device Accessories and Ports

#### Scenario

You have a variety of mobile device accessories and cables. You need to determine which accessories and cables work with which of the mobile devices you have.

- 
1. Examine the ports available on the mobile devices you have.
    - a) Compare the ports between the mobile devices.
    - b) Determine which ports are common between the devices and which appear to be proprietary to the device.
  2. Examine the accessories available for mobile devices.
    - a) Determine which accessories will work with which of the mobile devices you have been given.
    - b) Determine if the accessories will work with multiple, different types of mobile devices, or if they work only with one specific mobile device.
-

# TOPIC E

## Mobile Device Connectivity

You have worked with various mobile devices so far in this course. In this topic, you will examine some of the features and methods those mobile devices use to connect to networks.

### Radio Firmware

*Radio firmware* in a mobile device contains an operating system that is separate from the end-user operating system (for example, Android or iOS). This other operating system controls all of the low-level timing-dependent functions of the mobile device, including USB, network, and GPS. The radio firmware is also referred to as the baseband runtime operating system (*baseband RTOS*).

### IMEI and IMSI Numbers

All wireless devices are assigned an *International Mobile Equipment Identity (IMEI) number*. This is usually printed on a label in the battery compartment on a mobile phone. If it is a sealed case, then the number will be found on the back or bottom of the device. You can also access the IMEI number by dialing \*#06# and it will display the IMEI on the device screen. Any phone connected to a GSM network (Global System for Mobile Communications) must have the IMEI number stored in the Equipment Identity Register (EIR) database. If a phone is reported as being lost or stolen, the IMEI number is marked to be invalid in the EIR.

The *International Mobile Subscriber Identity (IMSI) number* is a unique number identifying the subscriber. The number is stored on the SIM card in the format:

- Three-digit mobile country code.
- Two-digit mobile network code.
- Up to 10 digit mobile station identification number.



**Note:** The IMEI number identifies the device. The IMSI number identifies the subscriber.

### PRI, PRL, and Baseband Updates

*PRI (Preferred Roaming Index)* works in conjunction with *PRL (Preferred Roaming List)* to provide the best data/voice quality to the phone while roaming. The definition of roaming in this context means “while the device is moving from location to location,” not like five years ago when it was more prevalent to pay for roaming charges. PRL/PRI are often bundled together in one package and are sometimes included in Over the Air (OTA) updates.

Typically, your carrier and the phone manufacturer update the PRI, PRL, and baseband updates as they are needed. However, if you are traveling frequently to other regions than where your phone was originally set up for, you might need to update manually.

PRL is a database built by CDMA service carriers to indicate which radio bands should be used when connecting to a cell tower. The phone must have a valid PRL in order to roam outside the home network. The database contains two tables. The first is a System table that identifies the towers the phone can connect to and in which order they should be tried. The other is the Acquisition table, which identifies the radio frequencies to search for and in which areas to search for them. Updates are typically received over the air, but you might need to manually update if you are traveling.

The baseband updates are sent by the phone manufacturer. However, for customized ROMs, you will need to perform your own updates.

## Network Configuration Settings

Most smartphones have the functionality to connect to both a cellular network and a Wi-Fi network. Both modes allow web browsing, email, and a variety of push notifications from apps, and they can be enabled or disabled in the general settings for the device.

Cellular data networks are subscribed to through a mobile carrier such as Verizon and GSM networks. Users can subscribe to an appropriate wireless data plan that typically comes with usage and bandwidth restrictions based on the chosen plan. On the other hand, connecting to Wi-Fi networks provides users with unlimited use of network resources.

To connect to a Wi-Fi network, you must first verify that the mode is enabled on the smartphone. Once its enabled, the phone will automatically detect local area networks (LANs) within the discoverable range of the device. If the network is open to the public, then you can simply connect, but if the network has been secured, you will need the wireless password to establish a secure connection.

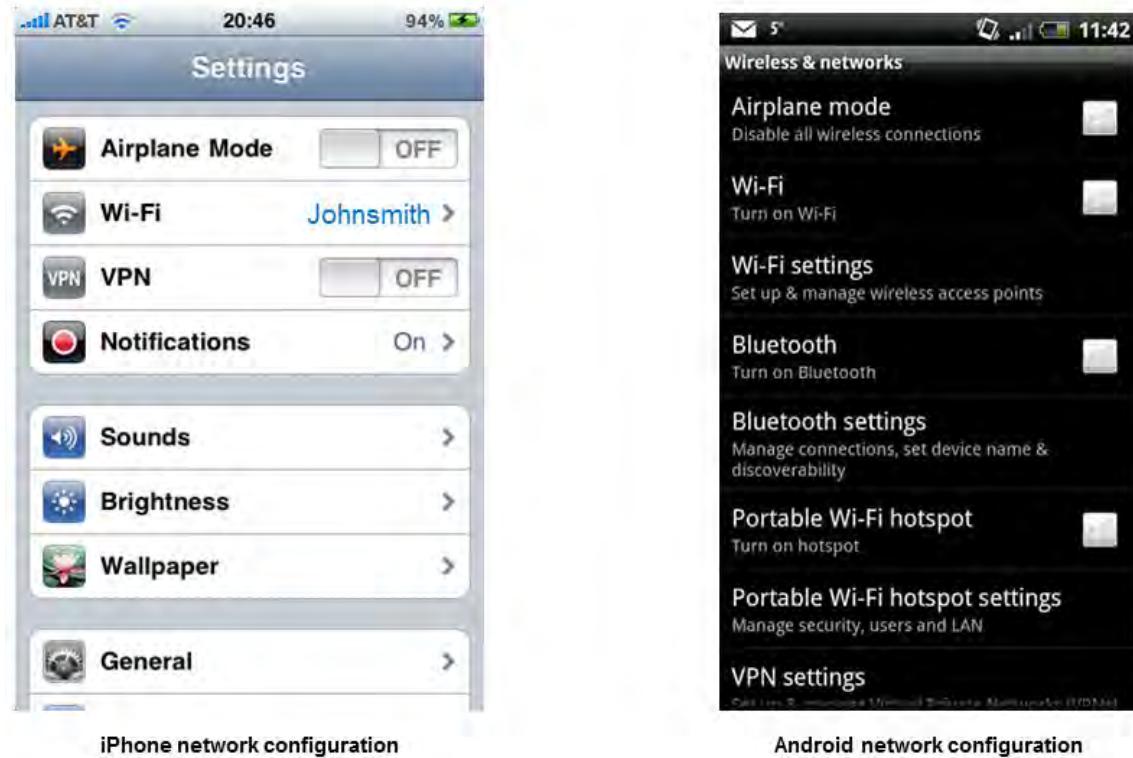


Figure 15-4: Smartphone network settings.

### Data Usage Conservation

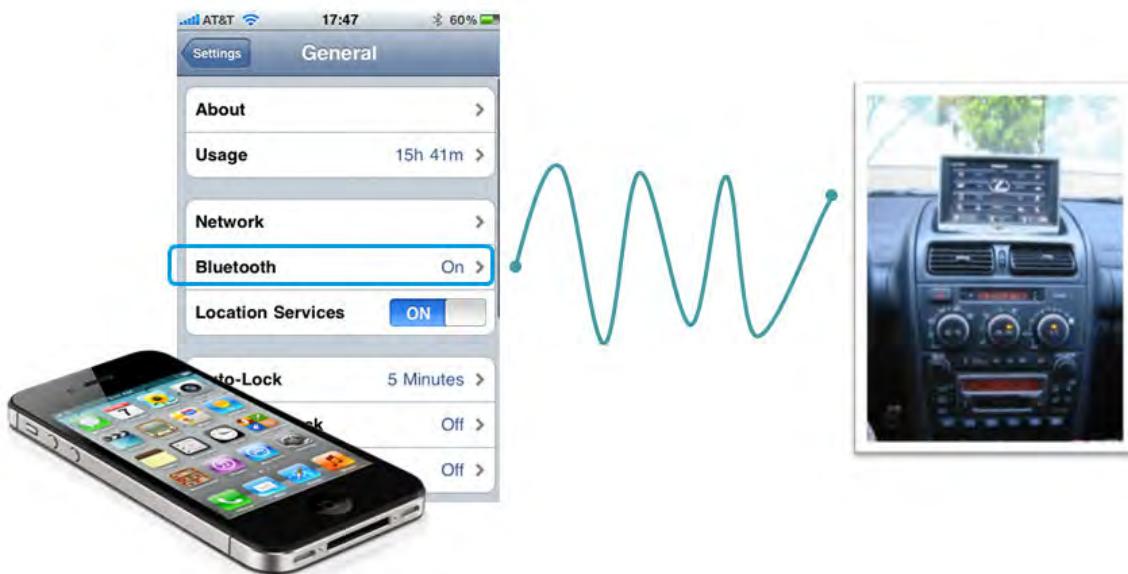
To conserve data usage on a cellular plan, many mobile devices offer Airplane Mode, which typically turns off cellular network connections while allowing you to still use free Wi-Fi connectivity. Additionally, when Wi-Fi is unavailable, some mobile device can enable tethering to connect to a different device (like a laptop) and supply it with the cellular network connection. This avoids the need for two separate data plans for the two different devices. Devices like phones and tablets can also be converted into mobile hotspots, creating a wireless access point for other devices to connect to.

## Bluetooth Connectivity

Bluetooth® is a wireless radio protocol that is used to communicate from one device to another in a small area, usually less than 30 feet. Bluetooth is commonly used to enable communication between

small personal electronic devices, such as between a cellular phone and a wireless earpiece or between an electronic organizer and a personal computer.

Bluetooth enables mobile devices to connect wirelessly to various devices such as headsets, carputers, laptops, MP3 players, and gaming consoles. Newer computers come with a Bluetooth radio built right into the system, while older computers require an adapter, such as a USB-enabled Bluetooth adapter. Devices in *discovery mode* will transmit their Bluetooth-friendly name, which in most cases is the manufacturer's name. Once the name has been transmitted, the device can be paired with another device also transmitting a signal. Using Bluetooth technology, mobile devices can establish a connection through a process called *pairing*. When two devices pair, they share a secret key in order to establish a wireless connection.



**Figure 15-5: Pairing.**

Bluetooth uses the 2.4 GHz spectrum to communicate a 1 Mbps connection between two devices for both a 232 Kbps voice channel and a 768 Kbps data channel (technically, Bluetooth detects other devices in the 2.4 GHz spectrum and avoids the frequencies they use by "hopping" to an available frequency).

## Version History

The first Bluetooth specifications were released in 1999, and there have been several important revisions since then.

- Bluetooth 2.0 is an improved version of Bluetooth, has a range up to 100 meters, offers faster data transfer speeds (up to 3 Mbps), and also uses less power to extend battery life. Bluetooth 2.0 is backwards-compatible with earlier versions of Bluetooth, but the connection between devices is governed by the slowest device; in other words, connecting a Bluetooth 1.2 device to a Bluetooth 2.0 device means the data transfer is at the rate of Bluetooth 1.2.
- Bluetooth 3.0 launched in 2009. Bluetooth 3.0/3.1 provides transfer speeds up to 24 Mbit/s by using 802.11 wireless protocols to carry the data while Bluetooth is used to establish the connection.
- Bluetooth 4.0 was released in 2010. It provides lower power consumption, is more secure, and is faster than prior versions.
- Bluetooth Low Energy (LE), also called Bluetooth Smart or Version 4.0+ is a low-power, standardized application development architecture that provides tight security, native support on every major OS, and connectivity to the cloud. It was built for the Internet of things.

## Bluetooth Naming and Addressing

Each Bluetooth device has its own unique 48-bit address. But instead of requiring you to connect via this address, most Bluetooth devices also have their own Bluetooth names. By default, manufacturers set the Bluetooth name for devices to the name of the manufacturer and model of the device. If you have several users you support that are in close proximity to each other and have the same devices, these default Bluetooth names can cause problems. In this scenario, you should be sure to rename each user's Bluetooth device.

## Bluetooth Pairs

Most Bluetooth devices require you to establish a trusted relationship between two devices (referred to as pairing). This trusted relationship is established through the use of an encrypted shared secret or passkey. After the relationship is established, the pair of devices can encrypt the data transmissions they exchange. However, most Bluetooth printers permit all devices to use their services without requiring pairing.

## Unpairing from a Bluetooth Device

The exact method for unpairing from a paired device varies between operating systems and hardware devices. In general, though, you should be able to find a setting for Bluetooth connections, then there should be a menu option or button to use to forget the pairing that was previously established.

## The Bluetooth Pairing Process

The pairing process involves devices sharing a secret key in order to create a working relationship. The basic steps in this process include:

1. On the mobile device, enable Bluetooth through the device's system settings. This allows the device to be discovered by other devices.
2. Enable pairing on the device.
3. On your mobile device, find a device for pairing.
4. Once the device is found, it will ask for a PIN code.
5. Depending on the type of device, the PIN code will be sent via a text, or will be a standard code, such as "0000" used for wireless headsets.
6. Verify that a connection message has been displayed.
7. Test the connection by using the two devices together to either make a phone call, transfer data, or play music.

## Email Configuration Methods

Once you've established a network connection with your mobile device, you can set up and configure your email. Mobile devices can be configured to automatically update your email account information and manage mail. Mobile devices support a number of different email providers such as Yahoo! Mail, Microsoft Exchange, Outlook.com, Gmail/Inbox, and iCloud.

Email can be accessed in one of two ways on a mobile device: web-based or client-based. Web-based access is accomplished by installing the email provider's application available in the mobile devices store. This method requires you to enter your user name and password to access the web-based email application. On the other hand, client-based email access is a bit more complicated and requires more information to access email services. Microsoft Exchange is a client-based email system that allows mobile devices to sync with the server. Before you can set up your mobile device's email, you need to determine the type of email account you will be configuring.

Businesses will typically rely on a client/server email service like Microsoft Exchange. A corporate email account is therefore usually configured by an IT administrator and not the user. In contrast, users that take advantage of their ISPs' free email offers will typically have more control over their account and may use it more for personal communications than professional.

## Email Server and Configuration Settings

Depending on which email provider you use, there may be additional settings that you need.

<b>Server Information</b>	<b>Description</b>
Protocol	<p>Your email server will be configured to support either POP3 or IMAP.</p> <p><i>Post Office Protocol version 3 (POP3)</i> is a protocol that enables an email client application to retrieve email messages from a mailbox on a mail server. With POP3, the email messages wait in the mailbox on the server until the client retrieves them, either on a schedule or manually. Once the messages are retrieved and downloaded to the client, they are generally deleted from the server. The client then stores and works with the email messages locally.</p> <p><i>Internet Mail Access Protocol version 4 (IMAP4)</i> is a protocol that enables a client to retrieve messages from a mail server. With IMAP4, messages generally remain on the server while the client works with them as if they were local. IMAP4 enables users to search through messages by keywords and to choose which messages to download locally. Messages in the user's mailbox can be marked with different status flags that denote states such as "deleted" or "replied to." The messages and their status flags stay in the mailbox until explicitly removed by the user. Unlike POP3, IMAP4 enables users to access folders other than their mailbox.</p> <p>POP3 and IMAP are used for ISP and web email setup. These protocols are not used with a mail management server such as Exchange, but servers like Microsoft Exchange provide support for both protocols.</p>
Security	In order to establish secure authentication to and from an email server, a security protocol should be used. Security protocols used in email communications are <i>SSL/TLS</i> , S/MIME, and PGP.
Ports	Email servers use different ports for incoming and outgoing mail depending on the protocols used. Before you can configure email settings, you will need to determine the specific port numbers that are used.

## Android Email Configuration Requirements

In order to fully configure an email account on an Android mobile device, you may need additional email provider server information. Common required settings include:

- The email domain which is the @\_\_\_\_\_ portion of your full email address.
- Your email authentication information.
- The access domain, which is the unique hostname that is assigned to the email provider's server. You may need to visit your email provider's website to verify the hostname.



**Note:** For additional information, check out the LearnTO **Configure Email on a Mobile Device** presentation in the LearnTOs for this course on your CHOICE Course screen.

## Mobile Device VPN Connections

Many organizations have a VPN server configured to allow users secure access to network resources when they are out of the office. Most mobile smartphones and tablets have VPN capabilities. VPN configuration options are usually found in the same menu area where other network services are enabled and configured. The specific steps for configuring a VPN connection will vary with each mobile OS.

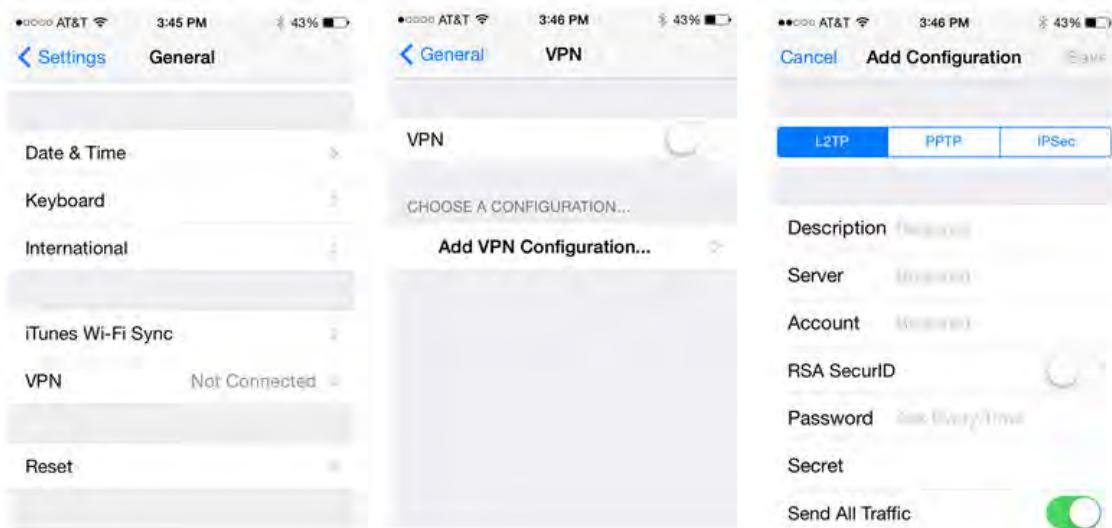


Figure 15–6: Configuring VPN connections in iOS.

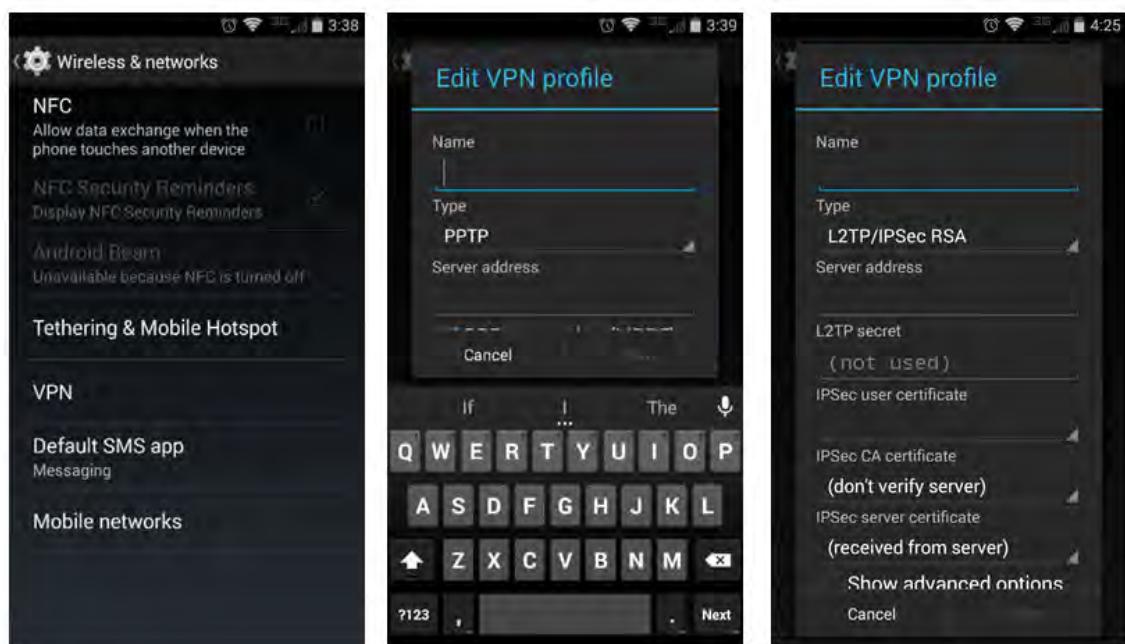


Figure 15–7: Configuring VPN connections in Android.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Configure Mobile Devices.

# ACTIVITY 15–5

## Configuring Mobile Devices

### Scenario

You want to practice configuring features on mobile devices so that if users need your help in configuring features, you will have some familiarity with doing so.

1. Determine the mobile device IMEI and IMSI numbers.
2. Examine or configure the mobile device to use the email address provided for your use during class.  
Depending on the device you are configuring, and the type of email address you are using, the steps will vary. If you need help with the procedure, search online or ask your instructor for assistance.
3. Create a Bluetooth connection between two Bluetooth capable devices.
  - a) Enable Bluetooth on the mobile device through system settings.
  - b) Enable pairing on the device.
  - c) On your mobile device, find a device for pairing.
  - d) Once the device is found, it will ask for a PIN code. Depending on the type of device, the PIN code will be sent via a text, or will be a standard code, such as "0000" used for wireless headsets.
  - e) Verify that a connection message has been displayed.
  - f) Test the connection by using the two devices together to either transfer data, answer or make a call, or play music.
4. Investigate the VPN options available on the mobile device.

# TOPIC F

## Mobile Device Synchronization

Now that you've configured mobile devices so that they can connect with and communicate with networks and other devices, you can configure those devices to contain the same information as other devices contain. In this topic, you will identify methods and best practices for synchronizing mobile devices.

Some people have a computer and a cell phone, while others might have a smartphone, a tablet, and multiple computers. In situations where data is kept on multiple devices, it's a good idea to try and keep the information accurate and up-to-date on each device to alleviate confusion.

### Data Synchronization

*Data synchronization* is the process of automatically merging and updating common data that is stored on multiple devices. For example, a user can access his email contacts list from both his mobile device and his laptop computer. Synchronization is established when the devices are either connected via a cable or wirelessly, or over a network connection. In some cases, you may need to install synchronization software on the devices you choose to synchronize. The synchronization rate can be controlled and limited to allowing and restricting push and pull notifications from the cloud over the Internet.



Figure 15–8: Data synchronization.

### Types of Data to Synchronize

There are many types of data that can be synchronized:

- Contacts
- Programs
- Email
- Pictures
- Music
- Videos
- Calendar
- Bookmarks
- Documents
- Location data

- Social media data
- eBooks

## Data Synchronization Methods

Microsoft has its own synchronization protocol called *Exchange ActiveSync (EAS)* that enables mobile devices to connect to an Exchange Server to access mail, calendars, and contacts. Exchange administrators can control what devices can connect and synchronize with the server and which ones are blocked.



**Note:** You can sync to the cloud or sync to your desktop or laptop device, or even between mobile devices.

If you have access to a cloud service such as iCloud or OneDrive®, a subscription service such as Dropbox, or another online storage service, you can use the built-in features of the service to synchronize data between devices. You might need to install an app on your mobile device to access the online storage. Data is often automatically synchronized whenever a network is available. You can configure services so that data synchronization only occurs over a Wi-Fi network so that you don't use up your monthly allotment of data in synchronizing data.

Some services, such as iTunes, synchronize data whenever the mobile device is connected to a computer. This keeps the apps, music, and videos you purchased on one device synchronized with the other computing device.

## Data Synchronization Requirements

Synchronization requirements will vary and will be specific to each mobile device. There are a number of factors to consider when enabling data synchronization on a mobile device:

- You might need to use a specific system account to enable synchronization.
- You might require an email account.
- If you are using Microsoft Exchange, then control may be given to the Admin.
- Organizations may have specific requirements to synchronize data.
- Certain devices might require additional software to enable synchronization.
- Certain devices might require using specific network protocols to enable synchronization.
- The device may need to authenticate a service, not just vice versa.

## ACTIVITY 15–6

### Discussing Mobile Device Synchronization

#### Scenario

You want to do a little research to make sure you know how to synchronize data between various mobile devices and a user's computer. You and the other technicians in your department each were assigned a different scenario at your last team meeting to research.

---

1. Based on the mobile device you are using, the email account you are using, any cloud storage you are using, and whether you are connecting to the other device over Wi-Fi, a data cable, or cellular, search online for the most appropriate method of synchronizing your data.
    - a) Determine which method is most efficient for syncing data between the mobile device you are using and a computer.
    - b) Determine if any settings need to be changed on your mobile device to prevent cellular connections for large data transfers.
    - c) Determine if any additional apps need to be installed to sync data.
  2. Share your results with the rest of the class.
-

# TOPIC G

## Troubleshoot Mobile Device Hardware

In this lesson, you have installed, configured, and managed several types of mobile device hardware. As with desktop PCs, part of your duties as an A+ technician will be helping users when they encounter problems with their mobile devices. In this topic, you will troubleshoot issues with mobile device hardware.

### Handling and Maintenance Techniques

Mobile devices are small and can easily be damaged. Using appropriate handling techniques when performing maintenance on the devices will help keep the devices from being damaged. Some recommendations include:

- As convenient as it might be, avoid putting small mobile devices in pockets where they could be damaged when you sit down.
- When applying a screen protector, make sure not to get fingerprints on the glass or on the sticky side of the screen protector.
- Avoid dropping the mobile devices.
- When possible, place the mobile devices in protective cases. If you need to remove the protective case to access the device, be careful not to damage either the case or the mobile device.
- Avoid leaving mobile devices in hot cars or leaving them out in the cold. The cold might damage the delicate screen.
- Avoid getting mobile devices wet.

There are many general maintenance and handling techniques that should be considered when supporting laptops, tablets, and smartphones.

<b>Issue</b>	<b>Techniques</b>
Cooling systems	<p>Because laptops do not have the air circulation that desktop PCs do, it is important to keep the device air ducts clean. Dust trapped in cooling passages acts as an insulator and can prevent proper cooling, possibly resulting in overheating. Excessive heat should be avoided in such devices as it can shorten the life of components. In servicing laptops, it is a good practice to regularly blow dust from the cooling passages using compressed air or vacuum it with an electronics vacuum. When using the compressed air to clean the inside of the laptop, you must be extremely cautious of the internal components. It is easy to damage other components inside the laptop while cleaning.</p> <p>The bottom surface of the laptop gets quite hot when improperly ventilated. This can easily happen when laptops are put on soft surfaces (i.e., tables with coverings such as table cloths), on people's laps, or in places where there is not enough room between the vents and a wall. Sometimes people will get careless and unwittingly cover the vents with books, mouse pads, etc.</p>

<b>Issue</b>	<b>Techniques</b>
Batteries	<p>Properly caring for the battery in a mobile device not only prolongs battery life, but also diminishes health and safety concerns. Using an incorrect battery charging cable or exposing a battery to harsh environmental conditions, such as extreme heat, can result in an explosion. Some simple guidelines for acceptable battery maintenance include:</p> <ul style="list-style-type: none"> <li>• Follow manufacturer instructions on the proper charging and discharging of the battery.</li> <li>• Use the battery charger provided by the manufacturer or an approved replacement charger.</li> <li>• Never expose the battery to fire or water.</li> <li>• Do not drop, throw, or jolt the battery.</li> <li>• Only use the recommended battery for your device.</li> <li>• Make use of power management features included with your device/OS to prolong battery life.</li> </ul>
Transportation and handling	<p>Because mobile devices are carried from place to place, they are exposed to hazardous environments far more frequently than desktop computers. Careless handling can substantially reduce the life expectancy of such devices.</p> <p>Whether storing, shipping, or just transporting a laptop, it is important to choose an appropriate enclosure for the device. Such enclosures should protect the device from moisture, heat and cold, and dust and debris. The enclosure should shield the device from objects that could scratch or scrape, and also withstand the impact of a drop.</p> <p>When carrying a laptop or other mobile device, be careful not to hold on to it by a corner. This can cause the device to bend slightly and short out the system board.</p>

## Operating Environment Best Practices

If you can properly control environmental factors, such as temperature, humidity, RFI, and ESD, you can help ensure optimal performance and extend the life of your device.

<b>Environmental Factor</b>	<b>Description</b>
High temperature	Exposure to high temperatures can cause expansion within portable computing devices and compromise circuitry. High temperature can also lead to the failure of cooling systems to maintain adequate operating temperatures, leading to the overheating and failure of internal components such as the processor, video processor, and hard drive.
Rapid change in temperature	Rapid changes in temperature, such as those seen when transporting a device from one climate to another, could result in condensation within the device. Devices should be allowed to come to room temperature before being powered on after a temperature change.
High humidity	Avoid operating in high humidity as condensation within the device may occur and promote corrosion. All manufacturers specify operating humidity levels. It is important to follow manufacturer operating procedures/guidelines at all times. Most systems can operate at high humidity without a problem, as long as there is no condensation (5 to 95 percent relative humidity, non-condensing).
Low humidity	Be extra cautious as ESD is more likely to occur in low-humidity environments (those under 35 percent relative humidity).

<b>Environmental Factor</b>	<b>Description</b>
RFI	<p>Erratic errors may occur with mobile devices when exposed to <i>radio-frequency interference (RFI)</i>. Radio towers, two-way radios, and even cordless telephones and microwaves have been linked to RFI.</p> <p>Moving the device further from such sources will help in resolving interference issues. Properly shielded cables for peripherals will also minimize the effects of RFI.</p>

## General Mobile Device Issues

As an A+ certified technician, you will be responsible for interpreting a laptop's symptoms and determining what the specific issues are and how they can be resolved.

<b>Symptom</b>	<b>Description</b>
Display issues	<p>Some common display device issues include:</p> <ul style="list-style-type: none"> <li>• Cannot display to external monitor, video device, or projector. Often this feature requires the user to toggle between display modes. Check the device documentation for more information on toggle modes for your specific device.</li> <li>• No display.           <ul style="list-style-type: none"> <li>• In some cases, the LCD cutoff switch remains stuck down even after the laptop lid is opened. You may need to connect the laptop to an external monitor to verify that the graphics card is still working properly.</li> <li>• The mobile device might be out of power and need to be plugged in or recharged.</li> <li>• The mobile device unit's integrated screen might be damaged.</li> </ul> </li> <li>• Backlight/brightness functionality and pixelation have been changed. In some cases, the intensity of the backlight and the amount of pixelation can conserve power if configured correctly. Verify that the backlight and resolution settings are configured to suit the user's needs. Often, the display is optimized for certain dots per inch (DPI) and resolution settings. Changing these is not always recommended. In some mobile devices, the backlight/brightness settings are configured automatically, so check to see if you can enable or disable this setting.</li> <li>• Dim display. The screen goes dark and cannot be adjusted or the hues in the display are changing. This can be one of two issues: the screen has gone bad or the LCD inverter is bad. You may need to replace the screen or the inverter. Check the manufacturer's documentation to verify replacement options.</li> <li>• Flickering display. This can be a symptom of a number of different issues. First, verify that your video card drivers are up to date. Next, check the screen refresh rate within the display settings for the mobile device. If the flickering continues, then it is most likely a loose wire connection from the system board to the display. In this case, the only way to fix the issue is to disassemble the mobile device and secure the wires.</li> </ul>

Symptom	Description
Battery issues	<p>There are usually three main issues with mobile device batteries, the first being that the battery does not stay charged long enough. Battery life can be maximized using the power management features of your device. Many devices also offer extended life batteries. To extend battery life, disable devices not being used, such as wireless (Wi-Fi, Bluetooth®, and infrared [IR]). If not on a network, you can also disable the network interface card (NIC). These devices have their own power management options that need to be set.</p> <p>The second is that the battery is not charging. This could be because of a bad AC adapter or cable. Nickel cadmium (Ni-Cad) batteries have battery memory, which means that they can lose most of their rechargeability if you repeatedly recharge them without draining the batteries first. The only solution to this problem is to use a conditioning charger, which is designed to first drain the Ni-Cd batteries before recharging them. Battery memory can sometimes affect nickel-metal hydride (NiMH) batteries, too. Try replacing the cable and see if that fixes the issue. If it does not, then you will most likely have to replace the battery.</p> <p>The third issue is battery swelling. A swollen battery may expand beyond its container and cause issues with the device's casing, and it can also lead to the battery malfunctioning. Swollen batteries may also leak harmful chemicals. Batteries can become swollen through age, misuse, or manufacturing defects, and are typically caused by the batteries' cells overcharging. Most swollen batteries will need to be replaced. To avoid this effect, make sure to store the device in a cool, dry place, and make sure you're using the right power charger.</p> <p>Replacing batteries is not uncommon and will need to be done periodically.</p>
Device gets hot	<p>Because mobile devices have very little space in between their internal components, you can have problems with them overheating, which leads to system lockups and even hardware failures. Strategies you can use to help reduce the heat within mobile devices include:</p> <ul style="list-style-type: none"> <li>• Use the power management features even when the mobile device is connected to a power outlet, especially if you are using it in a warm room.</li> <li>• Try to keep the bottom of laptops ventilated. (For example, do not rest a laptop on a pillow in your lap.)</li> <li>• Be aware of the fan in a laptop. If you hear it running very fast on a regular basis, take steps to minimize heat in the laptop.</li> </ul>
Mobile device is not working properly when on battery power	<p>This can be an indication that the battery contacts are dirty. You can clean them by using alcohol preps or even just a dry cloth.</p>

Symptom	Description
No power when connected to AC power	The power cord or AC adapter might have failed, the outlet to which you are attempting to connect the mobile device is bad, or the power supply in the mobile device has failed. Start by checking the power outlet and plugging in a known good electrical device and verifying whether you can turn it on. If the problem persists, then try using a known good power cord and then an AC adapter to determine if either is the source of the problem. You might also test both AC and DC power by using a multimeter. For devices with a two-component charger, such as a USB cable into a USB-to-electrical-outlet adapter, or a laptop power cord with a separate cable from the transformer to the power outlet, make sure that the connections are firmly mated together.
Ghost cursor and pointer drift	Laptops commonly have touch pads or pointing sticks. Touch pads can suffer from dirt and hand grease contamination that can make the touch pad behave erratically; make sure to clean with alcohol preps. Pointing stick heads can wear out and become slippery, making them very difficult to use; order replacements from the manufacturer or vendor. In some laptop models, you can actually recalibrate the touch pad to try and fix the issue.  A <i>ghost cursor</i> is a cursor that jumps around on the screen randomly, or moves too slow, or opens windows and menus on its own. Causes of this problem include a corrupt driver, driver incompatibilities after an upgrade to a newer operating system, and a hardware failure. Steps to take to resolve this problem include reinstalling or upgrading the driver. If this does not resolve the problem, many portable devices allow users to connect an external mouse as a substitute for the touch pad or other integrated pointing devices.  <i>Pointer drift</i> is when the mouse pointer moves across the screen without the user touching the touchpad or mouse. This can often be resolved by uninstalling and reinstalling the drivers. The other reason this might occur is if the user is using the mobile device keyboard and their hands rest on the case near the touch pad, the touch pad might register their hands as touching the touch pad if the case flexes a bit from the user's hands. You also might need to recalibrate the touch pad or pointing stick.

## Common Mobile Device Keypad Issues

Mobile device keypads are the source of many user complaints due to their varied key arrangements.

Issue	Description
Nonstandard key placement	Due to size constraints, mobile device manufacturers often rearrange function keys to make them all fit.
Function keys	Some keys on a standard desktop keyboard would not fit on a mobile device keyboard and have instead been added as function keys. Several keys on a mobile device keypad are shared. For an explanation of key functions, consult the device manual.
Numeric keypad	Most mobile computers do not have the numeric keypad like desktop keyboards. Instead, many manufacturers place numbers on letter keys to be used when <b>NumLock</b> is on. <b>NumLock</b> indicator lights are displayed on the laptop to indicate that the <b>NumLock</b> function has been turned on.

<b>Issue</b>	<b>Description</b>
Sticking keys	On occasion, a key will remain in the depressed position due to debris buildup or a malfunction in the mechanism. These issues can often be resolved by removing the key, cleaning it, and replacing the key. Methods for removing keys vary from model to model. Removing a key on a laptop keyboard can be a risky proposition. They are typically not the type of key where the key cap is in a peg, which you find on full-sized keyboards. Laptop keys are usually floating on a dual-hinge mechanism, usually plastic, that will easily break if you attempt to remove it forcefully. Refer to the manufacturer's instructions when attempting to fix a key on the keyboard.
Keyboard too small	The strain of typing on a small or non-ergonomic keyboard may bother some users.
Keyboard not responsive	For mobile devices with detachable keyboards, ensure that the keyboard is properly connected to the computing device. If the mobile device has an operating system function to select between using internal, external, or on-screen keyboards, ensure the appropriate keyboard option is selected.

## Common Touch Screen Issues

Touch screen devices are gaining in popularity. They show up in everything from ATMs at the bank to store checkouts, to smartphones and tablets, to laptops and desktop computers. They are also used in some industrial applications where the environment would not be conducive to use of mechanical keyboards or a portable device is needed. As great as they can be, there are some issues you might encounter.

<b>Issue</b>	<b>Caused By</b>	<b>Possible Resolutions</b>
Dirty	Oils from the user's fingers, dusty surroundings, foreign matter adhered to the screen	<ul style="list-style-type: none"> <li>Wipe the screen with a soft cloth designed for eye glasses cleaning.</li> <li>Use solution designed for cleaning eye glasses, applied to a soft cloth.</li> </ul>
Touch not registering in the location where screen was touched	Lost calibration settings	Recalibrate the device using the built-in operating system tools.
Scratched, cracked, or broken screen	<ul style="list-style-type: none"> <li>Dropping device.</li> <li>Placing device in pocket or bag with sharp objects.</li> <li>Sitting on device.</li> </ul>	<ul style="list-style-type: none"> <li>To prevent this issue, place device in protective case and apply a screen protector.</li> <li>Some scratches might not cause any operating problems.</li> <li>Replace the touch screen, following manufacturer's directions.</li> </ul>
Erratic behavior	<ul style="list-style-type: none"> <li>Dirty screen, lost calibration settings, or scratched, broken, or cracked screen.</li> <li>Driver problem.</li> </ul>	<ul style="list-style-type: none"> <li>Follow the resolutions above.</li> <li>Remove and install the drivers.</li> </ul>

<b>Issue</b>	<b>Caused By</b>	<b>Possible Resolutions</b>
Can't see the screen	Device is being used in bright sunlight.	<ul style="list-style-type: none"> <li>Check device settings to adjust for sunlight conditions.</li> <li>Apply anti-glare screen cover.</li> </ul>
User is wearing gloves	<ul style="list-style-type: none"> <li>Cold weather necessitating need for gloves.</li> <li>Work with chemicals or other materials that requires the user to wear gloves.</li> </ul>	<ul style="list-style-type: none"> <li>Obtain and use gloves with capacitive finger tips that will work with the device.</li> <li>Use a stylus designed for the device.</li> </ul>

## Common Wireless Connectivity Issues

There are several portable device issues that can cause wireless signal reception and connectivity problems.

<b>Issue</b>	<b>Description</b>
Intermittent wireless connectivity	Several factors could play a part in poor or intermittent wireless reception, including low battery, radio interference, and signal barriers such as masonry walls or floors. Anything metal can also block signals, such as large metal file cabinets and metal-clad fire doors, things many people forget to consider when determining the best location of wireless access points in an office. If there is an external antenna, check to be sure the antenna is fully extended, properly connected, and is not damaged. In some cases, if the wireless card is installed independently from the system board, then you can upgrade the wireless card to improve connectivity.
No Bluetooth connectivity	<p>There are a number of issues that can cause Bluetooth connectivity problems:</p> <ul style="list-style-type: none"> <li>The drivers might need to be updated.</li> <li>The devices have not been set to "discoverable" mode. For security purposes, only enable discovery mode on your mobile device when you want a Bluetooth device to find your device; otherwise, keep that setting disabled.</li> <li>The Bluetooth settings must be configured to allow devices to connect to the device. This is also referred to as pairing.</li> </ul>
No wireless connectivity	<p>Some portable computing devices allow the user to turn off the wireless receiver switch, which would result in no reception. Or, the user might simply be out of range of the wireless access point. You may also need to enter the appropriate security key for the wireless access point.</p> <p>This issue might also be the result of damage or a failure in the wireless device or the embedded antenna on the wireless network card. Some cards might have a flip-up antenna that might be damaged through improper handling. If the card or antenna is damaged, you would typically replace the wireless card.</p>

## Mobile Device Disassembly Best Practices

When disassembling a mobile device, it's important to follow the proper disassembling process to ensure that the device can be reassembled correctly:

- Document and label all cable and screw locations as you go.
- Organize the parts as you remove them from the mobile device.

- Refer to the manufacturer's documentation to help with locating components.
- Use the appropriate hand tools, such as a small screw driver to remove the screws.

Servicing mobile device components can be difficult depending on where the component is located within the case. Many times, the components are not serviceable and replacing the entire mobile device is required. It's also important to check a manufacturer's warranty restrictions before you service a mobile device and its components. In some cases, you can actually break the warranty if you crack open the case.



**Note:** Remember, devices under warranty should not be disassembled because this typically voids the warranty.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Troubleshoot Mobile Device Hardware Issues.

# ACTIVITY 15–7

## Troubleshooting Mobile Device Hardware Issues

### Scenario

You are assisting users with some mobile device hardware issues today.

1. You received a user complaint about a laptop being extremely hot to the touch. What actions should you take in response to this issue?
  
  
  
  
  
  
2. A user reports that when they plug in anything to the USB port on the laptop, that it is not recognized by the system. Is this something you can easily repair?
  
  
  
  
  
  
3. Several laptops need to be replaced in the next fiscal cycle, but that doesn't begin for several more months. You want to improve functionality as much as possible by upgrading or replacing components in some of the laptops that are having problems. Which items are easily replaced in a laptop?
  
  
  
  
  
  
4. Your organization has several tablet devices that are loaned out as needed when employees are traveling. Some users have reported problems getting the Bluetooth keyboard to work with the tablet. What should you do?
  
  
  
  
  
  
5. A user reports that the touchscreen on their mobile device is not responding properly. What questions should you ask, and what steps might you take to resolve the issue?

## Summary

In this lesson, you worked with mobile computing devices. You examined mobile device technologies including laptops, smartphones, and tablets. As an A+ technician, you will need to be able to expertly support and troubleshoot mobile devices.

**In your professional experience, have you supported mobile devices? If not, what kind of experience do you have with them?**

**What type of technical support do you think will be expected of an A+ technician as mobile devices become even more prominent within the workplace?**



**Note:** Check your CHOICE Course screen for opportunities to interact with your classmates, peers, and the larger CHOICE online community about the topics covered in this course or other topics you are interested in. From the Course screen you can also access available resources for a more continuous learning experience.

# 16

# Supporting Printers and Multifunction Devices

**Lesson Time:** 1 hour, 15 minutes

## Lesson Objectives

In this lesson, you will support printers and multifunction devices. You will:

- Compare various printer technologies and the associated imaging processes.
- Install and configure printers.
- Perform printer maintenance.
- Troubleshoot printers using appropriate tools.

## Lesson Introduction

In previous lessons, you have installed, configured, and managed system hardware for desktops, laptops, and mobile devices, as well as the basic operating software and networking components on all three systems. The next logical step is to examine some of the most common external devices in use on personal computer systems: printers. In this lesson, you will support printers and multifunction devices.

Despite predictions that computers would bring about a paperless office environment, the need to transfer digital information to paper or back again remains as strong as ever. Therefore, printing and scanning are among the most common tasks for users in almost every home or business environment. As an A+ certified professional, you will often be called upon to set up, configure, and troubleshoot printing environments, so you will need to understand printer technologies as well as to perform common printer support tasks.

# TOPIC A

## Printer and Multifunction Technologies

In this lesson, you will support printers. Before you can provide the right level of support, you must fully understand how these systems are used in a production environment. You need to understand how the various components work within a printer to provide the desired outputs. In this topic, you will identify printer technologies.

As a professional support technician, you might be supporting the latest cutting-edge technology, or you might be responsible for ensuring that legacy systems continue to function adequately. So, you must be prepared for either situation and be able to provide the right level of support to users and clients. Having a working knowledge of the many printer technologies and components will help you to support users' needs in any technical environment.

### Printers

A *printer* is a device that produces text and images from electronic content onto physical media such as paper, photo paper, and labels. A printer is one of the most popular peripheral devices in use in most computing environments. Printers employ a range of technologies; the quality of the print output varies with the printer type and generally in proportion to the printer cost. A printer output of electronic documents is often referred to as hard copy. Printers can connect to computers using a variety of connection types, with the most popular methods being USB, networked, and wireless.



**Figure 16-1: Printers.**

### Microsoft Printing Terminology

Some Microsoft® technical content makes a firm distinction between the software components that represent the printer, and the physical printer itself. You may find that Microsoft refers to the software representation of the printer as the "printer object," "logical printer," or simply "printer," and refers to the printer itself as the "print device" or "physical printer." However, Microsoft

sometimes also uses the word "printer" as in common usage, to mean the physical print device. Be aware of the context usage of the terms.

## Printer Components

There are many types of printers. Each type of printer, and each printer from different manufacturers implements the printing process slightly differently. All of the printers will have the following common components.

<b>Printer Component</b>	<b>Description</b>
Mechanism for creating text and images	Impact printers typically use an ink coated ribbon. Low volume printers often use ink cartridges. High volume printers typically use toner. Store receipt printers might use ink or thermal process.
Paper feed mechanism	Printers need some method of moving the paper through the printer so that the ink or toner can be applied to the paper. Impact printers often use sprockets that engage holes on the edge of special continuous feed paper. Ink jet printers typically use wheels that pull the top sheet from a stack of cut sheets of paper, typically 8.5" x 11" or 14". Laser printers use pickup rollers to move cut sheets through the printing mechanism. Specialized printers might use these or other methods of moving the paper.
Connection to computing devices	A printer is not all that useful if it cannot communicate with the devices that contain documents to be printed. Printers might connect through a USB cable, a wired network card, or a wireless card. Some printers also include card readers so users can save files to the memory card and print from the memory card directly onto the printer.
Paper input and output	Printers that use cut-sheet paper have a tray or opening for a stack of paper. There will also be a tray or opening where the printed pages are stacked after printing. Printers that use continuous feed paper might or might not have input and output trays. Thermal printers often use paper on a roll that is placed inside the printer device and the output is pulled across a serrated edge to remove the printed output from the roll.

Printer types can vary, but there are many common technical components that are used to provide a number of common functions within the printer.

<b>Component</b>	<b>Description</b>
Printer memory	Printers typically come with their own installed memory to store information about the current device settings as well as the print jobs in the queue. Different devices will have a different amount of memory installed by default; you may be able to upgrade the memory. Upgrading the memory can enable a printer to handle higher-resolution jobs and to buffer more of each print job to increase throughput.  Printers store current print jobs in volatile Random Access Memory (RAM); they typically store device settings in flash-based non-volatile RAM. Consult your device documentation for the memory amounts and types your device supports, as well as procedures for installing or upgrading device memory.

<b>Component</b>	<b>Description</b>
Printer drivers	Like all hardware devices, printers require appropriate software drivers in order to enable the device to communicate with the computer system and function correctly. The driver controls all device-specific functions, including print resolution and quality choices, color rendition, contrast and brightness, and finishing options such as two-sided printing, collation, stapling, and so on. If you open a device's property sheet, you can see the driver functions on the <b>Advanced</b> page and on any custom pages the driver adds. Printers might also include management software that is separate from the low-level driver interface and provides sophisticated control over device settings and functions.
Printer firmware	Many printers include built-in firmware that provides the on-board device management interface. This enables you to configure printer functions, monitor and manage print jobs, select output options, and run diagnostic tests from a console on the device itself, rather than indirectly through a computer operating system. The firmware type and the functions provided by the firmware will vary depending upon your device. Check with your device vendor for any available firmware updates.
Printer interfaces	Most printers and multifunction devices used today use USB and wireless technologies, or are directly connected to the network via a network cable. Older printers connected to computers using parallel or sometimes serial cables and ports; those connection methods are considered obsolete.

## MFDs

A *multi-function device (MFD)* is a piece of office equipment that performs the functions of a number of other specialized devices. MFDs typically include the functions of a printer, scanner, fax machine, and copier. However, there are MFDs that do not include fax functions. Although the multi-function device might not equal the performance or feature sets of the dedicated devices it replaces, multi-function devices are very powerful and can perform most tasks adequately and are an economical and popular choice for most home or small-office needs.



**Figure 16–2:** An MFD.

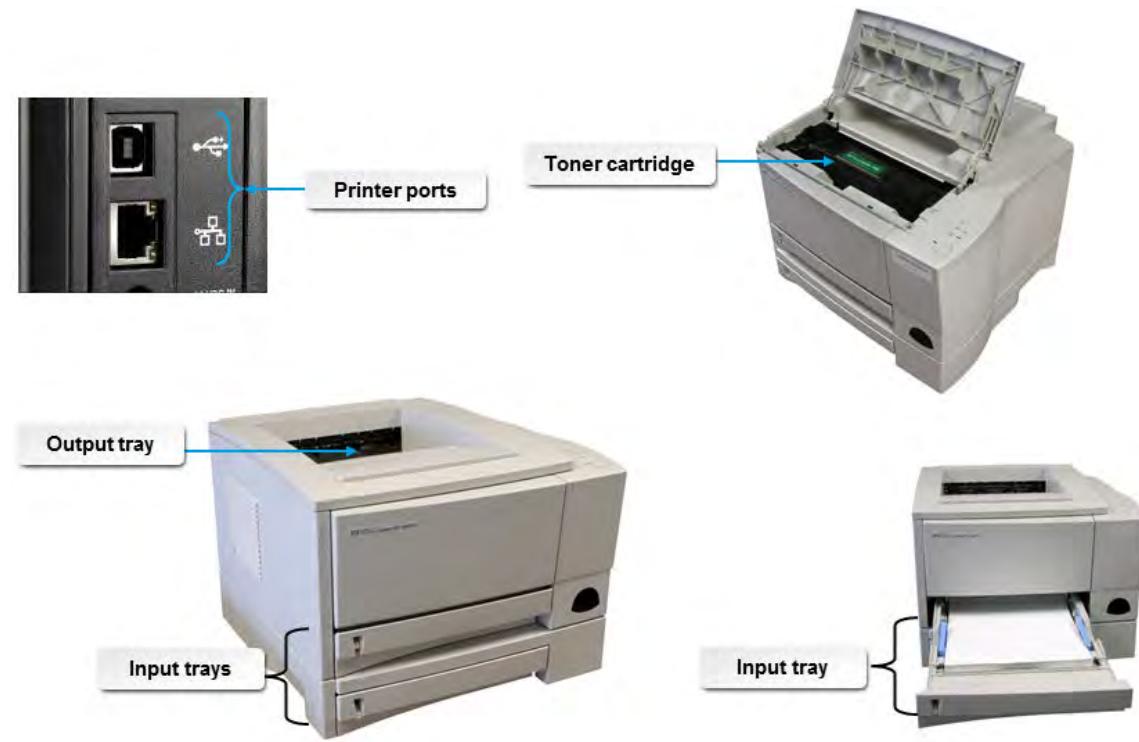
## Types of MFDs

MFDs can be broadly classified into three types, based on their size, cost, and functions.

Type of MFD	Description
All-in-one (AIO MFD)	These MFDs are small in size and include basic features of printing, scanning, and copying that are required for home users. Interestingly, some of them include features such as <i>PictBridge</i> and smart card readers that are not available on high-end MFDs. Some have limited or no fax features and do not support networking. Many can be connected using USB to a single computer, or to multiple computers through a Wi-Fi connection to the wireless router.
SOHO MFD	These MFDs are medium sized and are designed specifically for small and home offices. They can be connected to a network and can perform tasks at a faster pace than AIOs. They usually have enhanced faxing capabilities and some high-end models are loaded with additional time-saving features, such as an automatic document feeder, duplex printing, <i>duplex scanning</i> , extra paper trays, and stapling.
Heavy-duty MFD	As the name suggests, these MFDs are large, network-enabled machines that can cater to the documentation needs of an entire office. They may or may not include a fax. They are built to handle large volumes of printing, scanning, and copying. Additional features such as automatic document feeder, duplex printing and scanning, and enhanced storage space are available by default.

## Laser Printers

A *laser printer* is a printer that uses a laser beam to project (or "draw") a document onto an electrically charged drum; toner adheres to the charged image and is transferred onto the paper as the paper moves through the mechanism at the same speed the drum rotates.



**Figure 16-3: A laser printer.**

### Components of Laser Printers

Laser printers include some specialized components not found in other printer types:

- *Toner cartridge*. This is a single, replaceable unit that contains the fine powder used to create images as well as additional components used in image production.
- *Laser scanning assembly*. This is the unit that contains the laser.
- *High-voltage power supply*. This component converts the supplied current to optimal voltage for specific components and also converts the supplied alternating current (AC) to direct current (DC) for specific internal parts of the printer.
- *Paper transport mechanism*. This includes the transfer belt and separator pads that move the paper through the laser printer. If the printer is equipped with a duplexing assembly, then the rollers flip the paper and draw it back through the print mechanism to print the back side of the paper.
- *Electrostatic Photographic drum (EP drum)*, or *imaging drum*. This component carries an electrical charge that attracts the toner. It then transfers the toner to the paper.
- *Transfer corona assembly*. This is a component that contains the corona wires; it is responsible both for charging the paper so that it pulls the toner off the drum and also for charging the drum itself.
- *Fuser assembly*. This unit, also known as the fuser, applies pressure and heat to the paper to adhere the toner particles to the paper.
- *Formatter board*. This unit exposes and processes all of the data received from the computer and coordinates the steps needed to produce the finished page.

## LED Printers

*LED printers* are similar to laser printers but use the latest printing technology, namely Light Emitting Diodes (LEDs), to replace the laser beam. Some LED printers can print 420 pages per minute.

## The Laser Print Process

In the laser printing process, laser printers print a page at a time using a combination of electrostatic charges, toner, and laser light. The laser print process follows the steps detailed in the following table.



**Note:** This is sometimes referred to as the "six-step process"; however, there are actually seven steps involved.

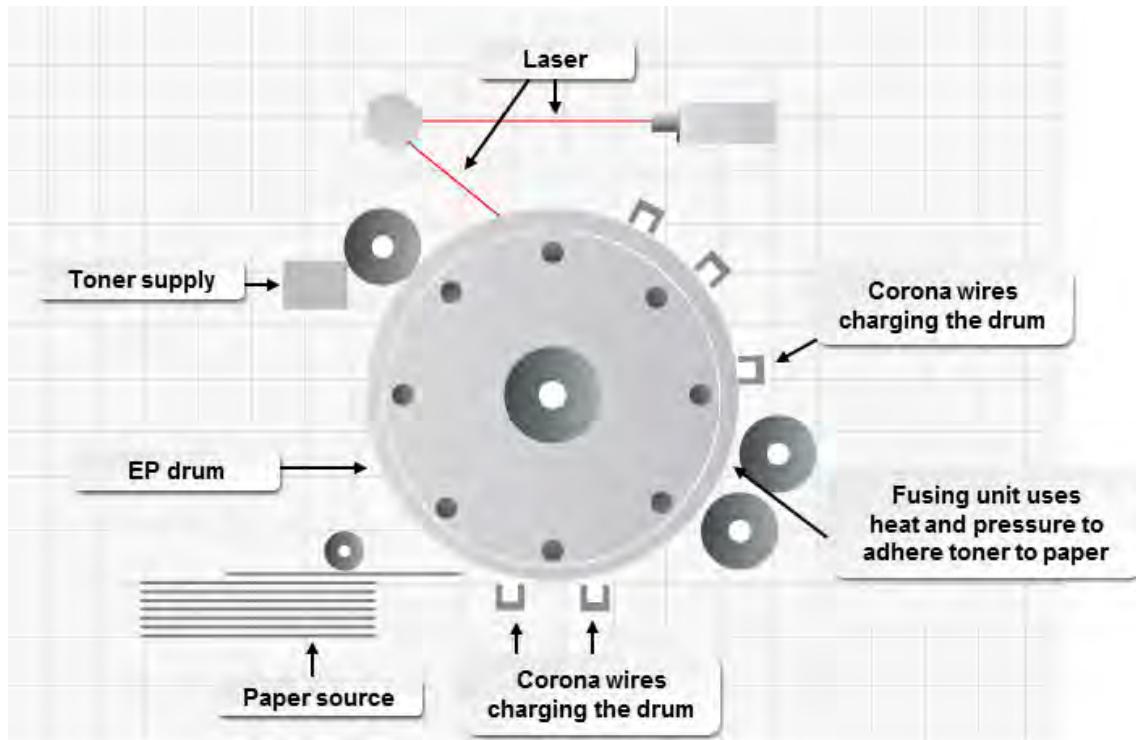


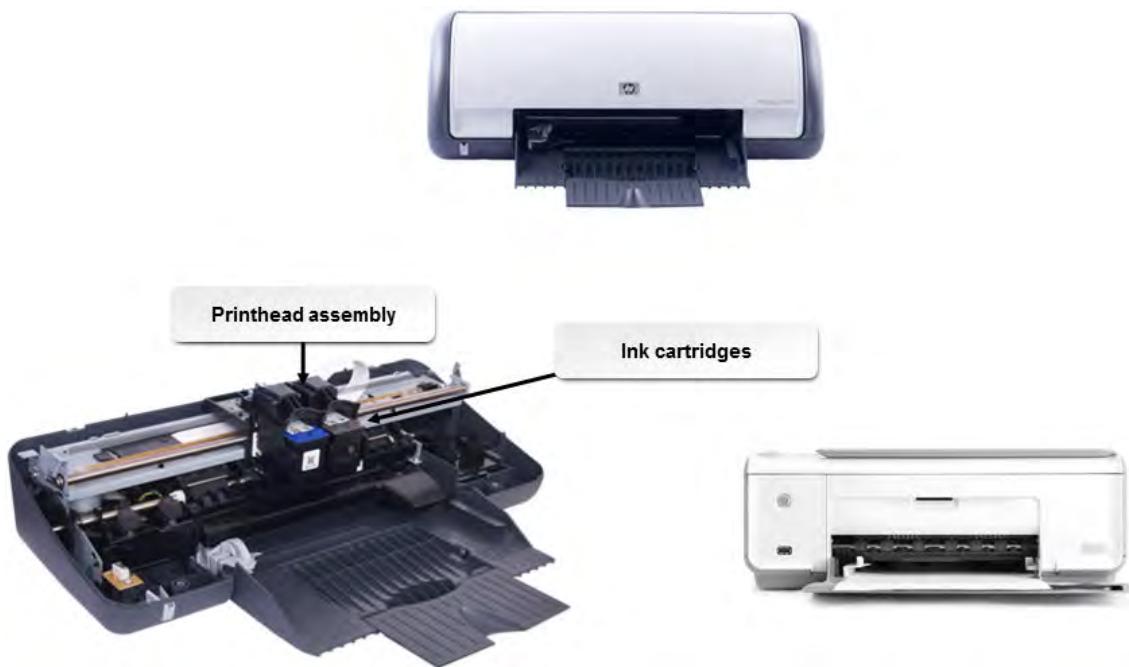
Figure 16–4: The laser print process.

Process Step	Description
1. Processing	The computer encodes the page in a printer language and sends it to the printer. The printer's firmware processes the data to create a bitmap of the page and stores it in the printer's RAM.
2. Charging (conditioning)	The imaging drum is conditioned by a charging roller powered by a high-voltage power supply assembly. The roller applies an electrical charge of -600 V across the drum's surface. Slightly older printers use a primary corona wire charged by a high-voltage power supply to apply the negative charge to the drum.

Process Step	Description
3. Writing (exposing)	A finely tuned laser beam neutralizes the negative charge on the photoreceptive drum to form an electrostatic image. The laser is activated to draw or write the image onto the drum. The laser beam remains stationary and bounces off a mirror that directs the beam through a series of lenses and mirrors that scans it over the rotating drum. The stream of rasterized data held in memory turns the laser on and off to expose the dots where toner will go to print the image. As the laser makes a single pass down the length of the drum, it reverses the charge on the dark parts of the image and leaves a static electric negative image on the drum surface as a -100 V charge. Areas of the page that should be white have a positive charge, and those that will be dark have a negative charge.
4. Developing	A roller (also called a developing cylinder) applies toner to the drum surface. The toner particles are charged and stick to the rotating cylinder, which is very close to the drum. The toner is attracted to the parts of the drum surface that have a -100 V charge and repelled from those areas with the -600 V charge. The toner sticks to those parts of the drum surface hit by the laser beam.
5. Transferring	Transferring is done using a transfer belt. A pickup roller moves a sheet of paper forward from the paper tray and a separation pad keeps more than one sheet of paper moving forward. A sheet of paper is pushed forward by the pick-up rollers and a charged transfer roller puts a positive charge on the paper to pull the toner from the drum and onto the paper. The paper moves past a static charge eliminator device, which reduces the charges on both the paper and the drum and keeps paper from sticking to the drum. (In some laser printers, the transfer corona wire applies the positive charge to the paper.)
6. Fusing	The toner is fused to the paper. The paper passes through the fuser assembly in which the heat roller applies heat to the paper and melts the toner. The pressure roller applies pressure against the heat roller to properly bond the toner with the paper. The printer monitors the temperature of the rollers and if they exceed the allowed maximum the printer shuts down.
7. Cleaning	A sweep strip cleans the drum of residual toner as it spins, and a rubber cleaning blade removes the toner from the area. The heat roller is lubricated to ensure an even transfer of heat and leftover charges on the drum are neutralized to return it to 0 V.

## Inkjet Printers

An *inkjet printer* is a printer that forms images by firing microscopic droplets of liquid ink out of microscopic ink jet nozzles mounted together on a carriage assembly that moves back and forth across the paper. The nozzles are mounted approximately one millimeter from the paper and aimed precisely on the printer. Inkjet printers have a self-cleaning cycle and will park the printhead when not in use. The printer can use heat or vibrations to release the ink.



**Figure 16-5: An inkjet printer.**

## Inkjet Printer Capabilities

Inkjet printers are very versatile. Inkjet printers vary by:

- The media they can print on:
  - Inexpensive copier paper
  - Bright paper made specifically for inkjet printers
  - Photo paper
  - Transparencies
  - Labels
  - Card stock
  - Envelopes
- Whether they produce black and white or color output.
- Whether they have duplexing capabilities.
- The cartridge design and the cost of cartridges.
- The speed at which they print.
- Whether the printhead is part of the printer or whether it is packaged together with the ink tanks in a print cartridge.
- The paper path. Some printers have a straight-through paper path and others turn the paper over as it passes through the printer.
- The resolution in dots per inch (DPI).
- How the ink is released. It could be:
  - The piezoelectric method, used in Epson printers. This uses a vibration to release a droplet of ink from the cartridge.
  - The thermal method, used in most other printers. This method releases a droplet of ink by heating up the ink.
- The volume of the ink drop, expressed in picoliters ( $10^{-12}$  liters). The smaller the drop, the less grainy the print output.

## Solid Ink Printers

*Solid ink printers* are somewhat of a cross between inkjet and laser printers except that they use ink from melted solid-ink sticks. The melted ink is forced into a printhead, where it is transferred to a drum, which then transfers the image to the paper as it rolls over the drum. Solid ink printers can produce an image with a clear, fine edge on a wide variety of media, such as standard paper or transparency film.

## The Inkjet Print Process

In the inkjet print process, inkjet printers spray ink on paper to form images. The inkjet print process follows the steps identified in the table.

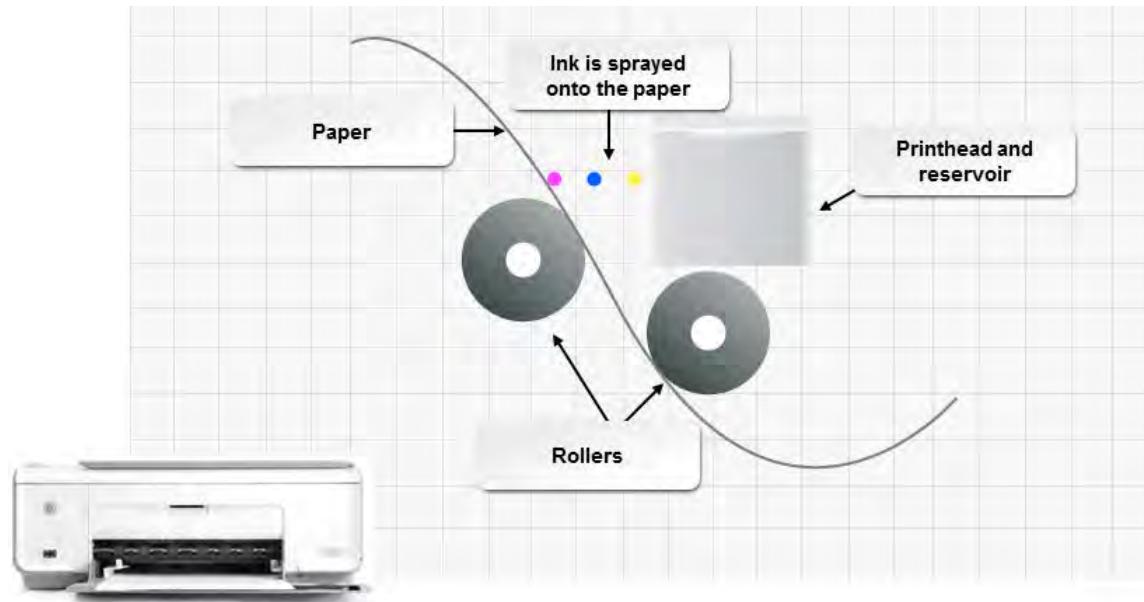


Figure 16–6: The inkjet printing process.

Process Step	Description
1. Preparation	When the print process is initiated, a motor and belt mechanism moves a printhead across the printer. Another stepper motor along with gears advance the paper into the printer.
2. Ink dispersion	As the printhead moves across the paper, images are formed by heat or vibration forcing liquid ink out of carefully aimed nozzles onto the paper. The printhead does not touch the paper. If the printer has double-sided printing capabilities, then the duplexing assembly will move the paper or other printing media through the printer twice.
3. Ink deposit	The printhead moves back and forth across the paper, printing one row of the image at a time. The amount of ink shot onto the page is determined by the driver software that controls where and when each nozzle deposits ink. The printhead typically produces at least 300 distinct DPI. Some printers can print at up to 1,200 DPI or more.
4. Paper advance	The paper advances using rollers and feeders after every row until the page is covered.

## Thermal Inkjet Printers

Thermal inkjet printers use heat to release the ink from the nozzle.

1. The ink in the printhead is heated to a specified temperature.

2. Once the ink is heated, bubbles are formed in the cartridge that burst and shoot ink onto the media.
3. The heat is turned off and the element cools.
4. More ink is sucked into the nozzle when the bubble collapses. Each thermal printhead has hundreds or thousands of nozzles that shoot spheres of ink that can create dots about 60 microns in diameter.

### Piezoelectric Inkjet Printers

Some inkjet printers use piezoelectric technology. Piezoelectric technology uses a piezo crystal that flexes when current flows through it. When current flows to the crystal, it changes shape just enough to force a drop of ink out of the nozzle and onto the paper.

### Thermal Printers

A *thermal printer* is a general term for any printer that uses a heating element to create the image on the paper with dye, ink from ribbons, or directly with pins while the feed assembly moves the media through the printer. There are several types of thermal printers that use significantly different technologies and are intended for different uses. The most sophisticated types of thermal printers can produce professional photo-quality images. There are also thermal printers for everyday office use and for special-purpose applications. Most thermal printers will require special *thermal paper* that contain chemicals designed to react and change color as it is heated by the heating element within the printer to create images. These printers are commonly used with cash registers to print receipts.



Figure 16-7: A direct thermal printer.

### Types of Thermal Printers

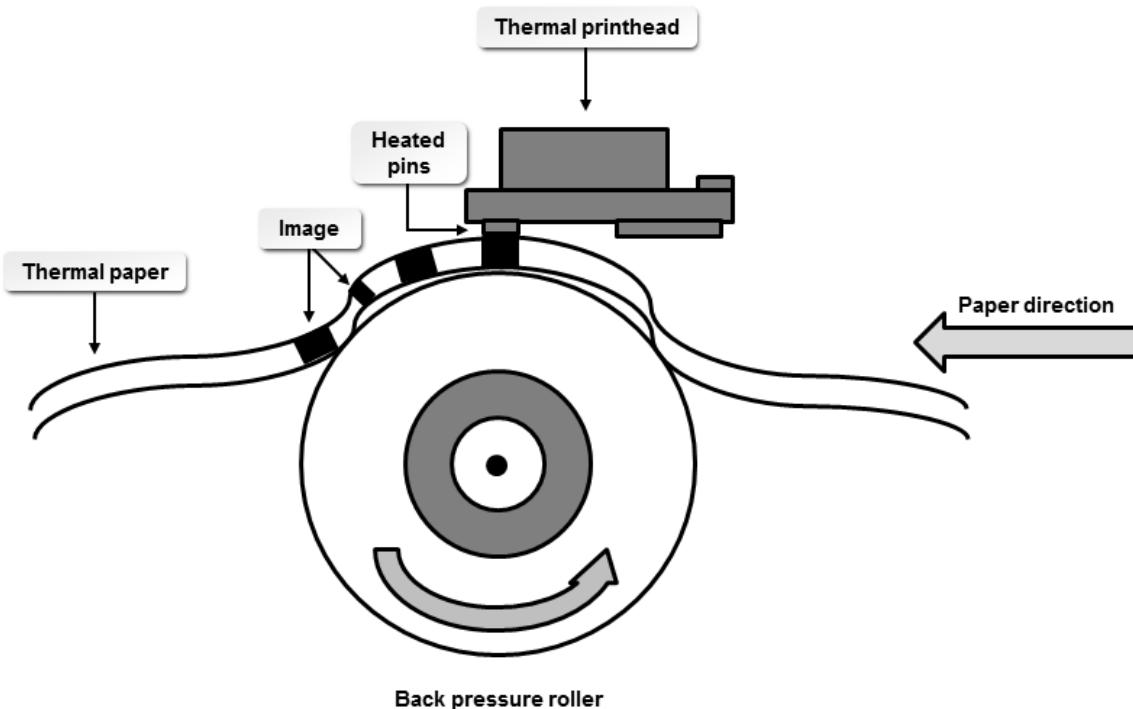
There are three basic categories of thermal printers.

<b>Thermal Printer Type</b>	<b>Definition</b>
Thermal dye transfer printer	A <i>thermal dye transfer printer</i> , also called a <i>dye sublimation printer</i> , is a sophisticated type of color printer that uses heat to diffuse dye from color ribbons onto special paper or transparency stock. The resulting continuous-tone image is similar in quality to photographic printing, and professional photographers employ them to produce prints quickly without having to send them to a photographic lab. However, the printers themselves are expensive and slow, and the special media is also expensive. Newer and less-expensive <i>snapshot printers</i> produce snapshot-sized images of acceptable photographic quality.
Thermal wax transfer printer	<i>Thermal wax transfer printers</i> have a thermal printhead that melts wax-based ink from a transfer ribbon onto the paper. These printers can be used in typical office settings as an economical way to produce color copies or color prints at an acceptable quality but at lower cost than dye sublimation printers. They are also used for standard text-based printing.
Direct thermal printer	<i>Direct thermal printers</i> use heated pins to form an image directly onto specially coated thermal paper. Early personal computer printers, such as Apple's first printer, the SilenType, were thermal printers. However, today's direct thermal printers are more commonly found in special-purpose printing devices such as cash registers and some fax machines.

## Thermal Print Processes

Each type of thermal printer uses a unique print process:

- Thermal dye transfer printers use a heating element to diffuse dye from color ribbons onto special thermal paper or transparency stock.
- Thermal wax transfer printers use a heating element to melt wax-based ink from the transfer ribbon onto special thermal paper.
- Direct thermal printers have a heating element with heated pins that create an image directly onto special thermal paper.



**Figure 16–8:** Direct thermal print process.

## Impact Printers

An *impact printer* is any type of printer that strikes a component directly against the ink ribbon to create characters on impact paper. The strike can be made with a group of pins or with a preformed type character. Impact printers tend to be noisy and slow compared to other printers and have largely been superseded by other printer technologies. The most common use is for printing carbon or carbonless multi-part forms such as receipts or invoices.



**Figure 16–9:** An impact printer.

## Types of Impact Printers

There are several terms used to categorize impact printers.

<b>Impact Printer Type</b>	<b>Description</b>
Dot-matrix printer	A <i>dot-matrix printer</i> is a type of impact printer that uses a set of pins to strike the ribbon. Dot-matrix printers create printed characters by using various combinations of dots. The printhead contains a vertical column of small pins that are controlled by an electromagnet. Because it uses an array of pins to form images, this type of printer can produce graphics as well as text.
Formed-character printer	A <i>formed-character printer</i> is any type of impact printer that functions like a typewriter, by pressing preformed characters against the ink ribbon to deposit the ink on the page.
Line printer	The printhead might be shaped like a golf ball, with the type distributed around the ball, or it might be in the form of a wheel with the characters around the perimeter of the wheel. Because of this type of printhead's resemblance to flower petals, they are referred to as daisy-wheel printers.

## Paper Feed Mechanisms

Impact printers can use either tractor feed when printing on continuous-roll impact paper, or friction feed when printing on individual cut sheets of paper. Tractor feed uses pairs of wheels with pins evenly spaced around the circumference at a set spacing. Continuous-roll paper with matching holes in the edges fits over the pins. The wheels turn and pull the paper through the printer. There are usually just two wheels, but there might be additional wheels or pin guides that the paper is latched to. There is usually a lever or other setting on the printer that needs to be engaged in order to use the tractor feed.

Friction feed uses two rollers placed one on top of the other. The rollers turn to force individual cut sheets of paper or envelopes through the paper path. This is used to print on individual sheets of paper (cut-sheet paper) and envelopes. Be sure to set the printer lever or other setting to the cut-sheet mode when printing using friction feed.

## The Impact Print Process

The impact print process consists of four steps.

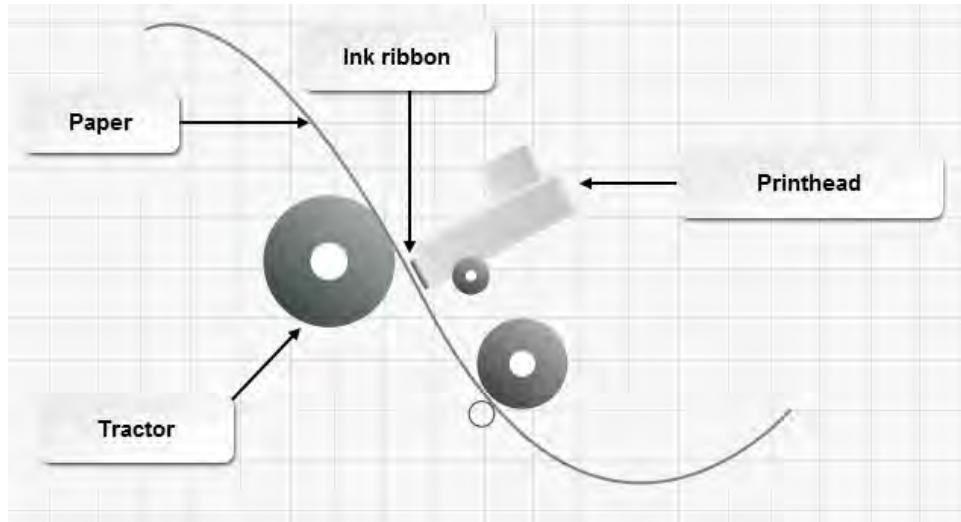


Figure 16-10: The impact print process.

Process Step	Description
Pin strike	The printhead has a vertical column of small pins that are controlled by an electromagnet. The pins shoot out of the printhead and strike an ink-coated ribbon. The dots created on the page become the printed text or graphics. More, smaller pins create better quality images. Printers come in 9-pin or 24-pin varieties.
Ink transfer	The impact of the pin transfers ink from the ribbon to the printed page. This physical impact is responsible for the printer's ability to print multiple-layer forms.
Printhead move	After a set of pins has fired, an electromagnet pulls them back in, the printhead moves a fraction of an inch across the page, and another set of pins is fired.
Letter quality pass	Near Letter Quality (NLQ) printers usually use two or more passes over a line of text to increase the number of dots used per letter. This connects the dots to form sharper and clearer letters.

## Virtual Printers

A *virtual printer* simulates a printer; however, there is no physical printer. Software is installed, or Microsoft Windows includes a virtual printer, and the virtual printer shows up in the **Printer** dialog box when you select to print something from your computer, tablet, or other device.

Some of the reasons users might need to print to a virtual printer include:

- Sending a document from their computer to a fax server.
- Creating a document that cannot be purposely or inadvertently changed.
- Making the document content available outside of the application which originally created the document.
  - Useful feature for sharing the document with others who don't have an application which can open the native file format.
- Combining multiple documents into a single document.
- Testing how the document will appear when printed on paper from a physical printer.
  - Useful feature to save on printer supplies.
  - If the document is not printing properly from the native application, sometimes it will print properly from a file created using a virtual printer.

Virtual printers typically print to a file of some type such as PDF, XPS, or an image file. The virtual printer might instead send the output to a fax queue on a fax server.

Examples of virtual printers include:

- Adobe Acrobat
- Nitro PDF Creator
- Microsoft XPS Document Writer
- Cute PDF
- GhostWriter
- Send To OneNote

The process for printing using a virtual printer is very similar to printing to a physical printer.

1. Install the virtual printer, if necessary.
2. From the application you wish to print from, open the document.
3. Using the application's **Print** option, select the virtual printer.
4. Configure any options provided in the **Print** dialog box as needed.
5. Select the **Print** button.
6. If necessary, specify the location and file name for the output.

# ACTIVITY 16-1

## Compare and Contrast Printers and Print Processes

### Scenario

There are several printers that are currently not deployed in your organization that are being stored in the IT department inventory cages. In order to determine which ones you will need when the time comes to replace currently deployed printers, you want to examine these printers to identify the features of each printer. You will then fill out the chart to identify which printers have which features.

- 
1. Examine the printers available to you, then fill out the table below. (Use the space on the bottom half of the page if necessary.)

<i>Printer Type</i>	<i>Creates Images Using</i>	<i>Connection Method</i>	<i>Paper Handling Mechanism</i>

2. Using the table you created, identify the similarities between the printer types. Identify the differences.
  3. Share your observations with the class.
-

# TOPIC B

## Install and Configure Printers

In the previous topic, you examined printer technologies, components, and processes. You can use this basic understanding when you install and configure printers. In this topic, you will install and configure printers.

Because printers are such a fundamental component of almost every computing environment, it is almost a guarantee that you will be called upon to set up and configure printing on devices no matter what professional environment you are working in. The skills you will learn in this topic should prepare you to install and configure a wide range of printer types efficiently and correctly.

### Printer Supplies and Media

There are a number of additional printer supplies and media that are necessary for a printer to function properly.

<b>Supply or Media</b>	<b>Description</b>
Printer toner	<p>Laser printer toner is a fine powder made of particles of iron, carbon, and resin. Laser printers require a toner cartridge, which is a single, replaceable unit that contains toner as well as additional components used in image production. You will need to maintain a supply of the proper toner cartridges for your printer model. Refill or recycle empty toner cartridges; do not dispose of them in regular trash.</p> <p>Users can change toner cartridges, but everyone should follow proper handling procedures, which are usually printed right on the cartridge. Toner particles can stain clothing or skin, especially when exposed to heat. Toner rarely spills, but when it does, clean it up with an electronics vacuum that has a fine filter and bag to contain the material. Using a regular vacuum can melt the toner if it gets on the vacuum motor. Use a dry paper towel, toner spill cloths, or cool water to clean toner from skin or clothing. Do not rub the area, because the heat from friction will make it harder to remove.</p>
Ink and ink cartridges	<p>Inkjet printers require ink cartridges to supply black or colored ink. You will need to maintain a supply of the ink cartridges for your printer model. Ink cartridges vary by:</p> <ul style="list-style-type: none"> <li>• The size of cartridges and how much ink each cartridge contains.</li> <li>• Whether black is produced using a separate cartridge or by combining the cyan, yellow, and magenta inks into a composite black output.</li> <li>• Whether there are separate cartridges for each color or if they are all in one unit. The black cartridge is separate on almost all printers, except for some very low-end printers. If the colors are in one unit and one color runs out, the entire cartridge needs to be replaced.</li> </ul> <p>Solid ink printers require you to supply solid ink sticks designed for your particular printer model.</p>

<b>Supply or Media</b>	<b>Description</b>
Paper and other media types	<p>Depending upon your printer, you may be able to print to a variety of media types, including:</p> <ul style="list-style-type: none"> <li>• Standard-quality copier paper in a variety of form sizes, such as letter, legal, tabloid, and so on.</li> <li>• Bright paper made specifically for inkjet or for laser printers.</li> <li>• Thermal paper for thermal printers.</li> <li>• Photo paper.</li> <li>• Transparencies.</li> <li>• Labels.</li> <li>• Card stock.</li> <li>• Envelopes.</li> </ul> <p>You will need to install paper trays that accommodate the media stock you select for your printer. You can also select paper trays in different orientations, whether letter or landscape. Some media sizes and types might need to be fed into the printer manually.</p> <p>Most printer output goes to an output bin on top of the printer, but there might be an additional or alternate straight paper path through a drop-down door, called a bypass tray, on the rear of the printer that you can use for specialized media, such as transparencies.</p> <p>Maintain an appropriate media stock on hand. Users can typically refill paper trays themselves if the correct stock is available.</p>

## Local and Network-Based Printers

There are two general types of printers you can install.

- *Local printers* are managed by and may be physically or wirelessly connected to the local computer. The local computer holds the *print queue*, which contains the print jobs waiting to print.
- *Network-based printers* are shared print devices that are managed by a network computer, called a *print server*. The print server holds the print queue.

*Network-connected printers* have built-in network adapter cards and connect directly to a network cable or via a wireless network interface. Print jobs are sent over the network using a network protocol such as Transmission Control Protocol/Internet Protocol (TCP/IP). Some network-connected printers have on-board print server software so they can be installed on the network directly and manage the print queue without requiring a separate print server computer.

### Printer Connections

Printers can be connected to a local printer or to the network through a wired connection or wireless connection. Wired connections use USB, serial, or Ethernet ports and cables. Wireless connections use Wi-Fi or Bluetooth connections. Wireless printers can be installed as part of the infrastructure of the local computer environment or the network environment. Alternatively, they can be part of an ad hoc network that is created for the current print session.

### Cloud Print Services

Using cloud print services, you can access printers. These are often public printers located in office supply stores or other specialty print shops. Accessing these public, shared printers can be accomplished using special apps available from the provider of the service. The app typically uses TCP, Bonjour, or AirPrint from your operating system along with print drivers and an app for the user to select where to print to.

Some reasons you might use cloud print services include:

- Print from a mobile device.
- Print to a specialized printer you don't have in your organization.

## Print Device Sharing

Depending on an organization's infrastructure, printers can be shared with computers, networks, or other devices using a variety of methods. Both local and network printers can be shared with other computers and devices.

<b>Method</b>	<b>Description</b>
Wired	With the increased use of USB and Ethernet cables over the years, parallel and serial cables and ports are just about obsolete. Most wired printers and MFDs found today will connect to devices using a USB port or are directly connected to a network via an Ethernet cable.
Wireless	Wireless printers offer many capabilities such as flexible printer locations. Printers can be connected to a wireless network using: <ul style="list-style-type: none"> <li>• Bluetooth®</li> <li>• 802.11x</li> <li>• Infrared (IR) technology</li> </ul> Like any other wireless device, you can connect a wireless printer to other devices in infrastructure mode (where the printer connects to an access point [AP]) or in ad hoc mode (where the printer connects directly to another wireless device).
Print server	Print servers hold the print queue for a number of printers connected to the same network. The server manages print jobs that come from client computers or devices, and sends the jobs on to the desired printer. You may also come across occasions when the print server is built into a printer, or is a component of an appliance that also provides additional functions, such as a firewall.
Operating system	Printers can be shared with other devices on the network by assigning print permissions that apply to local users and to users of a shared network printer. Permissions can be allowed or denied within the operating system settings, but if you deny a user the print permission, the user will have no access to the printer. Available permissions include: <ul style="list-style-type: none"> <li>• The print permission, which enables you to print to the shared printer. Assigned by default to Everyone.</li> <li>• Manage this printer, which enables you to print to the printer and fully administer the printer. Assigned by default to administrators.</li> <li>• Manage documents, which enables you to manage other users' documents. This permission includes the ability to manage all the jobs in the print queue.</li> <li>• Special permissions, which is generally only used by the system administrator to manage printer owner settings.</li> </ul>

## Data Privacy and Shared Devices

Security concerns become paramount when you begin to share devices among multiple users. You can configure the shared device to require user authentication when connections are requested. You can also create organizational policies that require hard drive caches to be cleared on shared devices.

## Workgroup Security Models and Print Permissions

To assign permissions to printer objects on a Windows® workgroup, you need to turn off **File Sharing** and enable **Classic authentication** so that local users can authenticate as themselves. In

the **Network and Sharing Center**, select **Change advanced sharing settings** from the left pane and then select the **Turn on file and printer sharing** option.

Once you do this, the **Security** tab will be available in the printer's property sheet.

### AirPrint

iOS and OS X include AirPrint. The AirPrint technology allows users to connect to a wireless printer that is located on the same network as the device from which you wish to print. Users select the AirPrint printer as the printer to which their document will be printed. By default, AirPrint only works over Wi-Fi, but following the documentation included with an AirPrint capable printer, you can also connect the printer via USB or Ethernet.

### Bonjour

Bonjour was created by Apple to provide zero-configuration networking. Through Bonjour, users can locate printers and file servers. It uses DNS service records to locate the devices offering print and file sharing services. The Bonjour software is part of OS X and iOS operating systems, and can be added to Microsoft Windows systems.

Various browsers have been created that enable users to graphically locate devices that can be found through Bonjour. These include the Bonjour Browser, jBonjourBrowser, Bonjour Browser for Windows, and mDNSBrowser.

### TCP

Networked printers on an Ethernet network will need an IP address. Users can then add the printer through the operating system's add printer method, using the IP address.

## Printer Configuration Options

Depending upon your particular printer, you will have various options for configuring and optimizing printer performance.

<i>Printer Configuration Option</i>	<i>Description</i>
Duplex	The printer might have a built-in <i>duplexing</i> feature that enables the user to automatically print on both sides of a page. For other printers, the user will need to manually remove the printed pages from the output tray and reload them in the proper orientation to print on the other side of the paper. Most printers with manual duplexing provide on-screen instructions for how to orient the paper for printing the second side.
Collate	If you are printing multiple copies of a file, the <i>collate</i> feature keeps all of the pages for each copy together. This prevents the user from needing to manually sort through the stack of output pages and assembling each copy by hand.
Orientation	The <i>orientation</i> option allows users to specify whether the document will be printed in <i>landscape</i> or <i>portrait</i> . For example, landscape on an 8.5 x 11 inch page would have the top and bottom of the page on the 11 inch sides of the paper, and portrait orientation would have the top and bottom of the page on the 8.5 inch sides of the paper.
Print quality	The <i>print quality</i> option enables users to specify whether they want to print draft, normal, or high quality output. Draft prints quickly and uses less ink or toner, while high quality takes longer and uses more ink or toner. Instead of generic terms like draft or high quality, some printers provide the <i>DPI</i> (dots per inch) of the output.

Other options you might need to configure include:

- Device calibration
- Tray assignments
- Tray switching
- Print spool settings
- Printer availability
- Color management
- Printer ports



**Note:** For additional information, check out the LearnTO **Install and Configure a Printer** presentation in the LearnTOs for this course on your CHOICE Course screen.

## Cloud and Remote Printing

With so many users being mobile and using mobile devices, the ability to print from those devices is becoming more and more important. Being able to print to the printer back at the office, or to a printer in another office, can be accomplished through remote printing. Printing from a device that doesn't normally have print capabilities can be accomplished by installing an app on the device and using cloud printing. Or, you might need to print handouts to a printer at the hotel or conference center; this can also be accomplished through cloud printing many times.

Printer manufacturers have created print servers which can be accessed through their app on your mobile device. Examples include Epson and HP. The print job is sent to the manufacturer's print server, then printed at a printer detected by the app. The printer might be in a hotel, an office store, or a copy shop. You will pay a per-page fee for using the printer.

Chances are, you don't want anyone but you or your intended audience to see the printed output. You should wait to print until you are near the public printer. Some apps provide you with a code that will hold the print job on the print server until the user enters a code they were emailed. The code is entered directly on the physical printer to release the job from the print queue to the printer.

One cloud printing solution is **Google Cloud Print**. This works with both newer and older printers. It allows you to make your printers available to you or the users you specify. Users can print from any web-connected device that has the ability to print. The user does not need to install the print driver for the selected printer in order to print when using this service.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Install and Configure Printers.

# ACTIVITY 16-2

## Installing and Sharing a Local Printer

### Scenario

One of users in the HR department has just asked you to install a printer that he purchased for the department. He would like to use this printer on his Windows 8 computer as his default printer. He has also asked that you make the printer available to other users in the department. Even though he has not yet received the printer, he would like you to configure his computer so that all he will need to do is plug in the printer when it arrives.

1. Install the printer.
  - a) Open **Control Panel** in **Category** view.
  - b) Under **Hardware and Sound**, select **View devices and printers**.
  - c) Select **Add a printer**. If the printer isn't listed, select **The printer that I want isn't listed** and then select **Add a local printer or network printer with manual settings**. Select **Next**.
  - d) From the **Use an existing port** drop-down list, select the desired port and then select **Next**.
  - e) On the **Install the printer driver** page, from the **Manufacturer** list, select a printer manufacturer.
  - f) From the **Printers** list, select a printer and select **Next**.
  - g) In the **Printer name** text box, type ***My Local Printer***
  - h) Select **Next**.
2. If the option is available, share the printer.
  - a) On the **Printer Sharing** page, verify that **Share this printer so that others on your network can find and use it** is selected.
  - b) In the **Location** text box, type ***IT testing area***
  - c) Select **Next**.



**Note:** If the option to share is not available, finish installing the printer, then right-click the printer and select **My Local Printer Properties**. On the **Sharing** tab, check **Share this printer**, and in the **Share Name** text box, type ***IT testing area*** and select **OK**.

3. Create a print job on the local printer.
  - a) Select **Print a test page**.
  - b) Select **Close**.
  - c) Select **Finish**.
  - d) In the **Devices and Printers** window, right-click **My Local Printer**.
  - e) Select **See what's printing**.
  - f) At least one print job should appear in the queue. Close the print queue window and the **Devices and Printers** window.

# TOPIC C

## Maintain Printers

Proper printer maintenance will extend the life of a printer and will help prevent mechanical issues in the future. Printer maintenance should become a routine part of your job as an A+ technician. Each type of printer has specific tasks you should perform to keep it in operating condition. In this topic, you will examine the maintenance required for various types of printers.

### Laser Printer Maintenance

Laser printers have many moving parts, parts that get very hot, and parts that can get quite dirty. Performing preventive maintenance is an important task that should be performed on a regular basis. The frequency of tasks varies based on printer, how much use it gets, and under what conditions it is operating.

- Replace the toner cartridge once it gets low.
- You might need to calibrate the printer if the automatic calibration is not effective in maintaining high-level print quality.
- Apply maintenance kit at intervals as specified by the manufacturer. Preventive maintenance kits typically include:
  - Fuser
  - Transfer roller
  - Rollers for feeding paper, picking up paper
  - Separation pads and rollers
- Clean excess toner out of the printer each time you replace the cartridge to avoid buildup inside the printer.
- Be mindful of the printer's location. Keep it well ventilated with proper spacing from other devices.

### Thermal Printer Maintenance

Thermal printers are often used in cash registers and for printing labels. Both of these uses require the printer to be available at all times, and to keep up availability, you should perform regular maintenance.

In cash registers, the cashier rips the paper across the serrated teeth to give the receipt to the customer. This can lead to a build-up of paper dust in the printer from tearing off receipts. It can also lead to bits of paper becoming lodged in the mechanism if a clean slice is not made and bits of leftover paper fall into the printer.

Label printers can end up with sticky residue inside the printer. If labels are not loaded correctly, they can separate from the backing while being fed through the printer. You will need to ensure users know how to properly load the labels and how to clean up if labels get stuck inside the printer.

- Replace the paper when needed.
- The heating element may need cleaning to prevent buildup and smudging.
- Remove debris from inside and outside printer to prevent unwanted particles from getting into the printer components.
  - Cleaning cards made specifically for cleaning thermal printers can be run through the printer to help clean the printhead and the rollers.
  - Only use cleaning cards when required, as they can be abrasive and wear down components.
  - Clean any sticky residue using isopropyl alcohol.

## Impact Printer Maintenance

Impact printers are often found in point-of-sale terminals and back-office environments. As with the other printer types, performing routine maintenance will help ensure the printer is performing properly when users need it.

- Regularly clean the paper path and the ribbon path using a dry, soft cloth.
- Replace the printhead, ribbon, and paper when needed.
- Regularly vacuum the dust from the wheels in the tractor feed assembly.
- To avoid overheating the printhead, be mindful of the printer's location. Make sure it is clear of clutter and other machines.

## Inkjet Printer Maintenance

Inkjet printers are an affordable printer type that enables users to print in black-and-white or in color. These are not usually designed for heavy workloads, so they might sit idle for long stretches of time. If they are in regular use, the consumables might be used up quite quickly. Performing proper maintenance will ensure the printer is available when it is needed.

- Use the printer often to prevent the ink from drying out and clogging the nozzles.
- Replace cartridges that are out of ink, are so low that incorrect colors are being printed, or that have dried out.
- Perform calibration as needed if colors are off, streaks are appearing in output, or the image is off-center.
- Run the printer's cleaning utility to clean the printhead.
- Run the printer's nozzle test.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Perform Printer Maintenance.

# ACTIVITY 16-3

## Performing Printer Maintenance

### Before You Begin

You have at least one printer available. If not, search for the maintenance procedures for specific models of printers.

### Scenario

It has been determined that in your organization, some maintenance tasks must be performed on a daily basis. Others need to be performed weekly, and others on an as-needed basis. It is your turn to take on printer maintenance today.

1. Review the documentation for your printer to determine the recommended printer maintenance.
  - a) Obtain the documentation, either in print form or by searching online for your printer model.
  - b) Briefly review the documentation and determine what maintenance tasks should be performed, and how often they should be performed.
2. Following the documentation you obtained in the previous step, perform any recommended maintenance on your printer.
  - a) Clean the exterior of the printer.
  - b) Clean the interior of the printer of any bits of paper, dust, or other foreign objects.
  - c) Verify that the ink or toner levels are adequate.
  - d) Verify that paper has been loaded in the printer, and that it is loaded correctly.
  - e) Determine if a maintenance kit should be used on your printer.

# TOPIC D

## Troubleshoot Printers

Earlier in the course, you employed troubleshooting tools and techniques for hardware components within the computer or mobile device. There are other peripheral devices that users may frequently use with their computer or mobile device, like printers, that will experience problems or malfunctions that require your assistance. In this topic, you will troubleshoot printers.

As a support professional, you are well aware that one of the most unpleasant problems for users is being unable to print. If users need hard copies of documents and the systems do not work, it can be very frustrating. Users will look to you to identify and resolve their problems quickly, so you will need to perform proper maintenance to prevent problems, to recognize common issues, and to correct them efficiently when they occur.

### Common Printer Troubleshooting Tools

Printing troubleshooting tools can be used to fix common printing issues and can also help you in diagnosing printer problems.

Tool	Description
Maintenance kit	<p>Printer maintenance kits for laser printers are made up of printer components that get worn out with regular everyday use. Most printers are designed to notify users when they have reached their predetermined page count and maintenance schedule. Usually, the printer will display a message such as "Perform Printer Maintenance." This means that the printer manufacturer recommends installing a printer maintenance kit at this time. Once the kit is installed, you must reset the page count on the printer to keep an accurate schedule for maintenance.</p> <p>Common components included in the kit are:</p> <ul style="list-style-type: none"> <li>• Transfer rollers and pickup rollers.</li> <li>• Corona assembly.</li> <li>• Fan assembly.</li> <li>• Fuser assembly.</li> <li>• Cloths and gloves for handling printer components.</li> </ul> <p>For newer printers, you also can purchase individual cartridges as needed. For example, fusing is done inside the fuser cartridge. It's possible to lower the cost of maintaining a laser printer by replacing only the appropriate cartridge.</p>
Toner vacuum	<p>When you suspect that the printer needs to be cleaned due to toner build up within the printer, then make sure to use a toner vacuum. Toner vacuums are specifically designed to clean up toner within a printer. The vacuum is able to reserve the particles within the tool so that it is not dispersed back into the air. Never use a conventional vacuum to clean up toner because the particles are so small that there is risk of them getting blown back into the air surrounding the printer. This can be harmful to your health.</p>
Compressed air	<p>Compressed air is sometimes used to clean out the dust and debris from inside the printer. Refer to your manufacturer's documentation for any guidelines on using compressed air to clean the printer. Some manufacturers advise against using the air, because it can actually cause moisture build up within the printer.</p>

Tool	Description
Extension magnet	A telescoping wand with a magnet attached to the end is used to pick up screws or other metal pieces that may fall into the printer or scanner. For inkjet printers and dot matrix printers, it can come in handy to retrieve paper clips people have dropped into the paper-feed mechanism. But for laser printers, reaching inside the printer can be hazardous. If you need to reach inside a laser printer, take <b>extreme</b> caution as there are fragile components and high-voltage electronics inside laser printers.

## Printer Software Tools

In addition to the standard toolkit, there are several specialized resources you can employ when you research and troubleshoot printing problems.

Troubleshooting Resource	Description
Test patterns	Depending upon your printer, you might be able to run test patterns to check the clarity and print quality of your printer. It allows you to determine what settings need to be adjusted or what ink colors need to be refilled. Test patterns are either built in or external to the printer and are used to test for calibration and alignment of the printhead and to check the color/grayscale tone.
Printer spooler	The printer spooler can be a useful tool when determining where a print job is faulting. If the job is getting through the spooler then it may indicate a hardware issue, but if its not, then it could be an issue with the application that the job was sent from or a connection issue.
Power cycling	Power cycling a device refers to turning the device off and letting it rest for 10 to 30 seconds before powering it back up. This can give the printer some time to clear the memory and start up again.
General diagnostic utilities	Many printers come with other self-diagnostic programs that can resolve basic hardware issues. Refer to the printer's manual on the specific steps required to perform the diagnostics.  Windows and other operating systems often provide help for troubleshooting general problems as well as for problems specific to that system. In particular, each version of Windows provides a troubleshooter that can walk you through the diagnosis and resolution of common printer problems or problems with other devices.  In Windows 7, common printer problems can be resolved by displaying the pop-up menu from the <b>Printer</b> icon and selecting <b>Troubleshoot</b> .  There are other generic utilities you can use, such as capturing a printer with the <code>net use</code> command, or redirecting output to a printer with the <code>prn</code> command.
Device documentation	For device-specific problems, consult the documentation that came with your printer or scanner.
Manufacturers' websites	Most device manufacturers will maintain technical information on their websites that can help with printer troubleshooting and ongoing maintenance. You can also download updated printer or scanner drivers or diagnostic software tools from the manufacturer, or use web-based utilities to help you diagnose the problem.

<b>Troubleshooting Resource</b>	<b>Description</b>
Software vendors' websites	Microsoft and other operating system vendors maintain libraries of technical information on their websites that can help with troubleshooting known problems with specific devices, or general issues related to the printing function in the specific operating system.
Error codes and reports	Review any error messages at the printer and at the computer. This might involve checking computer event logs. Some printers may have an out of memory error displayed when the printer memory is beyond capacity.
Service logs and reports	Check prior service records for the system to try to identify recurring problems. Check for previous user reports of similar issues to see how the issues were resolved.
Troubleshooting principles	As with all troubleshooting, follow a structured process: 1. Gather information and identify the symptoms. 2. Review the data and establish a possible cause. 3. Identify and test a solution.

## Common Printer Symptoms

When troubleshooting various printers and print job issues, keep in mind that some of the simplest tasks such as pausing, restarting, or canceling a print job from the queue can easily fix some common printing problems. User education and awareness of these common problems and solutions will enable you to better support users. There are a number of common issues related to all types of printers.

<b>Symptom</b>	<b>Possible Problems and Solutions</b>
Backed up print queue or printer will not print	<p>There are several issues that can cause a printer's queue to back up or not print at all:</p> <ul style="list-style-type: none"> <li>• If you suspect that the printer is out of toner, ink, or paper, then add what is necessary. Verify the printer's status and press the <b>Test</b> button on the printer.</li> <li>• If you suspect that there is a paper jam, or the printer is displaying an error code indicating a paper jam, then clear the jam. If the paper jams are frequent, then the printer may need to be serviced to clean or replace old or worn components such as rollers.</li> <li>• In Windows, there are several settings that will cause issues. The printer may be paused. In this case, right-click the printer and disable the pause printing option. The print spooler service may be stalled, so stop and start the service. Or, the <b>Use Printer Offline</b> option has been enabled.</li> <li>• If the printer has been configured to be available on a specified schedule, then you may need to verify and adjust the availability schedule.</li> <li>• An incompatible print driver will prevent sending print jobs to the printer. You may need to delete the driver and reinstall the updated one using the manufacturer's installation instructions, if available.</li> </ul>

Symptom	Possible Problems and Solutions
Creased paper	<p>Paper showing creases on output could indicate that the printer is jammed. Remove any obstructions in the paper path. Also verify that the paper rollers are functioning properly, as faulty rollers may warp paper as it is output from the printer.</p> <p>Creased paper may also indicate the wrong size of paper is loaded into the tray. Check the printer's manual to verify what sizes it accepts. The paper itself may also not be loaded correctly; ensure that the stack is flat and aligned properly within the loading tray.</p>
Paper not feeding from tray	<p>There are several possible issues that prevent paper from being fed from the tray into the printer:</p> <ul style="list-style-type: none"> <li>The printer's software may be malfunctioning. Shut down the printer, unplug it, wait a few seconds, then turn it back on.</li> <li>The printer driver may be misconfigured. If the paper you load into the tray is not the same size as what's configured in the printer driver, the printer may refuse to feed paper from the tray. Go into your printer's settings and adjust the size as needed.</li> <li>The paper in the tray may be damaged in some way that is preventing the feeding mechanism from moving the paper. Open the printer and check for obstructions.</li> <li>Dust or other debris inside the printer can affect its internal components, especially the rollers. Open the printer and use compressed air to clear out any debris.</li> </ul>
Printing blank pages	<p>There are several possible issues that could cause the printer to only print blank pages:</p> <ul style="list-style-type: none"> <li>The ink and toner may need to be replaced, or may not be installed properly.</li> <li>The printer's software may be malfunctioning. Shut down the printer, unplug it, wait a few seconds, then turn it back on.</li> <li>The computer you're printing from may also need to be restarted.</li> <li>It might be an application issue. Try printing from a different application. Also check the print preview of the application you're printing from and verify that it isn't blank.</li> <li>The printer settings may be misconfigured. Configure the settings to their default, and ensure that the printer is the computer's default printer.</li> <li>If your printer is wireless, other devices connected to the computer might be interfering with the signal. Disconnect mobile devices like phones and Bluetooth headsets.</li> </ul>

Symptom	Possible Problems and Solutions
No connectivity	<p>Depending on the nature of the connection, there could be several problems preventing connectivity to a printer:</p> <ul style="list-style-type: none"> <li>For wireless printers, ensure that no other wireless device is interfering with the connection.</li> <li>Ensure that your computer is within range of the printer's wireless signal.</li> <li>Certain physical objects like walls may distort a wireless signal or dampen its range. Try to position the computer or printer to minimize the amount of obstacles.</li> <li>For wired printers, ensure that the cable is properly connected and not showing signs of physical damage.</li> <li>Your computer may not be able to see the printer automatically, but you may still be able to connect manually. Obtain the printer's local IP address and connect to it directly. Windows' printer setup wizard enables you to do this, as well as connecting to the printer if it has a hostname on the network.</li> <li>Restart both the printer and the computer.</li> <li>Reinstall the printer's drivers on the computer.</li> </ul>
Unable to install printer	<p>Verify that you've downloaded the latest drivers from the printer manufacturer's website. Outdated drivers may not install properly on newer systems. Also ensure that your operating system is actually supported by these drivers, as they may differ between OS type and version.</p> <p>There's also the possibility that existing printer drivers are interfering with the one you're trying to install. Uninstall these other drivers, then try installing the new one. If you need these older drivers for other printers, try removing them from the default printer status, then install the new printer driver as the default.</p>
No image on printer display	<p>A blank display is most often a power issue. Unplug and replug the printer into a power source. Also verify the power source itself is functioning properly and is not overloaded with other electronics.</p> <p>If the power on the printer is on but the display is blank, try restarting the printer by holding the power button down for several seconds. Failing this, the printer's internal display components may need to be replaced.</p>
Printer does not print the way the user expects it to	<p>If the printout is not showing the output you expect, then this could be a page setup, printer property, or settings issue. You should verify that the page setup options and the printer properties are configured correctly. If you have confirmed the settings for the printer and the application you are printing from, then you may need to use a maintenance kit or a driver software update to fix the issues.</p> <p>If the printout is streaking, this could be a sign that the printhead needs to be cleaned.</p>

Symptom	Possible Problems and Solutions
Print quality issues	<p>There are a few different print quality issues that indicate the printer is experiencing problems:</p> <ul style="list-style-type: none"> <li>• Poor overall print quality might simply be due to running out of ink or toner. Check all ink or toner cartridges to ensure that they are not empty.</li> <li>• Streaks may indicate that the printer head needs to be cleaned due to clogged head openings.</li> <li>• Faded prints can be an indication of a bad toner cartridge. If you are using the re-manufactured cartridges, then you may need to try a new one. If that does not fix the issue, then there may be an issue with the fuser.</li> <li>• Vertical lines are a symptom of inkjet printheads being out of alignment. This can also be a sign that the printing ribbon needs to be replaced.</li> <li>• Color prints in the wrong color. Use the advanced printer settings to verify that the color settings are correct. You may need to select a different output option, such as the print quality.</li> <li>• On an impact printer, a white streak through the output can indicate there are damaged pins in the printhead.</li> </ul> <p>Print quality can also be affected by the quality of the paper being used.</p>
Access denied	<p>When users cannot access a network printer, then there is a possibility that there is no connectivity. Either the printer or the user has lost a connection to the network.</p> <ol style="list-style-type: none"> <li>1. Verify which device needs to be reconnected and make necessary changes.</li> <li>2. If the connections are functional, then check the printer or print server status and restart, if necessary.</li> <li>3. Also verify that the IP address assigned to the printer is correct.</li> <li>4. Finally, you can check the printer's power cycle to make sure it is coming online once it has been powered up.</li> </ol> <p>Another possible case for a user not being able to access a printer is that the user does not have permission to use the printer. Check share permissions and adjust as necessary.</p>
Garbled characters on paper, or is showing ghosted images	<p>When a printer outputs garbled or ghosted images, there is something wrong with the printer. These symptoms can mean several different things:</p> <ul style="list-style-type: none"> <li>• The printer is low on memory. Check to see if you can install additional memory.</li> <li>• The resolution needs to be adjusted in the printer settings.</li> <li>• The driver is incompatible, so update or replace the driver.</li> <li>• The cabling may be damaged or not fully connected, so check all cables to make sure they are secure and intact.</li> <li>• In laser printers, this can be a sign that the drum is not completely cleaned (erased) or the fuser assembly has been damaged. You should contact the manufacturer or check the website for additional information and troubleshooting steps.</li> </ul>

Symptom	Possible Problems and Solutions
Print jobs never appear in print queue	<p>General network problems. Check the network status of the client, printer, and print server.</p> <p>Insufficient user print permissions. The user probably got an error message. Update the permissions.</p> <p>Insufficient space on the drive containing the spool folder. Move the spool folder or add disk space.</p>
Other sporadic print problems	<p>Unfavorable environmental conditions can lead to unexplained problems with printers. Check for and correct these situations, if possible.</p> <ul style="list-style-type: none"> <li>If the printer is installed in an environment with a large quantity of dust and dirt, such as a factory floor or a pet shop, debris can accumulate in the printer case. Keep the printer clean in an enclosure in these environments if possible, but be mindful of heat accumulation in the enclosure.</li> <li>High humidity can lead to moisture problems; low humidity can lead to static problems. Try to maintain a relative humidity of 50 to 60 percent.</li> </ul> <p>Low memory errors can indicate that the print driver memory settings need to be changed, that the user's computer is not spooling documents properly, or that additional printer memory is required.</p> <ul style="list-style-type: none"> <li>Most print drivers will install a low memory default setting that can be changed, if needed. You can update the driver setting to match the printer memory capabilities to resolve this issue.</li> <li>Make sure the user's computer is spooling documents. In the printer settings, change the print spooling setting to <b>Start Printing Immediately</b>. You might also need to restart the print spooling service.</li> <li>Upgrade the printer's RAM.</li> </ul>



**Note:** In Windows 7, Windows 8, and Windows 8.1, you can troubleshoot a printer by right-clicking the printer and selecting **Troubleshoot**.

## Laser Printer Problems

Laser printers contain chemicals, high voltages, and high-temperature areas that can hurt you. Make sure the printer is off and the parts are cool before you attempt to work on the machine. Some of the exposed wires are very thin and can be damaged easily, so treat the printer gently.

Symptom	Possible Problems	Solutions
Smeared output, or output rubs off the paper	Fuser temperature is too low: if the fuser is not hot enough, the toner is not fused to the paper; fuser roller is uneven; problem in paper path; paper not smooth enough.	Follow the manufacturer's instructions to set fuser mode for the paper; adjust the fuser roller; clear the paper path; use good-quality paper.
Low-quality image	Poor-quality paper does not accept charge and transfer toner; transfer corona is dirty or faulty; there's a transfer corona power supply problem; a faulty primary corona or power supply does not charge print drum.	Use good-quality paper; follow the manufacturer's instructions to clean the transfer corona; follow the manufacturer's instructions to troubleshoot other faulty components.

Symptom	Possible Problems	Solutions
Repeating horizontal lines or white spaces	Dirty fuser roller; warped or worn fuser roller; scratched print drum due to debris between wipe blade and drum.	Clean all fuser rollers; compare the distance between the repetitions of the lines to the circumferences of the rollers, and consult manufacturer's documentation to find which may have the problem. Follow the manufacturer's instructions to adjust or replace rollers and fuser.  Follow the manufacturer's instructions to replace the scratched print drum.
Repeating vertical lines or white spaces	Scratched print drum; dirty primary corona or transfer corona produces uneven charge; refilled toner cartridge produced substandard output.	Follow the manufacturer's instructions to replace scratched print drum or clean corona wires; or replace with a new cartridge.
The paper slips or begins to pick up 2–3 pages or more at once, and then jams; paper is not feeding; paper is creased	Pickup and path wheels worn or dirty.	After a long period of use, these wheels lose their grip. Wheels either need to be cleaned with alcohol or replaced.

## Inkjet Printer Problems

Most issues related to inkjet printers can be resolved by cleaning the printer, cleaning the paper feed rollers, replacing the print cartridge, and using good-quality paper. There are, however, occasions when a component will need to be replaced. In this case, it may be more cost effective to just replace the printer instead of trying to repair it. The following are common symptoms and potential solutions you can use when supporting users.

Symptom	Possible Problems	Solutions
Poor print quality	Clogged nozzles; incorrect paper; empty or defective cartridge.	Clean the interior of the printer; perform one or more print cartridge cleaning cycles; switch to a paper specifically designed for inkjet printers.  Replace the cartridge. If you are using a refilled cartridge, replace with a new cartridge.
No output; paper passes through printer but is blank	Empty ink cartridges; clogged nozzles; tape sealing ink cartridge; incorrect cartridge or cartridge improperly seated.	Replace empty or incorrect ink cartridges; clean the printer and print cartridge; remove the tape seal from ink cartridge; align the cartridge; check the manufacturer's website for other troubleshooting procedures.
Feathering/ink bleed	Clogged nozzles; low ink in cartridge; faulty printhead; low-quality refilled cartridge.	Perform several cleaning cycles; replace ink cartridge with a new one (not refilled); replace the printhead; switch to a paper specifically designed for inkjet printers.

Symptom	Possible Problems	Solutions
The paper slips or begins to pick up 2–3 pages or more at once, and then jams	Pickup and path wheels worn or dirty.	After a long period of use, these wheels lose their grip. Wheels either need to be cleaned with alcohol or replaced.

## Common Impact Printer Problems

Dot-matrix printers and other impact printers are not as commonly used as the others but they are known to be rugged and dependable. Most issues related to these printers are due to printhead problems. The following are common symptoms and potential solutions you can use when troubleshooting.

Symptom	Possible Problems	Solutions
Horizontal lines appear in the print so parts of characters are missing	Printhead is damaged or needs to be cleaned.	Attempts to repair a printhead can damage it beyond hope. You can clean the printhead with a lubricant like WD-40 or alcohol. Remove any visible grime.
Flecks and smudges on the paper	The ribbon is not aligned correctly, not feeding correctly, or is over-inked.	Reposition the ribbon. Replace the ribbon cartridge; cartridges are not economical to repair. Clean and lubricate the gears that advance the printhead.
Poor print quality	The printer adjustment for paper thickness is set to an incorrect value; poor-quality paper; bad ribbon; dirty printhead.	Set the thickness to match the paper you are using. Use good-quality paper. Replace the ribbon. Clean the printhead.
Continuous-feed paper jams	Tractor feed problems.	Clean paper from gears. Align tractor feed. Replace worn gears.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Troubleshoot Printers.

# ACTIVITY 16–4

## Troubleshooting Common Printer Issues

### Before You Begin

Your instructor will introduce one or more problems with the printers in the classroom.

### Scenario

The printers in your office are a mix of types, brands, technologies, and reliability. You have been doing regular maintenance on them, but there are still some issues that users have encountered.

1. The user reports that the printed output is not up to the usual standards for their printer. You will need to resolve this issue so she can print their report.
  - a) Print out a test page to see if you can reproduce the problem the user reported.
  - b) If you see the same problem as reported by the user, take the appropriate steps, based on the type of printer, to resolve the problem.
  - c) Document the steps you took to resolve the problem.
2. The user reports that they can see their job in the print queue, but that the job never comes out of the printer.
  - a) Send a print job from Notepad or another application.
  - b) Verify that it shows up in the print queue for the printer in question.
  - c) Take steps to resolve the problem.
  - d) Document the steps you took to resolve the problem.
3. Resolve any other problems that are preventing getting good output from the printer.
  - a) Document what you think the problem might be.
  - b) Test your theory.
  - c) Document the steps you took to resolve the problem.

## Summary

In this lesson, you supported printers. Because printers enable users to transfer digital information to paper, they are among the most commonly used devices in almost every type of computing environment. As an A+ certified professional, you can use the skills and knowledge from this lesson when you are called upon to install, configure, or troubleshoot printers.

**When would you recommend to users that they user laser printers? Inkjet printers? Impact printers? Thermal printers?**

**Which printer maintenance tasks have you performed, on which types of printers? Which maintenance tasks are most important in your organization? Why are they so important?**



**Note:** Check your CHOICE Course screen for opportunities to interact with your classmates, peers, and the larger CHOICE online community about the topics covered in this course or other topics you are interested in. From the Course screen you can also access available resources for a more continuous learning experience.

17

# Security Threats, Vulnerabilities, and Controls

**Lesson Time:** 1 hour, 30 minutes

## Lesson Objectives

In this lesson, you will identify security threats, vulnerabilities, and controls. You will:

- Identify common security threats and vulnerabilities.
- Compare and contrast common threat prevention methods.
- Identify common security controls for mobile devices.
- Identify appropriate data destruction and disposal methods.

## Lesson Introduction

So far in this course, you have installed and configured hardware and software on PCs and other devices. Another facet of an A+ technician's duties involves protecting organizational computing assets from attacks. In this lesson, you will identify security threats, vulnerabilities, and controls.

In today's work environment, cybersecurity is everyone's responsibility. As an A+ technician, you are in the position to identify potential security issues before they become big problems. By identifying security threats and vulnerabilities, as well as some of the controls that can counteract them, you can help keep your organization's computing resources safe from unauthorized access.

# TOPIC A

## Common Security Threats and Vulnerabilities

In this lesson, you will identify security threats, vulnerabilities, and controls. To begin, you will identify common security threats and vulnerabilities.

By identifying common security threats and vulnerabilities, you will be better equipped to suggest or implement the most effective counteractive measures.

### Types of Malware

There are a few malicious code attacks you should be aware of that fall into the general malware category.

<b>Malware Type</b>	<b>Description</b>
<i>Virus</i>	A piece of code that spreads from one device to another by attaching itself to other files. The code in a virus executes when the file it is attached to is opened. Frequently, viruses are intended to enable further attacks, send data back to the attacker, or even corrupt or destroy data.
<i>Worm</i>	A piece of code that spreads from one device to another on its own, not by attaching itself to another file. Like a virus, a worm can enable further attacks, transmit data, or corrupt or erase files.
<i>Trojan horse</i>	An insidious type of malware that is itself a software attack and can pave the way for a number of other types of attacks. There is a social engineering component to a Trojan horse attack since the user has to be fooled into executing it.
<i>Logic bomb</i>	A piece of code that sits dormant on a target computer until it is triggered by a specific event, such as a specific date. Once the code is triggered, the logic bomb "detonates," and performs whatever actions it was programmed to do. Often, this includes erasing and corrupting data on the target system.
<i>Spyware</i>	Surreptitiously installed malicious software that is intended to track and report the usage of a target system, or to collect other data the author wishes to obtain. Data collected can include web browsing history, personal information, banking and other financial information, and user names and passwords.
<i>Adware</i>	Software that automatically displays or downloads advertisements when it is used. While not all adware is malicious, many adware programs have been associated with spyware and other types of malicious software. Also, it can reduce user productivity by slowing down systems and simply by creating annoyances.
<i>Rootkit</i>	Code that is intended to take full or partial control of a system at the lowest levels. Rootkits often attempt to hide themselves from monitoring or detection, and modify low-level system files when integrating themselves into a system. Rootkits can be used for non-malicious purposes such as virtualization; however, most rootkit infections install backdoors, spyware, or other malicious code once they have control of the target system.

<b>Malware Type</b>	<b>Description</b>
Ransomware	Malicious code that restricts access to a user's device or the data stored on it until the victim pays the attacker to remove the restriction. Ransomware is often implemented as a Trojan horse and can use file encryption to restrict access to data.
Spam	Spam is an email-based threat that presents various advertising materials, promotional content, or get-rich-quick schemes to users. The messages can quickly fill a user's inbox and cause storage issues. Spam can also carry malicious code and other types of malware.

## Social Engineering

A *social engineering attack* is a type of attack that uses deception and trickery to convince unsuspecting users to provide sensitive data or to violate security guidelines. Social engineering is often a precursor to another type of attack. Because these attacks depend on human factors rather than on technology, their symptoms can be vague and hard to identify. Social engineering attacks can come in a variety of methods: in person, through email, or over the phone. Social engineering typically takes advantage of users who are not technically knowledgeable, but it can also be directed against technical support staff if the attacker pretends to be a user who needs help. Social engineering attacks can be prevented with effective user education.

### Types of Social Engineering

There are various types of social engineering attacks.

<b>Social Engineering Type</b>	<b>Description</b>
Shoulder surfing	This is a human-based attack where the goal is to look over the shoulder of an individual as he or she enters password information or a PIN. Shoulder surfing can happen in an office environment, a retail environment, at an ATM, or at the entryway of a secure physical facility.
Spoofing	This is a human-based or software-based attack where the goal is to pretend to be someone else for the purpose of identity concealment. Spoofing can occur in Internet Protocol (IP) addresses, network adapter's hardware (Media Access Control [MAC]) addresses, and email. If employed in email, various email message headers are changed to conceal the originator's identity.
Impersonation	This is a human-based attack where an attacker pretends to be someone he is not. A common scenario is when the attacker calls an employee and pretends to be calling from the help desk. The attacker tells the employee he is reprogramming the order-entry database, and he needs the employee's user name and password to make sure it gets entered into the new system. A related attack is tailgating, in which an attacker follows closely behind an authorized user and gains access to an office building or other secure area. The attacker is essentially impersonating an employee, and exploits the victim's trust or desire to avoid confrontation.

<b>Social Engineering Type</b>	<b>Description</b>
<i>Hoax</i>	This is an email-based or web-based attack that is intended to trick the user into performing undesired actions, such as deleting important system files, in an attempt to remove a virus. It could also be a scam to convince users to give up important information or money for an interesting offer.
<i>Phishing</i>	This is a common type of email-based social engineering attack. In a phishing attack, the attacker sends an email that seems to come from a respected bank or other financial institution. The email claims that the recipient needs to provide an account number, Social Security number, or other private information to the sender in order to "verify an account." Ironically, the phishing attack often claims that the "account verification" is necessary for security reasons. Individuals should never provide personal financial information to someone who requests it, whether through email or over the phone. Legitimate financial institutions never solicit this information from their clients. A similar form of phishing called <i>pharming</i> can be done by redirecting a request for a website, typically an e-commerce site, to a similar-looking, but fake, website.
<i>Vishing</i>	This is a human-based attack where the goal is to extract personal, financial, or confidential information from the victim by using services such as the telephone system and IP-based voice messaging services (Voice over Internet Protocol [VoIP]) as the communication medium. This is also called voice phishing.
<i>Whaling</i>	This is a form of phishing that targets individuals who are known to possess a good deal of wealth. It is also known as <i>spear phishing</i> . Whaling targets individuals that work in Fortune 500 companies or financial institutions whose salaries are expected to be high.
Spam and <i>spim</i>	Spam can also be categorized as a type of social engineering because it can be used within social networking sites such as Facebook and Twitter.  Spim is an Internet messaging (IM)-based attack similar to spam that is propagated through IM instead of through email.

## Types of Attacks

In the realm of information security, an *attack* is a technique that is used to exploit a vulnerability in any application on a device without the authorization to do so. Attacks on devices include those described in the following table.

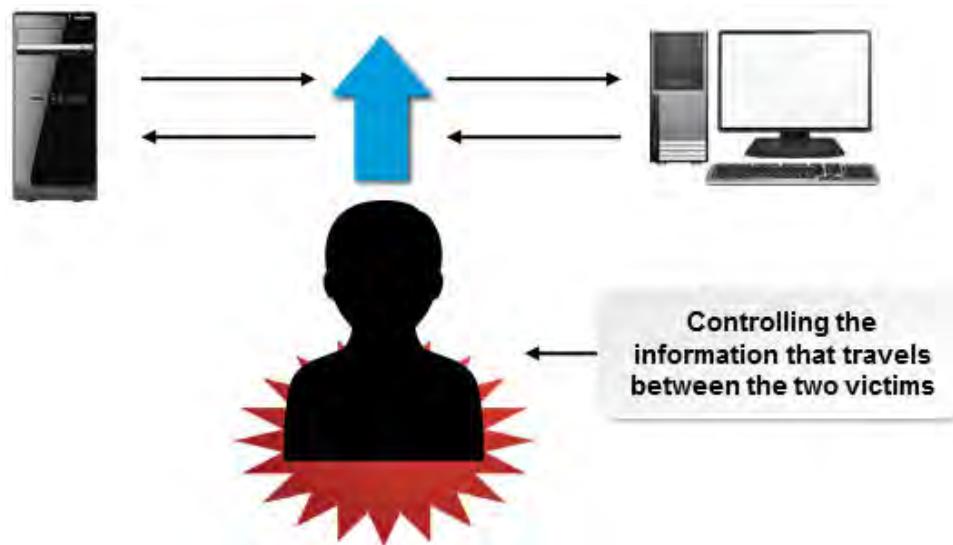
<b>Attack Type</b>	<b>Description</b>
Zero day attack	A <i>zero day attack</i> is an attack that exploits a previously unknown vulnerability in an application or operating system. In such a situation, developers have not had time to address the vulnerability and patch it. It is called a "zero day" because the developer has had zero days to fix the flaw.

<b>Attack Type</b>	<b>Description</b>
Brute force attack	In a <i>brute-force attack</i> , the attacker uses password-cracking software to attempt every possible alphanumeric password combination. Such an attack might be used when it is not possible to take advantage of other weaknesses. When password guessing, this method is very fast when used on short passwords, but for longer passwords it takes much longer. When key guessing, the key length used in the cipher determines the practical feasibility of performing a brute-force attack, with longer keys exponentially more difficult to crack than shorter ones.
Dictionary attack	A <i>dictionary attack</i> automates password guessing by comparing encrypted passwords against a predetermined list of possible password values. Dictionary attacks are successful against only fairly simple and obvious passwords, because they rely on a dictionary of common words and predictable variations, such as adding a single digit to the end of a word.
Eavesdropping or sniffing attack	An <i>eavesdropping attack</i> or <i>sniffing attack</i> uses special monitoring software to intercept private network communications, either to steal the content of the communication itself or to obtain user names and passwords for future software attacks. Attackers can eavesdrop on both wired and wireless network communications. On a wired network, the attacker must have physical access to the network or tap in to the network cable. On a wireless network, an attacker needs a device capable of receiving signals from the wireless network. Eavesdropping is very hard to detect, unless you spot an unknown device leasing an IP address from a Dynamic Host Configuration Protocol (DHCP) server.
	Many utilities are available that will monitor and capture network traffic. Some of these tools can sniff only the traffic that is sent to or received by the device on which they are installed. Other tools are capable of scaling up to scan very large corporate networks. Examples of these tools include: Wireshark®, the Microsoft Network Monitor Capture utility, tcpdump, and dsniff.
Man-in-the-middle attack	A <i>man-in-the-middle attack</i> is a form of eavesdropping in which the attacker makes an independent connection between two victims (two clients or a client and a server) and relays information between the two victims as if they are directly talking to each other over a closed connection, when in reality the attacker is controlling the information that travels between the two victims. During the process, the attacker can view or steal information to use it fraudulently.

## More About Man-in-the-Middle Attacks

In a typical man-in-the-middle attack, the attacker sets up a host on a network with IP forwarding enabled and a network-monitoring utility installed to capture and analyze packets. After analyzing network traffic to determine which server would make an attractive target:

1. The attacker intercepts packets from a legitimate client that are destined for the server.
2. The attacker's computer sends a fake reply to the client.
3. The attacker's computer forwards a fake packet to the server, which is modified so the attacker's computer looks like the original sender.
4. The server replies to the attacker's computer.
5. The attacker's computer replies to the server as if it were the original client.
6. The attacker stores any valuable information contained in the packets, such as sensitive data or user credentials, for use in future attacks.

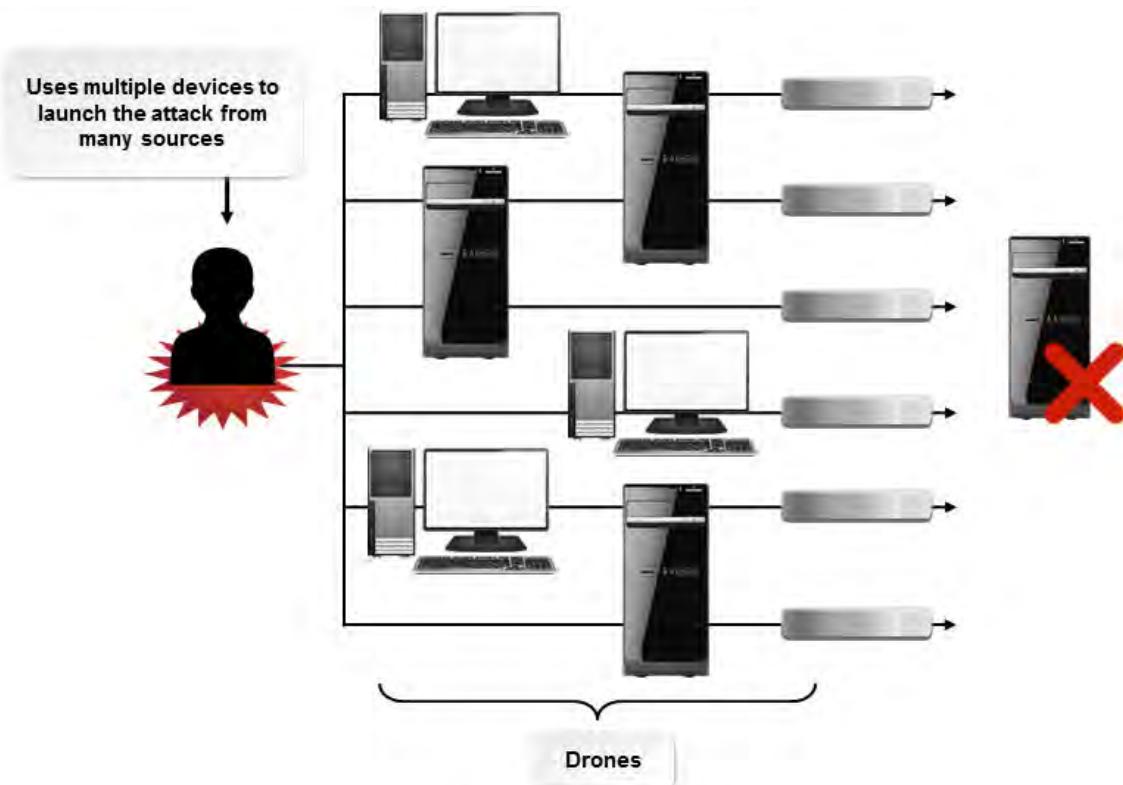


**Figure 17-1: A man-in-the-middle attack.**

Man-in-the-middle attacks are used to gain access to authentication and network infrastructure information for future attacks, or to gain direct access to packet contents. Generally, there will be no signs that a man-in-the-middle attack is in progress or has just taken place.

## Zombies and Botnets

A *Distributed Denial of Service (DDoS) attack* is a type of DoS attack that uses multiple devices on disparate networks to launch the coordinated attack from many simultaneous sources. These can sometimes be difficult to differentiate from traffic spikes when they first begin. The attacker introduces unauthorized software called a *zombie* or *drone* that directs the devices to launch the attack. A botnet is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks that can be used to send spam email or participate in DDoS attacks.



**Figure 17-2: DDoS attacks using zombies.**

A *botnet* is a set of devices that have been infected by a control program called a bot that enables attackers to exploit them and mount attacks. Typically, black hats use botnets for Distributed Denial of Service, or DDoS attacks, sending spam email, and mining for personal information or passwords.

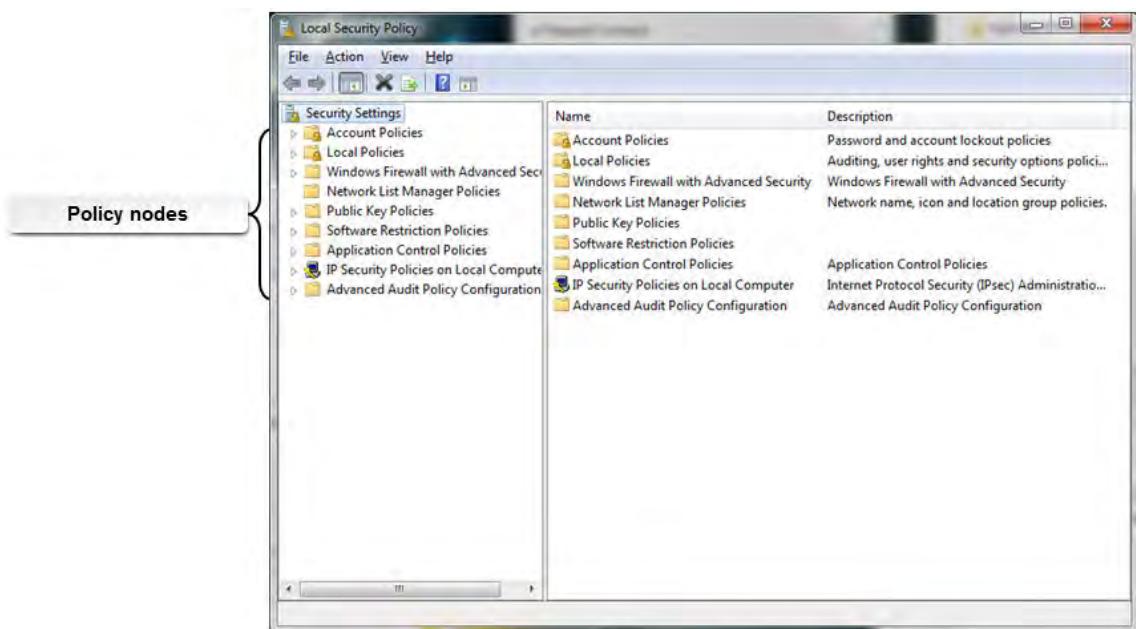
## Non-Compliant Systems

If systems try to connect to your organization's network, and those systems don't meet your minimum requirements, those systems are considered to be *non-compliant systems*. You can prevent non-compliant systems from connecting to your network through Windows security policies.

For example, your organization might require that at least certain updates and patches be installed on the operating system, that the virus software be installed and the data definitions be current, and no viruses or malware be present on the system. If any of these requirements are not met, the system is deemed non-compliant, and is not allowed to connect to the network.

## Windows Security Policies

*Windows security policies* are Windows configuration settings that control the overall security behavior of the system. The security policy consists of hierarchical groupings of related policy nodes, which contain individual policy entries you can enable, configure, or disable. The **Local Security Policy** is a subset of the comprehensive local policy object used to configure the general behavior of each Windows system.



*Figure 17-3: Windows security settings.*

### Local Policy Settings and Group Policy Settings

In Windows workgroups, all policies, including security policies, are set in the local policy object on each individual system. To view the full set of local policies, you can open the Microsoft Management Console (MMC) object. You can find the security policy settings under **Computer Configuration**→**Windows Settings**→**Security Settings**. The **Local Security Policy** utility in the **Administrative Tools** group enables you to access the **Security Settings** node alone.

When Windows computers are members of a centralized Windows domain, an administrator can also manage policies for all computers by using **Group Policy**. The structure of domain-based **Group Policy** objects and the local policy object are similar.

## Security Best Practices

When you select and apply computer security measures, you must make security adjustments that protect the devices and the applications and data on it, while ensuring that the system runs appropriately for legitimate users.

Some steps you might take to apply security measures include the following.

Steps	Description
Manage user authentication	<ul style="list-style-type: none"> <li>Change the default user name and password on each device.</li> <li>Require all users to create strong passwords and to protect the passwords from others.</li> <li>In high-security environments, implement multi-factor authentication that can include smart cards or biometric authentication systems.</li> </ul>
Install updates and patches	<ul style="list-style-type: none"> <li>Install the latest operating system service packs and security update patches.</li> <li>Install the latest application patches for utilities that are included in the operating system as well as for web browsers and third-party application software.</li> </ul>

<b>Steps</b>	<b>Description</b>
Manage user accounts	<ul style="list-style-type: none"> <li>• Use policy settings to disable or delete guest accounts or other unnecessary accounts, and rename default accounts, so attackers cannot use known account names to access the system.</li> <li>• Restrict user permissions so that only those users who absolutely need access are allowed into the system.</li> <li>• Disable any guest account on all devices to prevent unauthorized access to any shared files and folders on the device or system.</li> </ul>
Educate users	<ul style="list-style-type: none"> <li>• Educate users to follow best security practices, such as recognizing and avoiding hoaxes, phishing attacks, and potential malicious software sources.</li> </ul>
Apply device security measures	<ul style="list-style-type: none"> <li>• Implement antivirus software to protect against malicious software.</li> <li>• Block pop-ups in your web browser.</li> <li>• Install a firewall and configure the appropriate open and closed ports and the program filtering settings.</li> <li>• Implement warning messages or banners displayed at user login to warn users that only authorized use is allowed. These banners could be important in future civil litigation or criminal prosecution, and they can put all users on notice that their activities might be monitored. All warning banners should comply with the legal requirements of your jurisdiction.</li> <li>• Disable autorun to prevent malware and other viruses from being loaded automatically with a device, such as a USB drive. Disabling the autorun features will restrict any infected files from automatically loading.</li> <li>• Enable screen saver and password functionality to lock systems when idle.</li> <li>• Enable automatic operating system updates on the device.</li> <li>• Limit the number of shared resources on a system. Use share and file system permissions to restrict access to file and print resources.</li> </ul>

## Violations of Security Best Practices

If a system or device is determined to be non-compliant, there are several ways the device can be made compliant. The actions taken will depend on your organization's policies.

- Alert the user to the fact that their device is out of compliance with security policies.
- Automatically install any needed patches or updates to bring the device into compliance.
- Run an anti-malware test to verify that the device is not infected, then install or update malware protection software as needed.

Be sure to take steps to mitigate any violation of the items listed in the previous section under **Security Best Practices**.

## Security Incident Reports

A *security incident* is a specific instance of a risk event occurring, whether or not it causes damage. *Security incident management* is the set of practices and procedures that govern how an organization will respond to an incident in progress. The goals of incident management are to contain the incident appropriately, and ultimately minimize any damage that may occur as a result of the incident. Incident management typically includes procedures to log, and report on, all identified incidents and the actions taken in response.

A *security incident report* should include information such as:

- The type of incident that occurred.
- The severity of the incident such as how many people or devices were affected, whether it caused a work stoppage, and if any data was compromised or lost.
- The names and titles of those involved in the incident. Also include their contact information including phone number and email address.
- A full description of the incident.
- Any actions taken to mitigate the incident.

## ACTIVITY 17-1

### Identifying Common Security Threats and Vulnerabilities

#### Scenario

You are on IT help desk phone duty today. The following are some of the calls you take.

1. Early in the day a user called the help desk saying that his computer is running slowly and freezing up. Shortly after this user called, other help desk technicians who overheard your call also received calls from users who report similar symptoms. What type of attack might have occurred?
  
2. John brought in the new tablet he just purchased and attempted to connect to the network. He knows the SSID of the wireless network and the password used to access the wireless network. He was denied access, and a warning message was displayed that he must contact the IT Department immediately. What happened and why did he receive the message?
  
3. The contract ended recently for several workers who were hired for a specific project. The IT department has not yet removed all of those employees' login accounts. It appears that one of the accounts has been used to access the network, and a rootkit was installed on a server. You immediately contact the agency the employee was hired through and learn that the employee is out of the country, so it is unlikely that this person caused the problem. What actions do you need to take?

# TOPIC B

## General Security Controls

In the last topic, you identified common threats and vulnerabilities. Once you identify threats and vulnerabilities, you can then decide how to prevent and counteract them. In this topic, you will compare and contrast common threat prevention methods.

### Security Controls

*Security controls* are safeguards or prevention methods to avoid, counteract, or minimize security risks relating to personal or company property. For example, a firewall is a type of security control because it controls traffic by allowing only traffic that has specifically been permitted by a system administrator. Security controls can be classified by several criteria, such as by the time that they act relative to a security incident, according to their nature, or by people, technology, and operations/processes. In this course, we will categorize the security controls by their nature:

- Physical controls such as fences, doors, locks, and fire extinguishers.
- Procedural controls such as incident response processes, management oversight, security awareness, and training.
- Digital controls such as user authentication (login) and logical access controls, antivirus software, and firewalls.
- Legal and regulatory or compliance controls such as privacy laws, policies, and clauses.

### Physical Security

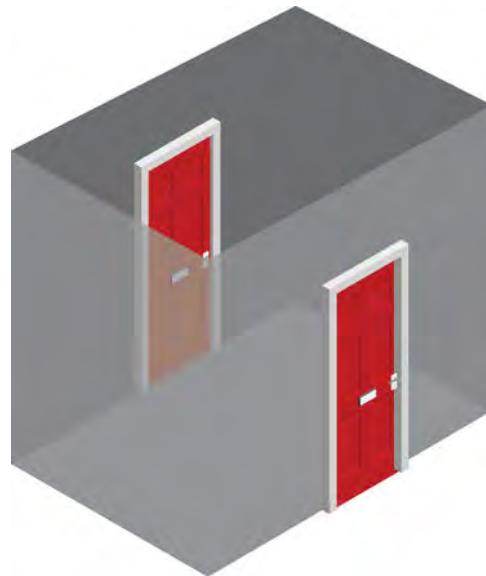
*Physical security* refers to the implementation and practice of various security control methods that are intended to restrict physical access to facilities. One case where physical security is important is when there is a need to control access to physical documents, password records, and sensitive documents and equipment. One successful unauthorized access attempt can lead to financial losses, credibility issues, and legalities. In addition, physical security involves increasing or assuring the reliability of certain critical infrastructure elements such as electrical power, data networks, and fire suppression systems. Physical security may be challenged by a wide variety of events or situations, including:

- Facilities intrusions.
- Electrical grid failures.
- Fire.
- Personnel illnesses.
- Data network interruptions.

### Physical Security Measures

There are several physical access controls available to ensure the protection of an organization's physical environment.

<b>Security Measure</b>	<b>Description</b>
Locking doors	<p>There are many locks that can be used to restrict unauthorized access to information resources:</p> <ul style="list-style-type: none"> <li>• Bolting door locks are a traditional lock-and-key method that requires a non-duplicate policy for keys to access a door.</li> <li>• Combination door locks, or cipher locks, use a keypad or dial system with a code or numeric combination to access a door.</li> <li>• Electronic door locks use an access ID card with an electronic chip or token that is read by the electronic sensor attached to a door.</li> <li>• Biometric door locks are commonly used in highly secure environments. This method uses an individual's unique body features to scan and identify the access permissions for a particular door. For example, retinal scanners are used to read the unique patterns of a person's eye to authorize access.</li> <li>• Hardware locks can be attached to a laptop, hard drive, or file cabinet to secure it from being opened or turned on.</li> </ul>
Mantraps	<p>A <i>mantrap</i> is two sets of interlocking doors inside a small space, where the first set of doors must close before the second set opens. If the mantrap is manual, a guard locks and unlocks each door in sequence. In this case, an intercom or video camera is typically used to allow the guard to control the trap from a remote location. If the mantrap is automatic, identification or a key of some kind may be required for each door, and sometimes different measures may be required for each door. Metal detectors are often built in to prevent entrance of people carrying weapons. Such use is particularly frequent in banks and jewelry shops.</p>



**Figure 17–4: A mantrap.**

<b>Security Measure</b>	<b>Description</b>
Logging and visitor access	<p>Logging should be used at all entrances that are open to the general public. An <i>entry control roster</i> requires all visitors to sign in and out when entering and leaving the building. Logging requirements will vary depending on the organization, but should include the following:</p> <ul style="list-style-type: none"> <li>• Name and company being represented.</li> <li>• Date, time of entry, and time of departure.</li> <li>• Reason for visiting.</li> <li>• Contact within the organization.</li> </ul>
	<p>When possible, one single entry point should be used for all incoming visitors. This decreases the risk of unauthorized individuals gaining access to the building and tailgating.</p>
Identification systems	<p>Identification systems can use different tokens and methods to identify an authorized person and allow them physical access to buildings, room, and grounds.</p>
	<ul style="list-style-type: none"> <li>• <i>Badges</i>, or security cards, can be used to swipe through an identification system or can be configured as a proximity card with radio-frequency identification (RFID) technology that is activated automatically when the card is within a specified distance from the system. <i>RFID badges</i> are security cards that contain a tag that reacts with the radio frequency of the identification system to allow or deny access.</li> <li>• <i>Key fobs</i> are security devices small enough to attach to a key chain that contain identification information used to gain access to a physical entryway. A user places the fob next to an identification system for validation and then access.</li> <li>• <i>Smart cards</i> are plastic cards that have an integrated circuit built into the card. These often look like regular ID cards or credit cards, but have a secure microcontroller or intelligent memory that contains data that can be read by a physical or RFID scanner.</li> </ul>
	<p>Security cards, such as swipe cards, proximity cards, and badges, provide identity information about the bearer, which is then checked against an appropriate access list for that location. The cards can be used along with a proximity reader to verify identification and grant access. A security card can also include a picture or some other identification code for a second authentication factor. Security cards should be required for all employees and should be visible at all times.</p>
Video surveillance	<p>Video or still-image surveillance can be put in place to deter or help in the prosecution of unwanted access. These systems can be placed inside and outside the building. All video recording should be saved and stored in a secure environment.</p>
Security guards	<p>Human security guards, armed or unarmed, can be placed in front of and around a location to protect it. They can monitor critical checkpoints and verify identification, allow or disallow access, and log physical entry occurrences. They also provide a visual deterrent and can apply their own knowledge and intuition to potential security breaches.</p>

<b>Security Measure</b>	<b>Description</b>
Physical barriers	The location of highly secure resources, such as a server room, should not have windows or be visible from the outside of a building. This creates a more secure barrier from the outside. Examples of physical barriers include fencing and true floor-to-ceiling wall architectures. Other types of physical barriers can be implemented to restrict viewing of a user's computer display. For example, you can install a <i>privacy filter</i> to cover a device's screen, making it difficult for anyone to read the screen who is not positioned directly in front of it.
Cable locks	Laptops and other devices that can easily be removed should be secured to a stationary object using a cable lock.
Secure physical documents	Physical documents such as printed output should be kept in a locked cabinet or drawer when not in use. Passwords should never be written down on a physical paper where it could be seen. When a document is no longer needed, it should be shredded. For highly sensitive physical documents, the pages should be placed in a locked recycling bin; some have shredders built in and others are picked up by a company hired specifically to shred the documents, usually on site in the presence of an organization employee.
Biometrics	A <i>biometric lock</i> is a lock that is activated by biometric features, such as a fingerprint, voice, retina, or signature. Biometric locks make it more difficult for someone to counterfeit the key used to open the lock. An example of a biometric lock is an optical or thermal scanner that reads and stores the fingerprints of authorized users. The user then places his or her hand on the scanner to gain access to a door.
Alarms	 <p>Alarms activated by an unauthorized access attempt require a quick response. Locally stationed security guards or police may respond to alarms. These responding individuals may trigger access control devices in the facility to automatically lock.</p>

**Figure 17–5: Thermal fingerprint scanner.**

Digital Security	Digital security refers to the idea that any information or data that is created, stored, and transmitted in digital form is secured to the desired level. This concept applies to many components of the digital world, such as the Internet, cloud-based computing, networks, mobile devices, tablets, laptops, and standard desktop computers.
------------------	---

Digital security refers to the idea that any information or data that is created, stored, and transmitted in digital form is secured to the desired level. This concept applies to many components of the digital world, such as the Internet, cloud-based computing, networks, mobile devices, tablets, laptops, and standard desktop computers.

There are several prevention methods used to manage and control security issues surrounding digital data. These include:

- Antivirus software.
- Anti-spyware software.
- Firewalls.
- User authentication and strong passwords.
- Directory permissions.

## Antivirus and Antimalware Software

*Antivirus software* is an application that scans files for executable code that matches patterns, known as *signatures* or *definitions*, that are known to be common to viruses. The antivirus software also monitors systems for activity that is associated with viruses, such as accessing the boot sector. Antivirus software should be deployed on various network systems as well as on individual computers, and the signature database and program updates should be downloaded and installed on a regular basis as well as whenever a new threat is active. Antivirus software does not usually protect against spam, but it can identify malware symptoms and can provide protection from adware and spyware.

Antivirus updates must be managed as they are made available. Antivirus engine updates can include enhancements, bug fixes, or new features being added to the software engine, improving the manner in which the software operates. Updates can be implemented automatically or manually depending on the software. Automatic updating refers to software that periodically downloads and applies updates without any user intervention, whereas manual updating means that a user must be involved to either initiate the update, download the update, or at least approve installation of the update.

*Anti-spyware software* is specifically designed to protect systems against spyware attacks. Some antivirus software packages include protection against adware and spyware, but in most cases, it is necessary to maintain anti-spyware protection in addition to antivirus protection. Some examples of anti-spyware include Webroot's Spy Sweeper and STOPzilla Anti-Spyware.

Most security software that is created in the past few years provides general, all-around antimalware protection. There are many complex and harmful threats on the Internet that can find their way onto your digital devices. Having good antimalware software installed will help protect your systems, and the other systems you connect to, from becoming infected through any malware you encounter.

## Firewalls

A firewall is a software program or hardware device that protects networks from unauthorized access by blocking outgoing and incoming unsolicited traffic. Firewalls allow incoming or outgoing traffic that has specifically been permitted by a system administrator and incoming traffic that is sent in response to requests from internal systems. Firewalls use complex filtering algorithms that analyze incoming network data based on destination and source addresses, port numbers, and data types.

There are two common firewall types:

- *Host or personal firewalls* are installed on a single computer and are used to secure most home computers.
- *Network-based firewalls* are dedicated hardware/software combinations that protect all the computers on a network behind the firewall.

## Software Firewalls

Software firewalls can be useful for small home offices and businesses. The firewall provides many features that can be configured to suit various computing needs. Some features include:

- Enabling or disabling port security on certain ports.
- Inbound and outbound filtering. The user can set up rules or exceptions in the firewall settings to limit access to the web.

- Reporting and logging activity.
- Malware and spyware protection.
- Pop-up blocking.
- Port assigning, forwarding, and triggering.

## Hardware Firewalls

A hardware firewall is a hardware device, either stand-alone or built into most routers, that protects computers on a private network from unauthorized traffic. They are placed between the private network and the public network to manage inbound and outbound traffic and network access.

## Windows Firewall Configuration

Windows® Firewall is a software-based firewall that is included with all current Windows operating system client and server versions. You can configure the firewall by using the Windows Firewall program in **Control Panel**, or through **Group Policy Settings**, although most versions of Windows will provide a wizard. You can use the **Windows Firewall with Advanced Security** console to monitor the rules that control the flow of information to and from the system, specify new rules, modify existing rules, or delete rules. For more information, see the Windows Firewall entries in the **Help and Support Center**, and the "Windows Firewall Technical Reference" on the Microsoft Technet website.

## User Authentication Methods

Most organizations will use a variety of authentication methods to prevent unauthorized access to the physical building, infrastructure, and resources, including the following.

- User name and password
- Biometrics
- Tokens
- Multifactor authentication
- Mutual authentication

## User Access Process

There are three phases in the user access process that a person or system must perform in order to gain access to resources:

- Identification: The claim of identity made by the user when entering a user name and password or other authentication method.
- Authentication: The verification of that claim.
- Authorization: The action taken as a result of verifying the claim.

## Password Strength

A strong password meets the complexity requirements that are set forth by a system administrator and documented in a security policy or password policy. Strong passwords increase the security of systems that use password-based authentication by protecting against password guessing and other password attacks.

Strong password policies often specify:

- The minimum and maximum length of the password.
- Required characters, such as a combination of letters, numbers, and symbols.
- Forbidden character strings, such as the user account name, personal identification information, or words found in a dictionary.
- The frequency for changing passwords.
- Whether or not passwords can be reused.

## Network Security Measures

In addition to physically securing access to buildings, resources, and devices, as an A+ technician you will need to be knowledgeable about network security measures. Network security is typically handled by network administrators, but as a PC technician, you will need to interact with the network admins regularly. This might be to request access to network resources for users, to determine if a user's problem is local or network related, or to work with the network admins to ensure the proper level of access is available to users.

Some of the network security measures you might encounter include:

- Directory permissions
- VPNs
- Data loss prevention (DLP)
- Disabling ports
- Access control lists

### Directory Permissions

A *permission* is a security setting that determines the level of access a user or group account has to a particular resource. Permissions can be associated with a variety of resources, such as files, printers, shared folders, and network directory databases. Permissions can typically be configured to allow different levels of privileges, or to deny privileges to users who should not access a resource.

- File-level permissions allow users to set access control to individual files and folders. File-level permissions will prevent any unauthorized access to a file or folder both across the network and locally by prompting all users, including the user who created the file, to enter the correct user name and password for access. In Windows operating systems, file-level permissions can be implemented only on those hard disks or partitions that use NTFS file systems.
- Share-level permissions are permissions set for network shares. A network share is a folder on a computer that can be remotely accessed from other computers through a local area network as if it were a resource in the local machine. By setting up a share-level permission, a user can prevent the remote users from accessing or modifying the files in the user's network share. Although share-level permissions work well across a network, they offer no protection against a user who's logged on locally to the computer or server containing the shared resource.

A downside to share-level security is that the server may eventually contain so many shares that it's hard for users to remember their folders. If users want to search for information and they don't know which share it is contained in, they will have to find the server and search each share on the server for the desired information.

Separate permissions at the share level and file level is unique to Windows environments. In Linux, the same set of read, write, and delete permissions are valid at both the local level and across the network.

### UNIX Permissions

Because UNIX and related systems are multiuser by nature, there is a series of permissions associated with all files and directories. There are three types of permissions.

<b>Permission</b>	<b>Allows the User To</b>
r (read)	<ul style="list-style-type: none"> <li>• View file content.</li> <li>• See what is in the directory.</li> </ul>
w (write)	<ul style="list-style-type: none"> <li>• Modify file contents.</li> <li>• Create and delete directory contents.</li> </ul>

Permission	Allows the User To
x (execute)	<ul style="list-style-type: none"> <li>Run the file (if it is an executable program and is combined with read).</li> <li>Move into the directory. When combined with read, you can also see a long listing of the contents of the directory.</li> </ul>

## VPNs

With a VPN, TCP/IP communications are encrypted and then packaged within another TCP/IP packet stream. The VPN hardware or software can encrypt just the underlying data in a packet or the entire packet itself before wrapping it in another IP packet for delivery. If a packet on the public network is intercepted along the way, the encrypted contents cannot be read by a hacker. Such encryption of data or packets is typically implemented by using a protocol suite called Internet Protocol Security (IPSec).

IPSec was initially developed for IPv6, but many current IPv4 devices support it as well. IPSec enables two types of encryption. With transport encryption, the underlying data in a packet is encrypted and placed within a new packet on the public network. With tunnel encryption, the entire packet, including its header, is encrypted and then placed in the public network's packet.

With IPSec in place, a VPN can virtually eliminate packet sniffing and identity spoofing. Only the sending and receiving computers hold the keys to encrypt and decrypt the packets being sent across the public network. Anyone sniffing the packets would have no idea of their content and might not even be able to determine the source and destination of the request.

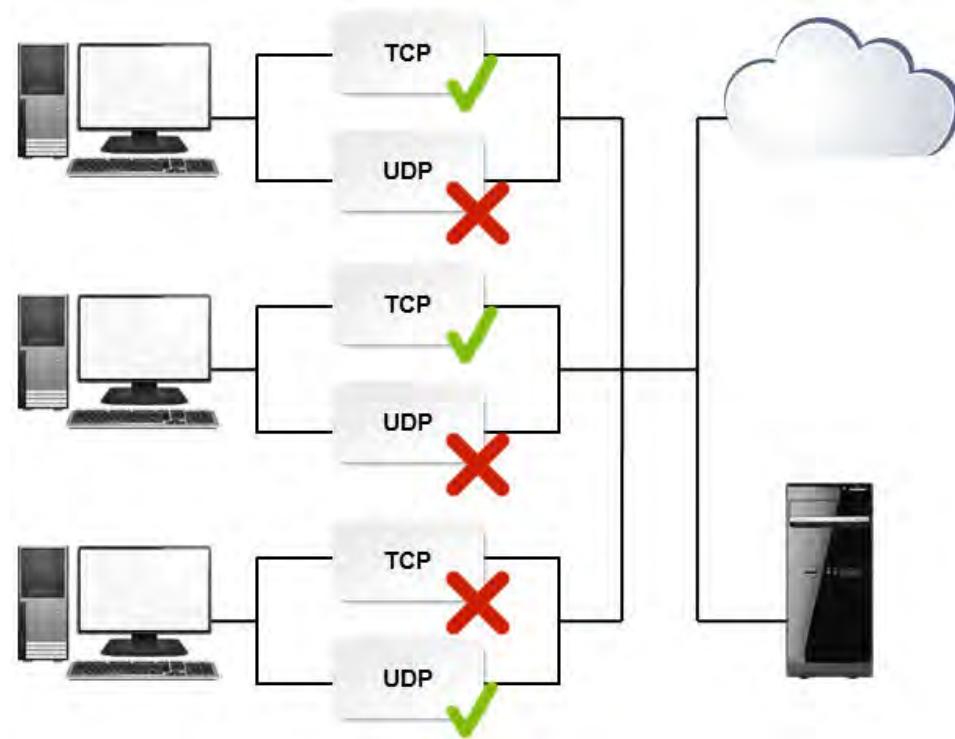
## DLP

*Data loss prevention (DLP)* is typically software or a software suite that helps protect data from being stolen while the data is moving across the network. It uses a variety of techniques to detect the data and ensure that it is not lost, stolen, or compromised in any way as it travels from its point of origin to its destination.

## Port Disabling and Filtering

Any ports that are not being used should be disabled. This will help prevent intruders accessing the network through one of those ports.

*Port filtering* is a technique of selectively enabling or disabling TCP and UDP ports on computers or network devices. It ensures that no traffic, except for the protocol that the administrator has chosen to allow, can pass through an open port. Port filtering works by examining the packet's header, source address, destination address, and port number. However, a packet's header can be spoofed; a sender can fake his IP address or any other data stored in the header.



**Figure 17-6: TCP and UDP ports disabled in computers on a network.**

Port filtering is most often used in firewalls and for device hardening. Normally, in organizations, administrators disable/block ports above 1024 as a security measure. They selectively enable ports above 1024 during the installation of the associated services that use the port number.

### ACLs

An *Access Control List (ACL)* is a set of data (user names, passwords, time and date, IP addresses, MAC addresses, etc.) that is used to control access to a resource such as a computer, file, or network. ACLs are commonly implemented as MAC address filtering on wireless routers and access points. When a wireless client attempts to access the network, that client's MAC address is compared to the list of authorized MACs and access is granted or restricted based on the result.



**Figure 17-7: ACLs control access to network resources.**

## Smart Cards

Smart cards have a built in processor or smart memory chip. The data in the credit-card sized card holds information. The information can be about the person assigned to the smart card, or other information. They can be used with proximity card readers to allow the user to have access to a building, room, or device. They can also be used with a hard drive by connecting a reader via a data cable to the drive; a slot for the smart card is connected to the other end of the cable. In order to access the drive, the user needs to insert the smart card. The user might also need to enter other information such as a PIN or passcode to access the drive.

## Email Filtering

Most users get a lot of email messages every day. Email providers and email servers are getting better at recognizing spam or junk messages, and not delivering them to users' Inboxes. However, some messages that should get to users get caught up in the filtering process and are not delivered.

In most email applications, the users can further filter their email messages, defining what constitutes junk or spam messages, and what should be delivered. Again, some messages might get marked as junk or spam when they shouldn't be. Other filtering users can perform is to have messages delivered to specific folders they have created. This might be based on the sender, message content, or subject.

By adding a sender's email address to the contacts list, users can usually prevent messages from that sender from being sent to junk or spam folders.



**Note:** Users should periodically check their junk or spam folder to ensure that no messages have been sent to those folders that should have been delivered to their Inbox.

## Trusted Software Sources

Installing software from a well-known software creator or author is usually pretty safe. This software can be considered trusted. However, some applications that you find while searching the Internet might not be quite so trustworthy. You need to make sure that the software is not pirated software.

Also make sure, usually by doing research and using antimalware applications, that the software does not contain malicious or backdoor software.

Obtaining your software from a well-known source, getting it from the app store for your device, and researching the software and vendor are all ways to make sure that you can trust the software. If your antimalware software feels that the software you are installing is untrusted, it will likely prevent you from installing the software. If you know that the software should be trusted, you might need to temporarily disable the antimalware application to install the software.

Linux prompts when you attempt to install untrusted software. Software is signed with a cryptographic key. Packages need the public key for the repository in order to install the software. When prompted that you are installing untrusted software, you can either respond that you want to install it anyway or cancel the installation. If you want to permanently trust previously untrusted software, from the command line add the `sudo apt-get-add-repository` command to add the untrusted source to the repository.

Programmers can digitally sign software. Users must manually authorize untrusted software.

# ACTIVITY 17-2

## Identifying Security Protection Methods

### Scenario

The IT department security team has invited members from various departments, including PC Support, HR, Marketing, and Software Development, to join them in reviewing and updating the security documents for the organization. You were selected to represent the PC Support team on the committee.

You received an email outlining the topics for the next meeting. You want to write down some ideas you think are important to include, and write down your justification for including the items.

1. Fill in the table with the information you feel is important to discuss during a meeting about security protection methods.

<i>Item</i>	<i>Details to Discuss</i>	<i>Justification</i>
Physical security		
Digital security		
Antimalware software		
Firewalls		
Strong passwords		
Email filtering		

2. Share your table with the class. See which items you all included and if there are important items you should have included.

# TOPIC C

## Mobile Security Controls

Now that you are more familiar with the different mobile device technologies available, you are ready to learn how they can be configured for optimal performance while maintaining an acceptable level of security. In this topic, you will configure mobile device security.

Mobile devices can be used for a number of functions within the professional workplace. Knowing that, you must be able to provide basic level support to your users, including configuring security settings.

### Mobile Security

Mobile devices today can do just about anything a laptop or desktop computer can do when it comes to end-user productivity such as making and receiving phone calls, emailing, capturing and editing photos and videos, accessing the Internet, and in some cases, remotely accessing data and resources on a private or public network. With all these functions, you can assume all the same threats related to desktop computers and laptops will apply. For example, viruses and spam can infect mobile devices as they would desktop and wireless devices by email or downloaded applications and due to the portability, small size, and always-connected state, threats such as loss, theft, and damage due to dropping are prominent.

### Mobile Device Security Techniques

Securing a mobile device is a necessary task that should be required and enforced by any employer or user. There are a number of security methods that can be implemented to provide the right level of security while still providing access to desired resources and applications.



**Note:** One of the most important steps you can take to maintain security of mobile devices is to not leave the devices unattended.

<b>Security Control</b>	<b>Description</b>
Enable screen lock and passcode settings	<p>The screen lock option on all mobile devices should be enabled with a passcode, and strict requirements on when the device will be locked. You can specify how long the device is active before it locks, which typically ranges from 1 minute to 5 minutes. Once the device is locked, it can only be accessed by entering the passcode that has been set up by the user. This security control prevents access to the device if it is misplaced or stolen.</p>
	<p>On some devices, you can configure the passcode settings to erase all data stored on the device after a certain number of failed logon attempts.</p>
	<p>Often, enabling screen lock can be a requirement in an organizational security policy, no matter if the mobile device is provided by the employer or the individual.</p>
	<p>Be aware of pattern passcodes that require a user to complete a specific action on the touch screen to activate the device. Most of the time, the smudge pattern is visible on the surface and can be re-created to gain access to the device. Using a numeric pin or a password is considered more secure.</p>
	<p>Other secure screen lock methods include fingerprint locks and face locks. Both of these use biometrics to authenticate the user to their device. An insecure screen lock method is the swipe lock, which simply requires that the user swipe as indicated on the screen. Although this is faster and more convenient than other locking methods, it should be avoided.</p>
Configure device encryption	<p>When available, all mobile devices should be configured to use data encryption to protect company-specific and personal data that may be stored and accessed on the device. This method is effective as long as the hardware cannot be accessed to steal the data. Along with device encryption, data encryption should also be used so when data is accessed by physically taking the device apart, the data remains secured.</p>
	<p>Device encryption can also be a requirement in an organizational security policy.</p>
Require remote wipes	<p><i>Data wiping</i> is a method used to remove any sensitive data from a mobile device and permanently delete it.</p>
	<p>Remote wiping is also available for some devices, so you can perform these functions remotely in case the phone is lost or stolen. Wipe and sanitization guidelines and requirements might be included in an organization's security policy if mobile devices are issued to employees for professional use. In some cases, Admins will have rights to remote in to any device that is supported by the organization.</p>
Enable location services and applications	<p>GPS tracking service functionality is available on a number of mobile devices and can be added in most cases when required for business reasons. This feature is used as a security measure to protect and track mobile devices that may be lost or stolen.</p>
	<p>If a mobile device does not have the locating functionality built in, then you can download a locator application that can track and locate a lost or stolen device.</p>

<b>Security Control</b>	<b>Description</b>
Enable remote backup	Depending on the type of mobile device, there are remote backup services available through the OS. For example, Apple offers remote backup services to its iCloud® through the <b>General Settings</b> of the device. From there, you can specify what application data to back up. Android offers remote backup using Google Drive. Both these services offer the first 5 GB of data for free, then you can purchase more backup space as needed. These features allow you to recover your data when a device is either lost or stolen.
Install antivirus software	There are many different options when it comes to mobile antivirus solutions. Organizations that allow mobile devices to connect to the network and transfer data should require that antivirus get installed to prevent unauthorized access to data, systems, and resources. There are many solutions available: <ul style="list-style-type: none"> <li>• BullGuard Mobile Security</li> <li>• Kaspersky Mobile Security</li> <li>• ESET Mobile Security</li> <li>• Lookout Premium</li> <li>• Trend Micro Mobile Security</li> <li>• Webroot Secure Anywhere Mobile</li> </ul>
Install updates and patches	Mobile device updates are similar to other computing devices updates and patches. Verify that devices are set up to automatically install updates from the manufacturer. Updates and patches can resolve security issues and systems flaws that present a security risk.



**Note:** For additional information, check out the LearnTO **Secure a Mobile Device** presentation in the LearnTOs for this course on your CHOICE Course screen.

# ACTIVITY 17-3

## Examining Mobile Security

### Scenario

In this activity, you will examine mobile security components and measures.

1. How can the use of mobile devices by employees affect the security of an organization as a whole?
  
  
  
  
2. Examine some of the security features on a mobile device. Using the main menu, open the security settings for your device. What specific security settings are available?
  
  
  
  
3. Now, pair up with a partner who has a different mobile device and examine the security features on that device. Use the main menu to open the security settings. Are the security settings similar? Are there different options available?
  
  
  
  
4. Tap to open the various options and check out the security settings that can be customized, such as the screen lock feature, device encryption options, and GPS tracking features. Compare the available settings on a couple of different devices.

# TOPIC D

## Data Destruction and Disposal Methods

Most computing storage devices have a limited life span due to mechanical wear, technological obsolescence, or slow access speeds. Instead of just sending these to the land fill or for recycling, you need to first make sure that the data that was stored on the storage device is no longer accessible. In this topic, you will examine methods for data destruction and disposal.

### Physical Destruction

Physical destruction of computer media components ensures that the data is unrecoverable. Effective methods include using a shredder, incinerator, drill, or smashing the platters completely to change the physical makeup of the component so that it cannot be reassembled or recognized. Other methods include using a degausser to demagnetize the internal components of the device so that they are unreadable or using electromagnetic waves to alter the magnetic components inside the device so that they are unreadable and unrecoverable.

Third parties that offer data destruction services often present their clients with a certificate of destruction upon completion. This certificate is meant to be an auditable record of the data's destruction. The certificate may include information such as the date of destruction, the model and serial number of the destroyed drive, the method of destruction used, and more.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Physically Destroy Information.

### Recycling or Repurposing

Disk formatting is the process of deleting file systems from a computing device in order to clean the computing device for reuse. Proper formatting should be conducted to prevent any data remnants from being accessed on the device. This process can be done in two ways:

- *Low level formatting* is the process of writing track sector markings on a hard disk. This level of formatting is performed when the hard disk is manufactured.
- *Standard formatting*, also called *high-level formatting*, is an operating system function that builds file systems on drives and partitions. It tests disk sectors to verify that they can be reliably used to hold data. It marks any unreliable sectors as bad sectors that cannot be used.

As a security best practice, standard formatting should be done to ensure that most data is removed from a device. However, some forensic tools may be able to recover data even after it has been formatted. To truly ensure that all data has been removed from a drive, while keeping the drive reusable, you need to securely wipe it. Wiping a drive most commonly involves overwriting the existing data with either random data, or with all zero bits. This ensures that your sensitive data is not recoverable.

### Guidelines for Recycling or Repurposing Hardware



**Note:** All of the Guidelines for this lesson are available as checklists from the **Checklist** tile on the CHOICE Course screen.

Here are some steps you should take to prepare storage media for recycling or repurposing.

- Consider formatting hard disks and using a disk wipe utility to replace the data with all zeros or with random data.

- Install remote wiping software on portable devices so the information can be wiped if the device is lost or stolen.
- Check the storage media after using any sanitation method and ensure that none of the data is readable or recoverable.



**Note:** A data wipe gets rid of all data. Data sanitization only gets rid of sensitive data.

## ACTIVITY 17-4

### Identify Data Destruction and Disposal Methods

#### Scenario

For your test lab, you were provided with a variety of older equipment that had been decommissioned by other departments within your organization. Some of the equipment is too outdated for your use, so you need to prepare it for disposal. A computer disposal company your organization has contracted with will be coming to pick up the devices next week, so you need to make sure that all of the storage media has been properly sanitized before then.

You also have several applications that were developed in-house that you tested. Final versions of the applications have been released and your manager wants to make sure that these preliminary versions are not deployed by mistake. These were provided to you on various storage media including DVD, USB drives, and portable hard drives. The USB drives and portable hard drives could come in handy for other purposes, so you want to make sure that the data is removed, but the devices are still functional.

In addition, your manager has asked you to research applications that can be deployed to users with portable devices so that in the case of loss or theft, the devices can be remotely wiped. There are a variety of smartphones, laptops, and tablets, running a variety of operating systems, deployed throughout the organization.

- 
1. **What steps will you take to make sure that the storage devices in the equipment being sent for disposal will be properly sanitized?**
  
  
  
  
  
  
  2. **What steps will you take to make sure that the software you were given cannot be accessed?**
  
  
  
  
  
  
  3. Search for remote wipe applications that might be deployed to users with portable devices. If possible, find applications that can be used on multiple operating systems so that you have fewer applications to support.
-

## Summary

In this lesson, you implemented and described many concepts and techniques that can be used to establish the desired level of security within an organization. Every organization will have different security requirements based on the type of business they conduct. It is your job to understand those requirements and know how security controls should be implemented to directly support those needs.

**What physical security controls have been employed at organizations where you have worked?**

**What steps has your organization taken to ensure the security of mobile devices? Have you planned ahead in case the devices are lost or stolen? If so, how?**



**Note:** Check your CHOICE Course screen for opportunities to interact with your classmates, peers, and the larger CHOICE online community about the topics covered in this course or other topics you are interested in. From the Course screen you can also access available resources for a more continuous learning experience.



18

# Implementing Security Controls

**Lesson Time:** 1 hour, 30 minutes

## Lesson Objectives

In this lesson, you will implement security controls. You will:

- Secure Windows and other operating systems.
- Deploy and enforce security best practices to secure a workstation.
- Secure SOHO wireless and wired networks.
- Identify methods for securing mobile devices.

## Lesson Introduction

In the last lesson, you identified security threats, vulnerabilities, and controls. Now, you can put that information to practical use in protecting your organization's hardware and data. In this lesson, you will implement security controls.

# TOPIC A

## Secure Operating Systems

In this lesson, you will implement various types of security controls. In this topic, you will secure operating systems.

### Types of Users

Windows includes several built-in user accounts to provide you with initial access to a computer.

User Account	Provides
<b>Administrator</b>	Complete administrative access to a computer. This is the most powerful account on a computer and should be protected with a strong password. In some situations, you might also consider renaming this account.
<b>Power User</b>	 <b>Note:</b> This older account type is no longer available. However, you can give users the same rights and permissions that were given to Power Users in previous versions of Windows by adding users to the Power Users group. By default, the Power Users group has no default user rights. <p>Fewer access privileges than administrators, but more access privileges than standard users. Power Users might be able to install most software and updates, but they will be restricted from making changes that affect security or the core operating system. This account is available <i>only</i> in Windows XP.</p>
<b>Standard User</b>	Access to use most of the computing software on the computer. However, higher permission is required to uninstall or install software and hardware. This account also limits the configuration of security settings, operational settings, and deletion of necessary system files. This account is sometimes referred to as a non-privileged user account.
<b>Guest</b>	Limited computer access to individuals without a user account. By default, the <b>Guest</b> account is disabled when you install the operating system. You enable this account only if you want to permit users to log on as a guest.

### Permissions

You already know that a permission is a security setting that determines the level of access a user or group account has to a particular resource. Permissions can be associated with a variety of resources, such as files, printers, shared folders, and network directory databases. Permissions can typically be configured to allow different levels of privileges, or to deny privileges to users who should not access a resource.



**Figure 18-1: Permissions determine the user access level.**

Rights and permissions can be assigned to individual user accounts. However, this is an inefficient security practice, because so many permission assignments must be duplicated for users with similar roles and because individual users' roles and needs can change frequently. It is more efficient to create groups of users with common needs, and assign the rights and permissions to the user groups. As the needs of individual users change, the users can be placed in groups with the appropriate security configuration.

## NTFS File and Folder Permissions

On Windows operating systems, file-level security is supported on drives that are formatted to use the Windows NT File System (NTFS). These permissions can be applied either to folders or to individual files. NTFS permissions on a folder are inherited by the files and subfolders within it. There are several levels of NTFS permissions, which can determine, for example, whether users can read files or run applications; write to existing files; and modify, create, or delete files.

There are five standard NTFS permissions that you can assign to files.

Permission	Enables the User To
Read	Read the file and view file attributes, ownership, and permissions.
Write	Overwrite the file and change file attributes.
Read & Execute	Run applications and perform Read tasks.
Modify	Modify and delete the file.
Full Control	Change permissions, take ownership, and perform all other tasks.

There are six standard NTFS permissions that you can assign to folders or to drives.

Permission	Enables the User To
List Folder Contents	View the names, attributes, and permissions of subfolders in the folder, but only see the names of files within the folder.
Read	View names, attributes, permissions, and contents of files and subfolders in the folder.
Write	Create new files and subfolders in the folder, and change their attributes.

<b>Permission</b>	<b>Enables the User To</b>
Read & Execute	Perform the same functions as Read and List Folder Contents tasks, as well as execute files.
Modify	Delete the folder and perform Write and Read & Execute tasks.
Full Control	Change permissions, take ownership, delete subfolders and files, and perform all other tasks.

## Special Permissions

Each of the standard NTFS file permissions is made up of several more granular permissions called special permissions. Standard permissions are the most frequently assigned groups of permissions; special permissions provide you with a finer degree of control.

For example, the standard Read permission is made up of the following special permissions:

- List Folder/Read Data.
- Read Attributes.
- Read Extended Attributes.
- Read Permissions.

## File Compression and Encryption

File compression and file encryption are two special features of the NTFS file system that are implemented as advanced attributes.

- File compression is a way to save disk space by removing blank or repeated characters within files. Windows file compression is rarely used, partly because disk space on most systems today is relatively plentiful, and partly because there are other ways to reduce file size, such as with a file-compression utility like WinZip®, which creates a new, compressed file that you can copy to other media or email to other users.
- File encryption is an NTFS security measure that scrambles the contents of a file so that only the person who encrypted the file can open it, even if the disk containing the file is physically removed from the computer and loaded into a different computer system. File encryption is a good way to protect data on portable devices such as laptop computers.



**Note:** Other than NTFS compression, Windows employs different compression algorithms to create Cabinet (CAB) archive files. Because of the different algorithms used, NTFS compression tools are not necessarily compatible with CAB files.

# ACTIVITY 18-1

## Exploring NTFS Permissions

### Data Files

C:\LocalData\New Text Document

### Scenario

In order to check your understanding of NTFS permissions, you previously created a new folder named **LocalData** and then created an empty file named **New Text Document**. You have a few free minutes, so you decide to examine the permissions for the **Administrators** and **Users** groups to the folder and file.

1. Turn off the **Sharing Wizard**.
  - a) Open **This PC**, and select **View→Options→Change folder and search options**.
  - b) Select the **View** tab. Scroll to the bottom of the **Advanced settings** list.
  - c) Uncheck **Use Sharing Wizard (Recommended)** and select **OK**.
2. Examine the NTFS permissions on a drive.
  - a) Select the **C** drive. Right-click the **C** drive and select **Computer→Properties**.
  - b) Select the **Security** tab.
  - c) In the **Group or user names** list, select the **Administrators** group.
  - d) Determine the permissions assigned to the **Administrators** group.
  - e) Select the **Users** group.
  - f) Determine the permissions assigned to the **Users** group and select **Cancel**.
3. What level of permissions did the **Administrators** group have?
  - Full Control
  - Modify
  - Write
  - Read & Execute
4. What level of permissions did the **Users** group have?
  - Full Control
  - Modify
  - Write
  - Read & Execute
5. Examine NTFS folder permissions.
  - a) Double-click the **C** drive. Select the **LocalData** folder, and then select **Home→Properties**.
  - b) Select the **Security** tab.
  - c) Select the **Administrators** group.
  - d) Determine the permissions assigned to the **Administrators** group.
  - e) Select the **Users** group.
  - f) Determine the permissions assigned to the **Users** group, and then select **Cancel**.

6. How were the permissions in the LocalData folder different from the permissions on the C drive?
- Administrators did not have Full Control to the LocalData folder.
  - Users could not read files in the LocalData folder.
  - The permissions on the C drive were set explicitly; the permissions on the LocalData folder were inherited from the C drive.
  - The available permissions were not different.
7. Examine NTFS file permissions.
- a) Double-click the **LocalData** folder.
  - b) Select the **New Text Document** file, and then select **Home→Properties**.
  - c) Select the **Security** tab.
  - d) Select the **Administrators** group.
  - e) Determine the permissions assigned to the **Administrators** group. Verify that the permissions of the **New Text Document** file is the same as that of the C drive and the **LocalData** folder.
  - f) Select the **Users** group.
  - g) Determine the permissions assigned to the **Users** group, and then select **Cancel**.
  - h) Close the window.
8. True or False? The permissions in the New Text Document file were inherited from the LocalData folder permissions.
- True  
 False
- 

## Shared Files and Folders

A *share* is any network resource that is available to other computers or users on the network. Typical shares include folders, printers, and drives. Because shares enable users to access a computer system from a remote location, you should secure all shared resources against unauthorized access.

## Share Permissions

You can set three different levels of permissions on shared files and folders in Windows.

Permission	Enables Users To
Read	<ul style="list-style-type: none"> <li>• View file and subfolder names.</li> <li>• View file contents and file attributes.</li> <li>• Run program files.</li> </ul> <p>The Read permission is granted by default to the <b>Everyone</b> group when a folder is shared and to new users when they are added to the <b>Permissions</b> list.</p>
Change	<ul style="list-style-type: none"> <li>• Perform all Read permission tasks.</li> <li>• Add files and subfolders.</li> <li>• Change file contents.</li> <li>• Delete subfolders and files.</li> </ul>
Full Control	<ul style="list-style-type: none"> <li>• Perform all Read and Change tasks.</li> <li>• Change NTFS permissions on files and folders inside the shared folder.</li> </ul>

---

## NTFS vs. Share Permissions

NTFS permissions apply to the actions that users can take on a file or folder either on the network or locally. Share permissions apply only to the folders (and possibly subfolders and files) that have been shared with other users and are being accessed over the network. Using both NTFS and share permissions on the same files and folders may seem like overkill, but they are often used together, and it is important to understand the differences between the two permissions and how they interact with one another.

In Windows, a shared folder has two sets of permissions: the NTFS permissions (which are on the **Security** tab of that folder's **Properties**) and the share permissions (which are on the **Shared** tab of that folder's **Properties**). The security permissions do not automatically change once a folder is designated as a share, and there is no propagation between the two. A folder can have NTFS permissions assigned, and then be shared and have share permissions assigned. When a user accesses the folder over the network, both the share and NTFS permissions are applicable, and the most restrictive of the two sets of permissions applies. So, if the network user has the Full Control NTFS permission but only the Read share permission, the user will have only the ability to read the contents of the folder.



**Note:** When a user accesses a file on the local system, however, only the NTFS permissions apply. The fact that the folder is shared is not relevant when you are accessing the folder locally.

# ACTIVITY 18-2

## Exploring Share Permissions

### Scenario

In this activity, you will create a network share and assign share-level permissions.

1. Navigate to the C: drive and create a folder named **Share#** with the # being your student number.
2. Share the **Share#** folder.
  - a) Select the folder, display its pop-up menu, and select **Share with**.
  - b) Select **Advanced Sharing**.
  - c) If necessary, in the **User Account Control** dialog box, in the user name text box, type **APLUS-CLASS/Admin##**.
  - d) Check **Share this folder**, and then select **OK**.
3. Grant the **Everyone** group **Read** and **Modify** share permissions.
  - a) Select **Properties**.
  - b) On the **Security** tab, select **Advanced**.
  - c) In the **Advanced Security Settings for share##** dialog box, select the **Effective Access** tab.
  - d) Select **Select a user**, and in the **Select User or Group** dialog box, type **everyone** and select **Check Names**.
  - e) Select **OK** and then select **View effective access**.

The **Everyone** group currently has no effective access.
  - f) Select the **Permissions** tab, and then select **Add**.
  - g) Select **Select a principal**.
  - h) Type **everyone**, select **Check Names**, and select **OK**

Now, three basic permissions are applied.
  - i) Select **Show advanced permissions**.
  - j) Select **Show basic permissions**.
  - k) Check **Modify**.

**Write** is selected automatically.
  - l) Show advanced permissions again, and examine the changes.
  - m) Select **OK**.
  - n) Select the **Effective Access** tab.

A banner across the top of the dialog box warns you that you need to apply changes.
  - o) Select **Apply**.
  - p) Examine the **Effective Access** section and verify that permissions have changed for **Everyone**.
  - q) Select **OK**, and then select **Close**.

### File System Security

There are some important considerations that you should keep in mind when applying permissions to files and folders.

Consideration	Description
Allow vs. Deny	<p>When choosing whether to allow or deny an action using permissions, you need to choose carefully between the two. Deny is more restrictive than Allow. If the Deny property is applied on either a file or a folder, it will override any Allow permissions that may have been granted to the user. Therefore, use of the Deny permission should be done sparingly. You should deny permissions (using explicit Deny) only to a specific user when it is necessary to override permissions that are otherwise allowed for the group to which this user belongs.</p>
	<p>When establishing permissions, administrators can specify whether the entry being added should have access (Allow) or not have access (not Allow) to the resource. It is more practical to clear all the Allow check boxes for a group or a user, in effect denying them access to the resource without using the absolute Deny option. “Not-Allow” access in this way is easier to troubleshoot, manage and configure.</p>
Moving vs. copying files and folders	<p>When permissions have been applied, moving a file or folder and copying that file or folder will have different results. It is important to consider those results when choosing whether to move or to copy your files or folders.</p> <p>When you move a file or folder from one folder to another on the same partition, it retains the permissions that were applied to it in its original location. When you copy a file or folder from one directory to another, it inherits the permissions of the folder or directory to which it has been copied.</p> <p>When you move a file or folder between partitions, the result is similar to copying the file or folder: it will inherit the target folder's permissions.</p>
File attributes	<p>You can set file attributes on files and folders, and these attributes can affect the actions a user can have on that specific file or folder, regardless of the permissions that have already been set. If a file or folder has the Read-Only attribute, the attribute will override the permissions applied to users who are accessing that file or folder.</p>

## Security for Shared Files and Folders

Recall that there are two kinds of shares: *administrative shares* and *local shares*.

- Administrative shares are hidden shares that are created and shared by default on every Windows system. They are displayed with a "\$" to indicate that they are hidden files. Although you can delete these administrative shares, the system will re-create them every time the system restarts. Anyone with administrator access to the system can interact with administrative shares.
- Local shares are folders that are created on the local network by system users and then shared with other network users by using shared folder permissions. Users, including administrators, can delete local shares, and they are not automatically created upon restart.

On Windows systems, you can share a folder by modifying the folder's properties. When you share a folder, you assign it a share name that can be different from the underlying folder name. You can share the folder more than once using different names.

Users can connect to the shared folder by browsing to the computer in **Network**, or by selecting **Start→Run** and entering the Universal Naming Convention (UNC) path to the folder, in the form `\computername\sharename`.

## Permissions Inheritance

Permissions that you assign to a folder are inherited by files and folders within that folder. It is generally most efficient to group similar files together in a folder and assign permissions to the

folder, rather than to the individual files. Inherited permissions are indicated by gray background check marks in the file or folder's security properties.

### Permissions Propagation

If you modify the permissions for a parent folder, you can choose whether or not to propagate the changes downwards, which means to apply those permissions changes to all of the subfolders within the folder.

## Security for System Files and Folders

System files and folders are configured as Read Only and they are hidden. This prevents you or other users from accidentally deleting or modifying those files and folders. If you need to modify or delete a system file or folder, you will need to modify the permissions for the file or folder to remove the Read Only permission.

## User Authentication

User authentication is a network security measure in which a computer user or some other network component proves its identity in order to gain access to network resources. There are many possible authentication methods; one of the most common is a combination of a user name and a password.

Most authentication schemes are based on the use of one or more authentication factors. The factors include:

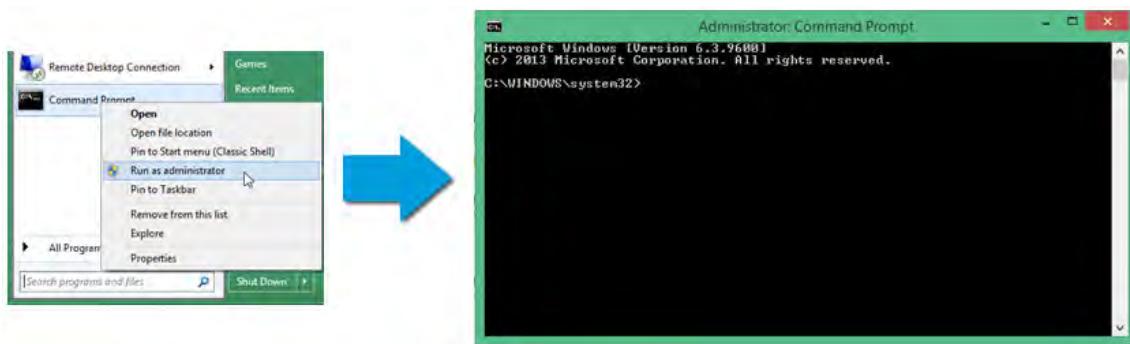
- Something you know, such as a password.
- Something you have, such as a key or an ID card.
- Something you are, including physical characteristics, such as fingerprints.

### SSO

Single sign-on (SSO) is an access control property that you can use to provide users with one-time authentication to multiple resources, servers, or sites. Users log in once with a single user name and password to gain access to a number of different systems, without being asked to log in at each access point. Different systems may use different mechanisms for user authentication, so SSO has to use different credentials to perform authentication. With the widespread use of SSO, it is important to ensure that user authentication is strong for the login; with one potential user name and password providing access to a host of systems, it is critical that this single access point is being properly secured.

## Run as Administrator

You should log in as a regular user most of the time. You will protect the system by not making it as easy to accidentally modify or delete files or folders, will know how other users will experience the system, and not give attackers as large a footprint to exploit. When you are logged in as a regular user and need to run an application or perform an action as an administrator, use the **Run as Administrator** command from the item's shortcut menu.



**Figure 18–2: Using Run as Administrator to open an administrative command prompt.**

## BitLocker

Windows BitLocker® is a security feature of Windows Vista, Windows 7, Windows 8/8.1, Windows Server® 2008, and Windows Server 2012. This security feature provides full disk-encryption protection for the operating system, as well as all the data stored on the operating system volume. BitLocker encrypts all data stored on the operating system volume and is configured by default to use a Trusted Platform Module (TPM). This feature ensures the protection of early startup components and locks any BitLocker-secured volumes in order to prevent access or tampering when the operating system is not running.

To use a TPM, you must have compatible system firmware and have TPM enabled in the firmware's settings. You can also configure BitLocker to operate without a TPM.

*BitLocker To Go* is used to encrypt removable storage devices such as USB flash drives or portable hard drives. These removable devices are locked and protected by default. You will need to specify how you will unlock the drive when you enable BitLocker To Go. Typically, the removable storage device is unlocked by using a password.

When you enable BitLocker or BitLocker To Go, you are prompted to save a recovery key backup. This is used to recover the password if it is lost or forgotten. If you lose the recovery key and don't know the password, the drive will remain inaccessible. The only way to use the drive would be to reformat it, thus losing all data on the drive.

Windows 8 encrypts drives more quickly than in previous versions of BitLocker and BitLocker To Go. Only the portion of the disk that is currently in use is encrypted. However, any additional data stored to the disk later will also be encrypted automatically.



**Note:** The OS X equivalent to BitLocker is FileVault.

## EFS

The *Encrypting File System (EFS)* is a file-encryption tool available on Windows systems that have partitions formatted with NTFS. EFS encrypts file data by using digital certificates. If a certificate authority is not available to issue a file-encryption certificate, the local system can issue a self-signed encryption certificate to users who want to encrypt files. Unlike NTFS permissions, which control access to the file, EFS protects the contents of the file. With EFS, you can keep data secure even if NTFS security is breached—for example, if an attacker steals a laptop computer and moves the laptop's hard drive to another system to bypass the NTFS security implementations.



**Figure 18–3:** Enabling EFS.

## Guidelines for Securing Microsoft Windows



**Note:** All of the Guidelines for this lesson are available as checklists from the **Checklist** tile on the CHOICE Course screen.

Follow these guideline to help secure Microsoft Windows:

- Log in as a regular user and use **Run as Administrator** when you need administrative access.
- Only provide the required permissions.
- Ensure that the combination of NTFS and share permissions don't give users excessive rights.
- Ensure that the combination of NTFS and share permissions don't remove users' needed rights.
- Use multifactor authentication for more secure resource access.
- Use BitLocker, BitLocker To Go, or EFS to encrypt file systems.

# ACTIVITY 18-3

## Securing the Windows File System

### Before You Begin

Several users and groups have been created in Active Directory, and related folders have been created on the domain controller.

### Scenario

You've been assigned to help a team of technicians who are implementing various security controls throughout your organization. Your tasks are focused on securing Windows file systems. You plan to investigate use of the **Run as administrator** command, as well as examine the interaction between NTFS permissions and share permissions. Finally, you want to explore ways to help keep sensitive information as secure as possible.

1. On your Windows 8.1 host computer, create a user named **tester**
  - a) Open **PC Settings**, and select **Accounts**.
  - b) Select **Other accounts**.
  - c) Select **Add an account**.
  - d) Because you are using this account to test the security of the local computer, select **Sign in without a Microsoft account (not recommended)**.
  - e) Select **Local account**.
  - f) For **User name**, type **tester**
  - g) For **Password** and **Reenter password**, type **!Pass1234**
  - h) For **Password hint**, type **same as admin account**
  - i) Select **Next**.
  - j) Select **Finish**.
  - k) On the **Manage other accounts** page, select **tester** and select **Edit**.
  - l) Verify that the **Account type** is set to **Standard user**, and then select **Cancel**.
  
2. Log on as **tester**, and open WordPad as a standard user.
  - a) Select **Start**, and select the arrow next to **Shut Down**, and then select **Switch User**.
  - b) At the login screen, select **tester** and enter **!Pass1234** as the password.
  - c) Select **Start**, and if necessary, select a menu type and select **OK**.
  - d) In the search box, type **wordpad** and select **WordPad** in the flyout menu.
 

WordPad opens automatically to a new, blank document.
  - e) Close WordPad.
  
3. Open WordPad with administrative privileges, and switch back to your **admin##** account.
  - a) Select **Start**, right-click **WordPad**, and select **Run as administrator**.
 

UAC prompts you to provide administrator credentials.
  - b) Select your **admin##** account, type your password, and select **Yes**.
 

WordPad now opens with a new, blank document.
  - c) Close WordPad.
  - d) Log off **tester**, and log back on as **admin##**.

4. You've been assigned to assist with securing certain Windows folders against unauthorized access. Only members of the Finance group should be able to view, access, and change files in the Finance folder that is stored on the server. How could you ensure that other employees cannot access the Finance folder?
  
  5. If Ali Lund is a member of the Finance group and she is also given explicit permissions of Read & Execute for the Finance folder, what are her effective permissions?
  
  6. Consider what would happen if share permissions were also assigned to the Finance folder. How might Finance users be affected?
  
  7. The sales representatives' laptops contain a lot of company confidential information. They want to keep this information secure as they travel. What recommendations would you make to help protect this data?
-

# TOPIC B

## Secure Workstations

In the last topic, you secured operating systems. There are additional tasks you can use to be sure workstations are protected from unauthorized access. In this topic, you will secure workstations.

### Password Best Practices

You know you need to create strong passwords that are not based on dictionary words; contain numbers, letters, and special characters; and have a minimum length. Some other best practices are provided in the following table.

<b>Best practice</b>	<b>Description</b>
Setting password expiration.	In most organizations, changing the password every two to three months is sufficient. In other organizations, changing it more frequently might be required. Remember that if it is changed too often, users will have more trouble remembering their password and might be tempted to write it down.
Changing default user names and passwords.	Some devices come with default user names and passwords. One example is wireless routers. Use the options built into the device to change the default user name and password so that unauthorized users cannot easily access the device. The default user name and password for wireless routers can easily be found in an Internet search.
	<b>Note:</b> Organizations often create users with a default password that must be changed when the user logs on for the first time.
Require screensaver passwords.	When a user steps away from the computer, they should lock the computer. If they forget to do so, having a screensaver that comes on after one minute and requires a password to unlock the system is a good backup to locking the computer.
Require BIOS or UEFI passwords.	Setting a BIOS or UEFI password will help prevent unauthorized users from accessing the BIOS or UEFI settings. If users make unauthorized changes to these settings, it might make their system stop working, make it work less efficiently, or make it out of compliance with organizational policies.
Require passwords.	On most modern systems, you have to set a password in order to set up the computer. If you are working with older systems, or other devices that don't have passwords by default, you should configure the device to use a password. Smartphones and tablets might not be configured to require a password. Printers and routers might also not require a password to change settings. All of these devices should require passwords whenever possible.

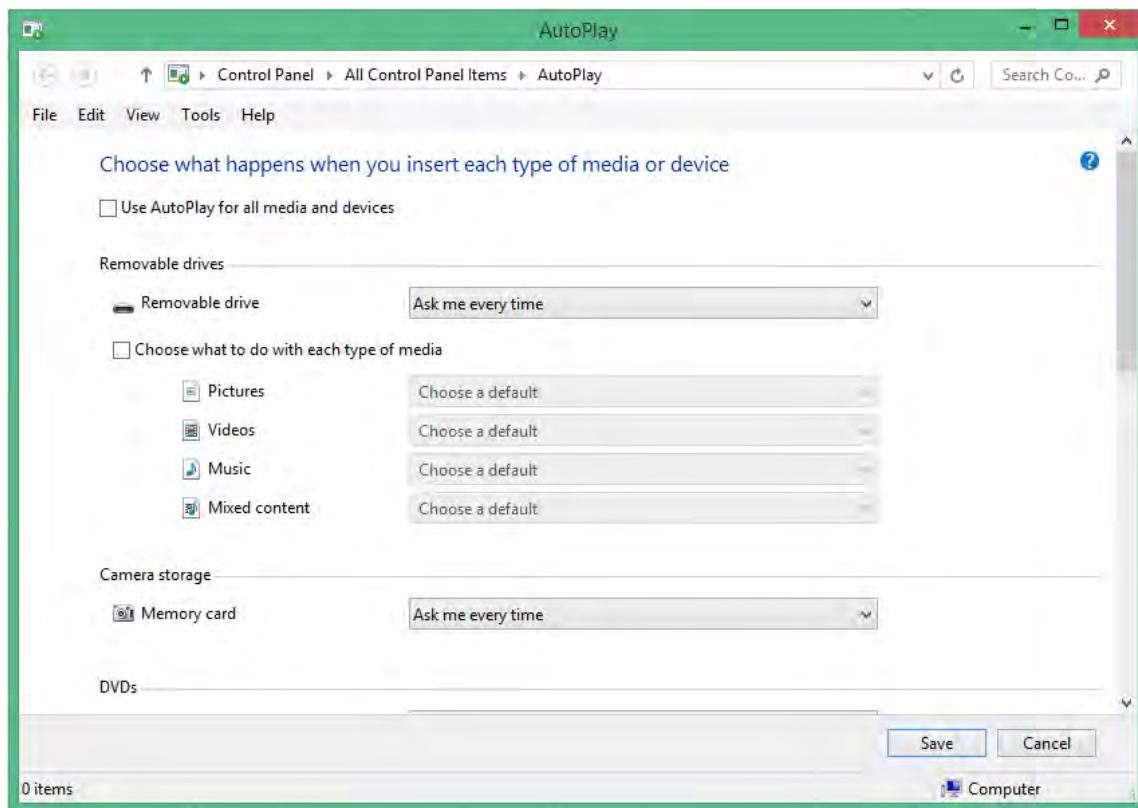
### Account Management

There are several account management techniques you can use to make your users and their data more secure. The items in the following table are just some of the most common; this is by no means a complete listing of the account management tasks you will need to perform.

<b>Account Management Task</b>	<b>Description</b>
Restrict user permissions.	Follow the principle of least privilege: Provide users with software with only the minimal level of access that is necessary for them to perform the duties required of them.
Configure login time restrictions.	You can configure the hours during which users can log in. You can also configure the account to allow the user access to the system for only a set number of hours during that time period.
Disable the guest account.	By default, the <b>Guest</b> account is disabled when you install Windows operating systems. Enable this account only if you want to permit users to log on as a guest.
Configure failed attempts lockout.	You can configure <b>Account lockout threshold</b> values. Most organizations set the value between three and five attempts, which allows users who mistype their passwords the chance to re-enter them before their accounts are locked. You can also configure how long the account will be locked. Many organizations set this interval to between 5 and 30 minutes; other organizations require that an administrator unlock the account.
Configure a timeout screen lock.	Most devices, including desktop computers, laptops, smartphones, and tablets, lock the screen after a certain period of time. This timeout value can be changed based on user needs. The user will need to enter a password or use another security unlock method to access the device again after it has been locked.

## Autorun

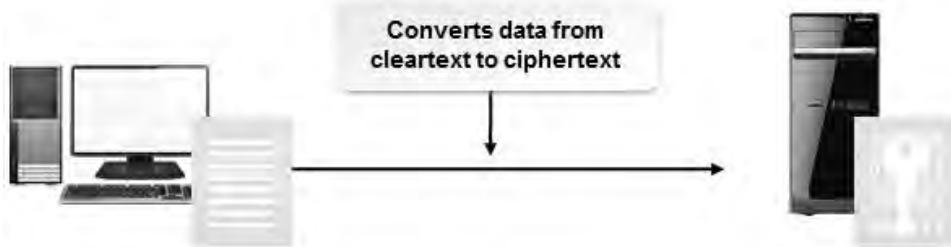
Disable autorun to prevent malware and other viruses from being loaded automatically with a device, such as a USB drive. Disabling the autorun feature will restrict any infected files from automatically loading.



**Figure 18–4:** Disabling AutoPlay in Windows 8.1.

## Data Encryption

Encryption is a *cryptographic* technique that converts data from plain, or *cleartext* form, into coded, or *ciphertext* form. Only authorized parties with the necessary decryption information can decode and read the data. Encryption can be one-way, which means the encryption is designed to hide only the cleartext and is never decrypted. Encryption can also be two-way, in which ciphertext can be decrypted back to cleartext and read.



**Figure 18–5:** Encryption converts plain data into ciphertext.

*Cryptography* is the science of hiding information. The practice of cryptography is thought to be nearly as old as the written word. Current cryptographic science has its roots in mathematics and computer science and relies heavily upon technology. Modern communications and computing use cryptography extensively to protect sensitive information and communications from unauthorized access.



**Note:** The word cryptography has roots in the Greek words *kryptós*, meaning “hidden,” and *“gráphein,”* meaning “to write,” translating into “hidden writing.”

A *cipher* is a specific set of actions used to encrypt data. *Plaintext* is the original, unencoded data. Once the cipher is applied via *enciphering*, the obscured data is known as *ciphertext*. The reverse process of translating ciphertext to cleartext is known as *deciphering*.

It is becoming common to encrypt many forms of communications and data streams, as well as entire hard disks. Some operating systems support whole-disk encryption, while some other commercially available open-source tools are capable of encrypting all or part of the data on a disk or drive.

An encryption *algorithm* is the rule, system, or mechanism used to encrypt data. Algorithms can be simple mechanical substitutions, but in electronic cryptography, they are generally complex mathematical functions. The stronger the mathematical function, the more difficult it is to break the encryption. A letter-substitution cipher, in which each letter of the alphabet is systematically replaced by another letter, is an example of a simple encryption algorithm.

## Patch Management

Patch management is the practice of monitoring for, obtaining, evaluating, testing, and deploying integral fixes and updates for programs or applications, known as patches. As the number of computer systems in use has grown over recent years, so has the volume of vulnerabilities and corresponding patches and updates intended to address those vulnerabilities. However, not every computer within an organization will necessarily be compatible with a certain patch, whether it be because of outdated hardware, different software versions, application dependencies, and so on. Because of the inconsistencies that may be present within the various systems, the task of managing and applying patches can become very time-consuming and inefficient without an organized patch management system. In typical patch management, software updates are evaluated for their applicability to an environment and then tested in a safe way on non-production systems. If the patch is validated on all possible configurations without causing more problems, only then will the valid patch be rolled out to all computers throughout the entire organization.

A patch management program might include:

- An individual responsible for subscribing to and reviewing vendor and security patches and updating newsletters.
- A review and triage of the updates into urgent, important, and non-critical categories.
- An offline patch-test environment where urgent and important patches can be installed and tested for functionality and impact.
- Immediate administrative push delivery of approved urgent patches.
- Weekly administrative push delivery of approved important patches.
- A periodic evaluation phase and full rollout for non-critical patches.

## Patch Management Policies

Many organizations have taken to creating official patch management policies that define the who, what, where, when, why, and how of patch management for that organization.

## Guidelines for Securing Workstations

When you select and apply computer security measures, you must make security adjustments that protect the workstation and the applications and data on it, while ensuring that the system runs appropriately for legitimate users. Follow these general guidelines for securing workstations:

- Manage user authentication.
  - Change the default user name and password on each workstation device.
  - Require all users to create strong passwords and to protect the passwords from others.
  - In high-security environments, implement multi-factor authentication that can include smart cards or biometric authentication systems.
- Install updates and patches.

- Install the latest operating system service packs and security update patches.
- Install the latest application patches for utilities that are included in the operating system as well as for web browsers and third-party application software.
- Manage user accounts.
  - Use policy settings to disable or delete guest accounts or other unnecessary accounts, and rename default accounts, so attackers cannot use known account names to access the system.
  - Restrict user permissions so that only those users who absolutely need access are allowed into the system.
  - Disable the guest account on all machines to prevent unauthorized access to any shared files and folders on the workstation.
- Educate users to follow best security practices, such as recognizing and avoiding hoaxes, phishing attacks, and potential malicious software sources.
- Apply workstation security measures.
  - Implement antivirus software to protect against malicious software.
  - Block pop-ups in your web browser.
  - Install a firewall and configure the appropriate open and closed ports and the program filtering settings.
  - Implement warning messages or banners displayed at user login to warn users that only authorized use is allowed. These banners could be important in future civil litigation or criminal prosecution, and they can put all users on notice that their activities might be monitored. All warning banners should comply with the legal requirements of your jurisdiction.
  - Disable autorun to prevent malware and other viruses from being loaded automatically with a device, such as a USB drive. Disabling the autorun features will restrict any infected files from automatically loading.
  - Enable the screensaver and password functionality to lock systems when idle.
  - Enable automatic operating system updates through the **Control Panel**.
  - Limit the number of shared resources on a system. Use share and file system permissions to restrict access to file and print resources.

# ACTIVITY 18-4

## Securing a Workstation

### Data Files

C:\Encrypt

### Scenario

A user recently received a new computer and has asked you to implement some of the security features provided in Windows 8.1 Pro. You decide to encrypt a folder that contains sensitive data and add more restrictive User Account Control settings.

1. Encrypt the **Encrypt** folder.
  - a) Open **This PC**, and navigate to **Local Disk (C:)**.
  - b) Locate and select the **Encrypt** folder, and display its pop-up menu.
  - c) Select **Properties**.
  - d) On the **General** tab, select **Advanced**.
  - e) Check **Encrypt contents to secure data**.
  - f) Select **OK** twice.
  - g) In the **Confirm Attribute Change** dialog box, verify that **Apply changes to this folder, subfolders and files** is selected, and select **OK**.  
A message is displayed in the status bar prompting you to back up your EFS certificate.
  - h) Select **Back up your file encryption key**.
  - i) Select **Back up later**.
  - j) Examine the **Encrypt** folder.  
The **Encrypt** folder name is now green to indicate that it and its contents are encrypted.
  - k) Close **This PC**.
2. Adjust the User Account Control settings to always notify the user when administrative-level changes are made to the computer.
  - a) Open **Control Panel**, and enter **uac** in the **Search Control Panel** text box.
  - b) Select **Change User Account Control settings**.
  - c) If prompted, by **UAC Credentials**, type **Admin##** with a password **!Pass1234**
  - d) Move the slider bar to **Always Notify**.
  - e) Select **OK**.
  - f) Select **Yes**.
  - g) Close **Control Panel**.

# TOPIC C

## Secure SOHO Networks

Earlier in the course, you installed and configured a SOHO network. As with any other computer network, SOHO networks need to be secured to prevent unauthorized access and other threats. In this topic, you will examine how security controls are implemented to secure both wired and wireless SOHO networks.

Securing your network is critical to keeping data, systems, and resources safe from unauthorized access. You must understand what the security implications are when a network is improperly secured. Security controls and implementations restrict access to sensitive data and system resources. As the A+ technician, it's your job to make sure that the right security controls are implemented and functioning as expected.

### SOHO Security Methods

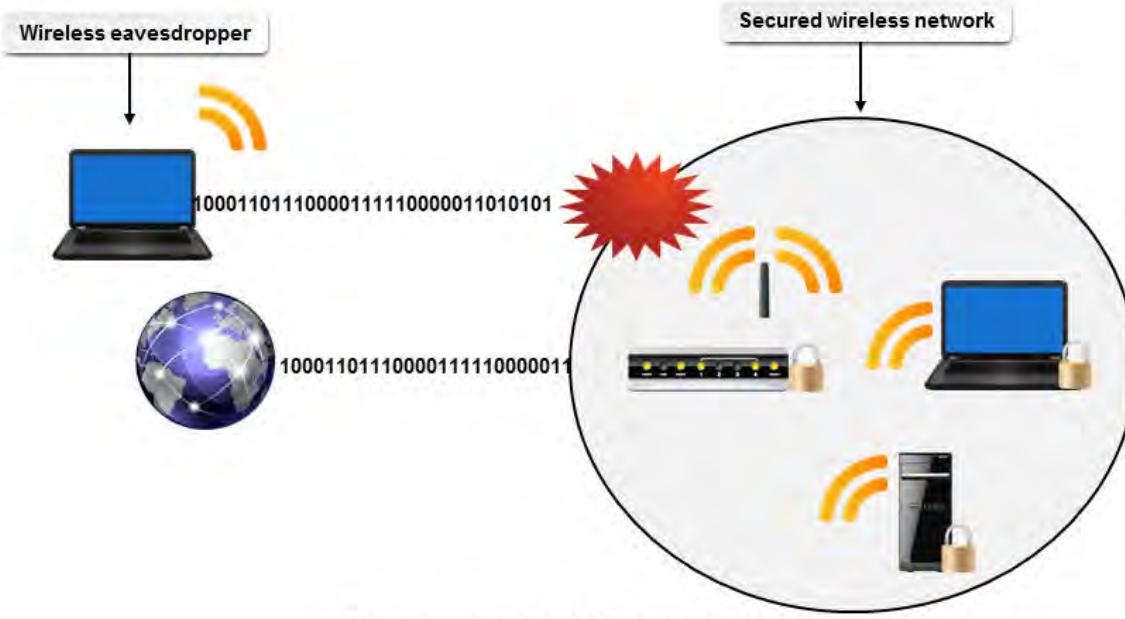
When implementing and configuring a SOHO network, you must ensure that the proper security measures have been taken to prevent any unauthorized access.

<b>Method</b>	<b>Description</b>
Change default user name and password	Change the default user name and password for all devices connected to the network. Use strong password guidelines when assigning the new passwords.
Enable MAC filtering	MAC address filtering provides a simple method of securing a network. Typically, an administrator configures a list of client MAC addresses that are allowed to join the network. Those pre-approved clients are granted access if the MAC address is known by the network.
Assign static IP addresses	When implementing a small network, you can assign each device on the network a static IP address. When each device has a designated IP address, you remove the plug-in-and-go capability that DHCP provides, so only those devices with IP addresses that are in the same range as the static addresses will be able to connect to the network.
Disable ports	Disabling unused network ports can prevent unauthorized access to your network. Attackers look for open ports on networks to launch an attack.

<b>Method</b>	<b>Description</b>
Firewall settings	<p>Windows client firewalls can be configured for networking to ensure that they are secure against unauthorized access attempts and attacks. Consider the following settings when setting up the firewall:</p> <ul style="list-style-type: none"> <li>• Enabling or disabling port security on certain ports.</li> <li>• Inbound and outbound filtering. The user can set up rules or exceptions in the firewall settings to limit access to the web.</li> <li>• Reporting and logging activity.</li> <li>• Malware and spyware protection.</li> <li>• Pop-up blocking.</li> <li>• Port assigning, forwarding, and triggering.</li> <li>• Enabling or disabling the Windows Firewall when necessary.</li> </ul>
	<p>Windows Firewall is a software-based firewall that is included with Windows Vista and later operating systems. Once an operating system is installed, Windows Firewall is automatically installed and enabled. By default, the firewall blocks unsolicited incoming traffic on all ports. You can open blocked ports and configure other firewall settings by using the Windows Firewall program in the <b>Control Panel</b> or through Windows Security Policy Settings. Windows Firewall can be configured to drop outgoing traffic as well as incoming traffic.</p>
Port forwarding/mapping	<p>NAT (network address translation) is used on most SOHO routers to redirect communication requests from one IP address and port number to another through port forwarding or mapping. This allows one IP address outside the network to be used by multiple devices and systems inside the network.</p>
Content filtering and parental controls	<p>Through operating system features or third-party apps, you can filter content. You can filter based on age ranges, adult content, or other specific terms. Parental control filtering can be configured to send a report to a specified email address on a regular basis to let you know where the user has gone while online, the amount of time spent online, and other configurable control settings.</p>
Firmware updates	<p>As with other devices, SOHO computers, printers, routers, and other devices need to have firmware updates applied as needed.</p>
Apply physical security controls	<p>Depending on the location of the network, you may need to ensure that the devices and network components cannot be accessed by unauthorized users. This may be as simple as making sure that all the entrances have proper security controls installed. This could be anything from locked doors, surveillance systems, to installing a biometric identification system.</p>
Perform assessments	<p>Perform regular security assessments to determine if current controls are meeting the needs of the organization.</p>

## Wireless Security

*Wireless security* is any method of securing a wireless local area network (LAN) to prevent unauthorized network access and network data theft. You need to ensure that authorized users can connect to the network without any hindrances. Wireless networks are more vulnerable to attacks than any other network system. For one thing, most wireless devices such as laptops, mobile phones, and other mobile devices search and connect automatically to the access point offering the best signal, which can be coming from an attacker. Wireless transmissions can also be scanned or sniffed out of the air, with no need to access physical network media. Such attacks can be avoided by using relevant security protocols.

**Prevents data access and wireless intrusions****Figure 18–6: Wireless security.**

## SOHO Wireless Security Methods

There are a number of security methods you can use to ensure that your wireless network is secure from unauthorized access.

<b>Method</b>	<b>Description</b>
Configure the network settings	<ul style="list-style-type: none"> <li>Secure your wireless router or access point administration interface.</li> <li>Disable remote administration.</li> <li>Secure/disable the reset switch/function.</li> <li>Change the default SNMP parameter.</li> <li>Change the default channel.</li> <li>Regularly upgrade the Wi-Fi router firmware to ensure you have the latest security patches and critical fixes.</li> <li>Use the Remote Authentication Dial-In User Service Plus (RADIUS+) network directory authentication where feasible.</li> <li>Use a VPN.</li> <li>Perform periodic rogue wireless access point scans.</li> </ul>
Configure the SSID	<ul style="list-style-type: none"> <li>Change the default Service Set Identifier (SSID).</li> <li>Disable the SSID broadcast.</li> </ul> <div style="border: 1px solid black; padding: 5px;"> <p> <b>Note:</b> PCs running Windows 7 and later will detect existing networks, even if it can't identify them by name (SSID). It's not difficult to unmask a SSID and when a person attempts to hide the SSID, it may actually attract more attention because it suggests the network may contain sensitive data.</p> </div>

Method	Description
Setting encryption	<ul style="list-style-type: none"> <li>Enable WPA2 encryption.</li> <li>Change the default encryption keys.</li> <li>Avoid using pre-shared keys (PSK).</li> </ul>
	<b>Note:</b> If you need to share keys, use asymmetric key sharing.
Properly place the antenna and access point	<p>Position the router or access point and antenna safely. The radio frequency range of each access point should not extend beyond the physical boundaries and layout of the organization's facilities.</p>
Secure the wireless access point	<p>Specific procedures for implementing security options on wireless devices, as well as the options your devices support, will vary. Always check the documentation from your wireless device manufacturer before implementing any security configurations. Common methods include:</p>
	<ul style="list-style-type: none"> <li>Implementing some form of user authentication.</li> <li>Implementing a security protocol that requires over-the-air data encryption.</li> <li>Updating firmware on the device to implement any manufacturer security patches and enhancements.</li> <li>Restricting unauthorized devices from connecting to the WAP by filtering out unauthorized MAC addresses.</li> <li>Implementing a firewall. For a small office or home office, enable a firewall on the WAP, and then also on the host computer to further secure your network.</li> <li>Configuring vendor-recommended security settings on your wireless router or access point.</li> </ul>
Radio power levels	<p>Adjust the radio power level controls on routers and access points as needed to help minimize power consumption within the wireless network. It can be difficult to manage the radio power of wireless to reduce the power used, while providing the right level of radio power to operate the network.</p>
	<b>Note:</b> This is also known as antenna power.
WPS	<p>The Wi-Fi-Protected Setup (WPS) standard was released by the Wi-Fi Alliance to enable an easy yet secure setup of small home networks. The goal of the standard was to ease the setup and complicated configuration settings of wireless routers designed for use in SOHO networks. The standard can easily be cracked by brute force attacks and has been reported to be less secure. If you encounter a router with WPS enabled by default, you may need to turn it off once the router is connected.</p>
Configure the workstation	<ul style="list-style-type: none"> <li>Do not auto-connect to open Wi-Fi networks.</li> <li>Enable firewalls on each computer and the router.</li> <li>Assign static IP addresses to devices to prevent inadvertent broadcasting of IP addresses to unauthorized parties.</li> </ul>

## Guidelines for Securing SOHO Networks

You have several options for increasing the security on your wireless clients; however, specific procedures for implementing security options on wireless clients, as well as the options your devices support, will vary. Consult the documentation for your wireless client devices. Some guidelines to consider are listed as follows:

- Implement a security protocol that requires over-the-air data encryption.
- Install antivirus software and/or adware and spyware blockers.
- Update clients regularly with any software security patches.

# ACTIVITY 18-5

## Securing a SOHO Wireless Network

### Before You Begin

You will need an Internet connection to access the emulator.

### Scenario

You will soon be setting up several SOHO wireless networks. Before you do so, you want to practice. You found an online simulator for the model of wireless router that you will be installing for the SOHO networks.



**Note:** Activities may vary slightly if the software vendor has issued digital updates. Your instructor will notify you of any changes.

1. Connect to the wireless router's configuration interface.
    - a) Open **Internet Explorer**.
    - b) In the **Address** bar, enter <http://ui.linksys.com>
    - c) From the list of routers, select the **E1200** link.
    - d) Select the **2.0.04/** link.
    - e) In the **Warning** message box, check the **Do not show me this again** check box and select **OK**.
- 
- Note:** This website emulates a common router configuration interface. When working with a real device, you will typically connect to http://192.168.1.1 and be prompted to enter a user name and password. For a list of default user names and passwords by router, navigate to <http://www.routerpasswords.com>.
2. Set an SSID for your wireless network.
    - a) On the menu bar at the top of the page, select the **Wireless** tab.
    - b) If necessary, select **Manual**.
    - c) In the **Network Name (SSID)** text box, double-click and type **child##.gcinteriors**
    - d) Select **Save Settings** and, in the **Message from webpage** message box, select **OK**.
    - e) Select **Save Settings** again, and then select **Continue**.
- 
- Note:** Because you are using an emulator, you can use all lowercase letters in the **Network Name (SSID)** text box.
3. Set WPA2 encryption with a passphrase.
    - a) Under the **Wireless** tab on the menu bar, select the **Wireless Security** link.
    - b) From the **Security Mode** drop-down list, select **WPA2 Personal**.
    - c) In the **Passphrase** text box, type **/Pass1234**
    - d) Select **Save Settings**, and then select **Continue**.
  4. Configure the router's administration settings.
    - a) On the menu bar, select the **Administration** tab.
    - b) In the **Router Password** text box, double-click the existing password (represented by asterisks) and type **P@ssw0rd**
    - c) In the **Re-Enter to Confirm** text box, type the same password.

- d) In the **Local Management Access** section, clear the **HTTP** check box and check the **HTTPS** check box.
  - e) In the **Local Management Access** section, for the **Access via Wireless** option, select **Disabled**.
  - f) In the **Remote Management Access** section, verify that **Remote Management** is disabled.
  - g) At the bottom of the web page, select **Save Settings**.
  - h) On the **Your settings have been successfully saved** page, select **Continue**.
  - i) Close **Internet Explorer**.
-

# TOPIC D

## Secure Mobile Devices

So far in this lesson, you have secured OSs, workstations, and SOHO networks. To fully protect your computing environment, there is one more category of devices that you need to secure. In this topic, you will identify methods for securing mobile devices.

### Screen Locks

The screen lock option on all mobile devices should be enabled with a locking option, and strict requirements on when the device will be locked. You can specify how long the device is active before it locks, which typically ranges from 1 minute to 5 minutes. Once the device is locked, it can only be accessed by entering the required input that has been set up by the user. This security control prevents access to the device if it is misplaced or stolen.

Locking options include:

- Passcode locks
- Fingerprint locks
- Face locks
- Swipe locks

On some devices, you can configure the passcode settings to erase all data stored on the device after a certain number of failed logon attempts.

Often, enabling screen lock can be a requirement in an organizational security policy, no matter if the mobile device is provided by the employer or the individual.

Be aware of pattern swipe locks that require a user to complete a specific action on the touch screen to activate the device. Most of the time, the smudge pattern is visible on the surface and can be re-created to gain access to the device. Using a numeric pin or an alphanumeric password is considered more secure.

### Remote Wipe

Data wiping is a method used to remove any sensitive data from a mobile device and permanently delete it.

Remote wiping is also available for some devices, so you can perform these functions remotely in case the phone is lost or stolen. Wipe and sanitization guidelines and requirements might be included in an organization's security policy if mobile devices are issued to employees for professional use. In some cases, Admins will have rights to remote in to any device that is supported by the organization.

### Locator Applications

GPS tracking service functionality is available on a number of mobile devices and can be added in most cases when required for business reasons. This feature is used as a security measure to protect and track mobile devices that may be lost or stolen.

If a mobile device does not have the locating functionality built in, then you can download a locator application that can track and locate a lost or stolen device.

If a mobile device has a locator app installed and the device is lost or stolen, some apps allow the user to remotely enable features in the app. One feature that can be quite useful is enabling the camera on the phone. It has been reported that sometimes the thief has been captured using the photos taken in this manner.

## Remote Backup Applications

Depending on the type of mobile device, there are remote backup services available through the OS. For example, Apple offers remote backup services to its iCloud® through the **General Settings** of the device. From there, you can specify what application data to back up. Android offers remote backup using Google Drive. Both these services offer the first 5 GB of data for free, then you can purchase more backup space as needed. These features allow you to recover your data when a device is either lost or stolen.

## Failed Login Attempts Restrictions

As part of the secure configuration of a mobile device, you should configure the number of times a user is allowed to enter the wrong passcode and what happens when the value is exceeded. An iOS device can be configured to disable the device for a certain number of minutes after a specified number of failed attempts at entering the correct PIN, password, swipe pattern, or other passcode. For up to 5 failed attempts, usually the device is not disabled. For additional failed passcode attempts, the device is disabled for 1 minute to 60 minutes, and after more than 10 attempts, the device data is deleted. If the data is deleted, then the data will need to be restored through the iTunes Restore option.

Android devices can also be configured for how many passcode attempts can be made before the device is locked or wiped. To unlock the device, the user will need to enter the Gmail account details that were used when the device was initially set up.

## Antivirus and Antimalware Applications

There are many different options when it comes to mobile antivirus solutions. Organizations that allow mobile devices to connect to the network and transfer data should require that antivirus get installed to prevent unauthorized access to data, systems, and resources. There are a number of solutions available:

- BullGuard Mobile Security
- Kaspersky Mobile Security
- ESET Mobile Security
- Lookout Premium
- Trend Micro Mobile Security
- Webroot Secure Anywhere Mobile

## Mobile OS Patches and Updates

Mobile device updates are similar to other computing devices updates and patches. Verify that devices are set up to automatically install updates from the manufacturer. Updates and patches can resolve security issues and systems flaws that present a security risk.

## Biometric Authentication

Some mobile devices can be accessed using biometric authentication. The device might use the built-in camera to do facial recognition. It also might have a fingerprint scanner. Both of these options need to be configured and multiple scans of the face or fingerprint will need to be completed to set up the device to use these features.

## Full Device Encryption

When available, all mobile devices should be configured to use data encryption to protect company-specific and personal data that may be stored and accessed on the device. This method is effective as

long as the hardware cannot be accessed to steal the data. Along with device encryption, data encryption should also be used so when data is accessed by physically taking the device apart, the data remains secured.

Device encryption can also be a requirement in an organizational security policy.

## Multifactor Authentication

Like computers, mobile devices can be configured to use multifactor authentication. This might include entering a PIN in addition to entering a swipe pattern, or using biometric authentication with a knowledge-based authentication factor.

Another multifactor authentication process has the user enter a passcode using any of the previously mentioned authentication methods, then enter a security code. The security code is sent to the user's email, as an SMS text message, or via a phone call. On a Microsoft account, using the two-step verification through the *authenticator app* will apply to all services and devices that support the two-step verification process. This includes services such as the Windows 8/8.1 operating systems, outlook.com, Microsoft Office applications, and OneDrive.

Google Authenticator is an authenticator app that can be configured for Android, Blackberry, and iOS devices. This enables you to set up two-step verification by using text messages or phone calls as well as by generating codes that can be received even without an Internet connection or mobile service.

## Trusted and Untrusted Sources

The source of applications and networks for mobile devices is varied. Some sources can be trusted and others are untrusted. Apps available through official app stores for a device are considered trusted. The apps are only made available if they pass a number of qualifications to be included in the app store. Apps that users find searching the Internet might or might not be from a trusted source. Secure wireless networks with an encrypted connection can usually be considered trusted. Ad hoc networks created via Bluetooth connections are untrusted as are public networks such as those found in coffee shops.

## Firewalls

Some mobile devices include firewall hardware and software built into the device. This helps protect from unauthorized connections from other devices that are attempting to connect to and communicate with or through the mobile device. The firewall can be configured to block apps on the device from connecting and communicating with services outside of the device. It provides protection against most common types of attacks.

## Policies and Procedures

Security policies and procedures are often a part of a larger, comprehensive document set called a *security profile*. Security profiles generally contain:

- *Policies* are documents that outline the specific requirements and rules everyone must meet, such as rules for appropriate mobile device usage in the workplace.
- *Procedures* provide detailed information about specific devices and technologies that support policies, such as how to configure corporate firewalls.
- *Standards* are tactical documents that specify processes to follow to meet policy requirements. For instance, a standards document for mobile device security controls might specify that company-owned mobile devices be configured with multifactor authentication, laptops require full disk encryption, and all devices lock after 5 failed login attempts.

- *Baselines* outline the minimum level of security required for a system, device, network, or premises. For instance, all visitors must agree to allow searches of bags or briefcases upon request.
- *Guidelines* are documents that outline best practices and recommendations to help conform to policies.

*Bring Your Own Device (BYOD)* and *Corporate Owned, Personally Enabled (COPE)* policies define how user-owned or organization-owned mobile devices are to be used when the device is used for organizational communication and data storage. This BYOD movement provides user satisfaction, but sometimes at a cost to the organization. Having users purchase their own devices and contracts saves organizations money initially, but might end up costing more in lost data and the introduction of malware on the corporate network if policies and procedures to protect the data are not created and adhered to. Organizations created COPE to address some of the concerns created by BYOD.

Some examples of BYOD and COPE policies can be found at <https://www.whitehouse.gov/digitalgov/bring-your-own-device>. As the document states, implementing these policies is an iterative process. Technologies evolve, new threats are identified, and new devices and services become available. Policies need to be updated to address these changes and improvements.

## Guidelines for Securing Mobile Devices

It is just as important to ensure mobile devices are secure as it is to secure desktops, laptops, and network resources. Some guidelines to consider are listed as follows:

- Require screen locks to prevent unauthorized access to mobile devices. The screen lock should be activated after a short time of device inactivity.
- Configure the mobile device for remote wipe in case of loss or theft of the device.
- Use or install locator apps to help find lost or stolen mobile devices.
- Back up mobile device apps and data to the cloud or a computer using appropriate synchronization techniques for the device.
- Configure failed login attempt restrictions. Give the users a few chances to enter the correct passcode, then lock or wipe the device as appropriate.
- Ensure that antivirus and antimalware apps are installed on mobile devices.
- Install appropriate mobile device OS patches and updates in a timely manner.
- Consider using biometric authentication if it is available on the device.
- Implement full device encryption to protect data stored on the mobile device.
- Consider using multifactor authentication, which might include two-step verification via email, SMS text message, or phone call.
- Make sure that apps and networks used are from trusted sources.
- Consider using mobile devices with built-in firewall capabilities.
- Create appropriate BYOD or COPE policies and procedures for mobile device use in your organization.

## ACTIVITY 18-6

### Securing Mobile Devices

#### Scenario

The number of mobile devices has grown substantially throughout the organization in the past few months. You want to make sure you are familiar with various ways to make mobile devices more secure.

1. Examine the **Security** settings for your mobile device.
  - a) Examine the lock screen options.
  - b) Determine if a locator app is installed.
  - c) Examine the encryption settings.
  - d) Examine installed certificates.
  - e) Examine any other security settings available on your device.
2. Verify that antivirus and antimalware apps are installed.



**Note:** If no antivirus or antimalware app is installed, your instructor might have you install an app.

## Summary

In this lesson, you implemented and described many concepts and techniques that can be used to establish the desired level of security within an organization. Every organization will have different security requirements based on the type of business they conduct. It is your job to understand those requirements and know how security controls should be implemented to directly support those needs.

**Which security measures do you feel are the most important? Which are the minimum measures that should be taken? Does your organization implement good security practices?**

**What physical security controls have you had experience with? What controls do you think are the most common?**



**Note:** Check your CHOICE Course screen for opportunities to interact with your classmates, peers, and the larger CHOICE online community about the topics covered in this course or other topics you are interested in. From the Course screen you can also access available resources for a more continuous learning experience.



19

# Troubleshooting System-Wide Issues

**Lesson Time:** 1 hour, 30 minutes

## Lesson Objectives

In this lesson, you will troubleshoot system-wide issues. You will:

- Troubleshoot PC operating system problems with appropriate tools.
- Troubleshoot common mobile operating system and application issues.
- Troubleshoot wired and wireless networks using appropriate tools.
- Troubleshoot common PC and mobile security issues using appropriate tools and best practices.

## Lesson Introduction

Throughout the course so far, you focused on troubleshooting the hardware components that physically make up a personal computer or mobile device. You are well aware that there are other essential components needed for the PC or mobile device to work properly; the OS, the network, and security are all integral parts of the computing environment. In this lesson, you will troubleshoot system-wide issues.

You can have all of the components of a PC or mobile device properly installed and configured, and still not be able to perform the tasks that you need to perform. Software, network, and security issues can present their own sets of problems for you to troubleshoot and resolve.

# TOPIC A

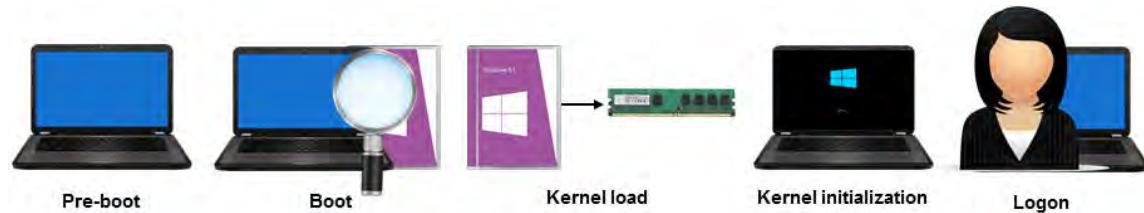
## Troubleshoot PC Operating Systems

In this lesson, you will troubleshoot system issues. The operating system is an essential component in the computer environment, managing all the resources that make up the system and providing the interface for users to interact with these resources. If the OS is not functioning properly, the computer will not be able to perform as needed. In this topic, you will troubleshoot PC operating systems.

As a computer support professional, you will be the first line of response to help users when problems arise with their PCs. You will need the knowledge to recognize and diagnose problem conditions, and you will need to respond to those problems with the appropriate corrective action. The information, utilities, and skills in this topic should provide you with the diagnostic and troubleshooting toolkit you will need to identify and correct a range of possible PC problems.

### The Windows Boot Process

There are five major sequences that occur during the Windows *boot process*.



**Figure 19-1: The Windows boot process.**

Sequence	Description
Pre-boot sequence	The pre-boot sequence begins when the power is turned on. The computer runs Power-On Self Test (POST) routines to determine the amount of physical memory and to identify and check the other hardware components present. If the computer has a PnP BIOS, the hardware is recognized and configured. The computer BIOS locates the boot device, and then loads and runs the Master Boot Record (MBR). The MBR scans the partition table to locate the active partition, loads the boot sector on the active partition into memory, and then executes it.
Boot sequence	The boot sequence is when the operating system is selected, and the hardware configuration is detected and loaded. It has four subphases: initial boot loader, operating system selection, hardware detection, and configuration selection. In Windows Vista and later, this is accomplished by the winload.exe and Windows Boot Manager components. (In Windows XP and earlier operating systems that use the NT kernel, this was done with NTLDR (NT Loader) and the boot.ini file.)
Kernel load sequence	During the kernel load sequence, the operating system components are loaded into memory.
Kernel initiation sequence	In the kernel initiation sequence, the Windows kernel takes control of the system. At this point, the Microsoft Windows logo appears, along with a status bar.

<b>Sequence</b>	<b>Description</b>
Logon sequence	During the logon sequence, Winlogon.exe starts the Local Security Authority (LSA), and the <b>Logon</b> screen or <b>Logon</b> dialog box appears. Users can now log on, while Windows continues to load low-level drivers and services in the background. The boot process is considered complete when a user successfully logs on. The <b>Clone</b> control set built is copied to a new control set called <b>LastKnownGood</b> , thus preserving a copy of the settings in the successful boot sequence.

## Windows 8 Secure Boot Options

Microsoft added four features to the Windows 8/8.1 OS that are designed to protect users from rootkit and botkit malware being loaded during system startup.

	<b>Note:</b> If you have UEFI and Windows 8, you have secure boot by default.
---	---

<b>Feature</b>	<b>Description</b>
Secure Boot	Newer computers equipped with UEFI and TPM are configured by default to only load trusted bootloaders. If you need to boot from another bootloader that is not trusted, you can configure Secure Boot to allow booting from the untrusted bootloader.
Trusted Boot	The integrity of all components of the startup process are checked by the operating system before the components are loaded.
Early Launch Anti-Malware (ELAM)	Before loading any drivers, they are tested by ELAM. Any drivers that are not approved are prevented from being loaded.
Measured Boot	The boot process is logged by the system firmware. This information can be sent by Windows to a trusted server. The server checks the health of the system and allows access to the network only if the health of the system meets the criteria set on the server. If the health parameters are not met, the server might be configured to allow the client access to a limited-access, quarantined network where remediation can be performed to bring the system into compliance with the health requirements.

## The Linux Boot Process

The Linux boot process is repeated each time your computer is started by loading the operating system from the hard drive. It involves a series of sequential steps that can be divided into BIOS initialization, boot loader, kernel and init initialization, and boot scripts.

The boot process consists of the following steps:

1. The processor checks for the BIOS program and executes it.
2. BIOS checks for peripherals, such as floppy disk drives, CD-ROMs, and the hard disk, for bootable media. It locates a valid device to boot the system.
3. BIOS loads the primary boot loader from the MBR into memory. The boot loader is a program that contains instructions required to boot a machine. It also loads the partition table along with it.
4. The user is prompted with a graphical screen that displays the different operating systems available in the system to boot from. The user should select an operating system and press **Enter** to boot the system. If the user does not respond, then the default operating system will be booted.

5. The boot loader determines the kernel and locates the corresponding kernel binary. It then uploads the respective `initrd` image into memory and transfers control of the boot process to the kernel.
6. The kernel configures the available hardware, including processors, I/O subsystems, and storage devices. It decompresses the `initrd` image and mounts it to load the necessary drivers. If the system implemented any virtual devices, such as LVM or software RAID, then they are initialized. The components configured by the kernel will be displayed one by one on the screen.
7. The kernel mounts the root partition and releases unused memory. To set up the user environment, the `init` program is executed.
8. The `init` program searches for the `inittab` file, which contains details of the runlevel that has to be started. It sets the environment path, checks the filesystem, initializes the serial ports, and runs background processes for the runlevel.
9. If graphical mode is selected, then `xdm` or `kdm` is started and the login window is displayed on the screen.
10. The user enters the user name and password to log in to the system.
11. The system authenticates the user. If the user is valid, then the profile, the `.login`, the `.bash_login`, and the `.bash_profile` files are executed. The shell is started and the system is ready for the user to work on.



**Note:** `xdm` refers to the X Window Desktop Manager. Users who utilize GNOME or KDE, use either `gdm` or `kdm`, respectively. In CentOS 7, the GNOME Display Manager `gdm` is the default desktop manager.

## Troubleshooting the Boot Process

The *Linux rescue environment* is a stand-alone Linux program for troubleshooting a corrupt Linux installation. It serves as an external environment through which errors in the Linux system can be fixed without the help of the existing installation files. The rescue environment mounts the standard Linux system directories in the `/mnt/sysimage` directory. These directories are mounted either in read-write mode or read-only mode, depending on the kinds of issues.

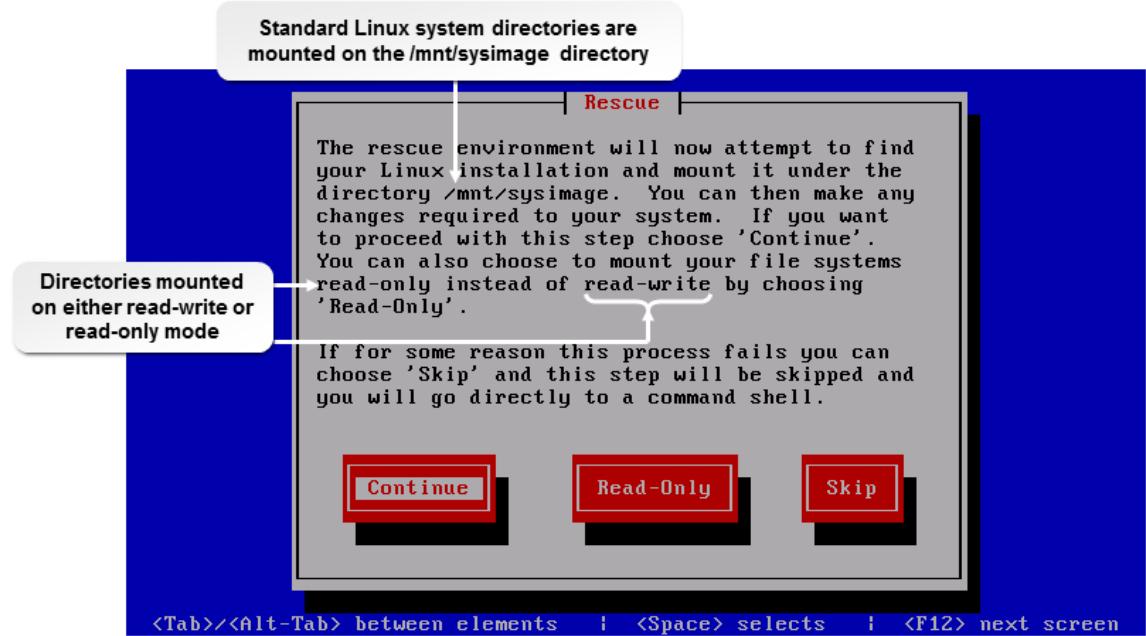


Figure 19-2: The rescue environment for troubleshooting Linux issues.



**Note:** In some cases, when system directories cannot be mounted on the `/mnt/sysimage` directory, the prompt will be available for troubleshooting.

The `chroot` mode shifts the root (/) directory to a different location for recovery. It is also known as jail mode because it can be used in production scenarios to ensure a user will not be able to access any other file or directory except this directory and its subdirectories.

The following table can help you troubleshoot the boot process.

Cause	Solution
If the boot loader screen does not appear, then GRUB (GRand Unified Bootloader) may not be properly configured.	Reconfigure the <code>/boot/grub2/grub.cfg</code> file and/or reinstall GRUB in rescue mode.
If Linux does not boot on a Windows/Linux dual boot system, then GRUB or LILO (LInux LOader) may not be installed.	Use the Linux distribution install disk to reinstall GRUB or LILO to the MBR.
If the <code>grub&gt;</code> prompt appears, then GRUB may be corrupted.	Install GRUB again in rescue mode.
If the kernel does not load, then the kernel image may be corrupted.	Install a new kernel in rescue mode.
If the kernel does not load, then the parameter passed during the system startup may be wrong.	Specify the correct parameter by editing GRUB on the boot loader screen.
If there is a kernel panic, then:	Use the applicable solution: <ol style="list-style-type: none"> <li>1. The boot loader may have been misconfigured.</li> <li>2. The <code>/etc/inittab</code> file is misconfigured, or Systemd configuration is incorrect or incomplete.</li> <li>3. The root filesystem is misconfigured.</li> </ol>
If the kernel loads, but <code>/etc/rc.d</code> (or <code>systemd</code> settings) causes an issue, then the <code>/etc/fstab</code> file may have an error.	In rescue mode, fix the <code>/etc/fstab</code> file.
If the kernel loads, but <code>/etc/rc.d</code> (or <code>systemd</code> settings) causes an issue, then the <code>fsck</code> utility may have failed.	In rescue mode, run the <code>fsck</code> command manually.
If the services do not start correctly, then they may not have been configured properly.	Configure the services properly.

## The OS X Boot Process

When you press the power button on a Mac, there are four main system initialization stages that happen. Each stage is composed of multiple processes. Various screens are displayed during each stage.

- Firmware initialization stage:
  - POST tests the hardware and if it passes, the hardware is initialized.
  - Booter is located and started.
  - A startup chime sounds, the power light flashes once, and all displays connected to the computer have a gray or black background.



**Note:** If FileVault has been used to enable full disk encryption, the user is prompted to enter their account name and password to unlock the startup disk.

- Booter initialization stage:

- System kernel is loaded.
- Kernel extensions (KEXTs) are loaded into main memory.
- KEXTs enable the kernel to take control of the system.
- Main display shows the Apple logo. This indicates that the `boot.efi` startup file has been located on the startup disk.
- Kernel initialization stage:
  - Loads additional drivers as needed.
  - Loads the core BSD UNIX system.
  - Main display shows a spinning wheel or a progress bar under the Apple logo while the Mac is reading files from the OS X System folder.
- System launchd initialization stage:
  - After core OS loads, system launchd starts, which is the first non-kernel process. This loads the rest of the system.
  - All displays show a white background briefly.
  - Login screen is displayed, or, if auto log in is configured, Finder is displayed.



**Note:** For a list of startup key combinations to access special features during startup, refer to <https://support.apple.com/en-gb/HT201255>.

## Other Boot Screens

If you configured the startup options to something other than the default startup routine, or if the Mac encounters a problem during boot, there are other screens you might see during boot.

Screen	Description
Question mark folder instead of Apple logo	The local or network startup disk could not be found. The disk it is looking for is specified in <b>System Preferences</b> in the <b>Startup Disk</b> pane. This might just be displayed because it is taking longer than normal to locate the startup disk. If it remains, use <b>Startup Manager</b> to start the Mac and reselect the startup disk in <b>System Preferences</b> .
Prohibitory symbol instead of Apple logo	The "Not" symbol (a circle with a slash through it) indicates that the system was unable to find a valid System Folder from which to start up. It might be because the Mac is attempting to start from the wrong OS X version or you might need to use OS X Recovery to reinstall the OS.
Lock icon	The lock icon is displayed if a firmware password has been set and you are attempting to boot the Mac from an external drive or through OS X Recovery.
Spinning globe	The spinning globe indicates that the Mac is being started from a network startup disk.
Battery icon	The battery icon is displayed when a notebook doesn't have enough power left in the battery to start up. You will need to connect the power adapter before attempting to start up again.
PIN code	The PIN lock screen is displayed if the Mac has been locked with <b>Find My Mac</b> . The user will need to enter the four or six digit PIN that was configured in order to start up.

## Windows Operating System Troubleshooting Tools

There are numerous tools and utilities available to help you troubleshoot operating system issues:

Tool	Description
WinRE	Use Windows Recovery Environment (WinRE) to troubleshoot and manage system errors that occur within the Windows operating system.
Bootrec.exe	<p>The <i>bootrec</i> tool is available within WinRE. It can be used to troubleshoot and resolve <i>master boot record (MBR)</i> issues, boot sector problems, and Boot Configuration Data (BCD) issues. Two bootrec options are commonly used to troubleshoot and fix issues:</p>
	<ul style="list-style-type: none"> <li>• The <i>fixmbr</i> option is used to fix MBR corruption issues by writing new files to the system partition.</li> <li>• The <i>fixboot</i> option is used to write a new boot sector to the system. It can be useful when you suspect that the boot sector is damaged or incompatible with the operating system.</li> </ul> <p>For more information on the bootrec tool capabilities, visit <a href="http://support.microsoft.com/kb/927392">http://support.microsoft.com/kb/927392</a>.</p>
sfc	<p><i>System File Checker (sfc)</i> is a Windows utility that scans systems for file corruptions on startup. There are several sfc commands that you can use to manage file corruptions:</p>
	<ul style="list-style-type: none"> <li>• <i>scannow</i> will scan all protected files.</li> <li>• <i>scanonce</i> scans all protected files one time.</li> <li>• <i>scanboot</i> scans all protected files every time the system boots up.</li> <li>• <i>revert</i> will revert the scan back to the default.</li> <li>• <i>purgecache</i> will purge all files in the Windows File Protection cache and scan protected files.</li> </ul> <p>For more information and full tool parameters, visit <a href="https://support.microsoft.com/en-us/kb/929833">https://support.microsoft.com/en-us/kb/929833</a>.</p>
System repair disks	<p>Windows allows for the creation of a system repair disk. This disk can be used to access system recovery options if you do not happen to have a Windows installation disk handy. To use this option, you must create the disk from the</p>
	<p><b>Backup and Restore</b> menu, and you will need to set the Basic Input/Output System (BIOS) to boot from a CD/DVD when you insert your repair disk into the drive. The System Repair Disk allows you to access:</p> <ul style="list-style-type: none"> <li>• Startup Repair</li> <li>• System Restore</li> <li>• System Image Recovery</li> <li>• Windows Memory Diagnostic</li> <li>• Command prompt</li> </ul>
Pre-installation environments	<p>Windows <i>pre-installation environments (Windows PE or WinPE)</i> are lighter versions of Windows and Server that can be installed in either 32- or 64-bit versions.</p>
	<p>Windows PE is commonly used by large manufacturing companies to load a pre-installed version of Windows to provide to end users. It can also be used for troubleshooting and file system recovery by allowing administrators to run forensic and disk imaging tools. The pre-installation environments are available for free in the Windows Automated Installation kit (WAIK).</p>

Tool	Description
Refresh	If you have attempted to resolve a Windows 8/8.1 problem and have had no success, you can refresh the system. You have three options when you select <b>Settings→Change PC Settings→Update and recovery→Recovery</b> from the Charms bar: <ul style="list-style-type: none"> <li>• <b>Refresh your PC without affecting your files.</b> Apps that came with the PC and any apps you installed using the Windows Store will be reinstalled. A list of apps installed from other sources such as downloads from the web and from DVD is created as these will need to be reinstalled. Also, if the system was upgraded from Windows 8 to 8.1, you will need to perform the upgrade again after performing the refresh. All of your data files will remain untouched.</li> <li>• <b>Remove everything and reinstall Windows.</b> This option is useful if the PC is being recycled or redeployed to another user.</li> <li>• <b>Advanced startup.</b> This option enables you to recover by starting up from a device or disk such as a USB drive or DVD. This option enables you to change the PC firmware settings, change Windows startup settings, or restore Windows from a system image.</li> </ul>
MSCONFIG	The <i>MSCONFIG</i> utility is a system configuration tool available in the <b>Tools</b> group from the <b>Help and Support Center</b> . This tool is frequently used to test various configurations for diagnostic purposes, rather than to permanently make configuration changes. Following diagnostic testing, permanent changes would typically be made with more appropriate tools, such as <b>Services</b> to change the startup settings of various system services. When troubleshooting system issues, you can use this tool to: <ul style="list-style-type: none"> <li>• Determine what files are initiated on startup.</li> <li>• Manage services that launch on startup.</li> </ul>
DEFRAG	When systems are running slow and performance is suffering, then you may want to run the DEFrag utility. This utility is used to reduce fragmentation on the hard disk by reorganizing stored data. This can affect disk performance. The tool can be launched from <b>Computer Management</b> .
REGSVR32	The <i>REGSVR32</i> utility is used to register Object Linking and Embedding (OLE) controls that are self-registerable. If you are having issues with Windows or Internet Explorer®, then you can launch this tool and unregister these controls, then re-register them. Common controls managed with this tool are Dynamic Link Library (DLL) and ActiveX files.
REGEDIT	Use the REGEDIT utility to make changes to infected or corrupted files within the Registry. Use caution when viewing or modifying these files in the Registry.
EXPAND	The EXPAND tool pulls one or more update files from a compressed product update package. If operating system files are damaged, you can pull their equivalent files from a fresh system image to replace the damaged ones.
Event Viewer	Use the Event Viewer to look at a system's event logs, which may contain specific information about system errors or significant events on the computer. This can be helpful in troubleshooting various system issues.
Safe Mode	<i>Safe Mode</i> is a Windows system startup method that loads only a minimal set of drivers and services. If a non-critical driver or service on your system is causing a severe error, you can use Safe Mode to omit all non-critical drivers and services from the boot sequence; start the system; load additional drivers, services, and applications as needed; and correct the problem.

Tool	Description
Command prompt	Command prompt can be used when troubleshooting a number of different issues. Windows provides several different command interpreters. The typical command prompt interface is the standard Windows command interpreter. To access the command prompt interface, you can either run cmd.exe or select <b>Command Prompt</b> from the <b>Accessories</b> menu.
Remote Desktop/ Remote Assistance	Remote Desktop can be used to access a user's computer to provide assistance with various types of issues. The problem with Remote Desktop for troubleshooting an end user's computer is that it must be enabled and a user must be granted privileges to log in with network access. If a user does not have a password set up to log in to his or her computer, Remote Desktop will not allow that user name to be used to log in. If no other user name exists, there is no opportunity for Remote Desktop to work.  Remote Assistance similarly requires an option to be enabled on the end user's computer, but it does not require that the connecting computer have a user name and password on the system. The end user invites the connecting user to view their screen. The end user can also grant limited control to the connecting user.

## Windows Safe Mode Options

There are a few different options to choose from when running Windows Safe Mode:

- Safe Mode: Starts the computer with a minimal set of drivers and services, including the mouse, keyboard, Video Graphics Array (VGA) display, and a hard disk. It is used when the system problem might be with the networking components.
- Safe Mode with Networking: Starts the computer with Safe Mode drivers and services, plus networking drivers and services. It is used when you need to use files on a network location to repair the system.
- Safe Mode with Command Prompt: Starts the computer with Safe Mode drivers and services, but with a command prompt interface. It is used when a system problem prevents the system from creating the Windows graphical user interface (GUI) desktop.

## BIOS/UEFI as a Troubleshooting Tool

Beyond the operating system itself, you can use a PC's BIOS or UEFI firmware interface to troubleshoot problems with the OS. Depending on the make and model of the PC and its motherboard, the firmware interface will provide you with different low-level diagnostic and resolution options. From many BIOS/UEFI utilities you can:

- Change boot order.
- Configure hardware ports.
- Configure CPU and GPU settings (voltage, clock value, etc.).
- Configure peripherals like fans and cooling systems.
- Configure memory settings.
- Configure power management settings.

Configuring these options may help reveal fundamental hardware issues that the operating system cannot detect while it's in use.

## BSOD

Blue screen of death (BSOD) errors, or system stop errors, can be a symptom of file system errors, viruses, hard disk corruption, or controller driver problems. Stop errors are rare in Windows Vista and later, but when they occur, they are normally preceded by a blue error screen containing a summary statement about the error condition and also hexadecimal memory data.



Figure 19-3: A BSOD error.

### Responding to Stop Errors

If you experience a BSOD error, you should try to capture as much information as possible from the error summary information at the top of the screen. You can sometimes use this information to diagnose the problem. You can record the error codes and then search for the meaning of the error codes either on the Internet or from Microsoft's website.

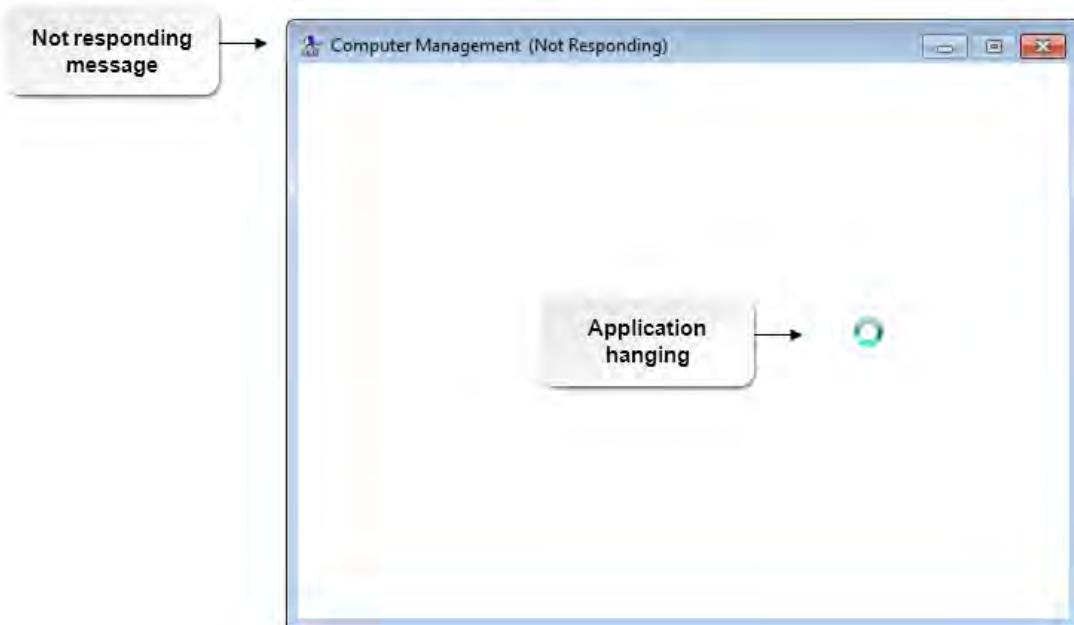
You can also configure **Startup and Recovery** settings to perform a *memory dump*, which means that the system writes the contents of memory at the time of the error to a *dump file* on the hard disk for diagnostic purposes. You would need special tools and support from Microsoft technical engineers to interpret a dump file. To configure **Startup and Recovery** settings, go to the **Advanced** page of the **System Properties** dialog box, and under **Startup And Recovery**, select **Settings**.

If you want to prevent the system from restarting automatically after the stop error, reboot and press **F8** during the boot sequence to bring up the **Windows Advanced Options** menu. Select **Disable Automatic Restart On System Failure** and allow the system to restart. Another way of preventing the system from restarting automatically is to change the settings for the computer. To do this:

1. Display the pop-up menu for **Computer**, and select **Properties**.
2. Select the **Advanced system settings**, select **Continue** if prompted by the **User Account Control**, select the **Advanced** tab, and in the **Startup and Recovery** area, select **Settings**.
3. Uncheck **Automatically restart** and select **OK**.

### System Lockup Errors

A *lockup error* is an error condition that causes the system or an application to stop responding to user input. The system display hangs or freezes in a particular state, or sometimes the contents of a window go blank. The system might return to normal after a brief delay for other processes to execute, or it might be necessary to terminate an unresponsive process. Often times a pinwheel or spinning circle is displayed, indicating that the application is locked up or hanging. Application lockup errors are more common than complete system lockups.



**Figure 19–4:** A lockup error.

## Responding to Lockup Errors

If your system or an application locks up, sometimes waiting a few minutes is sufficient for the system to recover resources and begin responding. If not, you can sometimes identify the particular offending process by running the **Task Manager**. On the **Applications** tab, look for applications with a **Not Responding** status. You can then select the **End Task** button to shut them down. On the **Processes** tab, look for processes that are monopolizing the central processing unit (CPU), and use the **End Process** button to shut them down. Sometimes it is necessary to restart the system.



**Note:** Force Quit on OS X and `kill -9` on Linux are the equivalent of **Task Manager End Task**.

Although applications might occasionally hang without indicating any serious problem, repeated system lockups or stop errors are a sign of trouble, and you should investigate them to see if there is an underlying hardware problem or if they could be caused by malicious software, such as a computer virus. In addition to hardware or malicious software, they could also be caused by unstable/incompatible drivers, applications conflicting with each other, resource allocation issues (multiple video-intensive applications trying to access the same resource), memory limitations (not enough memory or too many applications running at the same time), and so on.

## I/O Device Issues

Some of the input/output (I/O) device issues that can affect Windows operation include:

- A missing or loose mouse or keyboard connection.
- Blocked signals for wireless devices.
- A missing or incorrect driver for a specialty input or output device.
- Misconfigured monitor settings resulting in display anomalies.

## Display Configuration Issues

You can usually configure some settings for the monitor using controls on the device itself. For example, you can set the contrast and brightness, screen size, and screen rotation. If any of these are set to incorrect or extreme values, the display might not appear as desired.

You can also configure output settings from within Windows. Open the **Display Properties** dialog box from within the **Control Panel**, or by right-clicking the desktop and choosing **Display**. For example, the screen resolution might make items too small for some users to view comfortably. In this case, you can decrease the screen resolution, which will solve the problem, but a better solution is to increase the font dots per inch (DPI) setting. Also, the monitor might not display properly if advanced settings, such as the color quality or screen refresh rate, are set to a value that is not appropriate for the display device. You can reconfigure settings manually or use the Video Display Troubleshooter in the Windows **Help and Support Center** to walk through common problem scenarios.

## Application Errors

There are some common error messages that indicate problems with applications.

<b>Symptom</b>	<b>Suspected Problem</b>
Application will not install	You are trying to install an application that needs to overwrite a file that is currently in use on the computer.
Application will not start or load	The application was installed incorrectly, a version conflict between the application and other applications on the computer exists, or your computer is experiencing memory access errors.
Application not found	One or more of the application files has been deleted, moved, or become corrupt.
General Protection Fault (GPF)	An application is accessing Random Access Memory (RAM) that another application is using, or the application is attempting to access a memory address that does not exist.
Illegal operation	An application is attempting to perform an action that Windows does not permit. Windows forces the application to close.
Invalid working directory	The application cannot find the directory for storing its temporary files (typically \Temp). This can happen if you delete the folder that an application needs for storing its temporary files.
Windows Store app not working	This can occur if the app license is out of sync with the license installed on the computer. It can also occur if the app is damaged in some way, such as missing or misconfigured files.

## Boot Issues

There are several errors that can occur during the boot process or Windows startup.

<b>Issue</b>	<b>Description</b>
POST errors	If there are errors during the Power On Self-Test (POST), the system might display a numeric error message. Typically, you can press <b>F1</b> to acknowledge the error and continue booting.  For other POST errors, a series of audible beeps will tell you if a problem has been detected. The sequence of beeps is a code that indicates the type of problem.

<b>Issue</b>	<b>Description</b>
Invalid boot disk	The most common cause of this is a non-bootable disk in a drive. If your system has floppy-disk drives, or bootable CD-ROM or thumb drives, check to see if you need to remove a disk from the drive. However, there could be a hardware problem with the hard disk. Also verify that the complementary metal oxide semiconductor (CMOS) is set to boot from the hard drive. Most BIOSs allow for the configuration of four or more boot devices as first, second, third, etc. If one fails, it will automatically try the next in line. The only way this process will fail is if the boot devices are set to "None" or all the same (which many do not allow). Also, it cannot be assumed that the user will want the CMOS to be set to "boot from the hard drive," since many times there is a need to boot from CD, or even boot through the network.
Failure to boot	There might be a hardware problem with the hard disk or hard disk controller. Check hard drive and hard drive controller connections. You may also have a missing Boot.ini file. In this case, you need to use the Bootcfg.exe to rebuild the file.
Missing operating system	If you receive an error message on boot up that states the operating system is missing, then this could be a sign that the hard disk is damaged. You should try connecting the disk to another machine to see if it boots up; if not, then you will need to replace the hard drive.
Continuous reboots	If the computer continuously reboots, check to make sure that the power button is not stuck in its socket on the case. If the continuous reboots are not due to the power button being stuck, you will need to check for viruses or malware, and verify that the BIOS/UEFI settings are correct. In addition, you might try reseating components such as RAM, the CMOS battery, and removing and testing components in another system to see if any are the cause of the reboots.
Missing NTLDR	The NT loader (NTLDR) file might be missing or corrupt, in which case you might need to copy it from the Windows CD-ROM. However, the most common problem is that there is a non-bootable disk in the drive.
Missing dll message	On startup, if the device displays a "missing dll" message, then this can indicate an issue with one of the system files. A file may be disabled, damaged, or deleted completely. You should first boot to Safe Mode and run a virus scan on the computer to find any viruses that may have infected the system and remove them. The next step is to determine what files are missing. This can be a tedious task and in most cases a third party dll finder utility can be used. Once you determine the specific files needed, you can download them from the appropriate website or manufacturer and install them on the system.
System files fail to open or are missing	If NTOSKRNL.EXE is missing, you can copy it from the Windows installation CD-ROM. This error can also indicate a problem in the Advanced RISC Computing (ARC) path specifications in the Boot.ini file.
	If Bootsect.dos is missing on a dual-boot system, you will have to restore it from a backup file, as its contents are specific to a particular system.
	System files should not be deleted or become corrupt during normal system operation, so these errors are rare. They might indicate an underlying hardware problem, a disk error, or the presence of a computer virus.
Device or service fails to start	There might be a problem with a missing or corrupted device driver, or there could be hardware resource conflicts (although this is rare on a Plug and Play [PnP] system).

<b>Issue</b>	<b>Description</b>
Boots to safe mode	There may be a drive problem, if the computer continues to only boot into Safe Mode. Use the system BIOS utility to check drives and verify the boot order.
Device or program in Registry not found	A device driver or related file might be missing or damaged. You might need to reinstall the device.

## POST Beep Error Codes

POST beep codes vary from one BIOS manufacturer to another. The following table lists some typical POST beep error codes and their meanings.

<b>Beep Error Code</b>	<b>Video Output</b>	<b>Problem</b>	<b>Solution</b>
One short beep	Command prompt	None (normal startup beep)	None.
None	None	Power	Check power cords, wall voltage, PC's power supply.
None	Cursor	Power	Check the PC's power supply; check for sufficient wall voltage.
None	Command prompt	None	May be a defective speaker.
One short, one long beep	None	Display	Check for monitor power; check video cable; check display adapter.
Two short beeps	None or incorrect display (garbage)	Display	Check for monitor power; check video cable; check display adapter.
Two short beeps	None	Memory	Check to see that all RAM chips are seated firmly, swap out RAM chips to determine which is defective, and replace the defective chip.
Repeating short beeps	Probably none	Power	Check the PC's power supply; check for sufficient wall voltage.
Continuous tone	Probably none	Power	Check the PC's power supply; check for sufficient wall voltage.
One long, one short beep	Probably none	System board	Check to see that all adapters, memory, and chips are seated firmly; check for proper power connections to the system board; use diagnostics software or hardware to further troubleshoot the system board.
One long, two short beeps	Probably none	Display	Check for monitor power; check video cable; check display adapter.
One long, three short beeps	Probably none	Display	Check for monitor power; check video cable; check display adapter.
Two short beeps	Numeric error code		Varies depending upon the source of the problem as indicated by the numeric error code.

## POST Numeric Error Codes

The following table lists common POST numeric error codes and their meanings.

<b>POST Error Code</b>	<b>Problem</b>
02#	Power
01##	System board
0104	Interrupt controller
0106	System board
0151	Real-time clock or CMOS RAM
0162	CMOS checksum error
0163	Time and date (clock not updating)
164 or 0164	System memory configuration incorrect
199 or 0199	User-indicated device list incorrect
02##	Memory
201 or 0201	Memory error (may give memory address)
0202	Memory address error
03##	Keyboard
0301	Stuck key (scan code of the key may be indicated)
0302	Keyboard locked
06##	Floppy disk driver or controller
0601	Floppy disk adapter failure
0602	Disk failure
17##	Hard disk or adapter
1701	Drive not ready or fails tests
1704	Hard drive controller failure
1707	Track 0 failure
1714	Drive not ready
1730–1732	Drive adapter failure

## System Firmware Error Codes

In addition to the POST error codes, you might also see a system firmware error code. The following are examples of the error codes that you might see displayed after the POST.

- The error `Display Type Mismatch` is displayed if the video settings do not match the monitor attached to the system.
- The error `Memory Size Mismatch` is displayed if the amount of RAM detected and the amount specified in system firmware configuration do not match. This error is usually self-correcting, although you might need to reboot to fix it. Other devices such as hard drives can also generate mismatch errors. This generally happens when the physical device is different than what is specified in system firmware configuration.

## Common Operating System Symptoms

Operating systems can be difficult to troubleshoot because of their complex nature and file system. It is always helpful to first try to identify the cause of the problem, then categorize it, and finally document and take the appropriate actions.

<b>Category of Problem</b>	<b>Possible Causes and Actions to Take</b>
General issues	<p>General issue resolution includes:</p> <ul style="list-style-type: none"> <li>For boot process issues, use standard Safe Mode and boot-process troubleshooting techniques.</li> <li>Viruses can cause a variety of general system problems. Install or update the user's virus software and perform a complete virus scan to try to identify what is causing issues.</li> <li>If you suspect that the issue is stemming from a specific application, then use <b>Task Manager</b> to terminate the application and then troubleshoot its installation and configuration.</li> <li>Graphical interface fails to load. This can be an indication of a video card problem, or that a virus has infected the operating system files.</li> <li>Compatibility errors will display if an application or device software is not fully supported by the operating system.</li> <li>Files may fail to open. This can be an indication of a corrupt file or an operating system process or application that is unresponsive. Stopping the process or restarting the application or OS generally resolves the latter problem.</li> <li>Monitors in a multi-monitor setup may be misaligned or poorly oriented with respect to the OS's user interface. This can result from an obsolete or incompatible GPU, or the device's graphics drivers may need updating.</li> </ul>
Memory issues	<p>An application or service might be leaking memory, which means that it is not releasing previously allocated memory back to the system after use.</p> <ul style="list-style-type: none"> <li>Use <b>Task Manager</b> to see which applications are using memory. Have the user reboot and run for a period of time, then check again to confirm.</li> <li>Use <b>System Configuration</b> to see which applications are using memory. Have the user reboot and run for a period of time, then check again to confirm.</li> <li>Use system monitoring techniques to check the overall memory performance.</li> </ul>
Low system performance and disk issues	<p>Low disk space can slow system performance. If there is less than 500 MB of free disk space:</p> <ul style="list-style-type: none"> <li>Delete temporary Internet files in the Internet Explorer cache and other browsers.</li> <li>Empty the C:\Temp and C:\Tmp directories.</li> <li>Search for and delete .chk files.</li> <li>Run the <b>Disk Defragmenter</b>, <b>Disk Cleanup</b>, and <b>Check Disk</b> utilities.</li> <li>Reduce the size of the <b>Recycle Bin</b>.</li> <li>Reduce the amount of space allocated for virtual memory.</li> <li>Upgrade the hard disk, if possible.</li> </ul> <p>It is actually preferable to keep at least 20 percent of the hard drive available, when possible.</p>
CPU issues	<p>Use <b>Task Manager</b> to identify processes that dominate the available CPU usage. Use <b>Services</b> to disable any unnecessary processes at startup.</p>

<b>Category of Problem</b>	<b>Possible Causes and Actions to Take</b>
Kernel panic	If a user is unable to boot a system, it may be due to disk errors caused by hardware devices. When the “Kernel Panic” message is displayed, the filesystem is corrupted or inaccessible. To resolve this issue, log in to rescue mode and perform an integrity check on the filesystem.
Shutdown issues	<p>Common issues include:</p> <ul style="list-style-type: none"> <li>• Improper shutdown of system, which can lead to system file corruption and possible data loss.</li> <li>• Spontaneous shutdown or restart can indicate a hardware incompatibility issue or an incompatible application. If you receive an error code, then that may help you determine where the issue lies within the system.</li> </ul>
RAID not detected	If Redundant Array of Independent Disks (RAID) is not detected during operating system installation, then there could be an issue with an older RAID that may have been used with the system so there are residual firmware files that are blocking the new RAID from being visible to the system. You will need to verify that you have the latest firmware for the RAID being used.



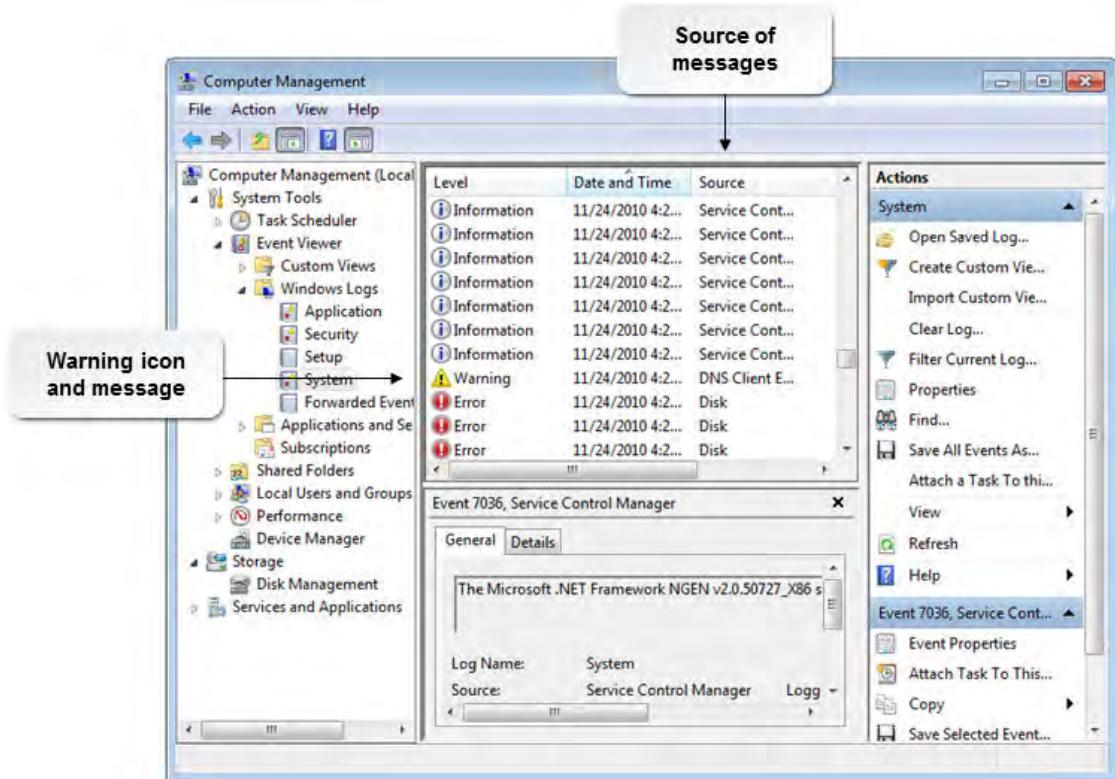
**Note:** For more troubleshooting and support information for Windows 7, visit <http://support.microsoft.com/ph/14019> and for Windows 8, visit <http://windows.microsoft.com/en-us/windows/windows-help#windows=windows-8>.



**Note:** The ultimate solution to some performance problems might be upgrading the system hardware by adding more memory or a larger hard disk. As a support technician, you might or might not be able to request this type of upgrade.

## Error and Warning Messages in Event Viewer

Warning and error messages in the system or application event logs do not necessarily indicate a major problem on your system. Many warning and error messages are usually benign and do not indicate a problem. If you review the contents of your own system's logs regularly, you will be familiar with the events logged by normal system operations and be able to distinguish these from true problem conditions that require action.



**Figure 19–5:** Error and warning messages in Event Viewer.



**Note:** Not everything reported with the level or Error is a problem. There are Errors that are normal for the system.

## The Structure of Event Log Entries

The structure of event log entries differs by operating system, but they generally share some common information, such as the type of log, the time the event occurred, the user name of who was logged on at the time of the event (or who caused the event), keywords, any identification numbers, and what category (or categories) the event belongs to.

### WER

The Windows Error Reporting (WER) node in the software environment category in **System Information** contains data about the faults generated by **Event Viewer**. When there is a severe error, Windows will also display an **Error Reporting** dialog box and generate report data. The **Error Reporting** dialog box gives you the option to send the report data to Microsoft for analysis.

## Registry Error Messages

In extremely rare cases, you may receive a stop error or another error message that reports a problem with Registry access, Registry value entries, or the Registry files. For example, a hard disk problem or power failure may have corrupted the Registry hive files. To protect the Registry, always maintain proper system backups. The best solution to a specific Registry problem is to search for the text of the specific error message at <http://support.microsoft.com> and follow the instructions in any resulting Knowledge Base article.

# ACTIVITY 19-1

## Identifying System Errors

### Scenario

Today you are working at the help desk. Below are some of the calls you received.

- 1. A user calls saying that her screen occasionally goes blue and the system shuts down. What should you advise her to do?**
  - Call the help desk the next time the shutdown is in progress.
  - Reboot manually after the automatic restart.
  - Record as much information from the top of the blue screen as she can so that you can research the particular error.
  - Run the system in Safe Mode.
  
- 2. A user reports that his Microsoft® Word window has gone blank and he cannot type text. What are possible approaches to resolving his problem?**
  - Reboot the computer.
  - Run another copy of Microsoft Word.
  - Wait a few minutes to see if the application returns to normal.
  - Use Task Manager to shut down the application if it has a status of "Not Responding."
  
- 3. A user reports that her monitor display is fuzzy and hard to look at. What is a possible cause of this problem?**
  - Display settings for the monitor are incorrectly configured.
  - The power cord is unplugged.
  - The monitor cable is not properly seated.
  - The monitor device is disabled in Windows.
  
- 4. A user reports that while she is editing a document, she receives an "invalid working directory" message from her application. What is the best diagnostic question to ask in response to this error?**
  - Did the application work yesterday?
  - Is anyone else having this problem?
  - Who installed the application?
  - Have you deleted any files or folders lately?
  
- 5. Share any experiences you have had with diagnosing and resolving system errors in your personal, school, or work life.**



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Troubleshoot PC Operating Systems.

## ACTIVITY 19-2

### Troubleshooting a Remote Computer with Remote Desktop

#### Scenario

You will be assisting a user located in another city. The technician assigned to their building is on vacation, so rather than making the user wait until the technician returns, you will attempt to assist them remotely.



**Note:** You are going to work with a partner to complete this activity. You will take turns playing the role of the helper and the user needing assistance. First, the user needing assistance will enable Remote Desktop. Then, the helper will connect to that computer using Remote Desktop Connection and the administrator user account.

1. Configure the first computer to support Remote Desktop connections.
  - a) Open the **Control Panel** and select **System and Security**.
  - b) Select the **System** link.
  - c) In the left pane, select **Remote settings**.
  - d) In the **Remote Desktop** section, select **Allow remote connections to this computer**.
  - e) Select **OK** twice and close the **System** window.
2. At the second computer, connect to the other computer using Remote Desktop Connection.
  - a) On the second computer, use search to locate and open **Remote Desktop Connection**.
  - b) In the **Computer** text box, type the name of your partner's computer.
  - c) Select **Connect**.
  - d) Log on as **Admin##** (where the ## is your partner's number) with a password of **!Pass1234** and select **Enter**.
  - e) If necessary, select **Yes** at the security prompt.
  - f) If necessary, press the arrow button.
3. From the second computer, change the desktop theme of your partner's computer, and then log off the remote session.
  - a) Display the pop-up menu for the **Desktop** and select **Personalize**.
  - b) Select a theme from the available options.
  - c) In the **Client##** bar at the top of the screen, select the **Close** button, and select **OK** to exit the Remote Desktop session.
4. Log back in to the first computer and verify the changes.
  - a) At the first computer, log back in as **Admin##**
  - b) Examine the desktop, and confirm that the theme has changed.

# TOPIC B

## Troubleshoot Mobile Device Operating Systems and Applications

You have used good troubleshooting practices to diagnose and repair PC operating system issues. The same practices can be used on mobile device operating systems and applications. In this topic, you will troubleshoot mobile device operating system and application problems.

### Common Mobile OS and Application Symptoms

Apps, operating system, and hardware are tightly integrated in mobile devices such as smartphones and tablets. You may need to troubleshoot all three components when you encounter a problem with mobile devices in order to determine which one is actually causing the issue.

#### Mobile OS Issues

The following table describes some common mobile OS issues.

<b>Symptom</b>	<b>Description</b>
Dim display	Dim display could occur when the user is trying to view the display in bright sunlight or if the display brightness has been turned down. Consider manually adjusting the screen brightness because using auto mode to adjust brightness sometimes doesn't adjust it to a level where the display content is visible. A screen protector designed for viewing the device under bright light can be applied to help make the screen more easily viewed.
Touchscreen non-responsive or inaccurate touch screen response	If the touchscreen is non-responsive, it could be that the screen protector is preventing the user's touch from registering; try removing the screen protector then cleaning the screen. If it still doesn't respond, try restarting the device, using a force quit if necessary. If the touch is registering, just not in the correct location, try recalibrating using the method in the documentation for your device.
No or intermittent network connectivity	If your cellular, Wi-Fi, or Bluetooth network is not allowing you to connect, you might be too far outside the coverage range. If you can connect, but lose the signal or have a weak signal, it is likely because you are on the edge of the coverage area. When the device is constantly attempting to reach the network, this can result in slow data speeds. Also, verify that the network type has been turned on for your device. Airplane mode turns all networks off and you would need to re-enable each separately on most devices, or disabling Airplane mode on some devices will automatically re-enable the networks that were previously turned on.
GPS malfunctioning	Your GPS may fail to lock on to a signal, or it may not update quickly enough to be useful. This may be a hardware issue, but is most likely related to the device's configurations or the apps that use GPS. You can configure some mobile devices to use both GPS satellites and nearby cell towers to help lock onto a signal. Some devices also allow you to flush your GPS cache and improve performance.

Symptom	Description
Cannot broadcast to external monitor	Display content from a smartphone, tablet, or laptop can be viewed on an external monitor or TV. You will need either an app that enables broadcasting to the external source or an HDMI cable. If the broadcast is not being received by a wireless connection, you might be too far from the source, or you might need to change settings in the app you are using. If you are using a wired connection, verify that it is within the length limits specified by the cable type.
Slow performance	<p>There are a variety of reasons your mobile device has slower performance than it did when it first came out of the box. These include:</p> <ul style="list-style-type: none"> <li>• OS updates that were installed might not be optimized for your particular device.</li> <li>• Apps running in the background. Make sure you are only running the apps you need to run.</li> <li>• Live wallpaper. Disable live wallpaper and remove unnecessary widgets.</li> <li>• Full or nearly full storage device. Clear the cache, remove unneeded data files (especially videos and photos), and uninstall unneeded apps.</li> <li>• Slow solid-state drives on Android devices. If you have an older Android device that doesn't use TRIM on solid-state drives, update to Android 4.3 or newer, or gain root access and run the LabFix app.</li> <li>• Small, slow, or full SD card. Consider moving files off the SD card, reformatting it or replacing it, then moving only the needed files back onto it.</li> </ul>
Extremely short battery life	<p>Power drain can be impacted by several factors. These include:</p> <ul style="list-style-type: none"> <li>• Using the mobile device to watch streaming video or play games. These activities use the display and the CPU which both will consume large quantities of your available power.</li> <li>• No cellular or intermittent cellular service. The device will use a lot of resources to search for a signal and try to connect to a cell tower. Switch to Airplane mode or, if a wireless network is available, to Wi-Fi, if you know you will be out of range of any cell towers.</li> <li>• Bright displays use more power than more dimly backlit displays.</li> <li>• Disable background data on services that you don't need to instantly know when new data is available. This can also help prevent data overages if you wait until you are connected to a Wi-Fi network to send or retrieve the data. Services you might want to disable background data for include email, social networking, or data backup apps.</li> <li>• Location services and geotagging, which use your GPS, will cause a power drain. Disable the location services and geotagging for some of the apps on your mobile device.</li> <li>• Disable Bluetooth, NFC, and Wi-Fi services unless you are actively using them to help prolong battery life. This has the added benefit of helping to prevent unauthorized connections over these networks to your mobile device.</li> </ul>
Frozen system	<p>For a mobile device that will not start (and you have verified that enough power is available to start the device), that repeatedly stops responding, or gets stuck (and you have verified that the updates have been applied and the issue is not caused by a particular app), you might need to perform a factory reset on the device. Refer to the device documentation for how to perform a reset on your particular device.</p>

Symptom	Description
System lockout	Entering the wrong credentials to unlock a mobile device can result in system lockout for a predetermined period of time. You can also configure mobile devices that have not been manually locked to lock after a set amount of idle time. Be more diligent about protecting the device from unauthorized physical access. Also be more diligent about remembering user names and passwords, or cleaning biometric fingerprint scanning surfaces. If your device is compromised due to login failures or the device becomes locked or wiped, you will need to do a factory reset in most cases.

## Application Issues

The following table details common app issues.

Symptom	Description
Apps not loading	The app does not seem to be present, does not seem to install, or does not function as expected. Data Call Failure (Error code 128) could be caused by your cell carrier pushing apps down to you. Updating your profile or resetting your browser to default often fixes this. Also, Google Play could give you an error "Installation Unsuccessful." This typically happens when your cache is full or your SD card has a problem. Clear the cache and/or swap out the SD card. Make sure your MDM (mobile device manager) is pushing apps as expected.
Unable to decrypt email	The email client reports that sending or receiving email failed. Try using other email clients, including a webmail browser, to access the Inbox. Make sure there is nothing wrong with the user name, password, server names, ports, or other security settings.
Overheating	When you use an app that makes intense use of resources, such as watching a video, it can cause the mobile device to become very hot. This can lead to overheating of the device, causing it to turn off without warning.
No sound from speakers	Make sure that the sound on your mobile device is not muted. Also, check within the app you are using to verify that the sounds have not been disabled within the app. Go to the Settings page for your device and test the sounds for ring tone, text messages, and so forth; if no sounds are heard, you might need to take the device in for servicing.

## Mobile OS and Application Tools

Some tools for troubleshooting mobile OSs and applications include:

- Performing a hard reset.
- Performing a soft reset.
- Performing a factory default reset.
- Closing running applications.
- Forcing applications to stop.
- Uninstalling and reinstalling applications.
- Adjusting device configuration and settings.



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on Guidelines for Troubleshooting Mobile Device OSs and Applications.

# ACTIVITY 19-3

## Troubleshooting Mobile Device OSs and Applications

### Before You Begin

This is a minds-on activity in which you will research and share the most common problems for mobile devices. Use your classroom computer browser to do the research. Be prepared to share your findings with the rest of the class. Your instructor will assign what website you will use to do your research.

### Scenario

"All of these new technologies will require whole new skill sets for my team. I need to make sure that my department is ramped up to handle what is sure to be a huge influx of calls from the users."

—Sally Waters, Help Desk Manager

The organization's mobile network has been up and running for some time now. The organization has recently implemented a BYOD policy for Android and iPhone devices. The help desk wants to be completely ready for known issues. As the technical liaison, the help desk manager has asked you to present a summary of some of the most common problems the team will encounter when supporting BYOD. You have prepared the following list of websites that have published common troubleshooting tips and tricks:

- [www.littlegreenrobot.co.uk/tips/53-common-android-problems-solved/](http://www.littlegreenrobot.co.uk/tips/53-common-android-problems-solved/)
- [www.digitaltrends.com/mobile/iphone-5-problems/](http://www.digitaltrends.com/mobile/iphone-5-problems/)
- [www.digitaltrends.com/mobile/iphone-6-problems/](http://www.digitaltrends.com/mobile/iphone-6-problems/)
- [www.dummies.com/how-to/content/common-android-problem-troubleshooting.html](http://www.dummies.com/how-to/content/common-android-problem-troubleshooting.html)
- [www.theatlanticwire.com/technology/2012/10/most-common-iphone-5-glitches-and-their-fixes/57474/](http://www.theatlanticwire.com/technology/2012/10/most-common-iphone-5-glitches-and-their-fixes/57474/)
- [www.inlovehewithandroid.com/android-problems-troubleshooting.html](http://www.inlovehewithandroid.com/android-problems-troubleshooting.html)
- [www.etradesupply.com/blog/iphone-5-issues-dont-5s/](http://www.etradesupply.com/blog/iphone-5-issues-dont-5s/)
- <http://www.etradesupply.com/blog/>
- [www.guidingtech.com/13028/solutions-android-wi-fi-problems-common/](http://www.guidingtech.com/13028/solutions-android-wi-fi-problems-common/)

- 
1. Spend 5 minutes finding an interesting mobile device problem and resolution that you would like to share with the class. Be prepared to present a summary of your findings to the group.
  2. **What interesting troubleshooting tips did you find that you would like to share with the group, and where did you find them?**
  
  3. **Having heard the various problems and their resolutions, what mobile device issues do you think you will most likely encounter in your own environments?**
-

# TOPIC C

## Troubleshoot Wired and Wireless Networks

In the previous topics, you examined troubleshooting for PC and mobile device operating systems. In most organizations, those operating systems will be running on a machine that is also running on a network to access the Internet and other important databases or servers. Just as the operating system is essential for the system to function, the network is essential for most organizations to function on a daily basis. In this topic, you will troubleshoot networks.

Every network will run into problems at some point. However, there is a lot you can do to minimize the problems you encounter. Regular, preventative maintenance will not only keep your network working at its peak, but it will also reduce the risk of network corruption. Difficulties will arise, though, and good troubleshooting skills will enable you to identify, assess, and repair any network issues quickly and efficiently.

### Common Network Issues

There are several common network issues you might be called upon to diagnose and resolve.

<b>Network Issue</b>	<b>Possible Problems and Solutions</b>
No connectivity or connection lost	No connectivity or a connection loss can be an indication that there is a physical problem with a loose cable or a defective network adapter. Check cables and connections and check for link or light emitting diode (LED) lights on the network adapter. Reseat connections, replace cables, or reinstall/replace the adapter, as necessary.  On IP networks, check for a missing or incorrect IP address. If the address is manually configured, this could be a data entry error; reconfigure the connection. If automatically configured, the Dynamic Host Configuration Protocol (DHCP) server might be unavailable or unreachable. Make sure the DHCP server is up and that the client is physically connected to the network.
Slow transfer speeds	The network might be experiencing high traffic and many collisions. Check the activity status indicator light for the collision frequency. This should be a temporary condition that will pass; if not, network engineers might need to upgrade the network bandwidth or data rate to increase throughput.
Local connectivity but no Internet connection	The default gateway address might be configured incorrectly, the gateway might be down, or there might be a problem with the Internet Service Provider (ISP). Check the default gateway address, verify that the default gateway is functioning, and contact the ISP to find out if there are any problem conditions. The proxy settings may also be incorrect. Check the proxy configuration of your network connection.
Limited connectivity	Limited connections to a resource or network location can be due to insufficient permissions or an unavailable target network resource. Check to make sure the printer or server is running and connected to the network, and check to make sure the user has appropriate permissions.
IP conflict	Connections by IP address but not by name can be an indication that the Domain Name System (DNS) configuration is incorrect or the DNS server is down. Or, the hosts file might be configured incorrectly. Check the IP configuration settings and verify that the DNS server is running. Check the hosts file to make sure it does not contain incorrect entries.

<b>Network Issue</b>	<b>Possible Problems and Solutions</b>
Intermittent connectivity	<p>Electrical noise, or <i>electrical interference</i>, is a general term for unwanted signals on the network media that can interfere with network transmissions. Interference or noise can come from natural sources, such as solar radiation or electrical storms, or from man-made sources, such as electronic interference from nearby motors or transformers. <i>Electrical noise</i> can also cause transient power problems. Some of the common sources of noise include:</p> <ul style="list-style-type: none"> <li>• Ambient noise can come from many sources, including solar disturbances that affect the earth's magnetosphere, or nearby radio broadcasting towers.</li> <li>• Nearby high-tension power lines or a building's own electrical wiring can create electrical noise.</li> <li>• Electric motors, such as those used in elevators, refrigerators, water fountains, and heating, ventilating, and air conditioning (HVAC) equipment, create noise while running, but it is worse when they start up. Motors require a huge amount of electricity to start up, causing a burst of noise. These bursts can create short temporary outages that resolve themselves when the motor reaches full speed or stops.</li> <li>• Like electric motors, electric heating elements use a lot of electricity and cause a significant amount of noise while running.</li> <li>• Fluorescent, neon, and high-intensity discharge (HID) lights produce a large amount of electrical noise, generally due to the transformers and ballasts required to make these lights work.</li> </ul>
Low RF signals	<p>If radio frequency (RF) signals are low, then it could mean that there is an issue with the access point. The access point may have failed, lost power, or been misconfigured. For example, if Media Access Control (MAC) filtering is enabled at the access point, then the PC may not be able to connect. If the issue is isolated to one PC, then it could be a configuration issue at the access point or the PC, so you will need to verify the configuration settings on both devices.</p>
APIPA/link local address issues	<p>Automatic Private IP Addressing (APIPA) is automatically enabled on Windows computers unless it has been disabled in the Registry. It is commonly used as a backup IP addressing service to DHCP, so when DHCP is unavailable, local computers can still get an IP address. The issue with this configuration is that APIPA can only connect to local computers that also have APIPA addresses assigned, so connecting to the Internet is not allowed.</p>
SSID not found	<p>If a computer's wireless interface does not detect the SSID of a wireless access point, it may be difficult or impossible to connect to that access point. This can happen if the access point has SSID broadcast turned off. If all other devices see the SSID, the connecting device's wireless adapter may be damaged, or its drivers corrupted. Also make sure that the connecting device is actually within range of the wireless signal, and that there is no electrical interference.</p>

## Windows Network Troubleshooting Utilities

Microsoft includes a variety of tools in its Windows operating systems that you can use to troubleshoot networks.

Command line utilities include:

- IPCONFIG
- PING
- NSLOOKUP
- TRACERT
- NETSTAT
- NBTSTAT
- NET
- NETDOM



**Note:** NETDOM is only available on Windows Server operating systems running Active Directory Domain Services.

Software-based utilities include:

- Network troubleshooters can be used to walk you through the resolutions to various common network problems. There are several network-related troubleshooters in the **Help and Support Center** that can help.
- *Wi-Fi locators* are utilities that can be installed on computing devices to locate wireless networks within range of the device. Most locating utilities will not only locate networks, but will monitor them for anomalies as well. They will usually display the Service Set Identifier (SSID), signal quality, MAC address, and other network identifiers.

## Linux and OS X Network Troubleshooting Utilities

The traceroute, ping, arp, and ifconfig utilities are very useful in troubleshooting issues related to remote network services.

Utility	Used To
traceroute	Track the route that data takes to get to its destination. Utilizing the Time to Live (TTL) field of the IP protocol, traceroute attempts to obtain an Internet Control Message Protocol (ICMP) <i>Time_Exceeded</i> response from each gateway encountered on the path between the sender and the final destination.  User Datagram Protocol (UDP) probe packets are sent with a short TTL. The traceroute utility then listens for an ICMP Time_Exceeded reply from a gateway. This continues until you can get an ICMP Port_Unreachable response, which means that you either got to the host or reached the default maximum number of hops (30). The address of each system that responds (each gateway you pass through) is printed to your screen; if no response is received within five seconds, an asterisk (*) is printed for that probe.
ping	Verify that a system can be reached on a network. It checks the hostname, the IP address, and whether the remote system can be reached.  ping uses the ICMP Echo_Request datagram to check connections among hosts, by sending echo packets and then listening for reply packets.
arp	Display information, such as the hardware address, the hostname, and the network interfaces, about the <i>Address Resolution Protocol (ARP)</i> cache.
ifconfig	Display the local system's network interface information, including IP address, hostname, and subnet mask. This tool also allows you to configure these parameters.

## Network Troubleshooting Tools

Network tools can be used when troubleshooting or managing network connections. Useful tools include:

- Cable tester
- Loopback plug
- Punch down tool
- Tone generator and probe
- Crimpers
- Wire strippers
- Wireless locator



Access the Checklist tile on your CHOICE Course screen for reference information and job aids on How to Troubleshoot Wired and Wireless Networks.

# ACTIVITY 19–4

## Troubleshooting Network Issues

### Scenario

You recently received a lot of trouble tickets, all of which are related to network connections. You need to check the cause of these network issues and troubleshoot them.

1. You receive a call from a client who reports that she is unable to access any websites in Internet Explorer. While talking with this user, you verify that she can ping the server's IP address on her network segment, the IP address of the default gateway, and the IP address of a computer on another network segment. You also determine that none of the other users on her network can connect to websites in Internet Explorer. What might be the problem?
  
2. One of your clients reports that he is unable to see computers when he opens the Network window. Which step should you take first?
  - Determine if any of the other users on the network are experiencing problems.
  - Ask the client to ping another computer on his network.
  - Ask the client to verify that the DHCP server is running.
  - Ask the client to run ipconfig /release and ipconfig /renew.
  
3. A user is trying to reach a website and is experiencing problems. How can you examine the path of the transmissions?
  
4. A client reports that he is unable to connect to any computers on the network or the Internet. You have him run the ipconfig command, and all his TCP/IP addressing parameters are correct. When you have him ping other computers on the network, his computer is unable to reach them. This computer is the only one that is experiencing a problem. What should you check next?
  - That the DHCP server is on and functioning properly.
  - That the default gateway is on and functioning properly.
  - That the DNS server is on and functioning properly.
  - That his computer's network cable is plugged into both the network card and the wall jack.
  
5. One of your network users is unable to connect to the SSH service, which is located on a different network. The error message indicates that the other network is unreachable. You verified that the network cable is intact and that the SSH service is up. What could be the probable cause of the error? (Select all that apply.)
  - The network service is not up.
  - The resolv.conf file does not contain entries for the name server.
  - Network parameters, such as the IP address, the subnet mask, or the default gateway, are not set correctly.
  - The firewall is disabled.

6. You verified that the network service is running and that the network parameters are properly set. However, the user is still unable to connect to the network. What will be your first step to troubleshoot the network issue?
    - Verify that the hostname is set.
    - Verify that the DNS entries are correct.
    - Verify that IP forwarding is enabled.
    - Verify that the ports of the service you are trying to access are open at the destination host.
  
  7. True or False? To set the hostname permanently, you need to modify the /etc/hostname file.
    - True
    - False
-

# TOPIC D

## Troubleshoot Common Security Issues

In the previous topics, you have examined troubleshooting for the operating systems, software, and network components of a computer system. As important as it is to maintain these more concrete components of a system, it is equally important to make sure that the computer system is secure and that all security measures are functioning properly; if problems arise with security, you must be ready to address them. In this topic, you will troubleshoot common security issues.

As with many areas of computer support, your responsibility for computer security does not end as soon as the security measures are implemented. As with printing, networking, hardware, and software, it is your responsibility to your users and clients to ensure proper security functions on an ongoing basis as well as to correct security problems that might compromise your systems or prevent users from accessing the resources that they need. The information and skills in this topic should help you troubleshoot any security issues that arise and restore your organization's security functions.

### Common PC Security Issues

Most common computer security problems stem from security that is too strict or too lenient, but there are some specific issues you should be aware of as well.

<b>Symptom</b>	<b>Description</b>
Pop-ups	<i>Pop-ups</i> are windows or frames that load and appear automatically when a user connects to a particular web page. They can sometimes contain buttons or links that include infected files.
Browser redirection	If users are complaining that browser links are taking them to an unwanted web page, then it probably means that the computer has been infected by a browser redirect virus. To remediate the issue, you need to remove the virus and verify that the browser functions properly.
Security alerts	In some cases, security alerts can be a sign that the computer has been infected with malware. Malware created today is complex and can be designed to look just like an actual security warning generated by the operating system so that you click on the rogue link and install the needed update that actually contains malware.
Internet connectivity issues	Internet connectivity issues can be a sign that a computer has been infected by malware. If a security breach has occurred, then an attacker gained access and changed IP configurations and reconfigured network interface cards (NICs) or DNS redirectors. Check any other network-connected devices for similar issues, and if none are found, then the issues are due to an infected device.
Slow performance	A system that is performing slowly may have too many applications or services installed and running simultaneously. This can make opening, using, and closing applications frustratingly slow for users. Another common culprit of slow performance is malware: infections like adware and spyware can run constantly in the background, taking up a great deal of the system's resources.
PC locks up	Slow performance can lead to a PC locking up. This can be an indication that there is a problem with the system files, malware services were installed, or too many programs have been loaded into memory. This can also be a symptom of a virus. Make sure to run antivirus software to identify and remove any infections.

Symptom	Description
Application crash	It can be difficult to diagnose the cause of application crashes, as there are many potential reasons why they happen. For example, applications may occasionally run out of memory. However, sometimes repeated crashes of multiple applications may signal a corrupt or infected system file.
Windows update failures	If Windows updates fail, it could be a sign that the state of the machine has changed. This can be due to a virus. Scan the computer for infections and remove them.
Rogue antivirus	Rogue antivirus is a very sneaky attack that can cause major damage to a system if the user carries out the actions expected by the attacker. The method involves designing a rogue antivirus application window that looks like a legitimate antivirus solution. If users follow the instructions, then they are at risk for downloading a slew of malware.
Email issues	<p>If there are noticeable changes to an email account, such as an excess amount of spam or you find that there have been emails sent from the account that the email account owner was unaware of, then the computer's security has been jeopardized.</p> <p>Email-specific issues to be aware of include:</p> <ul style="list-style-type: none"> <li>Spam is an email-based threat where the user's inbox is flooded with emails which act as vehicles that carry advertising material for products or promotions for get-rich-quick schemes and can sometimes deliver viruses or malware. Spam can harbor malicious code in addition to filling up your inbox. Spam can also be utilized within social networking sites such as Facebook and Twitter.</li> <li>Hijacked email is an account that has been accessed by an attacker and is being used by the attacker to send and receive emails. This means that an attacker can read, edit, and send emails from an account. In a corporate environment, a hijacked email account can result in unauthorized data access.</li> </ul>
Access denied	<p>Access may be denied if systems are unavailable or corrupted. The most common cause is when a user forgets a password or credentials. Have systems in place to reset passwords for users, when appropriate.</p> <p>Repeated patterns of access denial can be a sign of attempted security breaches.</p>
Malicious software	<p>Once malicious software has penetrated your system, numerous security issues can arise. The best solution to these problems is to prevent infections in the first place, but if your systems are infected, they must be isolated from the network and cleaned using various antivirus and security scanning tools.</p> <p>If your antivirus, anti-spyware, and pop-up blocker's protections are configured to be too restrictive, it is possible that users might not be able to load and run legitimate software. However, it is best to keep security tight in this area and deal with exceptions on a case-by-case basis.</p>

Symptom	Description
File system issues	<p>Changes in system files can indicate that there has been a breach in security. Common file system security symptoms include:</p> <ul style="list-style-type: none"> <li>• Renamed system files.</li> <li>• Files disappearing.</li> <li>• File permission changes.</li> </ul> <p>If permissions are set too tightly, users will not be able to access data. If they are too loose, there will be inappropriate access. Also, because permissions are cumulative, users may obtain permissions from a number of different groups of which they are members. If a user cannot access a resource, you might need to check the permissions assigned to all the relevant groups.</p>
Invalid certificate	<p>If a user's browser is displaying a warning that the website's certificate is invalid, it may be a maliciously spoofed address of a legitimate site. Most browsers will warn the user that this connection is untrusted and that they should not proceed. A user who ignores this warning may expose their computer to malware, or a malicious website might capture unencrypted credentials that they enter into a web form. A browser might also indicate that a certificate is invalid if the computer's clock is wrong, or if that particular certificate was removed from the browser's list of trusted certificates.</p>
Data access issues	<p>Data access across the network depends upon share permissions which, like file system permissions, might be set too high or too low. Also, like file system permissions, the user's effective permissions might be derived from several group memberships that you might need to examine.</p> <p>A special issue for Windows is the interaction of share and file system permissions—since both sets are evaluated for network file access, the user will have only the most restrictive of the two permission sets.</p> <p>If you have used policies to restrict accounts from accessing systems locally or across the network, make sure the policies are not so strict that legitimate users cannot gain access.</p>
Backup security	<p>Set system policies so that only legitimate users can restore data. However, if policies are too restrictive, you might not have enough users available to do backup restorations in an emergency. Verify that all legitimate backup administrators have the necessary rights. Do not forget to verify that the appropriate users have physical access to the backup storage location, especially if the backup tapes are maintained by a third party who has responsibility for controlling access.</p>

## Security Troubleshooting Tools

There are several tools available that can help you resolve common PC security issues.

Tool	Description
Anti-malware/antivirus software	This software scans a potentially infected system for malware and identifies any file signatures it recognizes as malicious. Most anti-malware solutions also provide quarantine and deletion functionality. Quarantining an infected file moves it into a protected container so that it cannot interact with the larger operating system. Deletion outright removes the malware from the system. Note that anti-malware software is vulnerable to false positives and false negatives, and even if it accurately detects malware, its removal functionality may not be thorough enough to truly purge the infection from the system.
Recovery console	An operating system's recovery console provides an interface with which you can execute a limited set of actions that may help you resolve boot issues. Common recovery options include repairing master boot records, formatting drive volumes, and repairing disk corruption.
MSCONFIG/safe boot option	MSCONFIG is a System Configuration utility that can also help you troubleshoot boot and system startup issues. The utility allows you to select and deselect certain services and device drivers you do or do not want to boot with. This can help you narrow down an issue to a particular process. Likewise, safe boot loads the operating system with only non-essential functionality, making it easier to isolate and remove a malware infection.
Refresh/restore options	Newer versions of Windows offer certain recovery scenarios that may resolve system slowness or corruption. Recovery scenarios include reinstalling the operating system but keeping all other files; rolling back to a previous build of the operating system; and full recovery from an operating system image.
Terminal	A PC's terminal or command-line interface will provide you with direct access to the operating system's available commands. This can be useful as configuration GUIs like the Control Panel don't offer access to every single diagnostic or troubleshooting command. Some of these commands, like CHKDSK, are more commonly initiated through a terminal.
System restore/snapshot	Operating systems like Windows can take a "snapshot" of your PC at a certain point in time. If you encounter a complex issue that isn't easily remedied, you can restore the previous snapshot and return your PC to its state before the issue appeared. This may be more ideal than a typical recovery operation as it affords minimal disruption to the system.
Pre-installation environments	Most operating systems offer some sort of configuration options as part of the installation process. For example, when you install Windows, you can format your computer's disk volumes without even needing an operating system. If you have installation media available, the pre-installation environment can help you ensure that a computer is completely wiped clean.
Event Viewer	The operating system's Event Viewer keeps a log of all recorded system and application events. This includes sign on attempts, shutdown signals, system crashes, device driver errors, and many more scenarios that can help you identify where problems exist.

## The Malware Removal Process

To properly remove malware from an infected computer, follow the process steps to ensure that the computer is clean.

<b>Process Step</b>	<b>Description</b>
Identify malware symptoms	Use adware and spyware detectors. If your antivirus software does not guard against adware and spyware, you can install separate tools to specifically protect against these types of threats.
Quarantine infected systems	Once an infected system is discovered, you can then quarantine it and fix it to prevent the further spread of the virus to other systems.
Disable system restore	When malware is detected, it is wise to disable system restore to prevent infected restore points in the system.
Remediate infected systems	In some cases, you may need to employ advanced scanning and removal techniques to ensure that systems are clear of infections. When viruses infect critical operating system files that are "in use" when the operating system is running, you may need to perform an alternate startup process in order to prevent the files from being locked against a clean and repair cycle. You may also need to boot into Safe Mode to clean the infected files, or it may be necessary to boot into a completely different pre-installation environment in order to clean viruses that are deep-rooted into the core operating system files. If you suspect that the boot blocks have been affected by a virus, you may need to repair infected boot blocks using the system recovery options in Windows.
Schedule scans and updates	Schedule scans and antivirus update schedules. By scheduling regular system scans and updating your antivirus software, you are taking a more proactive approach to vulnerability detection in the future. Scanning systems regularly allows you to discover potential malware threats and to develop useful removal techniques accordingly.
Enable system restore and create restore point	Once the system is clean of all malware infections, then you should enable system restore and make sure to create a fresh restore point of the clean system.
Educate end users	Provide user awareness and education, which is the best protection against malicious software or any security threat. Providing end user education will enable users to recognize and delete hoax email messages, avoid unauthorized software, and keep antivirus definitions updated.  Many types of malicious software are introduced through email attachments. Users should not save or open attachments they do not recognize, are not expecting, or are from senders they do not recognize.

## Malware Removal Best Practices

When identifying and removing malware, there are several techniques you can employ to fully protect systems attacks.

<b>Best Practice</b>	<b>Description</b>
Trusted installation sources	Always use trusted installation sources and websites. This may include various "mirror" websites that offer authorized software downloads. Even software you install deliberately can be infected with viruses. Do not install software just because a particular website or Internet page prompts you to do so.

<b>Best Practice</b>	<b>Description</b>
Email protection	Always use email attachment protection.
Research	Research malware types. In order to protect systems from infections, you must research all the possible malware types and symptoms. For example, using various virus encyclopedias, you can recognize possible malware types and develop solutions to fix them.

## Common Mobile Device Security Symptoms

Some of the security issues you might encounter are listed in the following table.

<b>Security Issue</b>	<b>Description</b>
Signal drop/weak signal	<p><i>Signal loss</i> is the weakening of a radio signal from a cell tower such that your phone cannot connect to the network. Mobile phones have a display at the top of the screen with bars that show the signal strength. This is usually shown in 5 bars. One bar means a weak signal, and 5 means an excellent one. If the signal strength drops off, you can have a dropped call.</p> <p>Mobile phone calls work by handing off the calls from one cell tower to another as someone is moving, such as in a vehicle. The problem with this is mobile phone signals are <i>line-of-sight</i>. This means if there is something like a mountain between you and the cell tower, you will have no signal.</p> <p>The radio spectrum is shared among mobile phone companies, police officers, firefighters, radio stations, and television stations. Radio and television station signals travel much further than mobile phone signals, because they operate at a lower frequency. Low-frequency signals travel as ground waves and can pass through waves and penetrate the leaves in a forest much more easily than can cellular signals that operate at a higher frequency. Since they follow the ground, they can go beyond the horizon.</p> <p>Signal strength is affected by many factors, including:</p> <ul style="list-style-type: none"> <li>• Weather.</li> <li>• Solar activity.</li> <li>• Electromagnetic interference.</li> <li>• Radio frequency (RF) interference.</li> <li>• Building materials such as concrete, steel, and thick walls.</li> </ul> <p>If you have a weak signal, there are some things you can do:</p> <ul style="list-style-type: none"> <li>• An app for Android called Antennas shows where cell towers are located. So, if you have a weak signal, you can move toward the towers.</li> <li>• You could also buy a network extender or repeater, which boosts the signal.</li> <li>• Install an external directional antenna if the phone permits it.</li> <li>• Change service providers. If Verizon has a weak signal, then switch to AT&amp;T. Each mobile phone company has their own separate towers although they usually co-locate (or share) them.</li> <li>• Use Wi-Fi to make calls. Some mobile phones let you use Unlicensed Mobile Access (UMA) to make calls, meaning you can use Wi-Fi.</li> <li>• Use Voice over IP (VoIP). If you have no signal at all and have no hope of getting one, you can make calls over the Internet using an app like Zoiper. You will likely need to pay a service provider to connect these Internet calls to mobile phones and land lines.</li> </ul>

<b>Security Issue</b>	<b>Description</b>
Power drain	A power drain is often a symptom of someone having gotten into your system and running apps. It could also be the result of a poorly coded app.
Slow data speeds	Apps that rely on fast, reliable data speeds can run into problems if users have slow data speed connections. Shopping cart apps, banking apps, and instant messaging apps all require that the data speeds are up to the task of sending and receiving the data in a timely manner. Slow data speeds can cause not only user frustration, but also allow attackers a bigger footprint in which to launch an attack.
Unintended Wi-Fi connection or Bluetooth pairing	<p>Unintended Wi-Fi or Bluetooth connections can result in data theft and eavesdropping. These should be turned off when not in use.</p> <p>Wi-Fi: There are many vulnerabilities with Wi-Fi, including:</p> <ul style="list-style-type: none"> <li>• Weak or no encryption and man-in-the-middle (MITM) attacks.</li> <li>• A mobile security blind spot, when a device is disconnected and not synced with the network.</li> <li>• Impersonation attacks over unsecured channels.</li> </ul>
	<p>Bluetooth technology connects headsets and audio headphones to mobile devices and is rarely secured. For this reason, these devices are also potentially subject to fuzzing, bluejacking, and snarfing as their communications and data can be accessed easily.</p>
Leaked personal files/data	<p>The number of stolen and lost smartphones and tablets is increasing. Lost and stolen devices can expose sensitive corporate data. <i>Data containers</i> mitigate this issue by isolating business data from personal data. Mobile data containers are software apps that are compatible with major mobile OSs.</p>
	<p>A data container creates a virtual environment when the app is launched. Using this virtual environment, the user accesses corporate emails and other corporate data. The app creates an encrypted data store, and the user is not permitted to copy data from outside the container or to move data from within the container. This keeps the business data isolated and secure.</p>
	<p><i>Content filtering</i> is a method of setting limits on user browser sessions. Content filtering can be based on location, time, and user privileges. With this option, administrators have the flexibility to whitelist and blacklist websites and applications so that employees are limited to browsing trusted websites. The software can be integrated with secure Domain Name System (DNS) services, Active Directory, and access databases so that content filtering works well. Umbrella software from OpenDNS is a good example of content filtering software.</p>
	<p>Data loss prevention (DLP) is a strategy for protecting corporate data from leakage and loss. It typically uses software to ensure the following:</p>
	<ul style="list-style-type: none"> <li>• Make sure users do not send sensitive information outside the company network.</li> </ul>
	<ul style="list-style-type: none"> <li>• Make sure that there is continuous, if not real-time, backup of data.</li> </ul>
	<ul style="list-style-type: none"> <li>• Make sure that lost or corrupt data can be easily restored.</li> </ul>
Data transmission over limit	<p>Most cellular plans included a pre-determined amount of data in the plan price. If the user exceeds this limit, they are charged for the additional data usage at a higher per megabyte rate than the plan data. If users exceed the plan data amount by large quantities on a regular basis, some carriers will suspend or terminate the accounts. Be sure to track usage to avoid exceeding data limits.</p>

<b>Security Issue</b>	<b>Description</b>
Unauthorized access	<p>Using passwords as authentication is one of the oldest basic methods for providing access to computers. While this method is basically easy to use, it provides a good way for hackers to intrude into a network. Today, password authentication systems are often augmented with high-level security measures to deny access to unauthorized users. Tokens offer a method of authentication. For enterprise networks, cryptographic keys are used in Secure Shell (SSH) protocols to authenticate users that access remote networks. In addition, message encryption and authentication can be performed. However, tokens are easy to create and can be reproduced as well.</p> <p>Biometric identifiers like fingerprint, iris, retina, and facial recognition provide a high level of authentication, but use analog systems that can create complexity for digital devices. When it comes to mobile devices, all the major platforms have fingerprint scanning as well as support for other forms of biometrics. However, there is no standard interface to collect biometric data. Moreover, false reject issues still need to be addressed.</p> <p>Apps often request access to resources on your mobile device. Be sure you understand the implications of allowing access. There are often legitimate reasons for the app to need access to the service or resource, but not always. Some of the items apps might request access to include:</p> <ul style="list-style-type: none"> <li>• root access.</li> <li>• location tracking.</li> <li>• camera activation.</li> <li>• microphone activation.</li> </ul>
High resource utilization	High resource utilization can be indications that there is a DNS attack. It can also be caused by a leaky app.

## Mobile Security Tools

The specific security tools you use to troubleshoot and resolve mobile device security issues will vary with the device and operating system. However, the following table lists the general types of tools you can use in troubleshooting mobile security problems.

<b>Tool</b>	<b>Description</b>
Antivirus/ Antimalware	Download and install antivirus, antimalware, or endpoint protection software. Keep the antivirus signatures updated, just as you would for a laptop or desktop computer. Make sure that your antivirus protects against worms, Trojans, viruses, keylogging, and other malware and malicious activity.
App scanner	An app scanner scans all of the apps on your mobile device to make sure there are no malicious apps installed. Each new app that is downloaded is checked as well to make sure it is not a malicious app.
Factory reset/Clean install	If a mobile device is being transferred from one user to another, if the device has been compromised in some way, or if performance issues are too great, the best solution is often to do a factory reset. This is akin to doing a clean install of the operating system. All apps, data, and any OS updates will be lost, so be sure to make a backup of anything that you need to keep before doing this.

<b>Tool</b>	<b>Description</b>
Uninstall/reinstall apps	Sometimes apps get out of sync with their desktop or web-based counterparts. Other times apps are damaged by a virus or other malicious attack. You might need to uninstall and then reinstall some apps in order to get them working properly again.
Wi-Fi analyzer	If users are experiencing connectivity problems or decreased bandwidth on your wireless network, use a Wi-Fi analyzer to try to locate a channel the access point can use that will be less crowded than the channel that is currently being used.
Cell tower analyzer	If users are experiencing call reception problems or data transfer issues over a cellular network, use a cell tower analyzer to identify locations where connection strength is limited.
Backup/restore	There are many cloud-based services that back up a mobile device's configurations or data. If the device is lost or its data erased locally, you can restore the data from the cloud service with minimal to no loss. Examples of backup services include iCloud, Google Sync, and OneDrive.
Force stop	If a mobile device app becomes unresponsive, you might need to force the app to close. The method used varies based on the mobile OS you are using.

## Guidelines for Troubleshooting Security Issues

Proper security management can reveal vulnerabilities within your security implementation, so hardening your security infrastructure can help prevent attacks. For a computer support technician, troubleshooting security usually means responding to user complaints that they are unable to access resources because security is too tight. As a computer support professional, you might have direct responsibility for security maintenance and troubleshooting, or you might be charged with identifying issues and escalating them to a dedicated security support team.

General guidelines to maintain and troubleshoot security include:

- Maintenance
  - Do walkarounds to check the status of physical access controls such as fences, security doors, parking lot lights, and cameras. Be sure intruders cannot easily access key equipment items such as network cables, routers, and switches.
  - Review security videos regularly.
  - Implement auditing on key systems and review the audit logs regularly. Investigate or report any unusual events.
  - Work with your security vendor to make sure all physical security devices, such as biometric controls, are properly calibrated and functional.
  - Review corporate security policies and verify that your systems are in compliance. Post the policies where users can access them. Make sure users know how to report security incidents if they do occur.
  - Hire a consulting company to perform an occasional security audit to evaluate your current security systems and make recommendations for improvements.
  - Some companies might undertake staged attacks to determine where an attacker might penetrate security holes.
- Troubleshooting
  - If a user cannot access websites, make sure the browser's security settings are not too restrictive.
  - If the user cannot access the contents of files, check the file permissions for the user and any groups the user belongs to. Also see if the file is encrypted; ask the file owner or an encryption recovery agent to open and decrypt the file.

- If the user cannot access network resources, check share permissions on folders and print permissions on printers for the user and any group the user belongs to. Check the local NT File System (NTFS) permissions for files and folders as well; when share and file system permissions combine, the most restrictive permission applies.
- If a user cannot log on using a biometric device, you might need assistance from the system vendor to resolve the problem.
- Train users to recognize possible social engineering attacks and hoaxes so that they can deflect these attacks in progress and report them for further investigation.
- If a user cannot access data outside the company, you might need to open ports on a firewall.

# ACTIVITY 19–5

## Troubleshooting Common Security Issues

### Scenario

You have been assigned to resolve several security issues raised by users.

1. John has reported that a pop-up security alert keeps coming up when he switches application windows on his laptop. What do you suspect is going on with his computer?
  
2. You have been asked to provide a list of common malware symptoms for users to be aware of in order to prevent security breaches within your organization. What common symptoms would you provide?
  
3. True or False? The safest way to deal with unsolicited email is to delete it without opening it.  
 True  
 False
  
4. Alex reports that in the midst of composing an email at work, an unfamiliar pop-up appeared on his screen, indicating that his email connection has been dropped and that he should log on again by using the pop-up screen. What do you suggest he do in this situation?

## Summary

In this lesson, you used many different troubleshooting methods to resolve common issues related to operating systems, network connectivity, and security. In your role as an A+ technician, you will be advising and supporting users in a number of areas surrounding computing devices, so using the guidelines and procedures provided in this lesson will enable you to provide the required level of support to users.

**In what system-wide area do you think you will provide the most support to users?**

**Have you ever recovered a severely compromised computer system? If so, then describe your experience.**



**Note:** Check your CHOICE Course screen for opportunities to interact with your classmates, peers, and the larger CHOICE online community about the topics covered in this course or other topics you are interested in. From the Course screen you can also access available resources for a more continuous learning experience.

# Course Follow-Up

Congratulations! You have completed the *CompTIA® A+®: A Comprehensive Approach (Exams 220-901 and 220-902)* course. You have acquired the essential skills and information you will need to install, configure, optimize, troubleshoot, repair, upgrade, and perform preventive maintenance on PCs, digital devices, and operating systems. If you are getting ready for a career as an entry-level IT professional or PC service technician, and if your job duties will include any type of PC service tasks or technical support for end users, this course has provided you with the background knowledge and skills you will require to be successful. Completing this course is also an important part of your preparation for the CompTIA A+ certification examinations (220-901 and 220-902) that you must pass in order to become a CompTIA A+ Certified Professional.

## What's Next?

If you want to learn more about networking technologies and supporting network users, you might want to attend the Logical Operations *CompTIA® Network+® (Exam N10-006)* course. If you want to learn more about security and helping users use safe computing practices, you might want to attend the Logical Operations *CompTIA® Security+® (Exam SY0-401)* course.

You are encouraged to explore PC and network support further by actively participating in any of the social media forums set up by your instructor or training administrator through the **Social Media** tile on the CHOICE Course screen.



# A Mapping Course Content to CompTIA A+ Certification Exam 220-901

Obtaining CompTIA A+ certification requires candidates to pass two examinations. This table describes where the objectives for CompTIA exam 220-901 are covered in this course.

<i>Domain and Objective</i>	<i>Covered In</i>
<b>1.0 Hardware</b>	
<b>1.1 Given a scenario, configure settings and use BIOS/UEFI tools on a PC.</b>	
• Firmware upgrades—flash BIOS	Lesson 8, Topic C
• BIOS component information <ul style="list-style-type: none"><li>• RAM</li><li>• Hard drive</li><li>• Optical drive</li><li>• CPU</li></ul>	Lesson 8, Topic C
• BIOS configurations <ul style="list-style-type: none"><li>• Boot sequence</li><li>• Enabling and disabling devices</li><li>• Date/time</li><li>• Clock speeds</li><li>• Virtualization support</li><li>• BIOS security (passwords, drive encryption: TPM, lock jack, secure boot)</li></ul>	Lesson 8, Topic D
• Built-in diagnostics	Lesson 8, Topic D

<i><b>Domain and Objective</b></i>	<i><b>Covered In</b></i>
<ul style="list-style-type: none"> <li>• Monitoring           <ul style="list-style-type: none"> <li>• Temperature monitoring</li> <li>• Fan speeds</li> <li>• Intrusion detection/notification</li> <li>• Voltage</li> <li>• Clock</li> <li>• Bus speed</li> </ul> </li> </ul>	Lesson 8, Topic D
<b>1.2 Explain the importance of motherboard components, their purpose, and properties.</b>	
<ul style="list-style-type: none"> <li>• Sizes           <ul style="list-style-type: none"> <li>• ATX</li> <li>• Micro-ATX</li> <li>• Mini-ITX</li> <li>• ITX</li> </ul> </li> </ul>	Lesson 7, Topic A
<ul style="list-style-type: none"> <li>• Expansion slots           <ul style="list-style-type: none"> <li>• PCI</li> <li>• PCI-X</li> <li>• PCIe</li> <li>• miniPCI</li> </ul> </li> </ul>	Lesson 7, Topic A
<ul style="list-style-type: none"> <li>• RAM slots</li> </ul>	Lesson 7, Topic A
<ul style="list-style-type: none"> <li>• CPU sockets</li> </ul>	Lesson 7, Topic A
<ul style="list-style-type: none"> <li>• Chipsets           <ul style="list-style-type: none"> <li>• Northbridge</li> <li>• Southbridge</li> </ul> </li> </ul>	Lesson 7, Topic A
<ul style="list-style-type: none"> <li>• CMOS battery</li> </ul>	Lesson 7, Topic A
<ul style="list-style-type: none"> <li>• Power connections and types</li> </ul>	Lesson 7, Topic A
<ul style="list-style-type: none"> <li>• Fan connectors</li> </ul>	Lesson 7, Topic A
<ul style="list-style-type: none"> <li>• Front/top panel connectors           <ul style="list-style-type: none"> <li>• USB</li> <li>• Audio</li> <li>• Power button</li> <li>• Power light</li> <li>• Drive activity lights</li> </ul> </li> </ul>	Lesson 7, Topic A
<ul style="list-style-type: none"> <li>• Reset button</li> </ul>	Lesson 7, Topic A
<ul style="list-style-type: none"> <li>• Bus speeds</li> </ul>	Lesson 7, Topic A

**1.3 Compare and contrast various RAM types and their features.**

<b>Domain and Objective</b>	<b>Covered In</b>
• Types <ul style="list-style-type: none"> <li>• DDR</li> <li>• DDR2</li> <li>• DDR3</li> </ul>	Lesson 8, Topic A
• SODIMM	Lesson 15, Topic B
• DIMM	Lesson 7, Topic A; Lesson 8, Topic A
• Parity vs. non-parity	Lesson 8, Topic A
• ECC vs. non-ECC	Lesson 8, Topic A
• RAM configurations (single channel vs. dual channel vs. triple channel)	Lesson 8, Topic A
• Single sided vs. double sided	Lesson 8, Topic A
• Buffered vs. unbuffered	Lesson 8, Topic A
• RAM compatibility	Lesson 8, Topic A

**1.4 Install and configure PC expansion cards.**

- Sound cards
- Video cards
- Network cards
- USB cards
- Firewire cards
- Thunderbolt cards
- Storage cards
- Modem cards
- Wireless/cellular cards
- TV tuner cards
- Video capture cards
- Riser cards

**1.5 Install and configure storage devices and use appropriate media.**

- Optical drives
  - CD-ROM/CD-RW
  - DVD-ROM/DVD-RW/DVD-RW DL
  - Blu-ray
  - BD-R
  - BD-RE

<b>Domain and Objective</b>	<b>Covered In</b>
<ul style="list-style-type: none"> <li>Magnetic hard disk drives           <ul style="list-style-type: none"> <li>5400 rpm</li> <li>7200 rpm</li> <li>10,000 rpm</li> </ul> </li> <li>Hot swappable drives</li> <li>Solid state/flash drives           <ul style="list-style-type: none"> <li>Compact flash</li> <li>SD</li> <li>Micro-SD</li> <li>Mini-SD</li> <li>xD</li> <li>SSD</li> <li>Hybrid</li> <li>eMMC</li> </ul> </li> <li>RAID types           <ul style="list-style-type: none"> <li>0</li> <li>1</li> <li>5</li> <li>10</li> </ul> </li> <li>Tape drive</li> <li>Media capacity           <ul style="list-style-type: none"> <li>CD</li> <li>CD-RW</li> <li>DVD-RW</li> <li>DVD</li> <li>Blu-ray</li> <li>Tape</li> <li>DVD DL</li> </ul> </li> </ul>	Lesson 1, Topic B; Lesson 8, Topic C  Lesson 1, Topic B  Lesson 1, Topic B; Lesson 8, Topic C  Lesson 8, Topic C  Lesson 1, Topic B; Lesson 8, Topic C  Lesson 1, Topic B

### **1.6 Install various types of CPUs and apply the appropriate cooling methods.**

- Socket types
  - Intel: 775, 1155, 1156, 1366, 1150, 2011
  - AMD: AM3, AM3+, FM1, FM2, FM2+
- Characteristics
  - Speeds
  - Cores
  - Cache size/type
  - Hyperthreading
  - Virtualization support
  - Architecture (32-bit vs. 64-bit)
  - Integrated GPU
  - Disable execute bit

<b>Domain and Objective</b>	<b>Covered In</b>
<ul style="list-style-type: none"> <li>• Cooling           <ul style="list-style-type: none"> <li>• Heat sink</li> <li>• Fans</li> <li>• Thermal paste</li> <li>• Liquid-based</li> <li>• Fanless/pассив</li> </ul> </li> </ul>	Lesson 7, Topic B
<b>1.7 Compare and contrast various PC connection interfaces, their characteristics and purpose.</b>	
<ul style="list-style-type: none"> <li>• Physical connections           <ul style="list-style-type: none"> <li>• USB 1.1 vs. 2.0 vs. 3.0 (connector types: A, B, mini, micro)</li> <li>• Firewire 400 vs. Firewire 800</li> <li>• SATA1 vs. SATA2 vs. SATA3, eSATA</li> <li>• VGA</li> <li>• HDMI</li> <li>• DVI</li> <li>• Audio [analog, digital (optical connector)]</li> <li>• RJ-45</li> <li>• RJ-11</li> <li>• Thunderbolt</li> </ul> </li> </ul>	Lesson 1, Topic D
<ul style="list-style-type: none"> <li>• Wireless connections           <ul style="list-style-type: none"> <li>• Bluetooth</li> <li>• RF</li> <li>• IR</li> <li>• NFC</li> </ul> </li> </ul>	Lesson 1, Topic D
<ul style="list-style-type: none"> <li>• Characteristics           <ul style="list-style-type: none"> <li>• Analog</li> <li>• Digital</li> <li>• Distance limitations</li> <li>• Data transfer speeds</li> <li>• Quality</li> <li>• Frequencies</li> </ul> </li> </ul>	Lesson 1, Topic D

#### 1.8 Install a power supply based on given specifications.

- Connector types and their voltages
  - SATA
  - Molex
  - 4/8-pin 12v
  - PCIe 6/8-pin
  - 20-pin
  - 24-pin

<b>Domain and Objective</b>	<b>Covered In</b>
<ul style="list-style-type: none"> <li>• Specifications <ul style="list-style-type: none"> <li>• Wattage</li> <li>• Dual rail</li> <li>• Size</li> <li>• Number of connectors</li> <li>• ATX</li> <li>• Micro-ATX</li> <li>• Dual voltage options</li> </ul> </li> </ul>	Lesson 7, Topic C
<b>1.9 Given a scenario, select the appropriate components for a custom PC configuration, to meet customer specifications or needs.</b>	
<ul style="list-style-type: none"> <li>• Graphic/CAD/CAM design workstation <ul style="list-style-type: none"> <li>• Multicore processor</li> <li>• High-end video</li> <li>• Maximum RAM</li> </ul> </li> </ul>	Lesson 12, Topic B
<ul style="list-style-type: none"> <li>• Audio/video editing workstation <ul style="list-style-type: none"> <li>• Specialized audio and video card</li> <li>• Large fast hard drive</li> <li>• Dual monitors</li> </ul> </li> </ul>	Lesson 12, Topic B
<ul style="list-style-type: none"> <li>• Virtualization workstation <ul style="list-style-type: none"> <li>• Maximum RAM and CPU cores</li> </ul> </li> </ul>	Lesson 12, Topic A
<ul style="list-style-type: none"> <li>• Gaming PC <ul style="list-style-type: none"> <li>• Multicore processor</li> <li>• High-end video/specialized GPU</li> <li>• High definition sound card</li> <li>• High-end cooling</li> </ul> </li> </ul>	Lesson 12, Topic B
<ul style="list-style-type: none"> <li>• Home theater PC <ul style="list-style-type: none"> <li>• Surround sound audio</li> <li>• HDMI output</li> <li>• HTPC compact form factor</li> <li>• TV tuner</li> </ul> </li> </ul>	Lesson 12, Topic B
<ul style="list-style-type: none"> <li>• Standard thick client <ul style="list-style-type: none"> <li>• Desktop applications</li> <li>• Meets recommended requirements for selected OS</li> </ul> </li> </ul>	Lesson 12, Topic A
<ul style="list-style-type: none"> <li>• Thin client <ul style="list-style-type: none"> <li>• Basic applications</li> <li>• Meets minimum requirements for selected OS</li> <li>• Network connectivity</li> </ul> </li> </ul>	Lesson 12, Topic A

<b>Domain and Objective</b>	<b>Covered In</b>
<ul style="list-style-type: none"> <li>• Home server PC           <ul style="list-style-type: none"> <li>• Media streaming</li> <li>• File sharing</li> <li>• Print sharing</li> <li>• Gigabit NIC</li> <li>• RAID array</li> </ul> </li> </ul>	Lesson 12, Topic B
<b>1.10 Compare and contrast types of display devices and their features.</b>	
<ul style="list-style-type: none"> <li>• Types</li> <li>• LCD (TN vs. IPS, fluorescent vs. LED backlighting)</li> <li>• Plasma</li> <li>• Projector</li> <li>• OLED</li> </ul>	Lesson 5, Topic A
<ul style="list-style-type: none"> <li>• Refresh/frame rates</li> <li>• Resolution</li> <li>• Native resolution</li> <li>• Brightness/lumens</li> <li>• Analog vs. digital</li> <li>• Privacy/antiglare filters</li> <li>• Multiple displays</li> <li>• Aspect ratios           <ul style="list-style-type: none"> <li>• 16:9</li> <li>• 16:10</li> <li>• 4:3</li> </ul> </li> </ul>	Lesson 5, Topic B
<b>1.11 Identify common PC connector types and associated cables.</b>	
<ul style="list-style-type: none"> <li>• Display connector types           <ul style="list-style-type: none"> <li>• DVI-D</li> <li>• DVI-I</li> <li>• DVI-A</li> <li>• DisplayPort</li> <li>• RCA</li> <li>• HD15 (i.e. DE15 or DB15)</li> <li>• BNC</li> <li>• miniHDMI</li> <li>• miniDin-6</li> </ul> </li> </ul>	Lesson 1, Topic D; Lesson 5, Topic A

<b>Domain and Objective</b>	<b>Covered In</b>
<ul style="list-style-type: none"> <li>• Display cable types           <ul style="list-style-type: none"> <li>• HDMI</li> <li>• DVI</li> <li>• VGA</li> <li>• Component</li> <li>• Composite</li> <li>• Coaxial</li> </ul> </li> <li>• Device cables and connectors           <ul style="list-style-type: none"> <li>• SATA</li> <li>• eSATA</li> <li>• USB</li> <li>• Firewire (IEEE1394)</li> <li>• PS/2</li> <li>• Audio</li> </ul> </li> <li>• Adapters and convertors           <ul style="list-style-type: none"> <li>• DVI to HDMI</li> <li>• USB A to USB B</li> <li>• USB to Ethernet</li> <li>• DVI to VGA</li> <li>• Thunderbolt to DVI</li> <li>• PS/2 to USB</li> <li>• HDMI to VGA</li> </ul> </li> </ul>	Lesson 5, Topic A  Lesson 1, Topic D; Lesson 7, Topic C; Lesson 8, Topic C  Lesson 1, Topic D
<b>1.12 Install and configure common peripheral devices.</b>	
<ul style="list-style-type: none"> <li>• Input devices           <ul style="list-style-type: none"> <li>• Mouse</li> <li>• Keyboard</li> <li>• Scanner</li> <li>• Barcode reader</li> <li>• Biometric devices</li> <li>• Game pads</li> <li>• Joysticks</li> <li>• Digitizer</li> <li>• Motion sensor</li> <li>• Touch pads</li> <li>• Smart card readers</li> <li>• Digital cameras</li> <li>• Microphone</li> <li>• Webcam</li> <li>• Camcorder</li> </ul> </li> <li>• Output devices           <ul style="list-style-type: none"> <li>• Printers</li> <li>• Speakers</li> <li>• Display devices</li> </ul> </li> </ul>	Lesson 6, Topic A  Lesson 5, Topic A; Lesson 5, Topic B; Lesson 6, Topic B; Lesson 16, Topic B

<b>Domain and Objective</b>	<b>Covered In</b>
<ul style="list-style-type: none"> <li>• Input &amp; output devices           <ul style="list-style-type: none"> <li>• Touch screen</li> <li>• KVM</li> <li>• Smart TV</li> <li>• Set-top box</li> <li>• MIDI enabled devices</li> </ul> </li> </ul>	Lesson 6, Topic C
<p><b>1.13 Install SOHO multifunction device / printers and configure appropriate settings.</b></p>	
<ul style="list-style-type: none"> <li>• Use appropriate drivers for a given operating system           <ul style="list-style-type: none"> <li>• Configuration settings (duplex, collate, orientation, quality)</li> </ul> </li> <li>• Device sharing           <ul style="list-style-type: none"> <li>• Wired (USB, serial, Ethernet)</li> <li>• Wireless [Bluetooth, 802.11(a,b,g,n,ac), infrastructure vs. ad hoc]</li> <li>• Integrated print server (hardware)</li> <li>• Cloud printing/remote printing</li> </ul> </li> <li>• Public/shared devices           <ul style="list-style-type: none"> <li>• Sharing local/networked device via operating system settings (TCP/Bonjour/AirPrint)</li> <li>• Data privacy (user authentication on the device, hard drive caching)</li> </ul> </li> </ul>	Lesson 16, Topic B
<p><b>1.14 Compare and contrast differences between the various print technologies and the associated imaging process.</b></p>	
<ul style="list-style-type: none"> <li>• Laser           <ul style="list-style-type: none"> <li>• Imaging drum, fuser assembly, transfer belt, transfer roller, pickup rollers, separate pads, duplexing assembly</li> <li>• Imaging process: processing, charging, exposing, developing, transferring, fusing and cleaning</li> </ul> </li> </ul>	Lesson 16, Topic A
<ul style="list-style-type: none"> <li>• Inkjet           <ul style="list-style-type: none"> <li>• Ink cartridge, print head, roller, feeder, duplexing assembly, carriage and belt</li> <li>• Calibration</li> </ul> </li> </ul>	Lesson 16, Topic A
<ul style="list-style-type: none"> <li>• Thermal           <ul style="list-style-type: none"> <li>• Feed assembly, heating element</li> <li>• Special thermal paper</li> </ul> </li> </ul>	Lesson 16, Topic A
<ul style="list-style-type: none"> <li>• Impact           <ul style="list-style-type: none"> <li>• Print head, ribbon, tractor feed</li> <li>• Impact paper</li> </ul> </li> </ul>	Lesson 16, Topic A

<b>Domain and Objective</b>	<b>Covered In</b>
<ul style="list-style-type: none"> <li>Virtual           <ul style="list-style-type: none"> <li>Print to file</li> <li>Print to PDF</li> <li>Print to XPS</li> <li>Print to image</li> </ul> </li> </ul>	Lesson 16, Topic A
<b>1.15 Given a scenario, perform appropriate printer maintenance.</b>	
<ul style="list-style-type: none"> <li>Laser           <ul style="list-style-type: none"> <li>Replacing toner, applying maintenance kit, calibration, cleaning</li> </ul> </li> </ul>	Lesson 16, Topic C
<ul style="list-style-type: none"> <li>Thermal           <ul style="list-style-type: none"> <li>Replace paper, clean heating element, remove debris</li> </ul> </li> </ul>	Lesson 16, Topic C
<ul style="list-style-type: none"> <li>Impact           <ul style="list-style-type: none"> <li>Replace ribbon, replace print head, replace paper</li> </ul> </li> </ul>	Lesson 16, Topic C
<ul style="list-style-type: none"> <li>Inkjet           <ul style="list-style-type: none"> <li>Clean heads, replace cartridges, calibration, clear jams</li> </ul> </li> </ul>	Lesson 16, Topic C

<b>Domain and Objective</b>	<b>Covered In</b>
<b>2.0 Networking</b>	
<b>2.1 Identify the various types of network cables and connectors.</b>	
<ul style="list-style-type: none"> <li>Fiber           <ul style="list-style-type: none"> <li>Connectors: SC, ST and LC</li> </ul> </li> </ul>	Lesson 13, Topic A
<ul style="list-style-type: none"> <li>Twisted pair           <ul style="list-style-type: none"> <li>Connectors: RJ-11, RJ-45</li> <li>Wiring standards: T568A, T568B</li> </ul> </li> </ul>	Lesson 1, Topic A; Lesson 13, Topic A
<ul style="list-style-type: none"> <li>Coaxial           <ul style="list-style-type: none"> <li>Connectors: BNC, F-connector</li> </ul> </li> </ul>	Lesson 13, Topic A
<b>2.2 Compare and contrast the characteristics of connectors and cabling.</b>	
<ul style="list-style-type: none"> <li>Fiber           <ul style="list-style-type: none"> <li>Types (single-mode vs. multi-mode)</li> <li>Speed and transmission limitations</li> </ul> </li> </ul>	Lesson 13, Topic A
<ul style="list-style-type: none"> <li>Twisted pair           <ul style="list-style-type: none"> <li>Types: STP, UTP, CAT3, CAT5, CAT5e, CAT6, CAT6e, CAT7, plenum, PVC</li> <li>Speed and transmission limitations</li> <li>Splitters and effects on signal quality</li> </ul> </li> </ul>	Lesson 13, Topic A

<b>Domain and Objective</b>	<b>Covered In</b>
<ul style="list-style-type: none"> <li>• Coaxial</li> <li>• Types: RG-6, RG-59</li> <li>• Speed and transmission limitations</li> <li>• Splitters and effects on signal quality</li> </ul>	Lesson 13, Topic A
<b>2.3 Explain the properties and characteristics of TCP/IP.</b>	
<ul style="list-style-type: none"> <li>• IPv4 vs. IPv6</li> <li>• Public vs. private vs. APIPA/link local</li> <li>• Static vs. dynamic</li> <li>• Client-side DNS settings</li> <li>• Client-side DHCP</li> <li>• Subnet mask vs. CIDR</li> <li>• Gateway</li> </ul>	Lesson 13, Topic B Lesson 13, Topic B
<b>2.4 Explain common TCP and UDP ports, protocols, and their purpose.</b>	
<ul style="list-style-type: none"> <li>• Ports <ul style="list-style-type: none"> <li>• 21 – FTP</li> <li>• 22 – SSH</li> <li>• 23 – TELNET</li> <li>• 25 – SMTP</li> <li>• 53 – DNS</li> <li>• 80 – HTTP</li> <li>• 110 – POP3</li> <li>• 143 – IMAP</li> <li>• 443 – HTTPS</li> <li>• 3389 – RDP</li> <li>• 137-139 - NetBIOS/NetBT</li> <li>• 445 - SMB/CIFS</li> <li>• 427 - SLP</li> <li>• 548 - AFP</li> </ul> </li> <li>• Protocols <ul style="list-style-type: none"> <li>• DHCP</li> <li>• DNS</li> <li>• LDAP</li> <li>• SNMP</li> <li>• SMB</li> <li>• CIFS</li> <li>• SSH</li> <li>• AFP</li> </ul> </li> <li>• TCP vs. UDP</li> </ul>	Lesson 13, Topic D Lesson 13, Topic D; Lesson 13, Topic D Lesson 13, Topic D

**2.5 Compare and contrast various Wi-Fi networking standards and encryption types.**

<b>Domain and Objective</b>	<b>Covered In</b>
<ul style="list-style-type: none"> <li>Standards <ul style="list-style-type: none"> <li>802.11 a/b/g/n/ac</li> <li>Speeds, distances and frequencies</li> </ul> </li> <li>Encryption types <ul style="list-style-type: none"> <li>WEP, WPA, WPA2, TKIP, AES</li> </ul> </li> </ul>	Lesson 14, Topic D
<b>2.6 Given a scenario, install and configure SOHO wireless/wired router and apply appropriate settings.</b>	Lesson 14, Topic D
<ul style="list-style-type: none"> <li>Channels</li> <li>Port forwarding, port triggering</li> <li>DHCP (on/off)</li> <li>DMZ</li> <li>NAT/DNAT</li> <li>Basic QoS</li> <li>Firmware</li> <li>UPnP</li> </ul>	Lesson 14, Topic D Lesson 14, Topic D Lesson 14, Topic D Lesson 14, Topic B Lesson 14, Topic B Lesson 14, Topic D Lesson 14, Topic D Lesson 14, Topic D
<b>2.7 Compare and contrast Internet connection types, network types, and their features.</b>	Lesson 13, Topic C
<ul style="list-style-type: none"> <li>Internet connection types <ul style="list-style-type: none"> <li>Cable</li> <li>DSL</li> <li>Dial-up</li> <li>Fiber</li> <li>Satellite</li> <li>ISDN</li> <li>Cellular (tethering, mobile hotspot)</li> <li>Line of sight wireless Internet service</li> </ul> </li> <li>Network types <ul style="list-style-type: none"> <li>LAN</li> <li>WAN</li> <li>PAN</li> <li>MAN</li> </ul> </li> </ul>	Lesson 3, Topic A Lesson 3, Topic A
<b>2.8 Compare and contrast network architecture devices, their functions, and features.</b>	Lesson 3, Topic B
<ul style="list-style-type: none"> <li>Hub</li> <li>Switch</li> <li>Router</li> <li>Access point</li> <li>Bridge</li> </ul>	Lesson 3, Topic B Lesson 3, Topic B Lesson 3, Topic B Lesson 3, Topic B Lesson 3, Topic B

<b>Domain and Objective</b>	<b>Covered In</b>
• Modem	Lesson 3, Topic B
• Firewall	Lesson 3, Topic B
• Patch panel	Lesson 3, Topic B
• Repeaters/extenders	Lesson 3, Topic B
• Ethernet over Power	Lesson 13, Topic A
• Power over Ethernet injector	Lesson 3, Topic B

**2.9 Given a scenario, use appropriate networking tools.**

• Crimper	Lesson 13, Topic E
• Cable stripper	Lesson 13, Topic E
• Multimeter	Lesson 13, Topic E
• Tone generator & probe	Lesson 13, Topic E
• Cable tester	Lesson 13, Topic E
• Loopback plug	Lesson 13, Topic E
• Punchdown tool	Lesson 13, Topic E
• Wi-Fi analyzer	Lesson 13, Topic E

<b>Domain and Objective</b>	<b>Covered In</b>
<b>3.0 Mobile Devices</b>	
<b>3.1 Install and configure laptop hardware and components.</b>	

• Expansion options

- Express card /34
- Express card /54
- SODIMM
- Flash
- Ports/adapters (Thunderbolt, DisplayPort, USB to RJ-45 dongle, USB to Wi-Fi dongle, USB to Bluetooth, USB optical drive)

Lesson 1, Topic D; Lesson 15, Topic A; Lesson 15, Topic B

<b>Domain and Objective</b>	<b>Covered In</b>
<ul style="list-style-type: none"> <li>• Hardware/device replacement           <ul style="list-style-type: none"> <li>• Keyboard</li> <li>• Hard drive ( SSD vs. hybrid vs. magnetic disk, 1.8in vs. 2.5in)</li> <li>• Memory</li> <li>• Smart card reader</li> <li>• Optical drive</li> <li>• Wireless card</li> <li>• Mini-PCIe</li> <li>• Screen</li> <li>• DC jack</li> <li>• Battery</li> <li>• Touchpad</li> <li>• Plastics/frames</li> <li>• Speaker</li> <li>• System board</li> <li>• CPU</li> </ul> </li> </ul>	Lesson 6, Topic A; Lesson 15, Topic A; Lesson 15, Topic B
<p><b>3.2 Explain the function of components within the display of a laptop.</b></p>	
<ul style="list-style-type: none"> <li>• Types           <ul style="list-style-type: none"> <li>• LCD (TTL vs. IPS, fluorescent vs. LED backlighting)</li> <li>• OLED</li> </ul> </li> <li>• Wi-Fi antenna connector/placement</li> <li>• Webcam</li> <li>• Microphone</li> <li>• Inverter</li> <li>• Digitizer</li> </ul>	Lesson 5, Topic A; Lesson 15, Topic B Lesson 15, Topic B
<p><b>3.3 Given a scenario, use appropriate laptop features.</b></p>	
<ul style="list-style-type: none"> <li>• Special function keys           <ul style="list-style-type: none"> <li>• Dual displays</li> <li>• Wireless (on/off)</li> <li>• Cellular (on/off)</li> <li>• Volume settings</li> <li>• Screen brightness</li> <li>• Bluetooth (on/off)</li> <li>• Keyboard backlight</li> <li>• Touch pad (on/off)</li> <li>• Screen orientation</li> <li>• Media options (fast forward/rewind)</li> <li>• GPS (on/off)</li> <li>• Airplane mode</li> </ul> </li> <li>• Docking station</li> <li>• Physical laptop lock and cable lock</li> </ul>	Lesson 15, Topic A Lesson 15, Topic A Lesson 15, Topic A

<b>Domain and Objective</b>	<b>Covered In</b>
• Rotating/removable screens	Lesson 15, Topic B
<b>3.4 Explain the characteristics of various types of other mobile devices.</b>	
• Tablets	Lesson 15, Topic C
• Smartphones	Lesson 15, Topic C
• Wearable technology devices (smart watches, fitness monitors, glasses and headsets)	Lesson 15, Topic C
• Phablets	Lesson 15, Topic C
• e-Readers	Lesson 15, Topic C
• Smart camera	Lesson 15, Topic C
• GPS	Lesson 15, Topic C
<b>3.5 Compare and contrast accessories &amp; ports of other mobile devices.</b>	
• Connection types	Lesson 15, Topic C
• NFC	
• Proprietary vendor specific ports (communication/power)	
• microUSB/miniUSB	
• Lightning	
• Bluetooth	
• IR	
• Hotspot/tethering	
• Accessories	Lesson 1, Topic B; Lesson 15, Topic D
• Headsets	
• Speakers	
• Game pads	
• Docking stations	
• Extra battery packs/battery chargers	
• Protective covers/water proofing	
• Credit card readers	
• Memory/MicroSD	

<b>Domain and Objective</b>	<b>Covered In</b>
<b>4.0 Hardware and Network Troubleshooting</b>	
<b>4.1 Given a scenario, troubleshoot common problems related to motherboards, RAM, CPU and power with appropriate tools.</b>	

<b>Domain and Objective</b>	<b>Covered In</b>
<ul style="list-style-type: none"> <li>• Common symptoms           <ul style="list-style-type: none"> <li>• Unexpected shutdowns</li> <li>• System lockups</li> <li>• POST code beeps</li> <li>• Blank screen on bootup</li> <li>• BIOS time and settings resets</li> <li>• Attempts to boot to incorrect device</li> <li>• Continuous reboots</li> <li>• No power</li> <li>• Overheating</li> <li>• Loud noise</li> <li>• Intermittent device failure</li> <li>• Fans spin—no power to other devices</li> <li>• Indicator lights</li> <li>• Smoke</li> <li>• Burning smell</li> <li>• Proprietary crash screens (BSOD/pin wheel)</li> <li>• Distended capacitors</li> </ul> </li>   <li>• Tools           <ul style="list-style-type: none"> <li>• Multimeter</li> <li>• Power supply tester</li> <li>• Loopback plugs</li> <li>• POST card/USB</li> </ul> </li> </ul>	Lesson 7, Topic D; Lesson 8, Topic B; Lesson 19, Topic A
<p><b>4.2 Given a scenario, troubleshoot hard drives and RAID arrays with appropriate tools.</b></p>	Lesson 7, Topic D
<ul style="list-style-type: none"> <li>• Common symptoms           <ul style="list-style-type: none"> <li>• Read/write failure</li> <li>• Slow performance</li> <li>• Loud clicking noise</li> <li>• Failure to boot</li> <li>• Drive not recognized</li> <li>• OS not found</li> <li>• RAID not found</li> <li>• RAID stops working</li> <li>• Proprietary crash screens (BSOD/pin wheel)</li> <li>• S.M.A.R.T. errors</li> </ul> </li>   <li>• Tools           <ul style="list-style-type: none"> <li>• Screwdriver</li> <li>• External enclosures</li> <li>• CHKDSK</li> <li>• FORMAT</li> <li>• File recovery software</li> <li>• Bootrec</li> <li>• Diskpart</li> <li>• Defragmentation tool</li> </ul> </li> </ul>	Lesson 8, Topic E
	Lesson 8, Topic E; Lesson 9, Topic D; Lesson 10, Topic C; Lesson 19, Topic A

<b>Domain and Objective</b>	<b>Covered In</b>
4.3 Given a scenario, troubleshoot common video, projector and display issues.	
<ul style="list-style-type: none"> <li>• Common symptoms           <ul style="list-style-type: none"> <li>• VGA mode</li> <li>• No image on screen</li> <li>• Overheat shutdown</li> <li>• Dead pixels</li> <li>• Artifacts</li> <li>• Color patterns incorrect</li> <li>• Dim image</li> <li>• Flickering image</li> <li>• Distorted image</li> <li>• Distorted geometry</li> <li>• Burn-in</li> <li>• Oversized images and icons</li> </ul> </li> </ul>	Lesson 5, Topic C
4.4 Given a scenario, troubleshoot wired and wireless networks with appropriate tools.	
<ul style="list-style-type: none"> <li>• Common symptoms           <ul style="list-style-type: none"> <li>• No connectivity</li> <li>• APIPA/link local address</li> <li>• Limited connectivity</li> <li>• Local connectivity</li> <li>• Intermittent connectivity</li> <li>• IP conflict</li> <li>• Slow transfer speeds</li> <li>• Low RF signal</li> <li>• SSID not found</li> </ul> </li> </ul>	Lesson 19, Topic C
<ul style="list-style-type: none"> <li>• Hardware tools           <ul style="list-style-type: none"> <li>• Cable tester</li> <li>• Loopback plug</li> <li>• Punch down tools</li> <li>• Tone generator and probe</li> <li>• Wire strippers</li> <li>• Crimper</li> <li>• Wireless locator</li> </ul> </li> </ul>	Lesson 19, Topic C
<ul style="list-style-type: none"> <li>• Command line tools           <ul style="list-style-type: none"> <li>• PING</li> <li>• IPCONFIG/IFCONFIG</li> <li>• TRACERT</li> <li>• NETSTAT</li> <li>• NBTSTAT</li> <li>• NET</li> <li>• NETDOM</li> <li>• NSLOOKUP</li> </ul> </li> </ul>	Lesson 13, Topic E; Lesson 19, Topic C

<b>Domain and Objective</b>	<b>Covered In</b>
<p><b>4.5 Given a scenario, troubleshoot and repair common mobile device issues while adhering to the appropriate procedures.</b></p> <ul style="list-style-type: none"> <li>• Common symptoms           <ul style="list-style-type: none"> <li>• No display</li> <li>• Dim display</li> <li>• Flickering display</li> <li>• Sticking keys</li> <li>• Intermittent wireless</li> <li>• Battery not charging</li> <li>• Ghost cursor/pointer drift</li> <li>• No power</li> <li>• Num lock indicator lights</li> <li>• No wireless connectivity</li> <li>• No Bluetooth connectivity</li> <li>• Cannot display to external monitor</li> <li>• Touchscreen non-responsive</li> <li>• Apps not loading</li> <li>• Slow performance</li> <li>• Unable to decrypt email</li> <li>• Extremely short battery life</li> <li>• Overheating</li> <li>• Frozen system</li> <li>• No sound from speakers</li> <li>• GPS not functioning</li> <li>• Swollen battery</li> </ul> </li> <li>• Disassembling processes for proper re-assembly           <ul style="list-style-type: none"> <li>• Document and label cable and screw locations</li> <li>• Organize parts</li> <li>• Refer to manufacturer resources</li> <li>• Use appropriate hand tools</li> </ul> </li> </ul>	Lesson 15, Topic G; Lesson 19, Topic B
<p><b>4.6 Given a scenario, troubleshoot printers with appropriate tools.</b></p>	Lesson 15, Topic G

<b>Domain and Objective</b>	<b>Covered In</b>
<ul style="list-style-type: none"> <li>• Common symptoms           <ul style="list-style-type: none"> <li>• Streaks</li> <li>• Faded prints</li> <li>• Ghost images</li> <li>• Toner not fused to the paper</li> <li>• Creased paper</li> <li>• Paper not feeding</li> <li>• Paper jam</li> <li>• No connectivity</li> <li>• Garbled characters on paper</li> <li>• Vertical lines on page</li> <li>• Backed up print queue</li> <li>• Low memory errors</li> <li>• Access denied</li> <li>• Printer will not print</li> <li>• Color prints in wrong print color</li> <li>• Unable to install printer</li> <li>• Error codes</li> <li>• Printing blank pages</li> <li>• No image on printer display</li> </ul> </li>   <li>• Tools           <ul style="list-style-type: none"> <li>• Maintenance kit</li> <li>• Toner vacuum</li> <li>• Compressed air</li> <li>• Printer spooler</li> </ul> </li> </ul>	Lesson 16, Topic D



# B

# Mapping Course Content to CompTIA A+ Certification Exam 220-902

Obtaining CompTIA A+ certification requires candidates to pass two examinations. This table describes where the objectives for CompTIA exam 220-902 are covered in this course.

<i>Domain and Objective</i>	<i>Covered In</i>
<b>1.0 Windows Operating Systems</b>	
<b>1.1 Compare and contrast various features and requirements of Microsoft Operating Systems (Windows Vista, Windows 7, Windows 8, Windows 8.1).</b>	
<ul style="list-style-type: none"><li>• Features:<ul style="list-style-type: none"><li>• 32-bit vs. 64-bit</li><li>• Aero, gadgets, user account control, bit-locker, shadow copy, system restore, ready boost, sidebar, compatibility mode, virtual XP mode, easy transfer, administrative tools, defender, Windows firewall, security center, event viewer, file structure and paths, category view vs. classic view</li><li>• Side by side apps, Metro UI, Pinning, One Drive, Windows store, Multimonitor task bars, Charms, Start Screen, Power Shell, Live sign in, Action Center.</li><li>• Upgrade paths—differences between in place upgrades, compatibility tools, Windows upgrade OS advisor</li></ul></li></ul>	<p>Lesson 2, Topic A; Lesson 2, Topic B; Lesson 7, Topic B; Lesson 9, Topic C; Lesson 9, Topic E</p> <p>Lesson 9, Topic E</p>
<b>1.2 Given a scenario, install Windows PC operating systems using appropriate methods.</b>	

<b>Domain and Objective</b>	<b>Covered In</b>
<ul style="list-style-type: none"> <li>• Boot methods           <ul style="list-style-type: none"> <li>• USB</li> <li>• CD-ROM</li> <li>• DVD</li> <li>• PXE</li> <li>• Solid state/flash drives</li> <li>• Netboot</li> <li>• External/hot swappable drive</li> <li>• Internal hard drive (partition)</li> </ul> </li> <li>• Type of installations           <ul style="list-style-type: none"> <li>• Unattended installation</li> <li>• Upgrade</li> <li>• Clean install</li> <li>• Repair installation</li> <li>• Multiboot</li> <li>• Remote network installation</li> <li>• Image deployment</li> <li>• Recovery partition</li> <li>• Refresh/restore</li> </ul> </li> <li>• Partitioning           <ul style="list-style-type: none"> <li>• Dynamic</li> <li>• Basic</li> <li>• Primary</li> <li>• Extended</li> <li>• Logical</li> <li>• GPT</li> </ul> </li> <li>• File system types/formatting           <ul style="list-style-type: none"> <li>• ExFAT</li> <li>• FAT32</li> <li>• NTFS</li> <li>• CDFS</li> <li>• NFS</li> <li>• ext3, ext4</li> <li>• Quick format vs. full format</li> </ul> </li> <li>• Load alternate third party drivers when necessary</li> <li>• Workgroup vs. Domain setup</li> <li>• Time/date/region/language settings</li> <li>• Driver installation, software and windows updates</li> <li>• Factory recovery partition</li> <li>• Properly formatted boot drive with the correct partitions/ format</li> </ul>	Lesson 9, Topic B
	Lesson 9, Topic B

<i>Domain and Objective</i>	<i>Covered In</i>
<b>1.3 Given a scenario, apply appropriate Microsoft command line tools.</b>	
• TASKKILL	Lesson 9, Topic D
• BOOTREC	Lesson 9, Topic D
• SHUTDOWN	Lesson 9, Topic D
• TASKLIST	Lesson 9, Topic D
• MD	Lesson 2, Topic B
• RD	Lesson 2, Topic B
• CD	Lesson 2, Topic B
• DEL	Lesson 2, Topic B
• FORMAT	Lesson 8, Topic E
• COPY	Lesson 2, Topic B
• XCOPY	Lesson 2, Topic B
• ROBOCOPY	Lesson 2, Topic B
• DISKPART	Lesson 9, Topic D
• SFC	Lesson 9, Topic D
• CHKDSK	Lesson 9, Topic D
• GPUPDATE	Lesson 9, Topic D
• GPRERESULT	Lesson 9, Topic D
• DIR	Lesson 2, Topic B
• EXIT	Lesson 9, Topic D
• HELP	Lesson 2, Topic B
• EXPAND	Lesson 19, Topic A
• [command name] /?	Lesson 2, Topic B
• Commands available with standard privileges vs. administrative privileges	Lesson 2, Topic B

**1.4 Given a scenario, use appropriate Microsoft operating system features and tools.**

<b>Domain and Objective</b>	<b>Covered In</b>
<ul style="list-style-type: none"> <li>• Administrative           <ul style="list-style-type: none"> <li>• Computer management</li> <li>• Device manager</li> <li>• Local Users and groups</li> <li>• Local security policy</li> <li>• Performance monitor</li> <li>• Services</li> <li>• System configuration</li> <li>• Task scheduler</li> <li>• Component services</li> <li>• Data sources</li> <li>• Print management</li> <li>• Windows memory diagnostics</li> <li>• Windows firewall</li> <li>• Advanced security</li> </ul> </li> </ul>	Lesson 6, Topic B; Lesson 9, Topic C; Lesson 9, Topic D
<ul style="list-style-type: none"> <li>• MSCONFIG           <ul style="list-style-type: none"> <li>• General</li> <li>• Boot</li> <li>• Services</li> <li>• Startup</li> <li>• Tools</li> </ul> </li> </ul>	Lesson 9, Topic D
<ul style="list-style-type: none"> <li>• Task Manager           <ul style="list-style-type: none"> <li>• Applications</li> <li>• Processes</li> <li>• Performance</li> <li>• Networking</li> <li>• Users</li> </ul> </li> </ul>	Lesson 9, Topic C
<ul style="list-style-type: none"> <li>• Disk management           <ul style="list-style-type: none"> <li>• Drive status</li> <li>• Mounting</li> <li>• Initializing</li> <li>• Extending partitions</li> <li>• Splitting partitions</li> <li>• Shrinking partitions</li> <li>• Assigning/changing drive letters</li> <li>• Adding drives</li> <li>• Adding arrays</li> <li>• Storage spaces</li> </ul> </li> </ul>	Lesson 8, Topic C
<ul style="list-style-type: none"> <li>• Other           <ul style="list-style-type: none"> <li>• User State Migration tool (USMT)</li> <li>• Windows Easy Transfer</li> <li>• Windows Upgrade Advisor</li> </ul> </li> </ul>	Lesson 9, Topic E

<b>Domain and Objective</b>	<b>Covered In</b>
<ul style="list-style-type: none"> <li>• System utilities           <ul style="list-style-type: none"> <li>• REGEDIT</li> <li>• COMMAND</li> <li>• SERVICES.MSC</li> <li>• MMC</li> <li>• MSTSC</li> <li>• NOTE PAD</li> <li>• EXPLORER</li> <li>• MSINFO32</li> <li>• DXDIAG</li> <li>• DEFrag</li> <li>• System restore</li> <li>• Windows Update</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Lesson 2, Topic A;</li> <li>Lesson 9, Topic B;</li> <li>Lesson 9, Topic D;</li> <li>Lesson 10, Topic C</li> </ul>

### 1.5 Given a scenario, use Windows Control Panel utilities.

- Internet Options Lesson 9, Topic D
  - Connections
  - Security
  - General
  - Privacy
  - Programs
  - Advanced
- Display/Display Settings Lesson 5, Topic B;  
Lesson 9, Topic D
  - Resolution
  - Color depth
  - Refresh rate
- User Accounts Lesson 9, Topic D
- Folder Options Lesson 9, Topic D
  - View hidden files
  - Hide extensions
  - General options
  - View options
- System Lesson 9, Topic D;  
Lesson 10, Topic A;  
Lesson 10, Topic B;  
Lesson 14, Topic C
  - Performance (virtual memory)
  - Remote settings
  - System protection
- Windows Firewall Lesson 9, Topic D
- Power Options Lesson 9, Topic D
  - Hibernate
  - Power plans
  - Sleep/suspend
  - Standby
- Programs and Features Lesson 9, Topic D

<b>Domain and Objective</b>	<b>Covered In</b>
• HomeGroup	Lesson 9, Topic D
• Devices and Printers	Lesson 9, Topic D
• Sound	Lesson 9, Topic D
• Troubleshooting	Lesson 9, Topic D
• Network and Sharing Center	Lesson 9, Topic D
• Device Manager	Lesson 9, Topic D
<b>1.6 Given a scenario, install and configure Windows networking on a client/desktop.</b>	
• HomeGroup vs. WorkGroup	Lesson 9, Topic B; Lesson 14, Topic A
• Domain setup	Lesson 9, Topic B; Lesson 14, Topic A
• Network shares/administrative shares/mapping drives	Lesson 14, Topic C
• Printer sharing vs. network printer mapping	Lesson 9, Topic D; Lesson 14, Topic A; Lesson 16, Topic B
• Establish networking connections <ul style="list-style-type: none"> <li>• VPN</li> <li>• Dialups</li> <li>• Wireless</li> <li>• Wired</li> <li>• WWAN (Cellular)</li> </ul>	Lesson 13, Topic C; Lesson 14, Topic A
• Proxy settings	Lesson 14, Topic B
• Remote Desktop Connection	Lesson 14, Topic C
• Remote Assistance	Lesson 19, Topic A
• Home vs. Work vs. Public network settings	Lesson 14, Topic A
• Firewall settings <ul style="list-style-type: none"> <li>• Exceptions</li> <li>• Configuration</li> <li>• Enabling/disabling Windows firewall</li> </ul>	Lesson 9, Topic D
• Configuring an alternative IP address in Windows <ul style="list-style-type: none"> <li>• IP addressing</li> <li>• Subnet mask</li> <li>• DNS</li> <li>• Gateway</li> </ul>	Lesson 13, Topic B; Lesson 14, Topic A

<b>Domain and Objective</b>	<b>Covered In</b>
<ul style="list-style-type: none"> <li>• Network card properties           <ul style="list-style-type: none"> <li>• Half duplex/full duplex/auto</li> <li>• Speed</li> <li>• Wake-on-LAN</li> <li>• QoS</li> <li>• BIOS (on-board NIC)</li> </ul> </li> </ul>	Lesson 13, Topic A; Lesson 14, Topic A
<b>1.7 Perform common preventive maintenance procedures using the appropriate Windows OS tools.</b>	
<ul style="list-style-type: none"> <li>• Best practices           <ul style="list-style-type: none"> <li>• Scheduled backups</li> <li>• Scheduled disk maintenance</li> <li>• Windows updates</li> <li>• Patch management</li> <li>• Driver/firmware updates</li> <li>• Antivirus/ Antimalware updates</li> </ul> </li> <li>• Tools           <ul style="list-style-type: none"> <li>• Backup</li> <li>• System restore</li> <li>• Recovery image</li> <li>• Disk maintenance utilities</li> </ul> </li> </ul>	Lesson 10, Topic B; Lesson 10, Topic C; Lesson 10, Topic D
	Lesson 10, Topic B; Lesson 10, Topic C

<b>Domain and Objective</b>	<b>Covered In</b>
<b>2.0 Other Operating Systems and Technologies</b>	
<b>2.1 Identify common features and functionality of the Mac OS and Linux operating systems.</b>	
<ul style="list-style-type: none"> <li>• Best practices           <ul style="list-style-type: none"> <li>• Scheduled backups</li> <li>• Scheduled disk maintenance</li> <li>• System updates/App store</li> <li>• Patch management</li> <li>• Driver/firmware updates</li> <li>• Antivirus/antimalware updates</li> </ul> </li> <li>• Tools           <ul style="list-style-type: none"> <li>• Backup/Time Machine</li> <li>• Restore/snapshot</li> <li>• Image recovery</li> <li>• Disk maintenance utilities</li> <li>• Shell/Terminal</li> <li>• Screen sharing</li> <li>• Force Quit</li> </ul> </li> </ul>	Lesson 11, Topic A
	Lesson 11, Topic A

<b>Domain and Objective</b>	<b>Covered In</b>
<ul style="list-style-type: none"> <li>• Features           <ul style="list-style-type: none"> <li>• Multiple desktops/Mission Control</li> <li>• Key Chain</li> <li>• Spot Light</li> <li>• iCloud</li> <li>• Gestures</li> <li>• Finder</li> <li>• Remote Disc</li> <li>• Dock</li> <li>• Boot Camp</li> </ul> </li>   <li>• Basic Linux commands           <ul style="list-style-type: none"> <li>• ls</li> <li>• grep</li> <li>• cd</li> <li>• shutdown</li> <li>• pwd vs. passwd</li> <li>• mv</li> <li>• cp</li> <li>• rm</li> <li>• chmod</li> <li>• mkdir</li> <li>• chown</li> <li>• iwconfig/ifconfig</li> <li>• ps</li> <li>• q</li> <li>• su/sudo</li> <li>• apt-get</li> <li>• vi</li> <li>• dd</li> </ul> </li> </ul>	Lesson 2, Topic A; Lesson 11, Topic A  Lesson 11, Topic B
<b>2.2 Given a scenario, setup and use client-side virtualization.</b>	
<ul style="list-style-type: none"> <li>• Purpose of virtual machines</li> <li>• Resource requirements</li> <li>• Emulator requirements</li> <li>• Security requirements</li> <li>• Network requirements</li> <li>• Hypervisor</li> </ul>	Lesson 9, Topic A Lesson 9, Topic A
<b>2.3 Identify basic cloud concepts.</b>	
<ul style="list-style-type: none"> <li>• SaaS</li> <li>• IaaS</li> <li>• PaaS</li> <li>• Public vs. Private vs. Hybrid vs. Community</li> </ul>	Lesson 3, Topic D Lesson 3, Topic D Lesson 3, Topic D Lesson 3, Topic D

<b>Domain and Objective</b>	<b>Covered In</b>
• Rapid Elasticity	Lesson 3, Topic D
• On-demand	Lesson 3, Topic D
• Resource pooling	Lesson 3, Topic D
• Measured service	Lesson 3, Topic D
<b>2.4 Summarize the properties and purpose of services provided by networked hosts.</b>	
• Server roles	Lesson 3, Topic C
• Web server	
• File server	
• Print server	
• DHCP server	
• DNS server	
• Proxy server	
• Mail server	
• Authentication server	
• Internet appliance	Lesson 3, Topic C
• UTM	
• IDS	
• IPS	
• Legacy/embedded systems	Lesson 3, Topic C
<b>2.5 Identify basic features of mobile operating systems.</b>	
• Android vs. iOS vs. Windows	Lesson 2, Topic A
• Open source vs. closed source/vendor specific	
• App source (play store, app store and store)	
• Screen orientation (accelerometer/gyroscope)	
• Screen calibration	
• GPS and geotracking	
• WiFi calling	
• Launcher/GUI	
• Virtual assistant	
• SDK/APK	
• Emergency notification	
• Mobile payment service	
<b>2.6 Install and configure basic mobile device network connectivity and email.</b>	
• Wireless/cellular data network (enable/disable)	Lesson 15, Topic D;
• Hotspot	Lesson 15, Topic E
• Tethering	
• Airplane mode	

<b>Domain and Objective</b>	<b>Covered In</b>
<ul style="list-style-type: none"> <li>• Bluetooth           <ul style="list-style-type: none"> <li>• Enable Bluetooth</li> <li>• Enable pairing</li> <li>• Find device for pairing</li> <li>• Enter appropriate pin code</li> <li>• Test connectivity</li> </ul> </li> </ul>	Lesson 15, Topic E
<ul style="list-style-type: none"> <li>• Corporate and ISP email configuration           <ul style="list-style-type: none"> <li>• POP3</li> <li>• IMAP</li> <li>• Port and SSL settings</li> <li>• Exchange, S/MIME</li> </ul> </li> </ul>	Lesson 15, Topic E
<ul style="list-style-type: none"> <li>• Integrated commercial provider email configuration           <ul style="list-style-type: none"> <li>• Google/Inbox</li> <li>• Yahoo</li> <li>• Outlook.com</li> <li>• iCloud</li> </ul> </li> </ul>	Lesson 15, Topic E
<ul style="list-style-type: none"> <li>• PRI updates/PRL updates/Baseband updates</li> </ul>	Lesson 15, Topic E
<ul style="list-style-type: none"> <li>• Radio firmware</li> </ul>	Lesson 15, Topic E
<ul style="list-style-type: none"> <li>• IMEI vs. IMSI</li> </ul>	Lesson 15, Topic E
<ul style="list-style-type: none"> <li>• VPN</li> </ul>	Lesson 15, Topic E
<b>2.7 Summarize methods and data related to mobile device synchronization.</b>	
<ul style="list-style-type: none"> <li>• Types of data to synchronize           <ul style="list-style-type: none"> <li>• Contacts</li> <li>• Programs</li> <li>• Email</li> <li>• Pictures</li> <li>• Music</li> <li>• Videos</li> <li>• Calendar</li> <li>• Bookmarks</li> <li>• Documents</li> <li>• Location data</li> <li>• Social media data</li> <li>• eBooks</li> </ul> </li> </ul>	Lesson 15, Topic F
<ul style="list-style-type: none"> <li>• Synchronization methods           <ul style="list-style-type: none"> <li>• Synchronize to the Cloud</li> <li>• Synchronize to the Desktop</li> </ul> </li> </ul>	Lesson 15, Topic F
<ul style="list-style-type: none"> <li>• Mutual authentication for multiple services (SSO)</li> </ul>	Lesson 15, Topic F
<ul style="list-style-type: none"> <li>• Software requirements to install the application on the PC</li> </ul>	Lesson 15, Topic F
<ul style="list-style-type: none"> <li>• Connection types to enable synchronization</li> </ul>	Lesson 15, Topic F

<b>Domain and Objective</b>	<b>Covered In</b>
<b>3.0 Security</b>	
<b>3.1 Identify common security threats and vulnerabilities.</b>	
• Malware	Lesson 17, Topic A
• Spyware	
• Viruses	
• Worms	
• Trojans	
• Rootkits	
• Ransomware	
• Phishing	Lesson 17, Topic A
• Spear phishing	Lesson 17, Topic A
• Spoofing	Lesson 17, Topic A
• Social engineering	Lesson 17, Topic A
• Shoulder surfing	Lesson 17, Topic A
• Zero day attack	Lesson 17, Topic A
• Zombie/botnet	Lesson 17, Topic A
• Brute forcing	Lesson 17, Topic A
• Dictionary attacks	Lesson 17, Topic A
• Non-compliant systems	Lesson 17, Topic A
• Violations of security best practices	Lesson 17, Topic A
• Tailgating	Lesson 17, Topic A
• Man-in-the-middle	Lesson 17, Topic A
<b>3.2 Compare and contrast common prevention methods.</b>	
• Physical security	Lesson 17, Topic B
• Lock doors	
• Mantrap	
• Cable locks	
• Securing physical documents/passwords/shredding	
• Biometrics	
• ID badges	
• Key fobs	
• RFID badge	
• Smart card	
• Tokens	
• Privacy filters	
• Entry control roster	

<b>Domain and Objective</b>	<b>Covered In</b>
<ul style="list-style-type: none"> <li>• Digital security           <ul style="list-style-type: none"> <li>• Antivirus/Antimalware</li> <li>• Firewalls</li> <li>• User authentication/strong passwords</li> <li>• Multifactor authentication</li> <li>• Directory permissions</li> <li>• VPN</li> <li>• DLP</li> <li>• Disabling ports</li> <li>• Access control lists</li> <li>• Smart card</li> <li>• Email filtering</li> <li>• Trusted/untrusted software sources</li> </ul> </li> <li>• User education/AUP</li> <li>• Principle of least privilege</li> </ul>	Lesson 17, Topic B Lesson 3, Topic E; Lesson 4, Topic D Lesson 3, Topic E
<p><b>3.3 Compare and contrast differences of basic Windows OS security settings.</b></p>	
<ul style="list-style-type: none"> <li>• User and groups           <ul style="list-style-type: none"> <li>• Administrator</li> <li>• Power user</li> <li>• Guest</li> <li>• Standard user</li> </ul> </li> <li>• NTFS vs. Share permissions           <ul style="list-style-type: none"> <li>• Allow vs. deny</li> <li>• Moving vs. copying folders and files</li> <li>• File attributes</li> </ul> </li> <li>• Shared files and folders           <ul style="list-style-type: none"> <li>• Administrative shares vs. local shares</li> <li>• Permission propagation</li> <li>• Inheritance</li> </ul> </li> <li>• System files and folders</li> <li>• User authentication           <ul style="list-style-type: none"> <li>• Single sign-on</li> </ul> </li> <li>• Run as administrator vs. standard user</li> <li>• Bitlocker</li> <li>• Bitlocker-To-Go</li> <li>• EFS</li> </ul>	Lesson 18, Topic A Lesson 18, Topic A

**3.4 Given a scenario, deploy and enforce security best practices to secure a workstation.**

<b>Domain and Objective</b>	<b>Covered In</b>
<ul style="list-style-type: none"> <li>• Password best practices           <ul style="list-style-type: none"> <li>• Setting strong passwords</li> <li>• Password expiration</li> <li>• Changing default user names/passwords</li> <li>• Screensaver required password</li> <li>• BIOS/UEFI passwords</li> <li>• Requiring passwords</li> </ul> </li> </ul>	Lesson 3, Topic E; Lesson 18, Topic B
<ul style="list-style-type: none"> <li>• Account management           <ul style="list-style-type: none"> <li>• Restricting user permissions</li> <li>• Login time restrictions</li> <li>• Disabling guest account</li> <li>• Failed attempts lockout</li> <li>• Timeout/screen lock</li> </ul> </li> </ul>	Lesson 18, Topic B
<ul style="list-style-type: none"> <li>• Disable autorun</li> </ul>	Lesson 18, Topic B
<ul style="list-style-type: none"> <li>• Data encryption</li> </ul>	Lesson 18, Topic B
<ul style="list-style-type: none"> <li>• Patch/update management</li> </ul>	Lesson 18, Topic B
<b>3.5 Compare and contrast various methods for securing mobile devices.</b>	
<ul style="list-style-type: none"> <li>• Screen locks           <ul style="list-style-type: none"> <li>• Fingerprint lock</li> <li>• Face lock</li> <li>• Swipe lock</li> <li>• Passcode lock</li> </ul> </li> </ul>	Lesson 17, Topic C
<ul style="list-style-type: none"> <li>• Remote wipes</li> </ul>	Lesson 17, Topic C; Lesson 18, Topic D
<ul style="list-style-type: none"> <li>• Locator applications</li> </ul>	Lesson 17, Topic C; Lesson 18, Topic D
<ul style="list-style-type: none"> <li>• Remote backup applications</li> </ul>	Lesson 17, Topic C; Lesson 18, Topic D
<ul style="list-style-type: none"> <li>• Failed login attempts restrictions</li> </ul>	Lesson 18, Topic D
<ul style="list-style-type: none"> <li>• Antivirus/antimalware</li> </ul>	Lesson 17, Topic C; Lesson 18, Topic D
<ul style="list-style-type: none"> <li>• Patching/OS updates</li> </ul>	Lesson 17, Topic C; Lesson 18, Topic D
<ul style="list-style-type: none"> <li>• Biometric authentication</li> </ul>	Lesson 18, Topic D
<ul style="list-style-type: none"> <li>• Full device encryption</li> </ul>	Lesson 17, Topic C; Lesson 18, Topic D
<ul style="list-style-type: none"> <li>• Multifactor authentication</li> </ul>	Lesson 18, Topic D
<ul style="list-style-type: none"> <li>• Authenticator applications</li> </ul>	Lesson 18, Topic D
<ul style="list-style-type: none"> <li>• Trusted sources vs. untrusted sources</li> </ul>	Lesson 18, Topic D

<b>Domain and Objective</b>	<b>Covered In</b>
<ul style="list-style-type: none"> <li>• Firewalls</li> <li>• Policies and procedures           <ul style="list-style-type: none"> <li>• BYOD vs. corporate owned</li> <li>• Profile security requirements</li> </ul> </li> </ul>	Lesson 18, Topic D
<b>3.6 Given a scenario, use appropriate data destruction and disposal methods.</b>	Lesson 18, Topic D
<ul style="list-style-type: none"> <li>• Physical destruction           <ul style="list-style-type: none"> <li>• Shredder</li> <li>• Drill / Hammer</li> <li>• Electromagnetic (Degaussing)</li> <li>• Incineration</li> <li>• Certificate of destruction</li> </ul> </li> <li>• Recycling or repurposing best practices           <ul style="list-style-type: none"> <li>• Low level format vs. standard format</li> <li>• Overwrite</li> <li>• Drive wipe</li> </ul> </li> </ul>	Lesson 17, Topic D
<b>3.7 Given a scenario, secure SOHO wireless and wired networks.</b>	Lesson 17, Topic D
<ul style="list-style-type: none"> <li>• Wireless specific           <ul style="list-style-type: none"> <li>• Changing default SSID</li> <li>• Setting encryption</li> <li>• Disabling SSID broadcast</li> <li>• Antenna and access point placement</li> <li>• Radio power levels</li> <li>• WPS</li> </ul> </li> <li>• Change default user-names and passwords</li> <li>• Enable MAC filtering</li> <li>• Assign static IP addresses</li> <li>• Firewall settings</li> <li>• Port forwarding/mapping</li> <li>• Disabling ports</li> <li>• Content filtering / parental controls</li> <li>• Update firmware</li> <li>• Physical security</li> </ul>	Lesson 18, Topic C
	Lesson 18, Topic C

<b>Domain and Objective</b>	<b>Covered In</b>
<b>4.0 Software Troubleshooting</b>	
<b>4.1 Given a scenario, troubleshoot PC operating system problems with appropriate tools.</b>	

<b>Domain and Objective</b>	<b>Covered In</b>
<ul style="list-style-type: none"> <li>• Common symptoms           <ul style="list-style-type: none"> <li>• Proprietary crash screens (BSOD/pin wheel)</li> <li>• Failure to boot</li> <li>• Improper shutdown</li> <li>• Spontaneous shutdown/restart</li> <li>• Device fails to start/detected</li> <li>• Missing DLL message</li> <li>• Services fails to start</li> <li>• Compatibility error</li> <li>• Slow system performance</li> <li>• Boots to safe mode</li> <li>• File fails to open</li> <li>• Missing NTLDR</li> <li>• Missing boot configuration data</li> <li>• Missing operating system</li> <li>• Missing graphical interface</li> <li>• Missing GRUB/LILO</li> <li>• Kernel panic</li> <li>• Graphical interface fails to load</li> <li>• Multiple monitor misalignment/orientation</li> </ul> </li>   <li>• Tools           <ul style="list-style-type: none"> <li>• BIOS/UEFI</li> <li>• SFC</li> <li>• Logs</li> <li>• System Recovery options</li> <li>• Repair disks</li> <li>• Pre-installation environments</li> <li>• MSCONFIG</li> <li>• DEFrag</li> <li>• REGSRV32</li> <li>• REGEDIT</li> <li>• Event viewer</li> <li>• Safe mode</li> <li>• Command prompt</li> <li>• Uninstall/reinstall/repair</li> </ul> </li> </ul>	Lesson 19, Topic A

#### 4.2 Given a scenario, troubleshoot common PC security issues with appropriate tools and best practices.

<b>Domain and Objective</b>	<b>Covered In</b>
<ul style="list-style-type: none"> <li>• Common symptoms           <ul style="list-style-type: none"> <li>• Pop-ups</li> <li>• Browser redirection</li> <li>• Security alerts</li> <li>• Slow performance</li> <li>• Internet connectivity issues</li> <li>• PC/OS lock up</li> <li>• Application crash</li> <li>• OS updates failures</li> <li>• Rogue antivirus</li> <li>• Spam</li> <li>• Renamed system files</li> <li>• Files disappearing</li> <li>• File permission changes</li> <li>• Hijacked email (Responses from users regarding email, Automated replies from unknown sent email)</li> <li>• Access denied</li> <li>• Invalid certificate (trusted root CA)</li> </ul> </li> </ul>	Lesson 19, Topic D
<ul style="list-style-type: none"> <li>• Tools           <ul style="list-style-type: none"> <li>• Antivirus software</li> <li>• Antimalware software</li> <li>• Recovery console</li> <li>• Terminal</li> <li>• System restore/Snapshot</li> <li>• Pre-installation environments</li> <li>• Event viewer</li> <li>• Refresh/restore</li> <li>• MSCONFIG/Safe boot</li> </ul> </li> </ul>	Lesson 19, Topic D
<ul style="list-style-type: none"> <li>• Best practice procedure for malware removal           <ol style="list-style-type: none"> <li>1. Identify malware symptoms</li> <li>2. Quarantine infected system</li> <li>3. Disable system restore (in Windows)</li> <li>4. Remediate infected systems               <ol style="list-style-type: none"> <li>a. Update antimalware software</li> <li>b. Scan and removal techniques (safe mode, pre-installation environment)</li> </ol> </li> <li>5. Schedule scans and run updates</li> <li>6. Enable system restore and create restore point (in Windows)</li> <li>7. Educate end user</li> </ol> </li> </ul>	Lesson 19, Topic D

**4.3 Given a scenario, troubleshoot common mobile OS and application issues with appropriate tools.**

<b>Domain and Objective</b>	<b>Covered In</b>
<ul style="list-style-type: none"> <li>• Common symptoms           <ul style="list-style-type: none"> <li>• Dim display</li> <li>• Intermittent wireless</li> <li>• No wireless connectivity</li> <li>• No Bluetooth connectivity</li> <li>• Cannot broadcast to external monitor</li> <li>• Touchscreen non-responsive</li> <li>• Apps not loading</li> <li>• Slow performance</li> <li>• Unable to decrypt email</li> <li>• Extremely short battery life</li> <li>• Overheating</li> <li>• Frozen system</li> <li>• No sound from speakers</li> <li>• Inaccurate touch screen response</li> <li>• System lockout</li> </ul> </li>   <li>• Tools           <ul style="list-style-type: none"> <li>• Hard reset</li> <li>• Soft reset</li> <li>• Close running applications</li> <li>• Reset to factory default</li> <li>• Adjust configurations/settings</li> <li>• Uninstall/reinstall apps</li> <li>• Force stop</li> </ul> </li> </ul>	Lesson 19, Topic B

#### 4.4 Given a scenario, troubleshoot common mobile OS and application security issues with appropriate tools.

- Common symptoms
  - Signal drop/weak signal
  - Power drain
  - Slow data speeds
  - Unintended Wi-Fi connection
  - Unintended Bluetooth pairing
  - Leaked personal files/data
  - Data transmission overlimit
  - Unauthorized account access
  - Unauthorized root access
  - Unauthorized location tracking
  - Unauthorized camera/microphone activation
  - High resource utilization

<b>Domain and Objective</b>	<b>Covered In</b>
<ul style="list-style-type: none"> <li>• Tools           <ul style="list-style-type: none"> <li>• Antimalware</li> <li>• App scanner</li> <li>• Factory reset/clean install</li> <li>• Uninstall/reinstall apps</li> <li>• Wi-Fi analyzer</li> <li>• Force stop</li> <li>• Cell tower analyzer</li> <li>• Backup/restore (iTunes/iCloud/Apple Configurator, Google sync, One Drive)</li> </ul> </li> </ul>	Lesson 19, Topic D

<b>Domain and Objective</b>	<b>Covered In</b>
<b>5.0 Operational Procedures</b>	
<b>5.1 Given a scenario, use appropriate safety procedures.</b>	
<ul style="list-style-type: none"> <li>• Equipment grounding</li> </ul>	Lesson 4, Topic B
<ul style="list-style-type: none"> <li>• Proper component handling and storage           <ul style="list-style-type: none"> <li>• Antistatic bags</li> <li>• ESD straps</li> <li>• ESD mats</li> <li>• Self-grounding</li> </ul> </li> </ul>	Lesson 4, Topic B
<ul style="list-style-type: none"> <li>• Toxic waste handling           <ul style="list-style-type: none"> <li>• Batteries</li> <li>• Toner</li> <li>• CRT</li> </ul> </li> </ul>	Lesson 4, Topic C
<ul style="list-style-type: none"> <li>• Personal safety           <ul style="list-style-type: none"> <li>• Disconnect power before repairing PC</li> <li>• Remove jewelry</li> <li>• Lifting techniques</li> <li>• Weight limitations</li> <li>• Electrical fire safety</li> <li>• Cable management</li> <li>• Safety goggles</li> <li>• Air filter mask</li> </ul> </li> </ul>	Lesson 4, Topic B; Lesson 4, Topic C
<ul style="list-style-type: none"> <li>• Compliance with local government regulations</li> </ul>	Lesson 4, Topic A
<b>5.2 Given a scenario with potential environmental impacts, apply the appropriate controls.</b>	
<ul style="list-style-type: none"> <li>• MSDS documentation for handling and disposal</li> </ul>	Lesson 4, Topic C
<ul style="list-style-type: none"> <li>• Temperature, humidity level awareness, and proper ventilation</li> </ul>	Lesson 4, Topic C
<ul style="list-style-type: none"> <li>• Power surges, brownouts, blackouts           <ul style="list-style-type: none"> <li>• Battery backup</li> <li>• Surge suppressor</li> </ul> </li> </ul>	Lesson 4, Topic C

<b>Domain and Objective</b>	<b>Covered In</b>
• Protection from airborne particles <ul style="list-style-type: none"> <li>• Enclosures</li> <li>• Air filters/mask</li> </ul>	Lesson 4, Topic C
• Dust and debris <ul style="list-style-type: none"> <li>• Compressed air</li> <li>• Vacuums</li> </ul>	Lesson 4, Topic C
• Compliance to local government regulations	Lesson 4, Topic A
<b>5.3 Summarize the process of addressing prohibited content/activity, and explain privacy, licensing, and policy concepts.</b>	
• Incident response <ul style="list-style-type: none"> <li>• First response (identify, report through proper channels, data/device preservation)</li> <li>• Use of documentation/documentation changes</li> <li>• Chain of custody (tracking of evidence/documenting process)</li> </ul>	Lesson 4, Topic E
• Licensing/DRM/EULA <ul style="list-style-type: none"> <li>• Open source vs. commercial license</li> <li>• Personal license vs. enterprise licenses</li> </ul>	Lesson 4, Topic E
• Personally Identifiable Information	Lesson 4, Topic E
• Follow corporate end-user policies and security best practices	Lesson 4, Topic E
<b>5.4 Demonstrate proper communication techniques and professionalism.</b>	
• Use proper language—avoid jargon, acronyms, slang when applicable	Lesson 4, Topic D
• Maintain a positive attitude/project confidence	Lesson 4, Topic D
• Actively listen (taking notes) and avoid interrupting the customer	Lesson 4, Topic D
• Be culturally sensitive <ul style="list-style-type: none"> <li>• Use appropriate professional titles, when applicable</li> </ul>	Lesson 4, Topic D
• Be on time (if late contact the customer)	Lesson 4, Topic D
• Avoid distractions <ul style="list-style-type: none"> <li>• Personal calls</li> <li>• Texting/social media sites</li> <li>• Talking to coworkers while interacting with customers</li> <li>• Personal interruptions</li> </ul>	Lesson 4, Topic D

<b>Domain and Objective</b>	<b>Covered In</b>
<ul style="list-style-type: none"> <li>• Dealing with difficult customer or situation           <ul style="list-style-type: none"> <li>• Do not argue with customers and/or be defensive</li> <li>• Avoid dismissing customer problems</li> <li>• Avoid being judgmental</li> <li>• Clarify customer statements (ask open ended questions to narrow the scope of the problem, restate the issue or question to verify understanding)</li> <li>• Do not disclose experiences via social media outlets</li> </ul> </li> </ul>	Lesson 4, Topic D
<ul style="list-style-type: none"> <li>• Set and meet expectations/timeline and communicate status with the customer           <ul style="list-style-type: none"> <li>• Offer different repair/replacement options if applicable</li> <li>• Provide proper documentation on the services provided</li> <li>• Follow up with customer/user at a later date to verify satisfaction</li> </ul> </li> </ul>	Lesson 4, Topic D
<ul style="list-style-type: none"> <li>• Deal appropriately with customers confidential and private materials           <ul style="list-style-type: none"> <li>• Located on a computer, desktop, printer, etc</li> </ul> </li> </ul>	Lesson 4, Topic D
<b>5.5 Given a scenario, explain the troubleshooting theory.</b>	
<ul style="list-style-type: none"> <li>• Always consider corporate policies, procedures and impacts before implementing changes.           <ol style="list-style-type: none"> <li>1. Identify the problem. Question the user and identify user changes to computer and perform backups before making changes</li> <li>2. Establish a theory of probable cause (question the obvious). If necessary, conduct external or internal research based on symptoms</li> <li>3. Test the theory to determine cause. Once theory is confirmed determine next steps to resolve problem. If theory is not confirmed re-establish new theory or escalate</li> <li>4. Establish a plan of action to resolve the problem and implement the solution</li> <li>5. Verify full system functionality and if applicable implement preventive measures</li> <li>6. Document findings, actions and outcomes</li> </ol> </li> </ul>	Lesson 4, Topic F

# C A+ Command Reference

This appendix summarizes the various commands used throughout the course, along with a brief description of their uses and proper command syntax.

## Microsoft Windows Commands

The following table describes the Microsoft Windows commands used throughout this course. For a complete description of a command, use the **help command** or *command /?*

<b>Command</b>	<b>Syntax and Description</b>
<i>command/?</i>	<b>Syntax:</b> <i>command /?</i>  <b>Description:</b> Displays the same information as <i>help command_name</i> . <i>md /?</i>
help	<b>Syntax:</b> <b>help [command]</b>  <b>Description:</b> The <b>help</b> command by itself lists the available commands. To get information on a specific command, enter <b>help command_name</b> .  <b>Example:</b> <i>help md /?</i>
MD	<b>Syntax:</b> <i>MD [drive:]path</i>  <b>Description:</b> Create a directory with the specified name.  <b>Example:</b> <i>md c:\MyNewDirectory</i>
RD	<b>Syntax:</b> <i>RD [/S] [/Q] [drive:]path</i>  <b>Description:</b> Remove the specified directory.  <b>Example:</b> <i>rd c:\MyDirectory</i>
CD	<b>Syntax:</b> <i>CD [/D] [drive:]path</i> <i>CD [...]</i>  <b>Description:</b> Change to the specified directory.  <b>Example:</b> <i>cd c:\MyNewDirectory</i>

<b>Command</b>	<b>Syntax and Description</b>
DEL	<p><b>Syntax:</b></p> <pre>DEL [/P] [/F] [/S] [/Q] [/A[[[:]]attributes]] names</pre> <p><b>Description:</b> Delete the specified file.</p> <p><b>Example:</b> del myfile.txt</p>
DIR	<p><b>Syntax:</b></p> <pre>DIR [drive:] [path] [filename] [/A[[[:]]attributes]] [/B]      [/C] [/D] [/L] [/N] [/O[[[:]]sortorder]] [/P] [/Q] [/R]      [/S] [/T[[[:]]timefield]] [/W] [/X] [/4]</pre> <p><b>Description:</b> List the contents of the current or specified directory.</p> <p><b>Example:</b> dir c:\MyDirectory</p>
COPY	<p><b>Syntax:</b></p> <pre>COPY [/D] [/V] [/N] [/Y   /-Y] [/Z] [/L] [/A   /B]       source [/A   /B] [+ source [/A   /B] [+ ...]]       [destination [/A   /B]]</pre> <p><b>Description:</b> Copy the specified file(s) to a different location. The other location can be a different file name in the current directory or the same or a different name in another directory. You can use wildcards such as * to match any number of any characters and ? to match any single character.</p> <p><b>Example:</b> copy *.txt c:\MyNewDirectory\MyTextFiles</p>
XCOPY	<p><b>Syntax:</b></p> <pre>XCOPY source [destination] [/A   /M] [/D[:date]] [/P]      [/S [/E]] [/V] [/W] [/C] [/I] [/Q] [/F] [/L] [/G] [/H]      [/R] [/T] [/U] [/K] [/N] [/O] [/X] [/Y] [/Z] [/B]      [/J] [/EXCLUDE:file1[+file2][+file3]...]</pre> <p><b>Description:</b> Copies the specified file(s), and if desired, a directory tree, to the specified destination. Wildcards can be used with this command.</p> <p><b>Example:</b> xcopy c:\MyOriginalFiles\*.txt c:\MyNewDirectory\MyTextFiles</p>

<b>Command</b>	<b>Syntax and Description</b>
ROBOCOPY	<b>Syntax:</b> <pre>robocopy source destination [file [file]...] [options]</pre> <p><b>Description:</b> Robust Copy for Windows (ROBOCOPY) has many more options than either XCOPY or COPY commands. In this command, you specify the source directory, followed by the destination directory, then the file(s) and any options you wish to use. You can use wildcards when specifying the files to copy.</p> <div style="border: 1px solid black; padding: 5px;">  <b>Note:</b> For a complete list of options, in addition to using help or the /? option, you can go to <a href="https://technet.microsoft.com/en-us/library/cc733145(WS.10).aspx">https://technet.microsoft.com/en-us/library/cc733145(WS.10).aspx</a>. </div> <p><b>Example:</b> robocopy c:\SourceDir f:\DestinationDir /e /minage: 14</p> <div style="border: 1px solid black; padding: 5px;">  <b>Note:</b> The command in this example will copy the contents of the source directory into the destination directory with all subdirectories, including empty subdirectories, for all files over 14 days old. </div> <p>For additional examples, refer to <a href="http://social.technet.microsoft.com/wiki/contents/articles/1073.robocopy-and-a-few-examples.aspx">http://social.technet.microsoft.com/wiki/contents/articles/1073.robocopy-and-a-few-examples.aspx</a>.</p>
CHKDSK	<b>Syntax:</b> <pre>CHKDSK [volume[[path]filename]] [/F] [/V] [/R] [/X] [/I] [/C] [/L[:size]] [/B] [/scan] [/spotfix]</pre> <p><b>Description:</b> Checks for fragmentation and other errors on the specified disk and displays a status report. Various options can be used to repair and clean up the disk.</p> <p><b>Example:</b> chkdsk c: /R</p> <p>In this example, the C: drive is checked, bad sectors are located, and readable information is recovered.</p>
FORMAT	<b>Syntax:</b> <pre>FORMAT volume [/FS:file-system] [/V:label] [/Q] [/L] [/A:size] [/C] [/I:state] [/X] [/P:passes] [/S:state] FORMAT volume [/V:label] [/Q] [/F:size] [/P:passes] FORMAT volume [/V:label] [/Q] [/T:tracks /N:sectors] [/P:passes] FORMAT volume [/V:label] [/Q] [/P:passes] FORMAT volume [/Q]</pre> <p><b>Description:</b> Formats the specified disk for use with Windows. Using parameters, you can specify the file system type and volume label.</p> <p><b>Example:</b> format h: /FS: NTFS /v:DATA</p> <p>In this example, the H: drive is formatted with the NTFS file system and given the volume label, DATA.</p>

<b>Command</b>	<b>Syntax and Description</b>
DISKPART	<p><b>Syntax:</b></p> <pre>DISKPART</pre> <p><b>Description:</b> DISKPART is a superset of the commands available in the GUI tool Disk Management. It should be used with extreme caution as you can easily remove a partition that contains data.</p> <p>At the Diskpart command prompt, these are the commands you can enter:</p> <pre>LIST Disk LIST Partition LIST Volume SELECT Disk=n SELECT Partition=n SELECT Volume=n_or_d (Number or Drive Letter) DETAIL Disk DETAIL Partition DETAIL volume ACTIVE (set the current in-focus partition to be the system partition) ASSIGN (allocate the next free drive letter) ASSIGN LETTER=E (Choose a free letter) ATTRIBUTES DISK [{set   clear}] [readonly] [noerr] ATTRIBUTES VOLUME [{set   clear}] [{hidden   readonly   nodefaultdriveletter   shadowcopy}] [noerr] AUTOMOUNT [enable] [disable] [scrub] [noerr] FILESYSTEMS (Use 'Select Volume' first) HELP INACTIVE (mark a system/boot partition as inactive [don't boot], use 'Select Partition' first) OFFLINE disk [noerr] (Take the current disc offline, use 'Select Disk' first) ONLINE {disk volume} [noerr] REM (remark/comment) REMOVE letter=E [dismount] [noerr] (Remove drive letter E from the in-focus partition) REMOVE mount=path [dismount] [noerr] (Remove mount point from the in-focus partition) REMOVE /ALL [dismount] [noerr] (Remove ALL current drive letters and mount points) RESCAN (Locate new disks that have been added to the computer) SHRINK [desired=n] [minimum=n] [nowait] [noerr] (Reduce the size of the in-focus volume) SHRINK querymax [noerr] EXIT UNIQUEID disk [id={dword   GUID}] [noerr] (Display or set the GUID partition table identifier or MBR signature for the disk with focus)</pre>

<b>Command</b>	<b>Syntax and Description</b>
DISKPART (Cont.)	<p><b>Commands to Manage Basic Disks:</b> ASSIGN MOUNT=path (Choose a mount point path for the volume) CREATE PARTITION Primary Size=50000 (50 GB) CREATE PARTITION Extended Size=25000 CREATE PARTITION logical Size=25000 DELETE Partition EXTEND Size=10000 GPT attributes=n (assign GUID Partition Table attributes) SET id=byte GUID [override] [noerr] (Change the partition type)</p> <p><b>Commands to Manage Dynamic Disks:</b> ADD disk=n (Add a mirror to the in-focus SIMPLE volume on the specified disk see 'Diskpart Help' for more.) BREAK disk=n (Break the current in-focus mirror) CREATE VOLUME Simple Size=n Disk=n CREATE VOLUME Stripe Size=n Disk=n,n,... CREATE VOLUME Raid Size=n Disk=n,n,... DELETE DISK DELETE PARTITION DELETE VOLUME EXTEND Disk=n [Size=n] EXTEND Filesystem [noerr] IMPORT [noerr] (Import a foreign disk group, use 'Select Disc' first) RECOVER [noerr] (Refresh disc pack state, attempt recovery on an invalid pack, &amp; resynchronize stale plex/parity data.) REPAIR disk=n [align=n] [noerr] (Repair the RAID-5 volume with focus, replace with the specified dynamic disk) RETAIN (Prepare an existing dynamic simple volume to be used as a boot or system volume) <b>Commands to Convert Disks:</b> CONVERT basic CONVERT dynamic CONVERT gpt CONVERT mbr CLEAN [ALL] (remove all partition and volume info from the hard drive) FORMAT [{fs=ntfs fat fat32} [revision=x.xx]   recommended] [label="label"] [unit=n] [quick] [compress] [override] [nowait] [noerr]</p>
TASKLIST	<p><b>Syntax:</b></p> <pre>TASKLIST [/S system [/U username [/P [password]]]] [/M [module]   /SVC   /V] [/FI filter] [/FO format] [/NH]</pre> <p><b>Description:</b> Displays a list of processes that are running on local or remote systems. In addition to the name of the command, the resulting list also displays the PID, or process ID, or the process.</p> <p><b>Example:</b> TASKLIST /APPS /FI "STATUS eq RUNNING"</p> <p>In this example, Store Apps and their associated processes, filtered to show the apps that are running, are listed.</p>
TASKKILL	<p><b>Syntax:</b></p> <pre>TASKKILL [/S system [/U username [/P [password]]]] { [/FI filter] [/PID processid   /IM imagename] } [/T] [/F]</pre> <p><b>Description:</b> Terminates the specified tasks identified by image name or PID.</p> <pre>taskkill /im cal*.exe</pre> <p>In this example, any task name that begins with "cal" and is an exe file, will be terminated.</p>

<b>Command</b>	<b>Syntax and Description</b>
GPUPDATE	<p><b>Syntax:</b></p> <pre>Gpupdate [/Target:{Computer   User}] [/Force] [/Wait:&lt;value&gt;] [/Logoff] [/Boot] [/Sync]</pre> <p><b>Description:</b> Updates Group Policy settings.</p> <p><b>Example:</b> gpupdate /force</p> <p>In this example, the /force option specifies that all policy settings are reapplied.</p>
GPRESULT	<p><b>Syntax:</b></p> <pre>GPRESULT [/S system [/U username [/P [password]]]] [/SCOPE scope] [/USER targetusername] [/R   /V   /Z]</pre> <p><b>Description:</b> Displays the Resultant Set of Policies (RSOP) for a target user and computer.</p> <p><b>Example:</b> gpresult /r</p> <p>In this example, the RSOP summary data is displayed.</p>
BOOTREC	<p><b>Syntax:</b></p> <pre>bootrec [ /RebuildBcd ] [ /FixBoot ] [ /FixMBR ] [ /ScanOs ]</pre> <p><b>Description:</b> Bootrec.exe is run from within the Windows RE. This is the system recovery done from the Windows Vista or Windows 7 DVD. After booting from the installation media in the DVD drive, selecting <b>Repair your computer</b>, and selecting the operating system to repair, you can open a command prompt and run bootrec.exe. It can be used to fix the master boot record and the boot sector, to rebuild the BCD store, and to scan for items not in the BCD store.</p> <p><b>Example:</b> bootrec /FixMbr</p> <p>In this example, bootrec writes a compatible master boot record to the system partition.</p>
SHUTDOWN	<p><b>Syntax:</b></p> <pre>shutdown [/i   /l   /s   /r   /g   /a   /p   /h   /e   /o] [/hybrid] [/f] [/m \\computer] [/t xxx] [/d [plu:]xx:yy [/c "comment"]]</pre> <p><b>Description:</b> This command is used to safely end processes that are currently running so that the system can be turned off or restarted.</p> <p><b>Example:</b> shutdown /r /t 0</p> <p>In this example, the computer shuts down immediately and restarts.</p>

<b>Command</b>	<b>Syntax and Description</b>
SFC	<p><b>Syntax:</b></p> <pre>SFC [/SCANNOW] [/VERIFYONLY] [/SCANFILE=&lt;file&gt;] [/VERIFYFILE=&lt;file&gt;] [/OFFWINDIR=&lt;offline windows directory&gt; /OFFBOOTDIR=&lt;offline boot directory&gt;]</pre> <p><b>Description:</b> SFC scans protected system files. If it finds any that are the incorrect version, the files are replaced with the correct Microsoft version of the file.</p>
	<p><b>Example:</b> <code>sfc /scannow</code></p> <p>In this example, the integrity of all protected system files are scanned. Any files that need repairs, are repaired if possible.</p>
(EXPAND, EXTRACT, EXTRAC32)	<p><b>Syntax:</b></p> <pre>EXPAND [-R] Source Destination EXPAND -R Source [Destination] EXPAND -I Source [Destination] EXPAND -D Source.cab [-F:Files] EXPAND Source.cab -F:Files Destination</pre>
	<p><b>Description:</b> Expands (or extracts) one or more compressed files from a .CAB file.</p> <pre>expand -d source.cab</pre> <p>In this example, the files contained in the <code>source.cab</code> file are listed.</p>
EXIT	<p><b>Syntax:</b></p> <pre>exit</pre> <p><b>Description:</b> Closes the Command Prompt or PowerShell window.</p>
REGEDIT	<p><b>Syntax:</b></p> <pre>regedit</pre> <p><b>Description:</b> Used to edit Registry settings. Entered from a command prompt or the Run dialog box, this command opens the <b>Registry Editor</b> window.</p>
RECIMG	<p><b>Syntax:</b> <code>recimg &lt;command&gt; &lt;arguments&gt;</code></p> <p>Commands include:</p> <ul style="list-style-type: none"> <li>• <code>/createimage directory</code></li> <li>• <code>/setcurrent directory</code></li> <li>• <code>/deregister</code></li> <li>• <code>/showcurrent</code></li> </ul> <p><b>Description:</b> Configures a recovery image from which Windows can refresh the computer.</p> <p><b>Example:</b> <code>recimg /createimage g:\MyUpdatedImage</code></p> <p>In this example, <code>recimage</code> captures a new custom recovery image and saves it to the G: drive in the MyUpdatedImage directory. This new image is set as the active recovery image.</p>

## Windows GUI Tools

The Windows GUI tools used in this course include:

<b>Tool</b>	<b>Description</b>	<b>Accessed from</b>
Computer Management	This tool gathers several frequently used tools into one application for easy access, including: <ul style="list-style-type: none"> <li>• System Tools               <ul style="list-style-type: none"> <li>• Task Scheduler</li> <li>• Event Viewer</li> <li>• Shared Folders</li> <li>• Performance</li> <li>• Device Manager</li> </ul> </li> <li>• Storage               <ul style="list-style-type: none"> <li>• Disk Management</li> </ul> </li> <li>• Services and Applications               <ul style="list-style-type: none"> <li>• Services</li> <li>• WMI Control</li> </ul> </li> </ul>	From the <b>Start</b> menu
Device Manager	View and configure properties for hardware devices installed on the computer.	From the <b>Start</b> menu, <b>Computer Management</b> , search for devmgmt.msc and select it from the results, or from the <b>Run</b> dialog box, enter <b>devmgmt.msc</b>
Local Users and Groups	Manage users and groups stored on the computer.	From the <b>Start</b> menu, add the <b>Local Users and Groups</b> snap-in to the MMC console, or from <b>Search</b> or <b>Run</b> , run <b>lusrmgr.msc</b>
Local Security Policy	Configure settings for local system, user, and security settings for the local computer. For the Windows 8 family of operating systems, this tool is only available on the Pro and Enterprise editions.	From <b>Search</b> or <b>Run</b> , run <b>secpol.msc</b>
Performance Monitor	View performance data from log files or in real time.	From the <b>Start</b> menu, from <b>Search</b> or <b>Run</b> , run <b>perfmon.msc</b> , or add the Performance Monitor snap-in to the MMC console
Services	Configure Windows services as well as start and stop services.	From the <b>Start</b> menu, from <b>Search</b> or <b>Run</b> , run <b>services.msc</b> , add the <b>Services</b> snap-in to the MMC console or run <b>msconfig.exe</b> and in the <b>System Configuration</b> dialog box, select the <b>Services</b> tab.
System Configuration/MSCONFIG	Configure what is run at system startup, troubleshoot system problems, manage services, configure boot options, and launch other tools.	From the <b>Start</b> menu, or search for <b>msconfig.exe</b> and select it from the results.

<b>Tool</b>	<b>Description</b>	<b>Accessed from</b>
Task Scheduler	Configure tasks to run automatically at set times.	From the <b>Start</b> menu, search for <b>task scheduler</b> and select it from the results, from the <b>Run</b> dialog box, enter <b>taskschd.msc</b> , add the <b>Task Scheduler</b> snap-in to the MMC console, or select it to run inside <b>Computer Management</b>
Component Services	Deploy and manage Computer Object Model (COM+) applications.	From the <b>Start</b> menu, from <b>Search</b> or <b>Run</b> , run <b>comexp.msc</b> , or add the <b>Component Services</b> snap-in to the MMC console.
Data Sources	Create and manage ODBC data sources.	From the <b>Start</b> menu, select <b>All Programs</b> → <b>Administrative Tools</b> → <b>ODBC Data Sources (xx-bit)</b> in Windows 8/8.1 or <b>All Programs</b> → <b>Administrative Tools</b> → <b>Data Sources (ODBC)</b> in Windows 7.
Print Management	Manage multiple printers, print servers, or print queues.	From the <b>Run</b> dialog box or the <b>Search</b> charm, enter <b>printmanagement.msc</b> or from <b>Control Panel</b> , select <b>Administrative Tools</b> then select the <b>Print Management</b> shortcut.
Windows Memory Diagnostics Tool	Detects problems with memory in the computer.	<ul style="list-style-type: none"> <li>• If a memory problem notification is displayed, in the <b>Windows Memory Diagnostics Tool</b> dialog box, select <b>Restart now and check for problems</b>.</li> <li>• To manually run the <b>Windows Memory Diagnostics Tool</b> in the <b>Control Panel</b> search box, enter <b>Memory</b>, and from the results, select <b>Diagnose your computer's memory problems</b>.</li> </ul>
Windows Firewall	A built-in firewall that creates a barrier between the Internet and your computer.	In <b>Control Panel</b> with <b>Large icons</b> or <b>Small icons</b> selected as your view, select <b>Windows Firewall</b> .
Task Manager	View, start or end, or monitor programs, processes, and services running on a computer.	From the <b>Start</b> menu or taskbar, right-click and select <b>Task Manager</b> , or from <b>Search</b> or <b>Run</b> , run <b>taskmgr.exe</b>
Disk Management	Create, delete, or resize hard disk partitions.	In the <b>Run</b> dialog box, enter <b>diskmgmt.msc</b> or from <b>Computer Management</b> , in the left pane, expand <b>Storage</b> and then select <b>Disk Management</b> .

Tool	Description	Accessed from
USMT	User State Migration Tool (USMT) is part of the Windows Assessment and Deployment Kit (ADK) and is used to customize user-profile migration from one version of Windows to a higher numbered Windows version (i.e., from Windows 7 to Windows 8).	Download the Windows ADK from Microsoft.
Windows Easy Transfer	A tool for assisting in transferring files and settings from one Windows computer to another.	Search for <b>easy transfer</b> and from the results list, select <b>Windows Easy Transfer</b> .
Windows Upgrade Advisor	A utility to identify possible compatibility issues that need to be addressed when upgrading from one Windows version to another.	Download the Windows Upgrade Advisor from Microsoft.

## Linux Commands

The following table describes the Linux commands used throughout this course. For a complete description of the command with its related options and arguments, refer to the **man** page for the command.



**Note:** Most of the Linux commands can also be used at the command line in OS X since it is a Linux derivative.

Command	Syntax and Description
ls	<p><b>Syntax:</b></p> <pre>ls [OPTION]... [FILE]...</pre> <p><b>Description:</b> Lists information about the files in the current directory (by default) or the specified directory. You can also specify a file to show just information for that file.</p> <p><b>Example:</b> <code>ls -laR</code></p> <p>In this example, a recursive listing of all files in the current folder, the subfolders and their contents, including empty or hidden folders.</p>
cd	<p><b>Syntax:</b></p> <pre>cd [dir]</pre> <p><b>Description:</b> Change the working directory to the specified directory.</p> <p><b>Example:</b> <code>cd /data/finance</code></p>
pwd	<p><b>Syntax:</b></p> <pre>pwd</pre> <p><b>Description:</b> Shows the name of the current directory.</p>

Command	Syntax and Description
mv	<p><b>Syntax:</b></p> <pre>mv [OPTION]... SOURCE... Destination</pre>
	<p><b>Description:</b></p> <p>Used to move or rename files. Important options are the -i (interactive), which prompts you before overwriting a destination file, and -n (noclobber), which will not overwrite an existing destination file.</p>
	<p><b>Example:</b> mv /data/finance/*2015* /home/jsmith/current_data</p> <p>In this example, files in the /data/finance folder that contain the numbers 2015 somewhere in the filename are moved to the /home/jsmith/current_data folder.</p>
ifconfig	<p><b>Syntax:</b></p> <pre>ifconfig {interface name} {options   address}</pre> <p><b>Description:</b></p>
	<p>Used for configuring network interfaces for Linux servers and workstations. It is also used to view the current TCP/IP configuration of a system, including the IP address and the netmask address.</p>
	<p><b>Example:</b> ifconfig eth0</p> <p>In this example, TCP/IP configuration for the eth0 interface is displayed.</p>
iwconfig	<p><b>Syntax:</b></p> <pre>iwconfig {interface name} {options   address}</pre> <p><b>Description:</b></p> <p>Used for configuring wireless network interfaces.</p>
ps	<p><b>Syntax:</b></p> <pre>ps [options]</pre> <p><b>Description:</b></p> <p>Displays the processes run by the current shell with details such as the PID, the terminal associated with the process, the accumulated CPU time, and the command that started the process.</p>
dd	<p><b>Syntax:</b></p> <pre>dd [operand]... or dd [option]</pre> <p><b>Description:</b></p> <p>Copies and converts files to enable them to be transferred from one type of medium to another.</p>
grep	<p><b>Syntax:</b></p> <pre>grep [command options] {keyword} {file name}</pre> <p><b>Description:</b> A search tool for locating text within a file or a file within a directory.</p>
	<p><b>Example:</b> grep 2015 audit</p> <p>In this example, the text 2015 is being searched for in the audit file.</p>
	<p><b>Example:</b> ls -l   grep audit</p> <p>In this example, the output from the ls command is being searched for the file named audit.</p>

<b>Command</b>	<b>Syntax and Description</b>
passwd	<p><b>Syntax:</b></p> <pre>passwd [user name]</pre> <p><b>Description:</b> Used to change a user's password. If no user name is given as an option, the current user's password is changed.</p> <p><b>Example:</b> <code>passwd jsmith</code></p> <p>In this example, the password will be changed for the user jsmith.</p>
rm	<p><b>Syntax:</b></p> <pre>rm [command options] {absolute or relative path of file or directory}/{file or directory name}</pre> <p><b>Description:</b> Delete files or directories.</p> <p><b>Example:</b> <code>rm -R report_files_directory</code></p> <p>In this example, the specified directory, its contents, and any subdirectories are deleted.</p>
shutdown	<p><b>Syntax:</b></p> <pre>shutdown [-t seconds] [-options] time [warning message]</pre> <p><b>Description:</b> Closes and safely shuts down the system.</p> <p><b>Example:</b> <code>shutdown -t 60</code></p> <p>In this example, the system will be shut down in 60 seconds.</p>
cp	<p><b>Syntax:</b></p> <pre>cp [options] {absolute or relative path of the file or directory to be copied}/{file or directory name} {absolute or relative path of the destination}</pre> <p><b>Description:</b> Copy files.</p> <p><b>Example:</b> <code>cp -R /home/jsmith/reports /data/reports</code></p> <p>In this example, a recursive copy of the files in the /home/jsmith/reports directory are being copied to the /data/reports directory.</p>
chmod	<p><b>Syntax:</b></p> <pre>chmod [option] {mode} {file name}</pre> <p><b>Description:</b> Modifies permissions for a file.</p> <p><b>Example:</b> <code>chmod 644 audit</code></p> <p>In this example, the audit file permissions are Read, Write for the file owner, and Read for groups and other users.</p>
chown	<p><b>Syntax:</b></p> <pre>chown [option] [owner][[:group]] [file name]</pre> <p><b>Description:</b> Change owner, the group, or both for a file or directory.</p> <p><b>Example:</b> <code>chown cfromme /data/reports/*2015*</code></p> <p>In this example, any files in the /data/reports directory containing 2015 in the file name will have their ownership changed to the user cfromme.</p>

<b>Command</b>	<b>Syntax and Description</b>
su	<p><b>Syntax:</b></p> <pre>su [options] [-] [user [argument...]]</pre> <p><b>Description:</b> Allows regular users to run programs with the security privileges of the specified user.</p> <p><b>Example:</b> su cfromme</p> <p>In this example, you are substituting the current user with the user cfromme.</p>
sudo	<p><b>Syntax:</b></p> <pre>sudo command-name command-options</pre> <p><b>Description:</b> Allows regular users to run programs with the security privileges of the root user.</p> <p><b>Example:</b> sudo ls /home/cfromme/private</p> <p>In this example, you are acting as root, but listing the contents of cfromme's private folder.</p>
apt-get	<p><b>Syntax:</b></p> <pre>apt-get [options] {command}</pre> <p><b>Description:</b> Used to install or upgrade packages through the Internet or from the distribution CD on Debian, Ubuntu, or related Linux distribution.</p> <p><b>Example:</b> apt-get upgrade MyPkg</p> <p>In this example, the MyPkg package is upgraded.</p>
vi	<p><b>Syntax:</b></p> <pre>vi [options] [filename]</pre> <p><b>Description:</b> A text editor.</p> <p><b>Example:</b> vi audit_2015</p> <p>In this example, the audit_2015 file in the current directory is opened in the vi editor.</p>

## OS X GUI Tools

The following table describes the OS X tools used throughout this course.

<b>Command</b>	<b>Description</b>	<b>Access by</b>
Time Machine	A backup utility that backs files and folders up to a separate hard drive (not removable media) that has been formatted as a Mac file system. Files and folders can be restored from the Time Machine drive.	From the Apple menu, select <b>System Preferences</b> → <b>Time Machine</b> .

<b>Command</b>	<b>Description</b>	<b>Access by</b>
Snapshot	On Mac notebooks that don't currently have access to the Time Machine drive, local copies of files that are created, modified, or deleted are stored on the startup drive. They are copied to the Time Machine drive when it becomes available. Files and folders can be restored from the local snapshot.	From the Apple menu, select <b>System Preferences</b> → <b>Time Machine</b> . The timeline is displayed on the right side of the <b>Time Machine</b> window.
Force Quit	If an app is not responding, you can open the <b>Force Quit Applications</b> window, then select the non-responsive app and select the <b>Force Quit</b> button.	From the Apple menu, select <b>Force Quit</b> to open the <b>Force Quit Applications</b> window. You can also access this window by pressing <b>Command+Option+Esc</b> .
Mission Control	Enables you to see all open windows and spaces.	<ul style="list-style-type: none"> <li>Using either three or four fingers, swipe up on the trackpad.</li> <li>Double tap a Magic Mouse surface with two fingers.</li> <li>From the Dock or Launchpad, select the <b>Mission Control</b> icon.</li> <li>For Apple keyboards with a dedicated key, press the <b>Mission Control</b> key.</li> </ul>
Keychain	A password management system.	Open the <b>Applications</b> folder, open the <b>Utilities</b> folder, select <b>Keychain Access</b> .
Spotlight	Utility to locate files, apps, or online information.	Select the magnifying glass icon in the menu bar or from within any app, press <b>Command+ Spacebar</b> .
iCloud	A cloud computing service offered by Apple.	Access through a browser using your Apple ID.
Gestures	Multi-touch gestures can be performed on a Mac multi-touch trackpad, a Magic Trackpad, or a Magic Mouse.	Use one or more fingers to tap or swipe the surface of the input device.
Finder	Used to manage the folders and files on your computer.	Finder is displayed when you turn on the Mac.
Remote Disc	Access a CD or DVD drive that has been configured to be shareable.	On the Mac without the optical drive, in the <b>Finder</b> sidebar, select the computer on which sharing of CDs and DVDs has been enabled and then select <b>Connect</b> . If the Mac you are using has an optical drive, <b>Remote Disc</b> will not appear in <b>Finder</b> .
Dock	All open windows and programs are represented by an icon in the row of icons at the bottom of the screen. You can also secure items to the dock so that they are always available from the dock.	Displayed at the bottom of most screens.

<b>Command</b>	<b>Description</b>	<b>Access by</b>
Boot Camp	A boot manager for OS X systems that enables users to install Microsoft Windows in a separate partition.	To install Boot Camp, open the <b>Applications</b> folder, open the <b>Utilities</b> folder, and select <b>Boot Camp Assistant</b> .  After setup and configuration, select which operating system to use at boot by pressing the <b>Option</b> key and selecting the desired operating system.



# D | A Brief History of Personal Computers

## Mechanical Computing Devices

Knowing a little about the history of computers can help you appreciate the current industry situation and prepare you for future developments. And, understanding how computers have evolved can help you appreciate how they are built and help you better understand why they work the way they do, which makes troubleshooting and repair that much easier.

### The Abacus

The abacus is usually listed as the first mechanical computation device. Developed 2,000 or more years ago in India or the Far East, an abacus consists of columns of beads that can slide up and down on rods that are held together in a frame. The position of the beads represents a number. Skilled users could perform calculations more quickly than early electronic computers could.



## Mathematical Advancements and Computing

The written number for zero appeared around 650 A.D. in India and made written calculations much easier. A Persian scholar wrote the first textbook on algebra in 830 A.D. During the 1100s, Europeans learned the written form of math used by the Arabs and wrote down multiplication tables to help merchants. Five hundred years later, John Napier, a

Scotsman, carved a set of multiplication tables on ivory sticks that could slide back and forth to indicate certain results. The use of logarithms on *Napier's Bones* in 1617 led to the development of the slide rule. Today's mature engineers can still remember using slide rules in their college days.

## Calculating Machines

The Frenchman Blaise Pascal is usually given credit for the first calculating machine. In 1642, to help his father—a tax collector—with his work, Pascal invented a machine with eight metal dials that could be turned to add and subtract numbers. Leonardo da Vinci and Wilhelm Schickard, a German, designed calculating machines before Pascal, but Pascal receives the recognition because he produced 50 models of his Pascaline machine, not just a prototype or description. In 1673, Gottfried von Leibniz, a German mathematician, improved on Pascal's design to create a Stepped Reckoner that could do addition, subtraction, multiplication, and division. Only two prototypes were produced.

A Frenchman, Thomas de Colmar, created an Arithmometer in 1820 that was produced in large numbers over the ensuing 100 years. The Swedish inventor Willgodt T. Odhner improved on the Arithmometer, and his calculating mechanism was used by dozens of companies in the calculating machines they produced.

## Punchcard Technologies

Punched cards first appeared in 1801. Joseph Marie Jacquard used the holes placed in the card to control the patterns woven into cloth by power looms. In 1832, Charles Babbage was working on a Difference Engine when he realized Jacquard's punched cards could be used in computations. The Analytical Engine, which is the machine Babbage designed but never manufactured, introduced the idea of using memory for storing results and the idea of printed output. His drawings described a general-purpose, fully program-controlled, automatic mechanical digital computer. Lady Ada Augusta Lovelace worked with Babbage on his machine. She became the first computer programmer when she wrote out a series of instructions for the Analytical Engine.



**Note:** Charles Babbage's Difference Engine No. 1 was the first successful automatic calculator. Although the 12,000 parts were never assembled into a finished engine, the parts that were completed functioned perfectly.

Punched cards were used in the United States census of 1890, and a data-processing machine created by Herman Hollerith tabulated the census results in only 2.5 years—much shorter than the predicted 10 years. Punched cards provided input, memory, and output on an unlimited scale for business calculating machines for the next 50 years. The company Hollerith founded to manufacture his card-operated data processors, which used electrical contacts to detect the pattern of holes in each card, eventually became IBM®.

## Electronic Computers and the Military

With the beginning of World War II, electronic computers took on national importance. The accurate calculation of projectile trajectories became a life-and-death concern for the military. The calculations needed to develop the atomic bomb also required more calculating power than was available before the war, and the calculations involved in trying to decode and break enemy codes saw researchers around the world start developing huge room-sized computers that could work on such problems more efficiently than a man with pencil and paper. Between 1939 and 1944, Howard H. Aiken developed the Harvard Mark I—also known as the IBM Automatic Sequence-Controlled Calculator (ASCC). The Mark I was made out of mechanical switches, electrical relays, rotating shafts, and clutches totaling 750,000 components weighing 5 tons. Programming instructions were fed to the Mark I on paper tape, and data was fed in on paper punched cards. Grace Hopper worked at Harvard on the Mark I, II, and III, and discovered the first real-life computer "bug" when she removed a moth that had flown into a mechanical relay, causing it to malfunction. Also, during the war, Konrad Zuse was working secretly on his Z3 computer in Germany. Because so little was known about the Z3 for so long, most people describe the Mark I as the first modern (but not electronic) digital computer.

Perhaps the most important and influential figure from this time was Alan Turing, an English mathematician who is now generally credited with being the father of computer science. Spending his time working in mathematics, logic, and cryptanalysis, Turing was heavily involved in Britain's codebreaking effort during World War II before he moved on to the University of Manchester. While at the University, he began work on the Manchester Mark I, one of the earliest computers. He is also credited with inventing the Turing Test, which has had profound implications in the development of Artificial Intelligence. The Turing Test was a low-tech test for the presence of Artificial Intelligence: if a person were to remotely converse by text with a human and a machine, and could not tell the difference between the two, then the machine would be said to pass the Turing Test.

## Vacuum Tube Systems

The advent of vacuum tube technologies changed the face of electronic computing.

### Vacuum Tubes and Digital Computing

Dr. John Vincent Atanasoff was an associate professor at Iowa State College when he designed an electronic digital computer that would use base two (binary) numbers. In 1939, with his assistant Clifford Berry, he built the world's first electronic digital computer using vacuum tubes. After a lecture, Dr. John W. Mauchly asked to see Atanasoff's computer and later used so many of Atanasoff's ideas in the ENIAC that it took a lawsuit to declare that Atanasoff was the first to use vacuum tubes in an electronic digital computer.

### ENIAC to UNIVAC

Dr. Mauchly and J. Presper Eckert were at the University of Pennsylvania in 1942 when they built the Electronic Numerical Integrator And Computer (ENIAC) to aid the United States military during World War II. ENIAC used 18,000 vacuum tubes, had 500,000 hand-soldered connections, was 1,000 times faster than the Mark I, and had to be rewired to change its program. ENIAC was used from 1946 to 1955, and because of its reliability, it is commonly accepted as the first successful high-speed electronic digital computer. Eckert and Mauchly also designed the Electronic Discrete Variable Automatic Computer (EDVAC), which contained 4,000 vacuum tubes and 10,000 crystal diodes. After their success with ENIAC, Eckert and Mauchly proposed to build a Universal Automatic Computer (UNIVAC) machine to help the Census Bureau handle all its data. After four years of delays and cost overruns, Remington Rand Inc. worked with the Eckert-Mauchly Computer Corporation to develop UNIVAC, the first commercially successful computer. The computer used magnetic tape to store data, a major change from IBM's punched cards, and introduced many other features that are common today. Starting in 1951, 46 UNIVAC I computers were made for the government and businesses, although some experts at the time thought that five computers would be enough to handle all the computational needs of the world.

### John von Neumann

John von Neumann did not design the electronics in computers, but he is credited with the theoretical work that all modern computers are based on. Von Neumann recommended that a computer program should be able to stop under certain conditions and start again at another point. He also recommended storing both the data and instructions in memory so both could be changed as needed. He realized that physically rewiring a computer to change the program, or feeding in another paper tape to meet different conditions, was not practical for successful high-speed computing. The Electronic Delay Storage Automatic Computer (EDSAC) at Cambridge University, England, and Eckert and Mauchly's EDVAC were among the first to use von Neumann's ideas. Combining von Neumann's stored program concept with a 1,000-word main memory, magnetic tape for secondary memory, printer and typewriter output, and a 2.25 MHz clock rate, UNIVAC set the standard for computers in the 1950s.

### Transistorized Systems and Other Technological Advances

In the 1950s, the progress of electronic computing was limited by technology. Vacuum tubes, which were used to control the flow of electricity in digital computer circuits, were large (several inches

high), red-hot to touch, and unreliable. Transistor technologies were the next great technical step forward in the development of computing power.

## Transistors

In the 1940s and early 1950s, Dr. William Shockley worked at Bell Telephone Laboratories as co-head of a solid-state research group that developed the transistor. Transistors performed the same function as vacuum tubes, but were the size of a pencil eraser, generated almost no heat, and were extremely reliable. The replacement of vacuum tubes with transistors opened up new possibilities.

## Magnetic Core Memory

Another important innovation was magnetic core memory, which allowed information to be stored in the magnetic orientation of tiny magnetic rings strung together on fine wire. Using magnetic core memory, the huge mainframes increased their memory from 8,000 to 64,000 words. Combining the computational capability made available through transistors with expanded magnetic core memory gave computers so much power that they had to be used in new ways to justify the cost. Some mainframes used batch processing, where a series of programs and data was stored on magnetic drums and fed to the computer one after the other so no computing time was wasted. Other computers used time sharing, where the computing power was shifted among several different programs running at the same time so no power was wasted waiting for an individual program's results to print or for more input to arrive.

## Miniaturization and the Space Race

At this time, the United States and the former Soviet Union were involved in a race to see who would be first in space. The complex rockets demanded sophisticated computers to control them. The Soviet Union concentrated on designing bigger rockets to carry larger computers into space, while the United States worked on making smaller, more powerful computers that fit into the smaller rockets they had. The millions spent on research to miniaturize computer components used in the space race produced the technology needed for current computers.

## Integrated Circuit Technologies

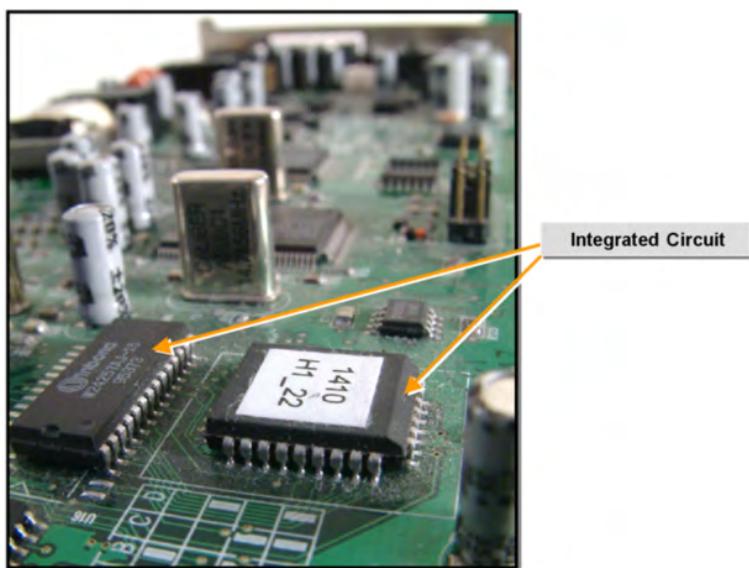
The development of the integrated circuit paved the way for the computers we know today.

## Integrated Circuits

Combining several transistors and the resistors needed to connect them on a single semiconductor chip in an integrated circuit was a tremendous technical advance. In 1958, Jack Kilby at Texas Instruments made several components on a single-piece semiconductor. By 1961, Fairchild and Texas Instruments were mass-producing integrated circuits on a single chip. In 1967, Fairchild introduced the Micromosaic, which contained a few hundred transistors. The transistors could be connected into specific circuits for an application using computer-aided design. The Micromosaic was an Application-Specific Integrated Circuit (ASIC).



**Note:** Now usually called just a chip, the first integrated circuit was fabricated in 1958 by Texas Instruments inventor Jack Kilby.



## Early RAM and Processor Circuits

In 1970, Fairchild introduced the first 256-bit static RAM *chip*, while Intel® announced the first 1,024-bit dynamic RAM. Computers that could make use of this memory were still monsters to maintain. Handheld calculators, on the other hand, appealed to everyone from scientists to school kids. Marcian "Ted" Hoff at Intel designed a general-purpose integrated circuit that could be used in calculators, as well as other devices. Using ideas from this circuit, Intel introduced, in 1972, the 8008, which contained approximately 3,300 transistors and was the first microprocessor to be supported by a high-level language compiler called PL/M.

## General-Purpose Microprocessors

A major breakthrough occurred in 1974 when Intel presented the 8080, the first general-purpose microprocessor. The 8080 microprocessor had a single chip that contained an entire programmable computing device on it. The 8080 was an 8-bit device that contained around 4,500 transistors and could perform 200,000 operations per second. Other companies besides Intel designed and produced microprocessors in the mid-1970s, including Motorola (6800), Rockwell (6502), and Zilog (Z80). As more chips appeared and the prices dropped, personal desktop computers became a possibility.

## Personal Computers

These developments led to the personal computer that is ubiquitous in homes and businesses today.

## The First PCs

About a dozen computers claim to be the first personal computer (PC). Credit for the first popular personal computer often goes to Ed Roberts, whose company, MITS, designed a computer called the Altair 8800 and marketed a kit for about \$400 in 1974. The Altair 8800 used Intel's 8080 microprocessor, contained 256 bytes of RAM, and was programmed by means of a panel of toggle switches. In 1975, Bill Gates and Paul Allen founded Microsoft® and wrote a BASIC interpreter for the Altair. More than 2,000 systems were sold in 1975.



In 1975, MOS Technology announced its 6502-based KIM-1 desktop computer, and Sphere Corporation introduced its Sphere 1 kit. Both kits were strictly for computer fanatics.

### **Early General-Purpose PCs**

In 1976, Steve Wozniak and Steve Jobs formed Apple® Computer Inc., and began creating their first commercial product, the Apple I. Unique for the time, the Apple I was a relatively inexpensive hobbyist computer that required users to provide their own case, monitor, keyboard and power supply. The Apple I was later modified to create the Apple II (with a 6502 microprocessor). In 1977, the Apple II cost \$1,300, came with 16 KB of ROM, 4 KB of RAM, a keyboard, and color output. The Apple II is usually listed as the first personal computer that was available for the general public. The Commodore PET (6502) and Radio Shack's TRS-80 (Z80) were also popular. In 1979, VisiCalc, a spreadsheet program for the Apple II, made desktop computers attractive to businesses. As more businesses bought Apples, demand appeared for word-processing applications, and the software development industry took off. In 1981, IBM joined the party with its first PC. Dozens of other models and companies followed IBM's lead, but in 1984, Apple broke from the pack and produced the Macintosh® computer with a mouse and graphical user interface that opened the computer world to artists and publishers. Of all the computers designed during this period, only the IBM PC and Apple Macintosh have withstood the test of time.

### **Today's PCs**

Today there are several types of PCs, including desktop, minitower, laptop, notebook, tablet PC, and handheld PDA. Most mobile devices have many of the functions of a small computer and the distinction between computer and communications device is blurring.

### **The Development of the Graphical User Interface**

With the near-ubiquity of personal and portable computers today, it is difficult to imagine a time when computers were large, expensive, took several days to process a request and, most importantly, could only understand instructions via a series of card punches. However, this accurately describes many computers well into the early 1970s. Therefore, alongside the development of the microprocessor, one of the most important technological developments encouraging the wide

adoption of easy-to-use personal computers has been the development of the graphical user interface (GUI).

Douglas Engelbart, a researcher at the Stanford Research Institute (SRI), is widely credited with developing the first GUI. Engelbart's research borrowed heavily from ideas spelled out by Vannevar Bush's 1945 essay titled "As We May Think." In this essay, Bush proposed a machine called a memex, which was a hypothetical way of navigating through large amounts of information using hypertext. The memex was based on how adults actually learn, store, and process information, and had increased relevance in an age where information was rapidly changing. While the memex was never created, Engelbart borrowed heavily from Bush's ideas when it came time to work on his own hypertext-based visual computer called the On-Line System, or NLS. The NLS debuted in 1968, and featured the first uses of a GUI, hypertext, a mouse, windows for organizing and displaying information, the use of a computer to deliver a presentation, and many other now-common computer features.

	<b>Note:</b> Vannevar Bush's 1945 essay "As We May Think" can be read online at <a href="http://www.theatlantic.com/doc/194507/bush">www.theatlantic.com/doc/194507/bush</a> .
	<b>Note:</b> A full-length video of Doug Engelbart's demo of the NLS can be found online at <a href="http://www.1968demo.org/">www.1968demo.org/</a> .

After the SRI's introduction of the NLS, work continued on graphical user interface design at Xerox PARC (Palo Alto Research Center). Xerox PARC created what many now consider the first personal computer that used a GUI, along with the now-familiar desktop metaphor. Dubbed the Xerox Alto, it was the first small-scale computer where a graphical tool could be used to create, delete, and manage local files—the Alto was *not* merely a terminal.

Apple founder Steve Jobs visited Xerox PARC, and during his visit became very interested in the mouse. The Alto was not available commercially for home use, but Apple was targeting a larger market. He incorporated what he liked about the Alto into Apple's design, and so the first two GUI computers from Apple—the Lisa and the Macintosh—featured both a GUI and a mouse. Apple's GUIs also continued the Alto's use of the desktop metaphor, with icons of documents and folders representing files and directories. This proved to be an enormously popular way to use a personal computer. Shortly after Apple debuted their GUI, Microsoft released their first operating system that had a graphical interface. Windows 1.0 was a GUI that ran on top of the existing MS-DOS operating system, which was purely text-based up until that point.

Windows greatly changed the look and feel of their GUI with the release of Windows® 95 (the first 32-bit version of Windows), and subsequent Windows operating systems have stayed fairly true to that design: this was the first use in Windows of the Start menu and taskbar, which have been mainstays for more than a decade. Most operating system GUIs since then have shared this basic layout, though the complexity of the graphics may have evolved.

Graphical interface design today has gotten both grander and smaller. With the exploding popularity of handheld multimedia devices, GUIs are no longer limited just to PCs. Thanks to cell phones and smartphones, MP3 players, mobile Internet devices, ebook readers, and more, interfaces have the added challenge of needing to operate on very small screens, drawing far less power, and using weaker processors. On top of this, interface development has had to straddle the line between graphical appeal (such as with 3D desktops) and usability (where the drive for a more user-friendly interface outweighs any flashier graphical features).

## Computing Today and Tomorrow

Today, in the early 21st century, computers and computing have become ubiquitous in the daily lives of almost everyone in the developed world. Computers are present not only as home and office productivity tools, but also as enhancements to everything from home appliances to SUVs. There is more computing power in the average consumer's automobile today than there was on board the Apollo spacecraft that took human beings to the moon and back in the 1960s and 1970s.

The Internet is no less influential than the PC in today's interconnected world. Since physicist Tim Berners-Lee of the CERN laboratory invented the basic technologies of the World Wide Web and

posted the first website in 1991, the growth of the Internet has exploded to the point where virtually all computers on the planet are interconnected. Ordinary users can now communicate sophisticated information with each other instantaneously around the globe. The ongoing vision of Web 2.0 may soon create a global society in which all types of information and all means of communication will be created and maintained cooperatively by ordinary individuals throughout the world. There is even a drive toward turning computers into little more than bootable machines with web browsers on them. In this system of cloud computing, all computing power is provided through remote computers that function, essentially, as application servers. Microsoft's Office 365™ is a prime example of cloud computing, and all reports indicate that cloud computing is here to stay.

The ubiquity of computing power and the omnipresence of the Internet: these two factors have changed our world to an unimaginable extent in an extraordinarily short period of time. Society as a whole can look forward eagerly to the equally unimaginable and extraordinary changes technology will bring us in the years and decades just ahead.

# Solutions

---

## ACTIVITY 1-1: Identifying PC Components

---

2. In this graphic, identify the (A) system unit(s), (B) display device(s), (C) input device(s), and (D) output device(s).

A: Moving clockwise from the far left, the components should be labeled: D, A, B, D, C, C.

3. What are the minimum requirements for a functioning PC?

- Input devices
- Speakers
- System unit
- Webcam
- Display device

4. Which computer components are part of the system unit?

- Chassis
- Internal hard drive
- Monitor
- Portable USB drive
- Memory

5. In this graphic, identify the components listed by placing the corresponding letters into the boxes. A. Motherboard, B. Power supply, C. Expansion card, D. Storage device, E. Memory, F. CPU.

A: Moving clockwise from the top-left corner, the components should be labeled B, E, D, A, C, F.

6. Where is the system BIOS stored?

- On the primary hard drive
- In BIOS memory
- On ROM chips
- In RAM

7. True or False? The GPT is what enables the UEFI to support booting from very large hard disks.  
 True  
 False
8. Which hardware components are checked during the POST?  
 Power supply  
 CPU  
 Display  
 RAM
9. Which system unit components are connected by the system bus?  
 CPU  
 Memory  
 Power supply  
 System board  
 Cooling system

---

## ACTIVITY 1–2: Identifying Storage Devices

---

2. Which storage device records data magnetically and is most often used for backups?  
 FDD  
 HDD  
 Optical disc drive  
 Tape drive  
 SSD
3. What is the primary benefit of using solid state storage?  
A: Answers will vary, but should include the portability of thumb drives and other smaller solid state devices, and the speed of data access when compared to traditional magnetic storage media.
4. Which two media types allow you to write to an optical disc only once?  
 CD-ROM  
 CD-R  
 CD+RW  
 DVD+R  
 DVD-RW
5. True or False? No optical disc can hold more than 50 GB of data.  
 True  
 False

**6. Which features are characteristic of SSHDs?**

- Solid state memory used to cache most-accessed data.
- Boot speed is diminished.
- Faster data access than with magnetic disks.
- Lower cost than pure solid state storage.

---

## ACTIVITY 1–3: Identifying Mobile Digital Devices

---

**1. What do you think are the two most popular types of mobile digital devices?**

A: Responses will vary, but will likely include laptops, tablets, and smartphones.

**2. What types of wearable technology have you experienced? If possible, share your experience with the other participants.**

A: Responses will vary, but might include fitness monitors and smart watches.

**3. Which other mobile devices do you have experience with?**

A: Responses will vary, but might include smart cameras, e-readers, and GPS devices.

**4. Do you have a preference for which mobile OS you use?**

A: Responses will vary, but most people do have a distinct preference for either iOS or Android.

---

## ACTIVITY 1–4: Comparing PC and Device Connection Interfaces

---

**2. In this graphic, identify the (A) audio ports, (B) video ports, and (C) USB ports.**

A: Moving from left to right, the components should be labeled: C, B, C, A.

**3. Which connection type supports up to 127 peripherals for a single connection?**

- IEEE 1394
- SATA
- Parallel
- USB

**4. Which connection interface is compatible with both copper wire and optical fiber cables?**

- IEEE 1393 connection
- SATA connection
- Thunderbolt connection
- DVI-D connection

**5. Of the adapters and converters discussed in this topic, which do you think you might use most often? Be prepared to share your thoughts.**

A: Responses will vary depending on the type of equipment being connected. For example, if you will be connecting PCs to many types of display devices, you might find the DVI to HDMI or DVI to VGA converters to be most useful.

## ACTIVITY 3–1: Identifying Network Types

---

1. **What is the one component that any device that connects to a network requires?**  
A: All devices require a network interface card.
2. **Which network model does a Windows workgroup use and which model does a company-wide server use?**  
A: A workgroup uses a peer-to-peer network model and a company-wide server uses the client/server network model.
3. **Your company has a global presence where all of the locations can communicate. Within each site, there is a network, and that network connects to the overall organizational network. In some locations, there are multiple sites within the city. Identify each type of network described here.**  
A: The global network is a WAN. The network within each site is a LAN. The sites within the city compose a MAN.

---

## ACTIVITY 3–2: Identifying Network Components

---

2. **Which network device would you recommend to someone who needs to control surveillance cameras that need to pan, tilt, and zoom?**  
A: A standard switch could be used, but more likely, you might use PoE.
3. **What situations would be best for wired or wireless networks?**  
A: Answers will vary, but might include using wireless networks for historic buildings that cannot be opened up to run wiring through; and wired networks are more secure, so sensitive data should be sent over wired connections instead of wireless ones.

---

## ACTIVITY 3–3: Discussing Common Network Services

---

1. **What are the minimum network services you would recommend for this organization based on the requirements given in the Scenario?**  
A: Answers will vary, but at a minimum, they should have file and print services.
2. **After some discussion amongst the members of the organization, they have decided that they do need a web site. However, they have no one in-house that can create and maintain the web site. Will they need web services on their server? Why or why not?**  
A: Answers will vary, but at a minimum, if they have a consultant create the web site, chances are that the consultant can also host the site as well, so no web services are needed at this time. If later down the line, the organization decides they need to host it internally, they can add web services at that time.

## ACTIVITY 3–4: Discussing Cloud Services

- How do the five components of cloud computing defined by the NIST work together to provide users with cloud computing services?

**A:** Resource allocation is provided through rapid elasticity and resource pooling. Resource allocation is requested through on-demand self-service. Broad network access makes the resources available to the user. Measured service enables the provider to meter customer usage and bill the customer accordingly.

- Which types of services would your organization be likely to use?

**A:** Answers will vary. You might use IaaS if your organization doesn't have the resources or knowledge to support its own data center. SaaS can be helpful for mobile or transient workforces. You might use PaaS if you want to rent a fully configured system that is set up for a specific purpose.

- Which type of cloud would your organization be likely to use?

**A:** Answers will vary. Depending on how much control you need over the storage or services provided through the cloud, you might select a private cloud solution as the most secure, and a community cloud solution as the least secure.

## ACTIVITY 3–5: Identifying Security Concepts

- Katie works in a high-security government facility. When she comes to work in the morning, she places her hand on a scanning device in her building's lobby, which reads her hand print and compares it to a master record of her hand print in a database to verify her identity. This is an example of:

- Biometric authentication
- Multi-factor authentication
- Data encryption
- Tokens

- How does multi-factor authentication enhance security?

**A:** Requiring two or more authentication factors to gain access to a resource or physical location enhances the security of the resource or location, because more than one password, token, or biometric attribute is needed to gain access. Multi-factor authentication can be particularly secure with biometric, or "who you are," authentication where at least one of the factors is a unique physical characteristic of an individual.

- While assigning privileges to the accounting department in your organization, Cindy, a human resource administrative assistant, insists that she needs access to the employee records database in order to fulfill change of address requests from employees. After checking with her manager and referring to the organization's access control security policy, Cindy's job role does not fall into the authorized category for access to that database. What security concept is being practiced in this scenario?

- The use of strong passwords.
- User education.
- The principle of least privilege.
- Common user security practices.

---

## ACTIVITY 4–1: Discussing Basic Maintenance Tools and Techniques

---

1. You are asked to correct a network cabling problem at a customer site. Which set of tools would be best suited for the task?
  - Phillips screwdriver (#0), torx driver (size T8, T10, and T15), tweezers, and a three-prong retriever
  - Wire strippers, precision wire cutters, digital cable tester, and cable crimper with dies
  - Chip extractor, chip inserter, ratchet, and Allen wrench
  - Anti-static cleaning wipes, anti-static wrist band, flashlight, and cotton swabs
2. You suspect that contaminants from the environment have prevented the fan on a PC from working optimally. Which set of tools would be best suited to fix the problem?
  - Phillips screwdriver (#0), torx driver (size T8, T10, and T15), tweezers, and a three-prong retriever
  - Wire strippers, precision wire cutters, digital multimeter, and cable crimper with dies
  - Chip extractor, chip inserter, ratchet, and Allen wrench
  - Anti-static cleaning wipes, anti-static wrist band, flashlight, and cotton swabs
3. True or False? Windows includes software diagnostic tests that help you find and correct hardware problems.
  - True
  - False

---

## ACTIVITY 4–2: Discussing Personal and Electrical Safety Issues

---

1. True or False? If you are using an anti-static ESD floor mat, you do not need any other ESD safety equipment.
  - True
  - False
2. Electrical injuries include electrocution, shock, and collateral injury. Would you be injured if you are not part of the electrical ground current?

A: Yes, you could receive a thermal burn from the head of an electric arc or electric equipment. Your clothes can catch on fire, or your skin can be burned.
3. Which computer component presents the most danger from electrical shock?
  - System boards
  - Hard drives
  - Power supplies
  - System unit

4. Have you had any personal experience with any of the electrical hazards covered in this topic? What safety precautions could have prevented the incident?

A: Answers will vary depending on individual experiences. Common precautions include disconnecting a computer from the electrical outlet or power strip before servicing it, using anti-static equipment to protect computer components, and implementing smoke and flame detectors to alert you of electrical fires.

---

## ACTIVITY 4–3: Discussing Environmental Safety and Materials Handling

---

1. You are on a service call, and you accidentally spill some liquid cleaner on the user's work surface. What actions should you take?

- Refer to the MSDS for procedures to follow when the material is spilled.
- Wipe it up with a paper towel and dispose of the paper towel in the user's trash container.
- Report the incident.

2. Ozone is classified as an environmental hazard. Which device produces ozone gas?

- Laser printer
- CPU
- Laptop
- Power supply

3. What item reacts with heat and ammonia-based cleaners to present a workplace hazard?

- Capacitor
- Laser
- Toner
- Battery

---

## ACTIVITY 4–4: Discussing Professionalism and Communication Techniques

---

1. Which is a good example of listening skills?

- Maintain a neat and clean appearance.
- Keep sensitive customer information to yourself.
- Interrupt the customer to ask for more details.
- Let your eyes wander around the room as the customer is speaking.
- Allow the customer to complete statements without interrupting.

2. You have received an off-site service call to service a network printer at a customer location. When you arrive, the user is at the printer and starts talking about how the printer is not working properly, and he cannot get his reports handed in on time. As a result, you start asking more clarifying questions to gather more information, so you can identify the specific issue with the printer. What type of technique are you using to gather information?
  - Passive listening
  - Non-verbal communication
  - Active listening

---

## ACTIVITY 4–5: Discussing Organizational Policies and Procedures

---

4. While answering a service call on a computer that is located in a common area of the office, you come across information showing that some unauthorized websites have been viewed. The activity has been linked to a particular user account. What is the appropriate action to take?

A: Answers will vary, but will most likely include referring to procedures and guidelines documented by your specific organization and following the best practices used when responding to an incident, such as first response procedures, chain of custody guidelines, and documenting the entire incident.

---

## ACTIVITY 7–1: Identifying Motherboards

---

1. What type of motherboard is displayed here, and what characteristics did you use to help you identify the board type?

A: Based on its small size dimensions and compact component design, this motherboard is a mini-ITX.  
Identifying Motherboards, Step 2
2. What type of motherboard is displayed here, and what characteristics did you use to help you identify the board type?

A: You can tell by the large size and vast number of available components and slots that this motherboard is an ATX.

---

## ACTIVITY 7–3: Identifying RAM Slots

---

2. How many RAM slots are on your motherboard? Are they all being used?

A: Answers will vary depending on the individual PCs.

---

## ACTIVITY 7–6: Discussing Cooling Systems

---

1. When might you need more than one cooling system in a computer?

A: Answers will vary, but should include instances such as high processing levels that generate excessive heat.

## 2. When would liquid cooling systems be more appropriate than adding a fan?

**A:** Answers will vary, but might include when there is not much room inside the computer case or when an externally mounted fan is not appropriate.

## ACTIVITY 7-9: Troubleshooting CPU Issues

### 1. What initial steps should you take to identify and resolve a potential CPU problem?

- Replace the CPU with a known-good processor.
- Verify that the CPU fan and other cooling systems are installed and functional.
- Replace the motherboard.
- If the CPU is overclocked, throttle it down to the manufacturer-rated clock speed.

### 2. All other diagnostic and corrective steps have failed. You need to verify that it is the CPU itself that is defective. What should you do?

- Replace the CPU with a known-good chip.
- Remove all the adapter cards.
- Reinstall the operating system.
- Replace the motherboard.

## ACTIVITY 7-10: Troubleshooting Motherboards

### 1. What should you do to resolve this issue?

**A:** This problem indicates that the CMOS memory on the motherboard has failed. Replace the CMOS memory.

### 2. What should you do to resolve this issue?

**A:** This problem indicates that the cooling fan on either the CPU or the motherboard is bad. Open the case to verify which cooling fan has failed. If it is the cooling fan on the CPU, replace the CPU. If it is the power supply's cooling fan, replace the power supply.

### 3. What should you do to resolve this issue?

**A:** This problem indicates either the power supply or the motherboard has failed, or there is an overheating problem. First, if you have an available replacement, try replacing the computer's power supply to see if that resolves the problem. Next, check to see if all cooling systems are functioning properly, and replace any cooling systems that are not functioning. If neither of these actions solve the issue, perform tasks such as scanning for viruses, verifying that all motherboard components are seated properly, updating the computer's system firmware, and, finally, replacing the motherboard.

## ACTIVITY 7-11: Troubleshooting Power Supplies

### 1. What would you do to resolve this problem?

**A:** Unplug the power cord. Remove the system cover. Using compressed air, remove the dust from around the fan spindle. Verify that there is no obvious reason the fan is not spinning. Replace the power cord and restart the computer. Verify that the computer starts properly. If these actions did not fix the problem, you would need to replace the power supply. Leaving the problem alone would allow heat to build up to dangerous levels, causing serious damage to the system.

**2. What would you do to resolve this problem?**

A: An odor coming from the power supply could be a sign that there is something wrong. Because you have just replaced the unit, verify that all the connections are secure and that the fan is functioning. Restart the machine and verify that the power supply is running as it should. Once the functionality of the unit is verified, then odor is probably a result of installing a new power supply unit. If the odor does not go away in a few days, then contact the power supply manufacturer.

**4. What would you do to resolve this problem?**

A: Verify that the power cord is securely connected to the power supply and to the electrical outlet on the surge protector. Verify that the surge protector is turned on and plugged in. Verify that the surge protector is working by plugging in a known good electrical device and turning it on. If the device did not turn on, check to see whether any reset buttons need to be reset on the surge protector, or check the electric outlet's circuit breaker. Restart the computer. If these actions did not solve the problem, you would need to replace the power supply.

---

## ACTIVITY 8–1: Comparing RAM Types and Features

---

**1. You have a typical system with RAM that runs at 10 ns, and you add a 12 ns memory module. How fast will the RAM run? Explain your reasoning.**

A: 12 ns, because RAM runs at the speed of the slowest DIMM.

**2. When selecting a RAM module, when would you choose RAM enabled with ECC as opposed to RAM with only parity?**

A: The difference between ECC and parity is that ECC can detect errors and correct them, while parity can only detect errors. If you are adding or replacing RAM in a high-end system or a server where errors can have a critical impact on data integrity, you should consider choosing ECC RAM.

---

## ACTIVITY 8–3: Troubleshooting RAM Issues

---

**1. After troubleshooting this trouble ticket, you have discovered symptoms of a memory problem. What factors could cause sudden memory problems in this situation?**

- New virus
- Power spike
- New memory not compatible
- Power surge

**2. What steps would you take to resolve this trouble ticket?**

A: First, verify that the correct memory was installed on the system, then check to see if the BIOS manufacturer has released any upgrades that would resolve the problem. Try swapping memory around in the memory banks, and finally, verify that memory was installed and configured correctly.

**3. Why is the user experiencing the problem only when additional applications are opened?**

- There is not enough memory in the system.
- Memory errors are occurring in one of the higher memory modules.
- The memory modules are incompatible with one another.

## ACTIVITY 8-7: Troubleshooting Hard Drive Problems

1. A user has reported that there are grinding noises coming from her computer case. Once you take a closer look, you suspect that it is the hard drive. What is the possible cause and solution to this type of issue?
  - Ⓐ The hard drive is physically damaged, probably due to a head crash, so the drive must be replaced.
  - Ⓑ A virus has attacked the hard drive, so use antivirus software to mitigate the issues.
  - Ⓒ Data is corrupt on the drive, and has not been shut down correctly.

3. You recently installed a second hard drive into a user's system. He is now reporting that the drive is not showing up or is not recognized. You know that one of the things you forgot to check when you first performed the installation was system firmware settings for the drive. What in particular do you need to check in system firmware for this problem?

A: You need to verify that drive is enabled in the BIOS or UEFI, and that the correct device settings for the hard drive are listed.

4. Another thing you should check when a second hard drive is not recognized is that the drive was installed correctly. What exactly should you be checking?

A: Verify that the power cable is connected to the drive, that the power cable voltages are correct, and that the data cable is connected correctly to the drive and to the controller or host bus adapter (HBA). For a SATA drive, restart the setup process and press **F6** when prompted to install the driver.

5. A second hard drive was properly installed, but you cannot access it by its drive letter. What should be your next step?

A: Use command line or Windows disk utilities to verify that the drive has been properly partitioned and formatted.

6. A user is encountering the following problem: Her computer boots fine and everything works until the user tries to access data on the second hard drive, the D drive. The message "Can't Access This Drive" is displayed when she tries to access the D drive. The user would also like an explanation about what the error message means. List some of the steps you might take to resolve this problem.

A: You see the "Can't Access This Drive" message when you attempt to access a drive that is not readable, or if the drive does not exist. Troubleshooting steps you should take include: determine if the user actually has a D drive; attempt to copy a file from the D drive to C or from C to D; run the Windows error-checking option. Open **This PC**, display the pop-up menu for the drive you want to check, and select **Properties**. On the **Tools** tab, in the **Error-checking** section, select **Check** and then select **Start** to determine if there are errors; if none of the earlier steps fixed the problem, verify that there is a recent backup and try reformatting the drive; and if the previous step does not fix the problem, replace the drive.

7. When a user tries to access the hard drive containing his data, the system locks up and makes a clicking sound. From the command prompt, he can change to drive D, but when he tries to access a file or list the files on the drive, it locks up and begins clicking again. What steps might you take to attempt to resolve this problem? What is the most likely cause of the problem?

A: You could try running the Windows error-checking option in the **Tools** pane of the **Local Disk Properties** dialog box. You could also try an older version of Scandisk from a removable disk to try to identify and repair the errors it encounters. Definitely back up the data if you can get to any of it. You can try using other software utilities to recover the data or take the drive to a data recovery facility. You will probably need to replace the hard drive. The most likely cause of this problem is a bad hard drive—some of the sectors on the hard drive are probably damaged.

8. A user reports that some of his folders have begun disappearing and some folder and file names are scrambled with strange characters in their names. What steps might you take to attempt to resolve this problem? What is the most likely cause of the problem?  
A: You could try running the Windows error-checking option in the **Tools** pane of the **Local Disk Properties** dialog box. Definitely back up the data if you can get to any of it. You can try using other software utilities to recover the data or take the drive to a data recovery facility. You will probably need to replace the hard drive. You should also check the system for viruses because the result of some infections looks like this problem. If it is not caused by a virus, the most likely cause of this problem is a bad hard drive.
9. A user is questioning the difference between the sizes in GB and bytes. Why is there such a big difference? The disk reports in some places as 9.33 GB and in others as 10,025,000,960 bytes. Why is it not 10 GB?  
A: Hard drive manufacturers usually round 1,024 bytes to 1,000 because it is easier to work with round numbers. By the time you get up to billions of bytes, those extra 24 bytes really add up.

---

## ACTIVITY 11-1: Identifying Features and Functions of OS X

---

1. What Windows and OS X features enable you to back up data and restore data from a backup?  
A: In Windows, you would use the **Backup** feature, and in OS X, you would use **Time Machine**.
2. What Windows and OS X features enable you to manage storage devices?  
A: In Windows, you would use **Disk Management**, and in OS X, you would use **Disk Utility**.
3. What Windows and OS X features enable you to identify which apps are running?  
A: In Windows, you would use the taskbar or **Task Manager**, and in OS X, you would use the **Dock**.
4. What Windows and OS X features enable you to end the running of a non-responsive program?  
A: In Windows **Task Manager**, select the non-responsive program and select **End Process**, and in OS X, you would use the **Force Quit** feature.
5. What Windows and OS X features provide you with cloud storage?  
A: In Windows, you would use OneDrive, and in OS X, you would use iCloud.
6. What Windows and OS X features enable you to search for items?  
A: In Windows, you can use the Search Charm, or in **File Explorer**, you can use the **Search** box. In OS X, you would use the **Spotlight** feature.

---

## ACTIVITY 11-3: Identifying Features and Functions of Linux

---

3. Based on your research, which distribution would you recommend testing for use as a web and network services server?

A: Answers will vary, but any of the distributions that are targeted for business use as a server would work.

4. Based on your research, which distribution would you recommend testing for use on older computers with limited resources?

A: Answers will vary, but any of the distributions that are targeted for end users could be tested to see how well they perform.

---

## ACTIVITY 12-1: Selecting Components for Common Business Clients

---

1. A user needs to be able to access the central employee data repository to run reports, but does not need access to any local applications used to create, edit, and manage the employee data. The employee data is managed on a server that can be accessed with a log in. What type of client is best in this case?

- Thin client
- Virtualization workstation
- Thick client

2. June has recently been put in charge of making updates to the Human Resource employee benefits website. She will be publishing a monthly newsletter and posting company wide announcements, among other small updates and changes, on a regular basis. All changes to the website must be tested on a number of platforms and web browsers to verify that the changes are correct regardless of the operating system and browser. What type of client setup would you suggest for her?

A: Answers will vary, but will most likely include a virtualization workstation so that she can switch from different operating systems and test any website changes quickly.

3. In order to properly support the HR employee benefits website, a new server running client VMs has been installed so that the environment that the application requires can be strictly administered by IT staff. Current PCs will be used to access the Client VM environment that is configured on the VM Server. What needs to be present at all PCs that will be accessing this new server and application?

- Appropriately configured VM Client.
- Fast network connection to server hosting the VM environment.
- Upgrade to video cards.

4. True or False? The HR manager's client computer must meet the recommended requirements to run Windows 8.1 so that she can access and use all of the HR-related applications used by the organization. In this case, the best client option is a thick client.

- True
- False

---

## ACTIVITY 12–2: Selecting Components for Custom Client Systems

---

1. Customer 1 is using a desktop PC to play home movies and to set up slide shows to show his family their vacation photos and is having difficulty with the computer freezing during the movies. He is looking for a solution that will allow him to store and play his movies seamlessly through a computer. He also wants his wife to be able to access the pictures and movies from her laptop within the house. What type of computer setup would you suggest for this customer? What specific questions might you ask this customer about additional component needs?

A: Answers may vary, but will most likely include setting up a home server PC for easy file sharing among the household computing devices and to provide more speed to play movies from the PC. You may ask if they are in need of additional storage space and if they are looking for redundancy through a RAID array in the PC.

2. Customer 2 is from a small real estate office who has recently hired a graphic designer to produce informational pamphlets and other marketing materials for the agency, such as property drop sheets and circular layout designs. The office manager has asked your company to determine the hardware and software needs for the designer's workstation so that it can be ordered and set up before their scheduled start date in two weeks. What hardware and software requirements would you suggest for the graphic designer's workstation?

A: Answers may vary, but will most likely include a PC with a high-end, multicore processor, a high end video card, and the maximum RAM that the motherboard can handle. In addition, the motherboard should contain multiple high-speed ports for peripherals such as external hard drives or additional video cards. The applications will most likely include Adobe's Creative Cloud or similar graphic-design software.

3. Customer 3 is looking to make the switch from a traditional TV cable box and DVD player to a home theater PC, so that she can stream Netflix and record shows and movies from her TV. She already purchased a computer from a local home entertainment store but cannot figure out why she cannot connect the cable TV wire into the computer. What would you check for first?

A: She needs to have a TV tuner card installed in the computer. The tuner card provides the port to connect the cable from the provider to the computer. You would also want to verify that the tuner card is correctly configured, and that all device drivers are installed and up-to-date.

---

## ACTIVITY 13–1: Identifying Network Cables and Connectors

---

4. What type of cable is used to connect your computer to the network?

A: Answers will vary depending on the location of the participant and the type of network interface in the computer, and could range from twisted pair to wireless to virtual.

5. Are there any LED lights on the cable ports indicating activity?

A: Answers will vary depending on the location of the participant and the level of network activity. Some participants might see the LED lights lit or blinking, while others might not.

---

## ACTIVITY 13-2: Examining TCP/IP Information

---

**4. If DHCP is enabled on your computer, when does the lease expire?**

A: Answers will vary depending on the last time the computer was restarted.

**6. How many DNS servers are listed?**

A: Answers will vary depending on the configuration of the network.

---

## ACTIVITY 13-3: Discussing Internet Connections

---

**1. Which communication method uses existing telephone lines to transmit digital signals?**

- Cable modem
- DSL
- ISDN
- Fiber
- Satellite

**2. Which communication method uses the same physical media to provide high-speed transmission of data and television signals?**

- Cable modem
- DSL
- ISDN
- Fiber
- Satellite

**3. Which communication method uses light to carry signals?**

- Cable modem
- DSL
- ISDN
- Fiber
- Satellite

**4. If you have remote employees that need to connect to the corporate network but they are located in a remote area with no access to high-speed Internet service, what do you think is the best Internet connection method to use in this situation?**

A: Answers will vary, but will most likely include using either dial-up or satellite. However, because these employees need to access the corporate network through a VPN connection, satellite will probably provide the faster connection. In some cases, tethering to a cell phone or connecting to a wireless network device is an option, but this will all depend on how remote the employees' location is and whether they can get a strong cellular signal.

---

## ACTIVITY 13–5: Identifying Networking Tools

---

1. You need to determine if a cable is carrying a signal. Which networking tools might help you?  
 Crimpers  
 Cable testers  
 Multimeters  
 Punch down tool
  
  2. You need to connect cable wires to a patch panel. Which networking tool might help you?  
 Crimpers  
 Loopback plug  
 Punch down tool  
 Toner probe
- 

## ACTIVITY 15–7: Troubleshooting Mobile Device Hardware Issues

---

1. You received a user complaint about a laptop being extremely hot to the touch. What actions should you take in response to this issue?  
A: Overheating can be a sign that dust and dirt is restricting the necessary airflow within the device, so start by cleaning the ventilation duct with compressed air and then make sure that the device is getting proper air circulation around the outside of the case.
  
2. A user reports that when they plug in anything to the USB port on the laptop, that it is not recognized by the system. Is this something you can easily repair?  
A: Typically, the processor, the AC port, and USB ports are attached directly on the board and cannot be replaced without replacing the whole laptop motherboard.
  
3. Several laptops need to be replaced in the next fiscal cycle, but that doesn't begin for several more months. You want to improve functionality as much as possible by upgrading or replacing components in some of the laptops that are having problems. Which items are easily replaced in a laptop?  
A: Generally, you can replace the hard drive, RAM, the fan, the screen, the battery, and the keyboard.
  
4. Your organization has several tablet devices that are loaned out as needed when employees are traveling. Some users have reported problems getting the Bluetooth keyboard to work with the tablet. What should you do?  
A: There are a number of issues that can cause Bluetooth connectivity problems. The drivers might need to be updated. The devices might not have been set to discoverable mode. For security purposes, only enable discovery mode on your mobile device when want a Bluetooth device to find your device; otherwise, keep that setting disabled. The Bluetooth settings must be configured to allow devices to connect to the mobile device. This is also referred to as pairing.

5. A user reports that the touchscreen on their mobile device is not responding properly. What questions should you ask, and what steps might you take to resolve the issue?

A: You should ask if the touch screen appears to be scratched, cracked, or otherwise damaged. If so, make arrangements to have the touch screen replaced. If it is not damaged, ask if the user has cleaned the touchscreen surface. If they have not, remind them to use only a soft cloth moistened with eye glass cleaner to gently wipe the screen. If it still doesn't work properly, recalibrate the screen for the user, check for updates, or remove and reinstall drivers.

---

## ACTIVITY 17-1: Identifying Common Security Threats and Vulnerabilities

---

1. Early in the day a user called the help desk saying that his computer is running slowly and freezing up. Shortly after this user called, other help desk technicians who overheard your call also received calls from users who report similar symptoms. What type of attack might have occurred?

A: This is some type of malware. It might be a virus or worm.

2. John brought in the new tablet he just purchased and attempted to connect to the network. He knows the SSID of the wireless network and the password used to access the wireless network. He was denied access, and a warning message was displayed that he must contact the IT Department immediately. What happened and why did he receive the message?

A: John's new tablet probably does not meet the compliance requirements for network access. Being a new device, it might not have had updates and patches applied, it might not have appropriate virus protection installed, or it does not meet some other compliance requirement. This caused the system to appear as a non-compliant system to the network and network access was denied.

3. The contract ended recently for several workers who were hired for a specific project. The IT department has not yet removed all of those employees' login accounts. It appears that one of the accounts has been used to access the network, and a rootkit was installed on a server. You immediately contact the agency the employee was hired through and learn that the employee is out of the country, so it is unlikely that this person caused the problem. What actions do you need to take?

A: You will need to create an incident report, remove or disable the login accounts, isolate the infected server and possibly any user computers that communicate with the server, and remove the rootkit from the server.

---

## ACTIVITY 17-3: Examining Mobile Security

---

1. How can the use of mobile devices by employees affect the security of an organization as a whole?

A: Mobile devices can function much like a regular computer; therefore, when they are used to send and receive corporate emails, and to access systems and data within the corporate network, they are a vulnerability. If lost or stolen, the devices can be used to access sensitive data or launch attacks. Mobile devices should be secured just as any other system on the corporate network.

2. Examine some of the security features on a mobile device. Using the main menu, open the security settings for your device. What specific security settings are available?

A: Answers will vary, but may include a screen lock setting, device encryption options, and GPS tracking features.

---

## ACTIVITY 17-4: Identify Data Destruction and Disposal Methods

---

1. **What steps will you take to make sure that the storage devices in the equipment being sent for disposal will be properly sanitized?**  
A: Answers will vary, but should include zeroing out the drive with disk wiping software, possibly physically destroying the platters inside the hard drive, and verifying that the data is unreadable and unrecoverable.
2. **What steps will you take to make sure that the software you were given cannot be accessed?**  
A: Answers will vary, but might include physically destroying DVDs. For any device that you might potentially reuse, you can use disk wiping software to destroy the data and preserve use of the drive.

---

## ACTIVITY 18-1: Exploring NTFS Permissions

---

3. **What level of permissions did the Administrators group have?**
  - Full Control
  - Modify
  - Write
  - Read & Execute
4. **What level of permissions did the Users group have?**
  - Full Control
  - Modify
  - Write
  - Read & Execute
6. **How were the permissions in the LocalData folder different from the permissions on the C drive?**
  - Administrators did not have Full Control to the LocalData folder.
  - Users could not read files in the LocalData folder.
  - The permissions on the C drive were set explicitly; the permissions on the LocalData folder were inherited from the C drive.
  - The available permissions were not different.
8. **True or False? The permissions in the New Text Document file were inherited from the LocalData folder permissions.**
  - True
  - False

---

## ACTIVITY 18-3: Securing the Windows File System

---

4. You've been assigned to assist with securing certain Windows folders against unauthorized access. Only members of the Finance group should be able to view, access, and change files in the Finance folder that is stored on the server. How could you ensure that other employees cannot access the Finance folder?

A: Answers might include: disabling any inherited permissions for other users, and explicitly assigning permissions to the Finance group.

5. If Ali Lund is a member of the Finance group and she is also given explicit permissions of Read & Execute for the Finance folder, what are her effective permissions?

A: Her effective permissions will be the combination of the permissions she gets from the group and the explicit permissions assigned to her user object.

6. Consider what would happen if share permissions were also assigned to the Finance folder. How might Finance users be affected?

A: If the share permissions are more restrictive than the NTFS permissions, they will take precedence and could cause access issues for the Finance group members.

7. The sales representatives' laptops contain a lot of company confidential information. They want to keep this information secure as they travel. What recommendations would you make to help protect this data?

A: Answers might include implementing multifactor authentication. Many laptops now ship with fingerprint scanners, so you might be able to easily implement two-factor authentication (user name/password and biometrics). Or, you might implement virtual smart cards through Windows 8.1.

---

## ACTIVITY 19-1: Identifying System Errors

---

1. A user calls saying that her screen occasionally goes blue and the system shuts down. What should you advise her to do?

- Call the help desk the next time the shutdown is in progress.
- Reboot manually after the automatic restart.
- Record as much information from the top of the blue screen as she can so that you can research the particular error.
- Run the system in Safe Mode.

2. A user reports that his Microsoft® Word window has gone blank and he cannot type text. What are possible approaches to resolving his problem?

- Reboot the computer.
- Run another copy of Microsoft Word.
- Wait a few minutes to see if the application returns to normal.
- Use Task Manager to shut down the application if it has a status of "Not Responding."

3. A user reports that her monitor display is fuzzy and hard to look at. What is a possible cause of this problem?

- Display settings for the monitor are incorrectly configured.
- The power cord is unplugged.
- The monitor cable is not properly seated.
- The monitor device is disabled in Windows.

- 
4. A user reports that while she is editing a document, she receives an "invalid working directory" message from her application. What is the best diagnostic question to ask in response to this error?
- Did the application work yesterday?
  - Is anyone else having this problem?
  - Who installed the application?
  - Have you deleted any files or folders lately?

---

## ACTIVITY 19–3: Troubleshooting Mobile Device OSs and Applications

---

2. **What interesting troubleshooting tips did you find that you would like to share with the group, and where did you find them?**

A: Answers will vary. Some will demonstrate how to deal with a battery that drains quickly. Others will talk about locking the screen. Still others will demonstrate how to resolve Wi-Fi problems.

3. **Having heard the various problems and their resolutions, what mobile device issues do you think you will most likely encounter in your own environments?**

A: Answers will vary. Some students may not use one platform or another in their own environments. Others may already have a sense of the most common problems. Some may say that the most common problems are user-related.

---

## ACTIVITY 19–4: Troubleshooting Network Issues

---

1. You receive a call from a client who reports that she is unable to access any websites in Internet Explorer. While talking with this user, you verify that she can ping the server's IP address on her network segment, the IP address of the default gateway, and the IP address of a computer on another network segment. You also determine that none of the other users on her network can connect to websites in Internet Explorer. What might be the problem?

A: The problem is most likely that her network's DNS server is down.

2. One of your clients reports that he is unable to see computers when he opens the Network window. Which step should you take first?

- Determine if any of the other users on the network are experiencing problems.
- Ask the client to ping another computer on his network.
- Ask the client to verify that the DHCP server is running.
- Ask the client to run ipconfig /release and ipconfig /renew.

3. A user is trying to reach a website and is experiencing problems. How can you examine the path of the transmissions?

A: Use the tracert command to trace the routes of packets between various source and destination hosts. This can help you locate a packet looping between routers or the point at which a route fails.

4. A client reports that he is unable to connect to any computers on the network or the Internet. You have him run the ipconfig command, and all his TCP/IP addressing parameters are correct. When you have him ping other computers on the network, his computer is unable to reach them. This computer is the only one that is experiencing a problem. What should you check next?
- That the DHCP server is on and functioning properly.
  - That the default gateway is on and functioning properly.
  - That the DNS server is on and functioning properly.
  - That his computer's network cable is plugged into both the network card and the wall jack.
5. One of your network users is unable to connect to the SSH service, which is located on a different network. The error message indicates that the other network is unreachable. You verified that the network cable is intact and that the SSH service is up. What could be the probable cause of the error? (Select all that apply.)
- The network service is not up.
  - The resolv.conf file does not contain entries for the name server.
  - Network parameters, such as the IP address, the subnet mask, or the default gateway, are not set correctly.
  - The firewall is disabled.
6. You verified that the network service is running and that the network parameters are properly set. However, the user is still unable to connect to the network. What will be your first step to troubleshoot the network issue?
- Verify that the hostname is set.
  - Verify that the DNS entries are correct.
  - Verify that IP forwarding is enabled.
  - Verify that the ports of the service you are trying to access are open at the destination host.
7. True or False? To set the hostname permanently, you need to modify the /etc/hostname file.
- True
  - False

## ACTIVITY 19–5: Troubleshooting Common Security Issues

1. John has reported that a pop-up security alert keeps coming up when he switches application windows on his laptop. What do you suspect is going on with his computer?  
**A:** Often, malware is delivered through legitimate-looking methods, such as a Windows security alert. In this case, his laptop was likely infected with a virus.
2. You have been asked to provide a list of common malware symptoms for users to be aware of in order to prevent security breaches within your organization. What common symptoms would you provide?  
**A:** Answers will vary, but should include: keeping an eye out for unusual email messages that may be a hoax or social engineering attempt. Do not open or forward unrecognized email attachments. Avoid downloading any software from the Internet that has not been approved by the IT department.
3. True or False? The safest way to deal with unsolicited email is to delete it without opening it.  
 True  
 False

4. Alex reports that in the midst of composing an email at work, an unfamiliar pop-up appeared on his screen, indicating that his email connection has been dropped and that he should log on again by using the pop-up screen. What do you suggest he do in this situation?

**A:** First, you let him know that he was right to report the incident without entering the information in the pop-up window. Next, you should run an antivirus scan to identify if the computer is infected and remove any viruses until the system is clean.

# Glossary

## **802.11**

A family of specifications for wireless LAN communication.

## **802.11a**

A fast, secure, but relatively expensive protocol for wireless communication. The 802.11a protocol supports speeds up to 54 Mbps in the 5 GHz frequency.

## **802.11ac**

A specification for wireless data throughput at a rate of up to 2 Gbps in the 5 GHz range.

## **802.11b**

Also called Wi-Fi, short for "wireless fidelity," 802.11b is probably the most common and certainly the least expensive wireless network protocol used to transfer data among computers with wireless network cards or between a wireless computer or device and a wired LAN. The 802.11b protocol provides for an 11 Mbps transfer rate in the 2.4 GHz frequency.

## **802.11g**

A specification for wireless data throughput at the rate of up to 54 Mbps in the 2.4 GHz band that is a potential replacement for 802.11b.

## **802.11i**

See WPA2.

## **802.11n**

A specification for wireless data throughput at a rate of up to 600 Mbps in

the 2.4 GHz or 5 GHz range. Released in 2009.

## **accelerometer**

Mobile technology that can determine the orientation of a device with a sensor that measures the acceleration of the device direction.

## **ACL**

(access control list) A set of data (user names, passwords, time and date, IP addresses, MAC addresses, etc.) that is used to control access to a resource such as a computer, file, or network.

## **activity light**

An indicator on a network adapter that flickers when packets are received or sent.

## **ad hoc mode**

A method for wireless devices to communicate directly with each other without the use of an AP.

## **administrative share**

A hidden share created by default on every Windows system. If administrative shares are deleted, by default, the system re-creates them when it restarts.

## **adware**

Unwanted software loaded onto a system for the purposes of presenting commercial advertisements to the user.

**Aero**

A color scheme available in Windows Vista and Windows 7 that provides a visually rich experience, with a glossy and transparent interface and dynamic visual effects.

**AES**

(Advanced Encryption Standard) A symmetric 128-, 192-, or 256-bit block cipher based on the Rijndael algorithm developed by Belgian cryptographers Joan Daemen and Vincent Rijmen and adopted by the U.S. government as its encryption standard to replace DES.

**AIO MFD**

(all-in-one multi-function device) A small sized MFD for home users with basic printing, scanning, and copying functions.

**algorithm**

In encryption, the rule, system, or mechanism used to encrypt data.

**analog transmission**

The transfer of information in the form of a continuous wave.

**Android**

An operating system for mobile devices such as tablets and smartphones.

**anti-spyware software**

Software that is specifically designed to protect systems against spyware attacks.

**antivirus software**

An application that scans files for executable code that matches patterns known to be common to viruses, and monitors systems for activity associated with viruses.

**AP**

(access point) A device or software that facilitates communication and provides enhanced security to wireless devices.

**APIPA**

(Automatic Private IP Addressing) A feature of Windows that enables a DHCP client computer to configure itself

automatically with a random IP address in the range of 169.254.0.1 to 169.254.255.254 if there is no DHCP server available.

**argument**

A file name or directory name that indicates the files on which a command will operate.

**ARP**

(Address Resolution Protocol) A protocol that maps IP addresses to MAC addresses.

**aspect ratio**

A characteristic of display devices that indicates the ratio of width to height.

**attack**

A technique that is used to exploit a vulnerability in any application on a device without the authorization to do so.

**ATX**

An older motherboard that was introduced by Intel in 1995 to provide better I/O support, lower cost, easier use, and better processor support than even earlier form factors.

**AUP**

(acceptable use policy) A policy that includes the practices and guidelines that should be followed by employees when using and accessing company resources and computer equipment.

**authentication server**

A server or server role that determines whether or not access credentials supplied by a user should enable them to access resources.

**authenticator app**

An application that generates single-use security tokens that are used as part of two-step verification and multifactor authentication.

**auto negotiation**

Negotiates a speed that is compatible with the network router or switch.

**backlight**

The typical form of illumination used in a full-sized LCD display.

**badge**

Also called a security card, an identification card or token that can be used to swipe through an identification system or can be configured as a proximity card and activated automatically when the card is within a specified distance from the system.

**baseband**

A transmission scheme where a single signal sends data using the entire bandwidth of the transmission media. Compare with broadband.

**baseband RTOS**

(baseband real time operating system) See radio firmware.

**baseline**

A subset of a security profile, and a document that outlines the minimum level of security required for a system, device, network, or premises.

**battery backup**

See UPS.

**beamforming**

A feature of 802.11ac that transmits radio signals directly at a specific device using smart antennas.

**biometric lock**

A lock that is activated by biometric features, such as a fingerprint, voice, retina, or signature.

**biometrics**

An automated method of recognizing a person based on a physiological or behavioral characteristic unique to the individual, such as a retina pattern, fingerprint, or voice pattern.

**BIOS**

(Basic Input/Output System) A set of instructions that is stored in ROM and that is used to start the most basic services of a computer system.

**BIOS memory**

Special memory that keeps track of its data even when the power is turned off, and is stored in EEPROMs.

**BitLocker**

A security feature in Windows 7 and Windows Server 2008 that provides full disk encryption protection for your operating system as well as all the data stored on the operating system volume.

**BitLocker To Go**

A Windows security feature that encrypts removable storage devices such as USB flash drives or portable hard drives.

**blackout**

A complete loss of electrical power.

**Bluetooth**

A wireless radio technology that facilitates short-range (usually less than 30 feet) wireless communication between devices such as personal computers, laptop, mobile phones, wireless headsets, and gaming consoles, thus creating a wireless personal area network.

**BNC**

(Bayonet Neill-Concelman) A twist lock connector that is used with coaxial cable to carry radio frequencies to and from devices.

**Boot Camp**

An OS X app that enables users to install Microsoft Windows and then switch between OS X and the Windows operating system.

**boot process**

A series of sequential steps that occur when you start a computer, with the final result being that the OS is loaded and all components are functional.

**bootrec**

A command line tool used via the Command Prompt in the Windows Recovery Environment (only in Windows Vista and Windows 7) to troubleshoot or repair startup issues.

**botnet**

A set of devices that has been infected by a control program called a bot that enables attackers to exploit them and mount attacks.

**bridge**

A software-based network device that has the same functionality as a switch.

**brightness**

The amount of light emitted from a display device, as measured in lumens.

**broadband communication**

A category of network transmission technologies that provide high throughput by splitting communications pathways into multiple channels transmitted simultaneously over the network media.

**brownout**

A temporary power reduction that is used by electrical power companies to deal with high power demands.

**brute-force attack**

An attack that uses password-cracking software to attempt every possible alphanumeric password combination.

**BSOD**

(blue screen of death) A system error that is severe enough to stop all processes and shut the operating system down without warning.

**bus**

In a computer system, a group of wires that connect components. They provide a pathway for data transfer.

**BYOD**

(Bring Your Own Device) An organizational policy that enables employees to use their personal devices for work purposes.

**cable**

Transmissions that use a cable television connection and a specialized interface device known as a cable modem to provide high-speed Internet access to homes and small businesses.

**cable modem**

A hardware device that connects a subscriber's device to a service provider's cable systems.

**cable stripper**

A device that enables you to remove the protective coating from wiring to facilitate installing a media connector.

**cable tester**

An electrical instrument that verifies if a signal is present on a cable. Also called a media tester.

**cache memory**

High-speed memory that the CPU can access directly.

**CCFL**

(cold cathode fluorescent lamp) A light source that uses electrodes and mercury vapor to create ultraviolet light.

**CDFS**

(Compact Disc File System) A file system standard for optical disc media that is supported by multiple operating system types.

**cellular**

Uses radio signals to transmit network data over the cellular telephone system.

**chain of custody**

The record of evidence history from collection, to presentation in court, to disposal.

**chipset**

The set of chips on the system board that support the CPU and other basic functions.

**CIDR**

(Classless Inter Domain Routing) A subnetting method that selects a subnet mask that meets an individual network's networking and node requirements and then treats the mask like a 32-bit binary word.

**CIFS**

(Common Internet File System) A file and resource sharing protocol that is related to SMB.

**cipher**

A method for concealing the meaning of text.

**ciphertext**

Data that has been encoded with a cipher and is unreadable.

**cleartext**

The unencrypted form of data. Also called plaintext.

**CLI**

(command line interface) A text-based interface for an operating system.

**client**

A computer that makes use of the services and resources of other computers.

**client-side virtualization**

Takes place at the endpoints and separates the elements of a user's logical desktop environment—the applications, operating system, programs, etc.—and divides them from each other and from the physical hardware or a physical machine.

**client/server network**

A network in which some computers act as servers to provide special services for other client computers.

**cmdlet**

A lightweight command that runs in the Windows PowerShell environment.

**CMOS**

(Complementary Metal-Oxide-Semiconductor) An old style of static memory that was used to store information about the computer setup that the system BIOS refers to each time the computer is started.

**coax**

Pronounced "CO-ax." A common abbreviation for coaxial cable.

**coaxial cable**

A type of cable that features a central conductor surrounded by braided or foil shielding. A dielectric insulator separates the conductor and shield and the entire package is wrapped in an insulating layer called a jacket. The data signal is transmitted over the central conductor. The outer shielding serves to reduce electromagnetic interference.

**collate**

When printing multiple copies of a multipage document, the collection and combination of pages in the proper order.

**command line interpreter**

A program that implements the commands entered in the text interface.

**command prompt**

In a CLI, the area of the screen where users enter commands to interact with the OS.

**Component Services**

An administrative tool that is used to deploy component applications and configure the behaviors of components and applications on the system.

**component/RGB**

A type of analog video information that is transmitted or stored as two or more separate signals.

**composite video**

The format of an analog (picture only) signal before it is combined with a sound signal and modulated onto a radio frequency carrier.

**computer case**

The enclosure that holds all of the components of a PC.

**computer connection**

A hardware component that enables a PC to communicate with internal or external devices.

**computer forensics**

Collecting and analyzing data from storage devices, computer systems, networks, and wireless communications and presenting this information as a form of evidence in a court of law.

**Computer Management**

The primary administrative tool used to manage and configure the system. It consolidates several administrative utilities into a single console to provide easy access to the most common system tools.

**content filtering**

A method of setting limits on user browser sessions.

**controller**

See disk controller.

**cooling system**

A system unit component that prevents damage to computer parts by dissipating the heat generated inside a computer chassis.

**COPE**

(Corporate Owned, Personally Enabled) An organizational policy that enables employees to use company-owned devices for personal use.

**corona**

An assembly within a laser printer that contains a wire (the corona wire), which is responsible for charging the paper.

**CPU**

(central processing unit) The main chip on the system board, the CPU performs software instructions and mathematical and logical calculations. Also referred to as the microprocessor or processor.

**cryptographic**

See cryptography.

**cryptography**

The science of hiding information to protect sensitive information and communications from unauthorized access.

**data backup**

A system-maintenance task that enables you to store copies of critical files and folders on another medium for safekeeping.

**data container**

On a mobile device, a scheme for isolating business data from personal data.

**data restoration**

A system recovery task that enables you to access the backed-up data.

**Data Sources**

An administrative tool that uses Open Database Connectivity (ODBC) to move data

between different types of databases on the system.

**data synchronization**

The process of automatically merging and updating common data that is stored on multiple devices.

**data wiping**

A method used to remove any sensitive data from a mobile device and permanently delete it.

**daughter board**

Any circuit board that plugs into another circuit board.

**DB-15**

See VGA.

**dd**

A Linux command that copies and converts files to enable them to be transferred from one type of media to another.

**DDoS attack**

(Distributed Denial of Service) A type of denial of service (DoS) attack that uses multiple devices on disparate networks to launch the coordinated attack from many simultaneous sources.

**dead pixels**

Pixels that do not display light as expected and will show up as small black dots.

**deciphering**

The process of reversing a cipher.

**default gateway**

An IP address of the router that routes remote traffic from the device's local subnet to remote subnets.

**Defender**

The anti-spyware software that is included with Windows XP, Vista, and 7 installations.

**definition**

A code pattern that identifies a virus. Also called a signature.

**DEFRAG**

(Disk Defragmenter) A system utility available in all versions of Windows that scans and analyzes how file fragments are arranged and accessed on the hard disk.

**Device Manager**

In Windows, an administrative tool that is used to manage and configure system devices in a hardware profile.

**DHCP**

(Dynamic Host Configuration Protocol) A network service that provides automatic assignment of IP addresses and other TCP/IP configuration information on network systems that are configured as DHCP clients.

**dial-up line**

Local-loop phone connections that use modems and standard telephone technology.

**dictionary attack**

An attack that automates password guessing by comparing encrypted passwords against a predetermined list of possible password values.

**digital transmission**

The transfer of information in a signal that comprises only ones and zeroes.

**digitizer**

On touch screen displays, a layer of sensors between the LCD display and a layer of glass that enables the translation of the analog touch signal to a digital signal.

**DIMM**

(Dual In-line Memory Modules) A RAM form factor that is found in most systems and that has a 64-bit data path.

**direct thermal printer**

A thermal printer that uses heated pins to form images directly onto specially coated thermal paper.

**directory**

A component in a file system hierarchy that provides a container to organize files and other directories (folders). Also called a folder.

**directory service**

On a network, a centralized database that includes objects such as servers, clients, computers, user names, and passwords, and provides centralized administration and authentication.

**discovery mode**

A device mode that will transmit a friendly signal to another device in close proximity.

**disk controller**

Circuitry that manages the transfer of data to and from a disk drive, whether it is a hard disk drive or an optical disc drive. The disk controller provides the communication path between the CPU and the disk drive.

**Disk Defragmenter**

See DEFrag.

**disk duplexing**

Disk mirroring in which the two drives in the mirror each have a dedicated disk controller.

**disk maintenance**

The process of monitoring and adjusting the configuration of HDDs and the file systems contained on those HDDs.

**disk partition**

An isolated section of a disk that functions like a separate physical drive.

**display device**

A personal computer component that enables users to view the text and graphical data output from a computer.

**DisplayPort**

A digital display standard that aims to replace DVI and VGA standards.

**dissipative material**

A conductor, but with high resistance that loses its electrical charge slowly.

**distribution**

See distro.

**distro**

A complete Linux implementation, including kernel, shell, applications, and utilities, that is

packaged, distributed, and supported by a software vendor.

### **DLP**

(data loss prevention) Software or a software suite that helps protect data from being stolen while the data is moving across the network.

### **DMZ**

(demilitarized zone) A small section of a private network that is located between two firewalls and made available for public access.

### **DNS**

(Domain Name System) The primary name resolution service on the network that maps computer names to their associated IP addresses.

### **Dock**

A bar along the bottom or side of the screen that contains icons for apps that come with a Macintosh computer.

### **docking station**

Desktop devices that connect portable computers to standard desktop peripherals without the need to connect and disconnect the peripherals themselves when the user switches from stationary to mobile use.

### **domain**

A Microsoft network model that an administrator implements by grouping computers together for the purpose of sharing a centralized user account database. Sharing this user account database enables users to use these accounts to log on at any computer in the domain.

### **domain controller**

A server that stores the user account database for the domain and is responsible for authenticating users when they log on to the domain.

### **dongle**

A small hardware component that, when attached to a computing device, enables additional functionality such as wireless connectivity.

### **dot-matrix printer**

An impact printer that forms images out of dots on paper by using a set of pins to strike an inked ribbon.

### **DPI**

(dots per inch) A measure of the ink density in a printed document. Higher DPI measures tend to provide clearer and more distinct output.

### **drive rails**

Metal strips that can be screwed onto an internal drive before installation.

### **DRM**

(digital rights management) A way to control access to copyrighted content that is presented in digital format.

### **drone**

See zombie.

### **DSL**

(digital subscriber line) A broadband technology that transmits digital signals over existing phone lines.

### **dump file**

The file that stores the contents of a memory dump.

### **dumpe2fs**

A Linux utility that manages extended filesystems.

### **duplex scanning**

A feature that scans both sides of a document automatically.

### **duplexing**

The process that enables automatic printing on both sides of printing media, such as paper and envelopes.

### **DVI**

(Digital Video Interface) A video standard for transferring both analog and digital video signals.

### **dye sublimation printer**

See thermal dye transfer printer.

**dynamic addressing**

A method used to assign addresses using the DHCP service.

**e-reader**

A mobile digital device designed primarily for reading digital publications such as e-books and digital periodicals.

**EAS**

(Exchange ActiveSync) Microsoft's synchronization protocol that enables mobile devices to connect to an Exchange Server to access mail, calendar, and contacts.

**Easy Transfer**

A built-in data migration utility in Windows Vista and Windows 7 that helps transfer files, data, and settings from one personal computer to another.

**eavesdropping attack**

An attack that uses special monitoring software to intercept private network communications, either to steal the content of the communication itself or to obtain user names and passwords for future software attacks.

**ECC**

(Error Correction Code) An error correction method that uses several bits for error-checking.

**EEPROM**

(electronically erasable programmable read-only memory) A ROM chip that can be reprogrammed by using software from the BIOS or chip manufacturer through the flashing process.

**EFS**

(Encrypting File System) A file-encryption tool available on Windows systems that have partitions formatted with NT File System (NTFS).

**EIA**

(Electronic Industries Alliance) A standards and trades organization that developed industry standards for technologies such as network cabling. The EIA ceased operations in February 2011.

**electrical interference**

A general term for unwanted signals on the network media that can interfere with network transmissions.

**electrical noise**

The same as electrical interference.

**EMI**

(electromagnetic interference) The degradation of signal that occurs when a magnetic field around one electrical circuit interferes with the signal being carried on an adjacent circuit.

**eMMC**

(embedded Multi-Media Controller) A storage component that contains flash memory and a flash memory controller integrated onto the same silicon die.

**emulator**

The software installed that allows the computer to virtually run another operating system, or another instance of the same operating system.

**enciphering**

The process of applying a cipher.

**encryption**

The process of converting data into a form that is not easily recognized or understood by unauthorized entities.

**entry control roster**

A document for all visitors to sign in and out when entering and leaving the building.

**EP drum**

(Electrostatic Photographic drum) The component in a laser printer that carries the electrical charge to attract toner and then to transfer the toner to the paper.

**ERD**

(emergency repair disk) A Windows XP troubleshooting tool that stores the contents of the \Windows\Repair folder.

**eSATA**

(external Serial Advanced Technology Attachment) An external interface for SATA

connections, enabling you to connect external SATA drives to PCs.

### **ESD**

(electrostatic discharge) The phenomenon that occurs when electrons rush from one body with a static electrical charge to another with an unequal charge, following the path of least resistance.

### **Ethernet**

A family of networking technologies that provide connectivity by using Ethernet network adapters, contention-based media access, and twisted pair, coax, or fiber media.

### **Event Viewer**

An administrative tool that is used to view the contents of event logs, which contain information about significant events that occur on your computer.

### **expansion card**

A printed circuit board that is installed in a slot on a system board to provide special functions for customizing or extending a computer's capabilities. Also referred to as adapter card, I/O card, add-in, add-on, or board.

### **ExpressCard**

A mobile expansion card designed by the PCMCIA to replace traditional PC Cards to provide PCI Express and USB 2.0 connectivity.

### **ext2**

A native Linux filesystem.

### **ext3**

A native Linux filesystem that improves on the data recovery and integrity measures provided with ext2.

### **ext4**

A native Linux filesystem that offers backwards compatibility, journaling, and support for extremely large volumes, in addition to all the features of ext3.

### **external device**

A personal computer component that provides alternative input or output methods or additional storage.

### **external enclosure**

A plastic barrier that protects the inner workings of a hard drive.

### **F-connector**

A coaxial cable connector used to connect TV and FM antennas.

### **FC**

(Face Contact ) Connectors that use a heavy duty ferrule in the center for more mechanical stability than SMA or ST connectors.

### **fdisk**

A menu-driven utility program that is used for creating, modifying, or deleting partitions on a disk drive.

### **fiber**

A method used to connect devices to the Internet using fiber optic cable.

### **fiber optic cable**

A type of cable in which one or more glass or plastic strands, plus additional fiber strands or wraps, are surrounded by a protective outer jacket. Light pulses carry the signal through fiber optic cable.

### **file attribute**

A characteristic that can be associated with a file or folder that provides the operating system with important information about the file or folder and how it is intended to be used by system users.

### **file recovery software**

Software that can recover deleted files from your computer system.

### **file server**

A computer that stores programs and files that are intended to be shared among network users.

### **filesystem**

A method that is used by an operating system to store, retrieve, organize, and manage files and directories on mass storage devices.

### **filesystem integrity**

The degree of correctness and validity of a filesystem.

**Finder**

The file and folder management app that is included with OS X.

**firewall**

A software program or hardware device that protects networks from unauthorized data by blocking unsolicited traffic.

**firmware**

Software stored in memory chips that retains data whether or not power to the computer is on.

**first response**

Refers to the individual and the immediate actions that follow an incident.

**fixboot**

A command line tool used to create a new partition boot sector to a hard drive partition.

**fixmbr**

A command line tool used to repair the master boot recovery record of the boot partition.

**flash drive**

See SSD.

**flashing**

Updating firmware electronically.

**folder**

See directory.

**form factor**

The size and shape of a given component. Often used in terms of motherboard and drive characteristics.

**formed-character printer**

Any type of impact printer that functions like a typewriter, by pressing preformed characters against the ink ribbon to deposit the ink on the page.

**frequency**

The number of complete cycles per second in an analog wave or a radio wave.

**frontlight**

A form of lighting devices from the front of the display.

**fsck**

A Linux command that checks the integrity of a filesystem.

**fstab**

A configuration file that stores information about storage devices and partitions and where and how the partitions should be mounted.

**full duplex**

Permits simultaneous two-way communication.

**fuser assembly**

A component in a laser printer that uses two rollers to heat toner particles, melting them onto the paper.

**gadget**

A mini application in Windows that can perform an information display task.

**gaming PC**

A computer that comes equipped with powerful graphics capabilities, fast processing capabilities, and a large amount of memory, and that is intended for use in computer gaming environments.

**GAN**

(global area network) Any worldwide network.

**gateway**

A device, software, or system that converts data between incompatible systems.

**gdisk**

A Linux partition management utility for partitions in the Globally Unique Identifier (GUID) Partition Table (GPT) format.

**generator**

A power protection device that creates its own electricity through the use of motors.

**gestures**

Finger movements on a trackpad or mouse that enable a user to scroll, zoom, and navigate desktop, document, and application content.

**ghost cursor**

A cursor that jumps around on the screen randomly, or moves too slow, or opens windows and menus on its own.

**GNU parted**

A Linux partition management utility for new hard disks.

**GPRS**

(General Packet Radio Service) A standard for wireless communications that runs at speeds up to 115 kbps and that supports a wide range of bandwidths.

**GPS device**

(global positioning system device) A mobile digital device that provides navigational directions to reach specified destinations.

**GPU**

(graphics processing unit) An electronic circuit designed to rapidly manipulate and alter memory to accelerate the creation of images intended for display output.

**GRUB2**

(GRand Unified Bootloader 2) A program used in Linux distributions that loads operating system kernels.

**GUI**

(graphical user interface) A collection of icons, windows, and other screen elements that help users interact with an operating system.

**guideline**

A subset of a security profile, and a document that outlines best practices and recommendations to help conform to policies.

**half duplex**

Permits two-way communication, but only in one direction at a time.

**HDD**

(hard disk drive) A personal computer storage device that uses fixed media and magnetic data storage.

**HDMI**

(High Definition Multimedia Interface) A proprietary audio/video interface for transferring uncompressed video data and compressed or uncompressed digital audio data from a display controller to a compatible peripheral device over a single HDMI cable.

**heat sink**

A passive heat exchanger that dissipates heat from a source such as a CPU and transfers it, normally via an enlarged surface area, to another medium such as air or water.

**heavy-duty MFD**

A large network-enabled MFD capable of handling the documentation needs of an entire office.

**hertz**

A unit of measurement that indicates cycles or occurrences per second.

**Hibernate**

A power option available in Windows environments in which the computer will store whatever is currently in memory on the hard disk and shut down, and then return to the state it was in upon hibernation when it is awakened.

**high-level formatting**

See standard formatting.

**hoax**

Any message containing incorrect or misleading information that is disseminated to multiple users through unofficial channels.

**host firewall**

A firewall installed on a single or home computer.

**HTPC**

(home theater PC) A computer that is dedicated and configured to store and stream digital movies, either from the local hard drive or through an online subscription such as Netflix.

**hub**

A networking device used to connect the drops in a physical star topology network into a logical bus topology. Also called a multiport repeater.

**hypervisor**

In virtualization technology, an application that is installed on the host machine and is used to configure and manage the VMs running on the host.

**IANA**

(Internet Assigned Numbers Authority) An international agency that manages port assignments.

**iCloud**

A cloud storage solution that is accessed by using the user's Apple ID.

**IDS**

(intrusion detection system) Software or hardware, or a combination of both, that scans, audits, and monitors the security infrastructure for signs of attacks in progress and automates the intrusion detection process.

**IEEE**

(Institute of Electrical and Electronic Engineers) Pronounced "I-triple-E." An organization of scientists, engineers, and students of electronics and related fields whose technical and standards committees develop, publish, and revise computing and telecommunications standards.

**IEEE 1394 connection**

A PC connection that provides a high-speed interface for peripheral devices that are designed to use the Institute of Electrical and Electronic Engineers (IEEE) 1394 standard.

**ifconfig**

A Linux command for configuring network interfaces for Linux servers and workstations.

**IMAP4**

(Internet Mail Access Protocol) A protocol used to retrieve email messages and folders from a mail server.

**IMEI number**

(International Mobile Equipment Identity) A number that uniquely identifies a mobile device.

**impact printer**

Any type of printer that strikes a component directly against the paper or ink to create characters on the paper.

**impersonation**

An approach in which an attacker pretends to be someone they are not, typically an average user in distress, or a help-desk representative.

**IMSI number**

(International Mobile Subscriber Identity) A number that uniquely identifies a mobile subscriber.

**in-place upgrade**

The process of installing a newer version of an operating system without first removing the existing operating system that is currently installed on the computer.

**in-rush**

A surge or spike that is caused when a device that uses a large amount of current is started.

**incident management**

A set of practices and procedures that govern how an organization will respond to an incident in progress.

**incident report**

A record of any instance where a person is injured or computer equipment is damaged due to environmental issues. Also, a record of accidents involving hazardous materials, such as chemical spills, that could have an impact on the environment itself.

**infrastructure mode**

A method for wireless devices to communicate with other devices by first connecting to an AP.

**inkjet printer**

A printer that forms images by spraying ink on the paper.

**input device**

A personal computer component that enables users to enter data or instructions into a computer.

**interface**

The point at which two devices connect and communicate with each other.

**Internet appliance**

A relatively inexpensive PC that enables Internet access and a specific activity.

**inverter**

A laptop component that converts DC power to AC power for the display.

**iOS**

The operating system designed for Apple devices. It is the base software that allows all other applications to run on an iPhone, iPod touch, or iPad.

**IP**

(Internet Protocol) A group of rules for sending data across a network. Communication on the Internet is based on the IP protocol.

**IPS**

(in-plane switching) An LCD panel technology designed to resolve the quality issues inherent in TN panel technology, including strong viewing angle dependence and low-quality color reproduction.

**IPv4 address**

A 32-bit binary number assigned to a computer on a TCP/IP network.

**IPv6**

An Internet standard that increases the available pool of IP addresses by implementing a 128-bit binary address space.

**IPv6 address**

The unique 128 bit identification assigned to an interface on the IPv6 Internet.

**IR**

(infrared) A form of wireless transmission in which signals are sent via pulses of infrared light.

**IR waves**

(infrared waves) Electromagnetic waves with frequencies ranging from 300 GHz to 400 THz.

**ISDN**

A digital transmission technology that carries both voice and data over digital phone lines or PSTN wires.

**ISO 9660**

A filesystem found on CDs and DVDs.

**ISP**

(Internet Service Provider) A company that provides access to the Internet.

**iwconfig**

A Linux command for configuring wireless network interfaces for Linux servers and workstations.

**JFS**

A 64-bit journaling filesystem that is fast and reliable.

**key fob**

A security device small enough to attach to a key chain that contains identification information used to gain access to a physical entryway.

**Keychain**

A password management system included with OS X.

**KVM switch**

(keyboard, video, mouse) A device that enables a computer user to control multiple computers with a single keyboard and mouse, with the display sent to a single monitor.

**LAN**

(local area network) A self-contained network that spans a small area, such as a single building, floor, or room.

**landscape**

In printing, a page orientation that is wider than it is tall.

**laptop**

A complete computer system that is small, compact, lightweight, and portable.

**laser printer**

A type of printer that forms high-quality images on one page of paper at a time, by using a laser beam, toner, and an electrophotographic drum.

**LC**

(Local Connector) A small form factor ceramic ferrule connector for both single-mode and multimode fiber.

**LCD**

(Liquid Crystal Display) A type of flat-panel display that uses Cold Cathode Fluorescent Lamps as the source of backlight and that comes in large-screen sizes of 17 inches and more, with high screen resolution and high color depth.

**LDAP**

(Lightweight Directory Access Protocol) A communications protocol that defines how a client can access information, perform operations, and share directory data on a directory server.

**least privilege**

The principle that establishes that users and software should only have the minimal level of access that is necessary for them to perform the duties required of them.

**LED printer**

A type of printer that uses LEDs to print.

**line noise**

A power problem that is caused by a fluctuation in electrical current.

**line printer**

A type of impact printer that can print a full line of text at a time, rather than printing character by character.

**link light**

An indicator on a network adapter that lights up when a network signal is detected.

**Linux**

An open-standards UNIX derivative originally developed and released by a Finnish computer science student named Linus Torvalds.

**Linux distribution**

A complete Linux implementation, including kernel, shell, applications, and utilities, that is packaged, distributed, and supported by a software vendor.

**Linux rescue environment**

A standalone Linux program for troubleshooting a corrupt Linux installation.

**liquid-based cooling**

Cooling methods that circulate a liquid or liquefied gas, such as water or freon, past the CPU to keep it cool.

**Local Area Connection**

A Windows troubleshooting tool used to verify that the computer is connected to the network and able to send and receive data.

**local printer**

A logical printer that is managed by the local computer, where the print device is generally directly attached.

**Local Security Policy**

An administrative tool that is used to view and edit the security settings for group policies.

**local share**

A folder that is created on the local network by an individual user and then shared with other network users via shared folder permissions.

**local snapshot**

In OS X, a copy of altered files that is stored on the startup drive until the Time Machine backup drive is available.

**Local Users and Groups**

An administrative tool that is used to manage user accounts on the local system.

**lockup error**

An error condition that causes the system or an application to stop responding to user input.

**logic bomb**

A piece of code that sits dormant on a user's computer until it is triggered by a specific event, such as a specific date. Once the code is triggered, the logic bomb "detonates," erasing and corrupting data on the user's computer.

**loopback plug**

A special connector used for diagnosing network transmission problems that redirects

electrical signals back to the transmitting system.

### **LOS**

(Line-of-Sight) Wireless signals that travel over a direct visual path from a transmitter to a receiver.

### **low-level formatting**

The process of writing track sector markings on a hard disk.

### **LTFS**

(Linear Tape File Systems) An IBM specification that enables data stored on magnetic tapes to be accessed in a file format.

### **lumen**

The unit of measurement for visible light that is being emitted from a light source.

### **MAC address**

(Media Access Control address) Same as the physical address.

### **mail server**

A computer that stores incoming email messages and forwards outgoing email messages.

### **malicious software**

Any unwanted software that has the potential to damage a system or create a nuisance condition.

### **malware**

Any unwanted software that has the potential to damage a system, impede performance, or create a nuisance condition.

### **MAN**

(metropolitan area network) A network that covers an area equivalent to a city or other municipality.

### **man-in-the-middle attack**

A form of eavesdropping where the attacker makes an independent connection between two victims and relays information between the victims as if they are directly talking to each other over a closed connection, when in reality the attacker is controlling the information that travels between the victims.

### **mantrap**

Two sets of interlocking doors inside a small space, where the first set of doors must close before the second set opens.

### **manual pages**

A series of pages that contain the complete documentation specific to every Linux command. Also referred to as man pages.

### **MBR**

(Master Boot Record) The first sector of a partitioned storage device, used for booting the computer and often a target of malware.

### **media tester**

See cable tester.

### **memory**

A personal computer component that provides temporary workspace for the processor.

### **memory dump**

The process of writing the contents of system memory at the time of a stop error to a file on the hard disk prior to system shutdown.

### **memory module**

A system unit component that holds a group of memory chips that act as a single memory chip.

### **MFD**

(multi-function device) A piece of office equipment that performs the functions of a number of other specialized devices.

### **microATX**

Introduced in late 1997, and is often referred to as µATX, and has a maximum size of 9.6 inches by 9.6 inches.

### **MicroDIMM**

(Micro Dual Inline Memory Module) A memory module standard used in some laptops.

### **Mini-ATX**

A smaller version of the full ATX board with a maximum size of 11.2 inches by 8.2 inches.

**Mini-BNC**

A bayonet-style connector using the traditional BNC connection method.

**Mini-HDMI**

(Mini High-Definition Multimedia Interface) A smaller version of the full size HDMI connector, except that it is specified for use with portable devices.

**mini-ITX**

A small compact board that fit the same form factor as the ATX, and the micro-ATX boards. They have a maximum size of 6.7 inches by 6.6 inches.

**Mini-PCIe**

(PCI Express Mini Card) An extremely small expansion card, often just a few centimeters in length, used to increase communication abilities by providing network adapters or modems and supports various connections and buses.

**mirroring**

A disk fault-tolerance method in which data from an entire partition is copied onto a second drive.

**Mission Control**

A feature of OS X that allows users to use multiple Spaces as if they were multiple desktops.

**mkfs**

A command used to build a Linux filesystem on a device such as a hard disk partition.

**mobile digital device**

An electronic device that provides computing power in a portable format.

**modem**

A device that converts digital data to an analog signal that can be sent over a telephone line.

**motherboard**

The main circuit board in a computer that acts as the backbone for the entire computer system. Also referred to as the system board.

**MSCONFIG**

A system utility that is specifically used to troubleshoot any issues with the system startup process.

**MSDS**

(Material Safety Data Sheet) A technical bulletin designed to give users and emergency personnel information about the proper procedures of storage and handling of a hazardous substance.

**MT-RJ**

(Mechanical Transfer Registered Jack) Also called a Fiber Jack connector, is a compact snap-to-lock connector used with multimode fiber.

**multi-factor authentication**

Any authentication scheme that requires validation of at least two of the possible authentication factors.

**multimedia device**

A computer peripheral or internal component that transfers sound, images, or both to or from a PC.

**multimeter**

An electronic instrument used to measure voltage, current, and resistance.

**multitouch**

The technology used on the surface of the touch screen on tablets and other mobile devices that can recognize more than one contact on the surface at once.

**mutual authentication**

A security mechanism that requires that each party in a communication verifies its identity.

**Napier's Bones**

A set of rectangular rods with numbers etched on them that let users do multiplication by adding the numbers on properly positioned rods. A precursor to the slide rule.

**NAT**

(Network Address Translation) A simple form of Internet connection and security that conceals internal addressing schemes from the public Internet.

**native resolution**

The fixed resolution for LCD or other flat panel display devices.

**network**

A group of computers that are connected together to communicate and share resources.

**network directory**

See directory service.

**network-based firewall**

A hardware/software combination that protects all the computers on a network behind the firewall.

**network-based printer**

A shared print device managed by a network print server. It's represented as a logical printer object on the client computer that accesses the server.

**network-connected printer**

Any print device than can connect directly to the network with a network adapter rather than using a physical cable to connect to a local computer or print server device.

**NFC**

(near field communications) A wireless communication method that enables wireless devices to establish radio communications by touching them together or by bringing them into close proximity with each other, typically within 10 cm or less.

**NIC**

(network interface card) An expansion card that enables a PC to connect to a LAN. Also referred to as a network adapter.

**non-compliant system**

Any system that tries to connect to an organization's network and that doesn't meet the minimum requirements of the organizational network, as defined by corporate security policies.

**Northbridge**

A component of the chipset that controls the system memory and the AGP video ports, and sometimes the cache memory.

**OLED display**

(organic light emitting diode) A type of LED flat panel display device that uses organic compounds that emit light when subjected to an electric current.

**Open Handset Alliance**

An association of 84 firms for developing open standards for mobile devices.

**OpenSSH**

An open source implementation of the SSH protocol that is included with most Linux distributions. See SSH.

**optical disc**

A personal computer storage device that stores data optically, rather than magnetically.

**optical drive**

A computer drive that is either internal or external to a computer system that reads and writes data to an optical disc.

**organizational policy**

A document that conveys the corporate guidelines and philosophy to employees.

**orientation**

In printing, the position of the page and the direction of the content printed on the page.

**OS X**

The proprietary operating system developed by Apple® Computing, Inc. and deployed on all Apple computers.

**overvoltage**

A power condition where the voltage in a circuit is raised above the circuit's upper voltage limit.

**page**

A section of memory addresses in which a unit of data can be stored.

**page fault**

An interrupt generated when an application requests data that is no longer present in its virtual memory location.

**pagefile**

In a virtual-memory system, the section of the hard disk used to store memory contents that have been swapped out of physical RAM. In Windows systems, the pagefile is called Pagefile.sys.

**paging**

See swapping.

**pairing**

The process two devices use to establish a wireless connection through Bluetooth.

**PAN**

(personal area network) A network of devices used by a single individual.

**parity**

An error correction method for electronic communications.

**partition management**

The process of creating, destroying, and manipulating partitions to optimize system performance.

**partitioning**

The process of dividing a single hard disk into isolated sections that function as separate physical hard drives, called partitions.

**partprobe**

A Linux program that updates the kernel with partition table changes.

**patch**

A fix or update for a software program or application, designed to eliminate known bugs or vulnerabilities and improve performance.

**patch management**

The practice of monitoring for, evaluating, testing, and installing software patches and updates.

**PCI**

(Peripheral Component Interconnect) See PCI bus.

**PCI bus**

(Peripheral Component Interconnect bus) A peripheral bus commonly used in PCs that

provides a high-speed data path between the CPU and peripheral devices.

**PCI Express**

(Peripheral Component Interconnect Express) A video adapter bus that is based on the PCI computer bus. PCIe supports significantly enhanced performance over that of AGP.

**PCIe**

(Peripheral Component Interconnect Express) See PCI Express.

**peer-to-peer network**

A network in which resource sharing, processing, and communications control are completely decentralized.

**Performance Monitor**

An administrative tool that monitors the state of services or daemons, processes, and resources on a system.

**peripheral device**

See external device.

**permissions**

In Windows, security settings that control access to individual objects, such as files.

**personal firewall**

See host firewall

**phablet**

A mobile digital device that is larger than a standard sized smartphone and smaller than a tablet.

**pharming**

Similar to phishing, this type of social engineering attack redirects a request for a website, typically an e-commerce site, to a similar-looking, but fake, website.

**phishing**

A type of email-based social engineering attack in which the attacker sends email from a spoofed source, such as a bank, to try to elicit private information from the victim.

**physical address**

For network adapter cards, a globally unique hexadecimal number burned into every adapter by the manufacturer.

**physical security**

The implementation and practice of various control mechanisms that are intended to restrict physical access to facilities.

**piconet**

A network of two to eight Bluetooth-enabled devices.

**PictBridge**

A technology that allows images to be printed directly on a printer from digital cameras.

**PII**

(personally identifiable information) Any information that can be used by itself or in combination with additional information as a way to identify, contact, or find a single person, or to identify a particular individual by using the various pieces of information together to determine the person's identity.

**pixel**

The smallest discrete element on a display. A single pixel is composed of a red, a blue, and a green dot.

**plaintext**

Unencoded data. Also called cleartext.

**plasma display**

A type of flat panel that uses a gas mixture placed between two sheets of glass that have electrodes attached to their surfaces.

**plastics**

The hard surfaces that protect the internal components of a laptop.

**plenum**

An air handling space, including ducts and other parts of the HVAC system in a building.

**plenum cable**

A grade of cable that does not give off noxious or poisonous gases when burned. Unlike PVC cable, plenum cable can be run through the plenum and firebreak walls.

**PoE**

(Power-over-Ethernet) An emerging technology standard that enables both power and data to be transmitted over an Ethernet cable.

**pointer drift**

A situation where the mouse pointer moves across the screen without the user touching the touchpad or mouse.

**policy**

A subset of a security profile, and a document that outlines the specific requirements and rules everyone must meet.

**pop-up**

Windows or frames that load and appear automatically when a user connects to a particular web page.

**POP3**

(Post Office Protocol version 3) A protocol used to retrieve email from a mailbox on the mail server.

**port**

A hardware connection interface on a personal computer that enables devices to be connected to the computer, or the endpoint of a logical connection that client computers use to connect to specific server programs.

**port filtering**

A technique of selectively enabling or disabling TCP and UDP ports on computers or network devices. It ensures that no traffic, except for the protocol that the administrator has chosen to allow, can pass through an open port.

**port replicator**

A scaled-down version of a docking station with only the standard ports available.

**portrait**

In printing, a page orientation that is taller than it is wide.

**POST**

(Power-On Self Test) A built-in diagnostic program that is run every time a personal computer starts up.

**POST card**

(Power-On Self Test card) A card that can be plugged directly into the motherboard in an available expansion card slot that can read and display any error codes that get generated during the POST process of a computer.

**power sag**

See sag.

**power supply**

An internal computer component that converts line voltage AC power from an electrical outlet to the low-voltage DC power needed by system components.

**power supply tester**

A tool that connects to the power supply's 24-pin connector that tests the functionality of the unit.

**pre-installation environment**

A lighter version of Windows or Windows Server that can be installed in either 32- or 64-bit versions.

**prestaging**

The process of creating computer accounts in Windows Active Directory before joining the computers to the domain.

**PRI**

(Preferred Roaming Index) An index that works with the PRL to provide the best data/voice quality to a phone while roaming.

**Print Management**

An administrative tool that is used to view and manage all of the printers and print servers installed on a network.

**print quality**

A combination of parameters that define the appearance of the printed output.

**print queue**

A list of print jobs waiting to print.

**print server**

A computer that enables network users to share printers.

**printer**

An output device that produces text and images from electronic content onto physical media such as paper or transparency film.

**privacy filter**

A cover for a device's screen, making it difficult for anyone to read the screen who is not positioned directly in front of the screen.

**private IP address**

Addresses used by organizations for nodes that require IP connectivity within their enterprise network, but do not require external connections to the global Internet.

**PRL**

(Preferred Roaming List) A database built by CDMA service carriers to indicate which radio bands should be used when connecting to a cell tower.

**procedure**

A subset of a security profile, and a document that provides detailed information about specific devices and technologies that support policies.

**process table**

A record that summarizes the current running processes on a system.

**proxy**

A system that acts as an intermediary for requests for resources.

**proxy server**

A computer or application that isolates internal clients from external servers by downloading and storing files on behalf of the clients.

**PSTN**

(Public Switched Telephone Network) An international telephone system that carries analog voice data.

**public IP addresses**

Addresses that can be used by organizations that can also be shared with external networks.

**punch down tool**

A tool used in a wiring closet to connect cable wires directly to a patch panel.

**PVC**

(polyvinyl chloride) A flexible rubber-like plastic used to surround some twisted pair cabling. It is flexible and inexpensive, but gives off noxious or poisonous gases when burned.

**QoS**

(Quality of Service) A set of parameters that controls the level of quality provided to different types of network traffic.

**radio firmware**

In a mobile device, memory that contains an operating system that is separate from the end-user operating system (for example, Android or iOS) and that controls all of the low-level timing-dependent functions of the mobile device.

**radio networking**

A form of wireless communication in which signals are sent via RF waves, in the 10 KHz to 1 GHz range, to wireless antennas.

**RAID**

(Redundant Array of Independent or Inexpensive Disks) A set of vendor-independent specifications for fault-tolerant configurations on multiple-disk systems.

**RAM**

(Random Access Memory) A computer storage method that functions as a computer's main memory.

**RAM module**

See RAM chip.

**rapid elasticity**

A cloud computing feature that provides seamless, scalable provisioning.

**RCA**

(Radio Corporation of America) A cable and connector that is used to carry audio and video transmissions to and from a variety of devices such as TVs, digital cameras, and gaming systems.

**ReadyBoost**

A performance enhancer, available on Windows Vista and Windows 7, that allows the user to supplement the computer's memory

with an external storage device like a flash drive.

**recovery image**

A file used by Windows to refresh your PC.

**refresh rate**

The number of times per second that the monitor is “refreshed,” or scanned to illuminate the pixels.

**Registry**

The central configuration database where Windows stores and retrieves startup settings, hardware and software configuration information, and information for local user accounts.

**regsvr32**

A troubleshooting utility that registers and unregisters OLE controls such as DLL and ActiveX files.

**ReiserFS**

A filesystem that handles small files more efficiently and faster than ext2 and ext3.

**Remote Desktop**

A software application that operates a Windows computer from a remote location.

**Remote Disc**

A feature of OS X that enables users to access external drives or share discs from another computer.

**resolution**

The number of pixels that make up the dimension of a display, represented in a ratio value as the number of horizontal pixels by vertical pixels.

**RF**

(radio frequency) Any of the electromagnetic wave frequencies that lie in the range extending from around 3 kHz to 300 GHz, which include those frequencies used for communications or radar signals. Commonly used as a synonym for wireless communication.

**RF**

(radio frequency) A frequency in which network or other communications take place

using radio waves in the 10 KHz to 1 GHz range.

### **RFI**

(radio frequency interference) See EMI.

### **RFID badge**

A security card that contains a tag that reacts with the radio frequency of the identification system to allow or deny access.

### **RIMM**

(Rambus Inline Memory Modules) A RAM form factor that has a metal cover that acts as a heat sink. Although they have the same number of pins, RIMMs have different pin settings and are not interchangeable with DIMMs and SDRAM.

### **riser card**

A board that is plugged into the system board and provides additional slots for adapter cards.

### **ROM**

(Read-Only Memory) Memory that saves and stores system data without a constant power source.

### **rootkit**

Malicious code that is designed to hide the existence of processes or programs from normal detection methods and to gain continuous privileged access to a computer system.

### **rotation method**

The schedule that determines how many backup tapes or other media sets are needed, and the sequence in which they are used and reused.

### **router**

A networking device that connects multiple networks that use the same protocol.

### **RPM**

(Red Hat Package Manager) A tool that provides a standard software installation mechanism, information about installed software packages, and a method for uninstalling and upgrading existing software packages.

### **RSA token**

A small device that includes cryptographic keys, a digital signature, or even biometric information that is verified against an identification system to allow or deny access to a physical location, system, or network location.

### **S-Video**

An analog video signal that carries the video data as two separate signals (brightness and color). S-Video works in 480i or 576i resolution.

### **Safe Mode**

A Windows system startup method that loads only a minimal set of drivers and services and that is used in troubleshooting Windows computers.

### **sag**

A momentary low-voltage power failure.

### **SATA**

(Serial Advanced Technology Attachment) A type of hard drive that requires a serial data channel to connect the drive controller and the disk drives.

### **SATA connection**

(Serial Advanced Technology Attachment connection) A drive connection standard that provides a serial data channel between the drive controller and the disk drives.

### **satellite**

Provides extremely long-range wireless network transmissions to relay network signals from the network service provider to individual customers.

### **SC**

(Subscriber Connector or Standard Connector) Box-shaped connectors that snap into a receptacle. SC connectors are often used in a duplex configuration where two fibers are terminated into two SC connectors that are molded together.

### **SCSI ID**

Identifiers assigned to each SCSI device connected to the bus. The ID numbers range from 1 to 15.

**security control**

A safeguard or prevention method to avoid, counteract, or minimize security risks relating to personal or company property.

**security incident**

A specific instance of a risk event occurring, whether or not it causes damage.

**security incident report**

Documentation of a security incident, including the type and severity of the incident, personnel involved in the incident, a description of the incident, and any mitigation actions taken.

**security policy**

A formalized statement that defines how security will be implemented within a particular organization.

**security profile**

A large, comprehensive document that describes the security measures for an organization.

**server**

A computer that provides services and resources on the network.

**server virtualization**

Takes place centrally on a server and utilizes one logical device, typically the server, to act as the host machine for the “guest” machines that virtually use the applications and programs provided by the host.

**server-side virtualization**

See server virtualization.

**Service Pack**

Comprehensive software update that generally includes all prior patches and updates, but which can also include important new features and functions.

**set-top box**

A device that converts video content to a format that can be viewed on a television. Also referred to as streaming players or media players.

**sfc**

(System File Checker) A command line tool used to verify system files and replace them, if needed.

**sfdisk**

A Linux partition management utility.

**Shadow Copy**

A feature available on Windows XP and newer operating systems that creates backup copies or snapshots of the system's data and stores them locally or to an external location, either manually or at regularly scheduled intervals.

**share**

A network resource, such as a disk, folder, or printer, that is available to other computer users on the network.

**shell**

A component that interacts directly with users and functions as the command interpreter for the Linux operating system.

**shoulder surfing**

A human-based attack where the goal is to look over the shoulder of an individual as he or she enters password information or a PIN.

**Sidebar**

A designated area of the Windows 7 and Windows Vista desktop, displayed vertically along the side of the desktop, where users can add gadgets of their choice to provide information and access to frequently used tools or programs.

**signal loss**

The weakening of a radio signal from a cell tower such that your phone cannot connect to the network.

**signature**

A code pattern that identifies a virus. Also called a definition.

**SIMM**

(Single In-line Memory Modules) A RAM form factor with a 32-bit data path.

**SLA**

(Service Level Agreement) An agreement entered into by the transmitter, or ISP, and the receiver, or subscriber.

**Sleep**

A power option available in Windows Vista, Windows 7, Windows Server 2008, and Apple OSs, in which the computer conserves as much energy as possible by cutting off power to the parts of the machine that are not necessary to function, excluding RAM.

**SMA**

(Sub Multi Assembly or Sub Miniature type A) Connectors that use a threaded ferrule on the outside to lock the connector in place.

**SMART**

(Self-Monitoring, Analysis, and Reporting Technology) A monitoring system that can help anticipate storage drive failures due to excess heat, excess noise, damaged sectors, or read/write errors.

**smart camera**

A digital camera that includes a processor, memory, cellular and Wi-Fi support, and a mobile operating system.

**smart card**

A device similar to a credit card that can store authentication information, such as a user's private key, on an embedded microchip.

**smart TV**

A hybrid device that is basically a television set with web and Internet features built into it.

**smart watch**

A multipurpose device that runs computing applications and that is worn on a person's wrist.

**smartphone**

A mobile digital device that combines the functionality of a portable phone with that of media players, GPS navigation units, personal digital assistants, and cameras.

**SMB**

(Server Message Block) A protocol that works on the Application layer and is used to share

files, serial ports, printers, and communications devices, including mail slots and named pipes, between computers.

**snapshot printer**

A printer that produces snapshot-sized images of acceptable photographic quality.

**sniffing attack**

See eavesdropping attack.

**SNMP**

(Simple Network Management Protocol) An Application-layer protocol used to exchange information between network devices.

**social engineering attack**

A type of attack where the goal is to obtain sensitive data, including user names and passwords, from network users through deception and trickery.

**SODIMM**

(Small Outline Dual In-line Memory Module) Memory that is half the size of DIMMs, are available in 32- or 64-bit data paths, and are commonly found in laptops and iMac systems.

**software diagnostic tool**

A computer repair program that can analyze hardware and software components and test them for problems. Also referred to as software diagnostic utility.

**SOHO MFD**

(small office/home office multi-function device) A medium-sized network-enabled MFD suitable for small and home offices with enhanced printing, scanning, copying, and faxing functions.

**SOHO network**

(small office/home office) A small network that provides connectivity and resource sharing for a small office or home office.

**soldered**

A means of securing electronic components to a circuit board by using a combination of lead, tin, and silver (solder) and a tool called a soldering iron.

**solid ink printer**

A type of printer that uses ink from melted solid-ink sticks.

**Southbridge**

A component of the chipset that controls input/output functions, the system clock, drives and buses, APM power management, and various other devices.

**space**

In OS X, a virtual desktop consisting of a collection of related windows, as created and managed by Mission Control.

**spam**

Originally, frequent and repetitive postings in electronic bulletin boards; more commonly, unsolicited or distasteful commercial email from anonymous sources.

**SPDIF**

(Sony Phillips Digital Interconnect Format) A digital format signal used to connect audio devices to output audio signals over a short distance.

**spear phishing**

See whaling.

**speed light**

An indicator on a network adapter that shows whether the adapter is operating at 10 Mbps, 100 Mbps, or 1,000 Mbps.

**spike**

A very short increase in the electrical supply voltage or current carried on any wire such as a power line, phone lines, and network lines. Usually lasts only a few milliseconds.

**spim**

An IM-based attack similar to spam that is propagated through instant messaging instead of through email.

**spoofing**

A human-based or software-based attack where the goal is to pretend to be someone else for the purpose of identity concealment. Spoofing can occur in IP addresses, MAC addresses, and email.

**Spot Light**

A feature of OS X that enables users to search for apps, documents, images, and other files.

**spyware**

Unwanted software that collects personal user data from a system and transmits it to a third party.

**SSD**

(solid state drive) A personal computer storage device that stores data in non-volatile special memory instead of on disks or tape.

**SSH**

(Secure Shell) A protocol that enables a user or application to log on to another computer over a network, execute commands, and manage files.

**SSHD**

(solid state hybrid drive) A personal computer storage device that offers the best features of solid state and magnetic data storage by combining the traditional rotating platters of a magnetic HDD and a small amount of high-speed flash memory on a single drive.

**SSID**

(Service Set Identifier) A 32-bit alphanumeric string that identifies a wireless access point and all devices that connect to it.

**SSL**

(Secure Sockets Layer) A security protocol that uses certificates for authentication and encryption to protect web communication.

**ST**

(Straight Tip) Connects multimode fiber. ST connectors look like BNC connectors.

**standard**

A subset of a security profile, and a tactical document that specifies processes to follow to meet policy requirements.

**standard formatting**

An operating system function that builds file systems on drives and partitions.

**standby**

A power-saving mode where the computer cuts power to the hard drive and peripherals while storing current data in RAM.

**static addressing**

Configuring TCP/IP statically on a network. Requires that an administrator visit each node to manually enter IP address information for that node.

**static electricity**

The buildup of stationary electrical charge on any object.

**stop error**

A system error severe enough to stop all processes and shut the system down without warning. Often referred to as "blue-screen errors" in Windows because they generate an error message screen with a blue background.

**storage device**

A computer component that enables users to save data for reuse at a later time, even after the personal computer is shut down and restarted.

**Storage Spaces**

The Windows 8/8.1 implementation of RAID.

**striping**

A disk-performance-enhancement feature in which data is spread across multiple drives to improve read and write access speeds.

**strong password**

A password that meets the complexity requirements that are set by a system administrator and documented in a security policy or a password policy.

**stuck pixels**

Pixels that only show one color of light, so they appear out of place when the display is on.

**subnet mask**

A 32-bit number that is assigned to each host to divide the 32-bit binary IP address into network and node portions.

**sudo**

(super user do) A Linux command that enables users to run programs with the security privileges of the root user.

**surge**

A sudden sharp increase in voltage or current that can last up to 50 microseconds.

**surge suppressor**

A power protection device that provides power protection circuits that can reduce or eliminate the impact of surges and spikes.

**Suspend**

A power option available in Linux, in which the computer conserves as much energy as possible by cutting off power to the parts of the machine that are not necessary to function, excluding RAM.

**swap**

A portion of the hard disk that is used in situations when Linux runs out of physical memory and needs more of it.

**swapping**

In a virtual memory system, the process of moving data back and forth from physical RAM to the pagefile. Also called paging.

**switch**

A smart network hardware device that joins multiple network segments together.

**system BIOS**

The BIOS that sets the computer's configuration and environment when the system is powered on.

**system board**

The same as motherboard.

**system bus**

The primary communication pathway between a CPU and other parts of the chipset. The system bus enables data transfer between the CPU, BIOS, memory, and the other buses in the computer. Also referred to as frontside bus or local bus.

**System Configuration**

An administrative tool that is used to identify and manage issues that may be causing the system to run improperly at startup.

**system files**

The files necessary for the operating system to function properly.

**system image**

A copy of Windows, applications, system settings, and data files that is stored in a separate location than where the originals of these items are stored.

**System Restore**

A utility available in Windows XP, Windows Vista, and Windows 7 that monitors the system for changes to core system files, drivers, and the Registry, and creates restore points to be used to help restore the system if a failure occurs.

**system restore point**

A snapshot of the system configuration at a given moment in time that contains information about any changes to these components and is stored on the computer's hard disk. Restore points can be used to restore system settings to an earlier state without affecting changes in user data since that time.

**system unit**

A personal computer component that includes other devices necessary for the computer to function, including the chassis, power supply, cooling system, system board, microprocessor, memory chips, disk drives, adapter cards, and ports for connecting external devices. Often referred to as a box, main unit, or base unit.

**tablet**

A mobile device that includes an integrated touch screen display, virtual onscreen keyboard, and flash memory for data storage.

**tape drive**

A personal computer storage device that stores data magnetically on a removable tape.

**Task Manager**

A basic system-diagnostic and performance-monitoring tool included with the Windows operating system.

**Task Scheduler**

An administrative tool that allows the user to create and manage certain system tasks that will be automatically carried out by the computer at predetermined times.

**TCP**

(Transmission Control Protocol) A connection-oriented, guaranteed-delivery protocol used to send data packets between computers over a network such as the Internet.

**TCP/IP**

(Transmission Control Protocol/Internet Protocol) A nonproprietary, routable network protocol suite that enables computers to communicate over a network, including the Internet.

**termination**

Adding a resistor to the end of a coax network segment to prevent reflections that would interfere with the proper reception of network signals.

**TFT**

(thin film transistor) A display type commonly used in laptops.

**thermal dye transfer printer**

A sophisticated type of color printer that uses heat to diffuse dye from color ribbons onto special paper or transparency blanks to produce continuous-tone output similar in quality to a photographic print. Also called dye sublimation printer.

**thermal paper**

Paper that contains a chemical designed to react with the heating element of a thermal printer to create images on paper.

**thermal paste**

A paste that is used to connect a heat sink to a CPU to provide a liquid thermally conductive compound gel that fills any gaps between the CPU and the heat sink to permit a more

efficient transference of heat from the processor to the heat sink.

### **thermal printer**

Any printer that uses heat to create the image on the paper with dye or ink from ribbons or with heated pins.

### **thermal wax transfer printer**

A printer that uses a thermal printhead to melt wax-based ink from a transfer ribbon onto the paper.

### **thick client**

A business computer that performs most or all computing functions on its own. Also referred to as a fat client.

### **thin client**

A business computer that relies heavily on another system, typically a server, to run most of its programs, processes, and services.

### **Thunderbolt connection**

A hardware interface that supports connecting a wide variety of peripheral devices to PCs and that can use optical fiber or copper wire to transmit signals.

### **TIA**

(Telecommunication Industry Association) A standards and trades organization that develops industry standards for technologies such as network cabling.

### **Time Machine**

An OS X application that provides automated file backups.

### **TKIP**

(Temporal Key Integrity Protocol) A security protocol created by the IEEE 802.11i task group to replace WEP.

### **TLS**

(Transport Layer Security) A security protocol that protects sensitive communication from eavesdropping and tampering by using a secure, encrypted, and authenticated channel over a TCP/IP connection.

### **TN**

(twisted nematic) An LCD panel technology where the panel is black when no electric current is running through the liquid crystal cells because the cells align themselves in a twisted state. When an electric current is applied, the liquid crystal cells untwist, allowing light to pass through, resulting in a white display screen.

### **token**

A physical or virtual object that stores authentication information.

### **tone generator**

An electronic device that sends an electrical signal through one set of UTP cables.

### **tone locator**

An electronic device that emits an audible tone when it detects a signal in a set of wires.

### **tone probe**

See tone locator.

### **toner**

An electrostatic-sensitive dry ink substance used in laser printers.

### **traces**

Wires etched on to the motherboard to provide electrical pathways.

### **trackpoint**

A small button found on some laptops that enables you to move the mouse pointer when no mouse is connected to the computer.

### **transistors**

Switches that are etched on one sliver of a semiconductor that can be opened or closed when conducting electricity.

### **triboelectric generation**

The use of friction to create a static charge.

### **Trojan horse**

Malicious code that masquerades as a harmless file. When a user executes it, thinking it is a harmless application, it destroys and corrupts data on the user's hard drive.

**twisted pair**

A type of cable in which multiple insulated conductors are twisted together and clad in a protective and insulating outer jacket.

**UAC**

(User Account Control) An enhanced security feature of Windows Vista and Windows 7 that aims to limit the privileges of a standard user unless a computer administrator decides otherwise.

**UDP**

(User Datagram Protocol) A connectionless, best-effort delivery protocol used to send data packets between computers over a network such as the Internet.

**UEFI**

(Unified Extensible Firmware Interface) A standard firmware interface for PCs that was designed to improve software interoperability and address the limitations in BIOSs.

**UNIX**

A family of operating systems originally developed at Bell Laboratories and characterized by portability, multiuser support, and built-in multitasking and networking functions.

**UPnP**

(Universal Plug and Play) A feature found in wireless routers to enable computers, printers, and other Wi-Fi-enabled devices to be easily discoverable by the router.

**UPS**

(uninterruptible power supply) A device that continues to provide power to connected circuits when the main source of power becomes unavailable. This can help save computer components from damage due to power problems such as power failures, spikes, and sags.

**USB**

(universal serial bus) A hardware interface standard designed to provide connections for numerous peripherals.

**USB connection**

A personal computer connection that enables you to connect multiple peripherals to a single port with high performance and minimal device configuration.

**user account**

A collection of credentials and important information about a person with access to the system, including the rights and privileges assigned to the user.

**user authentication**

A security measure in which a computer user proves its identity in order to gain access to resources.

**USMT**

(User State Migration Tool) A command-line utility that copies files and settings from one Microsoft Windows computer to another.

**UTM**

(unified threat management) The concept of combining the features of a firewall, gateway antivirus, and IDS/IPS into a single device.

**vfat**

A 32-bit filesystem that supports long file names and is compatible with the FAT filesystem found in older versions of Microsoft Windows.

**VGA**

(Video Graphics Array) A display standard that is implemented with a 15-pin DB-15 connector.

**virtual memory**

The allocation by the computer system of a portion of the hard disk as if it was physical RAM.

**virtual printer**

A software-based alternative to a physical printer that enables you to print to a file.

**virtualization**

The technological process of creating a virtual version of a computer environment by separating the elements of the computing environment from each other and from the

physical hardware it runs on via an additional software layer.

### **virtualization workstation**

A computer that uses both hardware virtualization and client virtualization resources to provide a comprehensive virtual workstation for users.

### **virus**

A piece of code that spreads from one computer to another by attaching itself to other files.

### **vishing**

A human-based attack where the goal is to extract personal, financial, or confidential information from the victim by using services such as the telephone system and IP-based voice messaging services (VoIP) as the communication medium.

### **visual artifact**

An error or anomaly in the visual display of a picture.

### **VMM**

(Virtual Memory Manager) The Windows system component responsible for managing physical-to-virtual memory mappings and virtual memory assignments.

### **VNC**

(virtual network computing) A platform-independent system through which a user can control a remote system.

### **VPN**

(virtual private network) A private network that protects communications sent through a public network such as the Internet.

### **WAN**

(wide area network) A network that spans multiple geographic locations, connecting multiple LANs using long-range transmission media.

### **WAP**

(Wireless Access Point) A device that provides connection between wireless devices and can connect to wired networks.

### **waveform**

The shape of an analog signal when plotted on an oscilloscope or graph.

### **wearable technology**

Small mobile computing devices that are designed to be worn under, with, or on top of a person's clothing.

### **web server**

A computer that provides access to personal, corporate, or educational website content.

### **WEP**

(Wired Equivalent Privacy) Provides 64-bit, 128-bit, and 256-bit encryption for wireless communication that uses the 802.11a and 802.11b protocols.

### **whaling**

A form of phishing that targets individuals who are known or are believed to be wealthy.

### **Wi-Fi**

The popular implementation of the 802.11b wireless standard.

### **Wi-Fi analyzer**

See wireless tester.

### **Wi-Fi locator**

A utility that can be installed on computing devices to locate wireless networks within range of the device.

### **WiMAX**

(Worldwide Interoperability for Microwave Access) A packet-based wireless technology that provides wireless broadband access over long distances.

### **Windows Defender**

The anti-spyware software that is included with Windows Vista and Windows 7 installations.

### **Windows Firewall with Advanced Security**

An administrative tool that is used to manage advanced firewall settings for the computer and any remote computers connected to the network.

**Windows Memory Diagnostic**

An administrative tool that is used to check the RAM on the system and make sure that it is functioning appropriately and efficiently.

**Windows PE**

See WinPE.

**Windows security policies**

Configuration settings within Windows operating systems that control the overall security behavior of the system.

**WinPE**

(Windows pre-installation environment) A lightweight version of Windows or Windows Server that can be used for deployment of the full version of the OS or for troubleshooting OS problems.

**wire crimper**

A tool that attaches media connectors to the ends of cables.

**wire stripper**

A tool that is often incorporated into a wire crimper and that enables the user to remove the protective coating from electrical wires.

**wireless connection**

A network connection that transmits signals without using physical network media.

**wireless encryption**

The process of concealing and protecting data during wireless transmissions.

**wireless locator**

See wireless tester.

**Wireless Network Connection**

A Windows troubleshooting tool used to verify that a computer or other wireless device is connected to the network and able to send and receive data.

**wireless security**

Any method of securing your wireless LAN network to prevent unauthorized network access and network data theft while ensuring that authorized users can connect to the network.

**wireless tester**

A Wi-Fi spectrum analyzer used to detect devices and points of interference, as well as analyze and troubleshoot network issues on a WLAN or other wireless networks.

**WOL**

(Wake-on-LAN) A networking capability that is built into a device's NIC circuitry that allows a device to turn on, or power up when a network message is received by another computing device.

**workgroup**

A peer-to-peer Microsoft network model that groups computers together for organizational purposes, often deployed in homes and small offices.

**worm**

A piece of code that spreads from one computer to another on its own, not by attaching itself to another file.

**WPA**

(Wi-Fi Protected Access) A strong authentication security protocol that was introduced to address some of the shortcomings in the WEP protocol during the pending development of the 802.11i IEEE standard.

**WPA2**

(Wi-Fi Protected Access version 2) A complete wireless standard that adds strong encryption and authentication security to 802.11 and relies on 802.1x as the authentication mechanism.

**WPAN**

(Wireless Personal Area Network) A network that connects devices in very close proximity but not through a wireless access point.

**WWAN**

(wireless wide area network) Uses wireless network technology to allow users to check email, surf the web, and connect to corporate resources accessible within the cellular network boundaries.

## **X forwarding**

A mechanism by which programs are run on one machine and the X window output is displayed on another machine.

## **XFS**

A 64-bit, high-performance journaling filesystem that provides fast recovery and can handle large files efficiently.

## **XP mode**

A downloadable add-on for Windows 7 that allows users running Windows 7 to access and use Windows XP-compatible software and programs directly on their desktops.

## **zero day attack**

An attack that exploits a previously unknown vulnerability in an application or operating system.

## **zombie**

Unauthorized software that directs the devices to launch a DDoS attack.



# Index

- 802.11i [488](#)
- 802.11 standard
  - versions [485, 488](#)
- 8088 [745](#)
- A**
  - abacus [741](#)
  - accelerometer [62](#)
  - acceptable use policy, *See* AUP
  - access point, *See* AP
  - account management [621](#)
  - ACLs [594](#)
  - Action Center utility [309](#)
  - activity light [421](#)
  - adapters [44](#)
  - Address Resolution Protocol, *See* ARP
  - administrative shares [480](#)
  - Administrative Tools [329](#)
  - Advanced Encryption Standard, *See* AES
  - adware [576](#)
  - AES [488](#)
  - AFP [454](#)
  - AIO, *See* MFD types
  - algorithms
    - for encryption [624](#)
  - Analytical engine [742](#)
  - Android
    - email configuration [523](#)
  - antimalware software
    - updates [357](#)
  - anti-spyware
    - software [357, 590](#)
  - anti-static bags [121](#)
  - antivirus software
    - updates [357](#)
- Apple File Protocol, *See* AFP
- application errors [652](#)
- applications
  - locator [634](#)
  - remote backup [635](#)
- argument [396](#)
- ARP [667](#)
- attack
  - types of [578](#)
- ATX [203](#)
- audio/video editing workstation
  - common hardware [413](#)
  - common software [412](#)
- AUP [140](#)
- authentication
  - biometric [635](#)
  - multifactor [636](#)
  - multi-factor [68](#)
  - user [68](#)
- authentication methods
  - biometric authentication [106](#)
- authentication server [97](#)
- authenticator app [636](#)
- Automatic Private IP Addressing, *See* APIPA
- auto negotiation [468](#)
- autorun [622](#)
- B**
  - backlight [508](#)

- backup
    - importance of [349](#)
    - schemes [350](#)
  - badges
    - RFID [588](#)
  - Basic Input/Output System, *See* BIOS
  - batteries [499](#)
  - battery backup, *See* UPS
  - Bayonet Neill-Concelman, *See* BNC
  - binary numbering [436](#)
  - biometric authentication [106, 586](#)
  - biometric locks [589](#)
  - biometrics [177, 678](#)
  - BIOS
    - diagnostics utility [271](#)
    - memory [268](#)
    - overview [9](#)
    - setting disk boot order [294](#)
  - BitLocker [56, 617](#)
  - BitLocker To Go [617](#)
  - black hat [581](#)
  - blackouts [132](#)
  - Blue Screen of Death, *See* BSOD
  - Bluetooth
    - characteristics [48, 520](#)
    - connectivity issues [535](#)
    - naming and addressing [522](#)
    - pairing [522](#)
    - vulnerabilities [677](#)
  - BNC [158](#)
  - boot process
    - Linux [643](#)
    - OS X [645](#)
    - Windows [642](#)
  - bootrec [647](#)
  - BOOTREC [276](#)
  - botnet [580, 581](#)
  - brightness [162](#)
  - bring your own device, *See* BYOD
  - broadcast transmissions [436](#)
  - brownouts [132](#)
  - browser redirection [671](#)
  - brute-force attack [579](#)
  - BSOD [168, 278, 649](#)
  - bus
    - function [6](#)
    - speed [217, 273](#)
  - BYOD [637](#)
- C**
- cable modem [445](#)
  - cable stripper [456](#)
  - cable tester [456, 458](#)
  - cache memory [252](#)
  - carputer [63](#)
  - cathode ray tube, *See* CRT
  - CCFL [152](#)
  - CDFS [299](#)
  - CDs [20](#)
  - cellular technology [447](#)
  - central processing unit, *See* CPU
  - certificates
    - self-signed [617](#)
  - chain of custody [141](#)
  - Check Disk, *See* CHKDSK
  - chipset architecture [215, 253](#)
  - CHKDSK [276, 352](#)
  - chmod command
    - modes [401](#)
  - chroot mode [645](#)
  - CIDR [438](#)
  - CIFS [453](#)
  - ciphers
    - letter-substitution [624](#)
  - ciphertext [623, 624](#)
  - classes A, B, C [437](#)
  - classless addressing [438](#)
  - classless inter-domain routing, *See* CIDR
  - clean install [295, 334](#)
  - cleartext [623](#)
  - CLI [375](#)
  - client/server networks [85](#)
  - clients [84](#)
  - cloud computing
    - benefits [101](#)
    - types [100](#)
  - cloud printing [559](#)
  - cloud services
    - types [99](#)
  - CMOS
    - battery [217, 218](#)
    - error codes [655](#)
  - coax, *See* coaxial cable
  - coaxial cable
    - characteristics [158, 425](#)
  - cold cathode fluorescent lamp, *See* CCFL
  - collate [558](#)
  - command interpreters [329](#)
  - Command Line Interface, *See* CLI
  - command line interpreter [375](#)
  - command line tools [327](#)
  - command prompt [375, 649](#)

- commands
- apropos 400
  - apt-get 399
  - chmod 398
  - chown 398
  - date 400
  - dd 399
  - debugfs 393
  - dump2fs 393
  - e2label 380
  - fsck 393
  - grep 400
  - ifconfig 399
  - iwconfig 399
  - man 400
  - mount 393
  - partprobe 393
  - ps 399
  - Run as Administrator 616
  - sudo 399
  - umount 393
  - vim 399
  - vncserver 378
  - vncviewer 378
  - whoami 400
- Common Internet File System, *See* CIFS
- communication skills
- importance of 138
- Compact Disc File System, *See* CDFS
- compatibility mode 57
- compliance security controls 586
- Component 157
- Component Services 329
- composite video 157
- computer cases 4
- computer connections 32
- Computer folder 73
- computer forensics 142
- computer image 296
- Computer Management 329
- computer networks 84
- computer removal 141
- computer security
- best practice violations 583
- computers for entertainment 413, 415
- computing components 2
- connections
- Thunderbolt 37
- connectors
- types 430
  - wireless device 47
- Control Panel
- overview 309, 318
- converters 44
- cooling system
- characteristics 7
  - fans 219
  - issues with 241
  - laptop computers 509, 529
  - liquid-based 229
  - system firmware monitoring 272
  - types 228
- COPE 637
- corona 544
- corporate owned, personally enabled, *See*
- COPE
- CPU
- cooling 228
  - operational characteristics 225
  - overview 2
  - troubleshooting 239
- CRT 153
- cryptographic 623
- cryptographic techniques
- encryption as 623
- cryptography 623

## D

- data
- loss prevention, *See* DLP
  - data backup 349
  - data duplexing, RAID 1 266
  - data encryption 623
  - data loss prevention, *See* DLP
  - data restoration 349
  - data sanitization 599, 634
  - data security 673
  - Data Sources 329
  - data synchronization 526, 527
  - data wiping 599, 634
  - daughter board 9
  - DB-15 154
  - DC jack 499
  - DDoS 580, 581
  - dead pixels 167
  - deciphering 624
  - default gateway address 437
  - DEFRAG utility 648
  - degaussing 602
  - demilitarized zone, *See* DMZ
  - Device Manager
  - accessing 190, 326

- uses [190](#), [326](#)
- devices
  - encryption [599](#), [635](#)
  - pairing [521](#), [522](#)
- DHCP
  - client-side settings [441](#)
- dial-up lines [446](#)
- dictionary attack [579](#)
- digital security [589](#)
- Digital Subscriber Line, *See* DSL
- Digital Video Interface, *See* DVI
- digitizer [507](#)
- DIMM [214](#)
- diodes [743](#)
- directories [71](#)
- directory services [472](#)
- direct thermal printer [550](#)
- DirectX Diagnostic tool [330](#)
- discovery mode [521](#)
- Disk Cleanup [352](#)
- disk controller [14](#)
- Disk Defragmenter [352](#)
- disk maintenance
  - check disk [353](#)
  - disk defragmentation [353](#)
  - scheduled [353](#)
- Disk Management [261](#)
- DISKPART [276](#)
- disk partitions
  - overview [297](#)
  - types [298](#)
- display cables
  - digital video interface [39](#)
  - DVI [39](#)
  - HDMI [39](#)
  - high definition multimedia interface [39](#)
  - VGA [39](#)
  - video graphics array [39](#)
- display devices
  - aspect ratio [159](#)
  - connections [153](#)
  - settings [162](#)
  - types [152](#)
- DisplayPort [157](#)
- displays
  - multiple [163](#)
  - Windows configuration tools [164](#)
- display settings [162](#)
- Display utility [319](#)
- dissipative material [121](#)
- distros [373](#)
- DLP [593](#), [677](#)
- DMZ [476](#)
- DNAT [477](#)
- DNS
  - addresses [441](#)
  - client-side implementation [442](#)
  - name resolution [442](#)
- docking station [502](#)
- domain
  - membership [471](#)
  - overview [300](#)
- domain controller [300](#)
- Domain Name Server (or System), *See* DNS
- Domain Name System [96](#)
- dot-matrix printer [552](#)
- dotted decimal notation [436](#)
- drive rails [260](#)
- drivers
  - third-party [297](#)
  - updates [355](#)
- drone [580](#)
- DSL [446](#)
- Dual In-line Memory Module, *See* DIMM
- dump file [650](#)
- duplex [558](#)
- duplexing [543](#)
- duplex scanning [543](#)
- DVDs [20](#)
- DVI
  - cables [155](#)
  - single link vs. dual link [155](#)
- dye sublimation printer [550](#)
- dynamic addressing [440](#)
- Dynamic Host Configuration Protocol [96](#)
  - See also* DHCP

## E

- EAS [527](#)
- Easy Transfer [335](#)
- eavesdropping [579](#)
- ECC [253](#)
- EDSAC [743](#)
- EDTV [156](#)
- EEPROM [268](#), [269](#)
- EFS [617](#)
- EIA [425](#)
- electrical hazards
  - ESD [123](#)
  - power supply [123](#)
- electrical interference [666](#)
- electrical safety precautions [124](#)

electromagnetic interference, *See* EMI  
 Electronic Delay Storage Automatic Computer, *See* EDSAC  
 Electronic Industries Alliance, *See* EIA  
 Electronic Numerical Integrator and Computer, *See* ENIAC  
 electrostatic discharge, *See* ESD  
 Electrostatic Photographic drum, *See* EP drum  
 email  
     client-based 522  
     configuration 523  
     filtering 595  
     security 523  
     security issues 671  
     web-based 522  
 embedded Multi-Media Controller 23  
 EMI  
     causes 122  
 eMMC 23  
 emulator 288  
 enciphering 624  
 encryption  
     one-way vs. two-way 107, 487  
     wireless 487  
 Enhanced Digital TV, *See* EDTV  
 ENIAC 743  
 environmental safety  
     atmospheric considerations 128  
     chemical hazards 133  
     disposal of hazardous material 135  
     incident reports 134  
     laser safety standards 131  
     liquid hazards 133  
     MSDS 133  
     OSHA 118, 133  
     situational hazards 129  
 EP drum 544  
 EPROM 269  
 equipment  
     grounding 124  
 e-reader 29, 514  
 Error-Correcting Code, *See* ECC  
 eSATA 38  
 ESD  
     causes 120  
     electrical hazards 123  
     prevention 120  
     toolkit 121  
 Ethernet 421  
 event log entries 658  
 Event Viewer

errors and warnings 657  
 Exchange 522  
 Exchange ActiveSync, *See* EAS  
 expansion cards  
     characteristics 8  
     configuring 198  
     installing 198  
     types 197  
 expansion slots 209  
 ExpressCards 501  
 extenders 92  
 external devices 2  
 external enclosure 276  
 external power source issues 132  
 External SATA, *See* eSATA

## F

Face Contact connector, *See* FC connector  
 failed login  
     attempts restrictions 635  
 FAT 299  
 FC connector 431  
 F-connector 427  
 FDISK 276  
 fiber connections 446  
 fiber optic cable  
     mode types 429  
 file attributes  
     changing 75  
     viewing 75  
 File Explorer 72  
 file extensions 74  
 file recovery software 277  
 files  
     attributes 74, 614  
     compression 610  
     encryption 610  
     extensions 74  
     fstab 393  
     NTFS permissions 609  
     sharing 327  
 file server 96  
 file sharing 480  
 filesystem integrity 393  
 file systems  
     types 299  
 firewalls  
     features 94  
     mobile devices 636  
     overview 308, 324  
     software configuration 475, 628

software vs. hardware 590  
 types 590  
 Windows configuration 591  
 firmware  
   overview 9  
   updates 355  
   upgrading 355  
 first response 141  
 fixboot 647  
 fixmbr 647  
 flashing 9  
 Flash ROM 269  
 Folder Options utility 321  
 folders  
   shared permissions 613  
   sharing 615  
 forensic response procedures 142  
 FORMAT 276  
 formed-character printer 552  
 form factor 202  
 fox and hound 458  
 frames  
   plastics 498  
 frequency variation 245  
 frontlight 508  
 full duplex 468  
 fuser assembly 544

## G

gaming PC  
   peripherals 414  
   requirements 414  
 gateways 437  
 genders 31  
 General Protection Fault, *See* GPF  
 ghost cursor 533  
 global positioning system, *See* GPS  
 GPF 652  
 GPRS 27  
 GPS 514  
 GPS device 29  
 GPS tracking 599, 634  
 GPU 411  
 GRand Unified Bootloader, *See* GRUB  
 graphical user interface, *See* GUI  
 Graphical User Interface, *See* GUI  
 Graphics Processing Unit, *See* GPU  
 group policy settings 582  
 groups  
   local 68  
 GRUB

overview of 377  
 GRUB 2  
   overview of 377  
 GUI 54, 374

## H

half duplex 468  
 hard disk drive, *See* HDD  
 hard drive disposal  
   formatting 602  
   physical destruction 602  
 hardware  
   upgrading 334  
 hazardous material disposal 135  
 HDD  
   diagnostic tools 115  
   overview 14  
 HDMI  
   cables 156  
 HDTV 156  
 heat sinks 7, 228  
 heavy duty MFD, *See* MFD  
 hertz, *See* Hz  
 Hibernate 325  
 High Definition Multimedia Interface, *See* HDMI  
 High-Definition TV, *See* HDTV  
 high-level formatting 602  
 hoaxes 578  
 homegroup 301, 471  
 home server PC  
   requirements 416  
 home theater PC, *See* HTPC  
 host firewall 590  
 host name 436  
 hosts 436  
 hot swappable device 15

HTPC  
   requirements 416  
   software 416  
 hypervisor 287  
 Hz 162

## I

IDS 97  
 IEEE 36  
 IHA chipset 216  
 IMAP4 523  
 impact printer  
   common issues 572

- maintenance 562  
 paper feeding 552  
 process 552  
 types 551  
 impersonation 577  
 incident management 583  
 incident reports 134  
*infrared, See IR*  
*inkjet printer*  
 characteristics 547  
 common issues 571  
 maintenance 562  
 piezoelectric vs. thermal 547, 548  
 process 548  
 supplies 555  
*in-place upgrade* 334  
*input/output device issues* 651  
*input/output devices* 192  
*input devices*  
 biometric types 177  
 installation considerations 181  
 multimedia 176  
 optical 175  
 security 177  
 third-party utilities 183  
 Windows configuration tools 182  
*Institute of Electrical and Electronic Engineers, See IEEE*  
*integrated circuit* 744  
*Integrated Services Digital Network, See ISDN*  
*Intel Hub Architecture chipset, See IHA*  
*chipset*  
*internal devices* 2  
*International Mobile Equipment Identity number, See IMEI number*  
*International Mobile Subscriber Identity number, See IMSI number*  
*Internet appliances* 97  
*Internet connectivity* 445  
*Internet Mail Access Protocol version 4, See IMAP4*  
*Internet Options* 318  
*Internet Protocol, See IP*  
*Internet Service Provider, See ISP*  
*intrusion detection* 272  
*Intrusion Detection System, See IDS*  
*Intrusion Protection System, See IPS*  
*inverter* 508  
*iOS* 62  
*IP* 449  
*IP addresses*  
 addressing schemes 440  
 alternates 470  
 classes 437  
 private 440  
 public 440  
 static vs. dynamic 440  
*IPCONFIG* 460  
*IPS* 97  
*IPv4 addresses* 436  
*IPv4 vs. IPv6* 440  
*IPv6 addresses*  
 double colon 439  
*IPv6 standard* 439  
*IP version 6, See IPv6 standard*  
*IR* 49  
*ISDN* 446  
*ISP* 445

## K

- Kensington locks* 503  
*keyboard* 497  
*keyboard, video, mouse switch, See KVM switch*  
*keyboards* 172  
*key fobs* 588  
*kill commands* 403  
*KVM switch*  
 uses 192

## L

- LAN* 85  
*laptop computers*  
 batteries 508  
 characteristics 25, 496  
 common keypad issues 533  
 cooling methods 509  
 CPU 505  
 device issues 531  
 display components 507  
 docking 502  
 expansion cards with 508  
 function keys and buttons 501  
 hardware components 497  
 internals 505  
 locking 503  
 maintenance 529  
 memory 506  
 motherboard 505  
 operating conditions 530  
 power supply 508

- servicing 535
  - storage drive 506
  - technical support considerations 500
  - vs. tablet PC 511
  - laser printer
    - common issues 570
    - components 544
    - electrical safety 123
    - maintenance 561
    - process 545
  - LC connector 431
  - LCD 3, 152
  - LDAP 451
  - least privilege 104, 622
  - LED 153, 421
  - LED printer 545
  - legal security controls 586
  - light emitting diode, *See* LED
  - Lightweight Directory Access Protocol, *See* LDAP
  - Linear Tape File Systems, *See* LTFS
  - line noise 244
  - line printer 552
  - link light 421
  - Linux
    - best practices 403
    - CLI 375
    - distributions 60, 61, 373
    - features 376
    - file sharing 480
    - GUI 374
    - hardware compatibility 379
    - installation 379
    - management tools 391
    - remote access 377
    - shell commands 395
    - shells 393
    - software compatibility 380
    - superuser 376
    - system requirements 379
    - tools 78
  - Linux filesystems
    - definition 380
    - ext3 380
    - ext4 380
    - labels 380
    - ReiserFS 380
    - swap 380
    - types 380
  - Linux rescue environment 644
  - liquid crystal display, *See* LCD
  - Local Area Connection status 460
  - Local Area Network, *See* LAN
  - Local Connector, *See* LC connector
  - local policy settings 582
  - local printer
    - characteristics 556
  - Local Security Policy 70, 329
  - Local Users and Groups 329
  - lockup errors
    - responding to 651
  - logic bomb 576
  - loopback plug 239, 458
  - low-level formatting 602
  - LTFS 22
  - lumens 162
- M**
- MAC addresses 421
  - Macintosh
    - software compatibility 362
    - trackpad 363
  - magnetic core memory 744
  - mail server 97
  - maintenance
    - cleaning materials 116
    - techniques 115
    - tools 112
  - malicious software, *See* malware
  - malware
    - issues 671
    - protection against 356, 590
    - removing 675
    - types 576
  - MAN 87
  - managing security incidents 583
  - man-in-the-middle attack 579
  - mantraps 587
  - manual pages 400
  - Mark I 742
  - master boot record, *See* MBR
  - Material Safety Data Sheet, *See* MSDS
  - materials handling
    - chemical hazards 133
    - disposal of hazardous material 135
    - liquid hazards 133
    - MSDS 133
  - mathematical functions 624
  - MBR 647
  - Mechanical Transfer Registered Jack connector, *See* MT-RJ connector

- Media Access Control addresses, *See* MAC addresses  
 media design workstation  
     requirements 411  
 media tester, *See* cable tester  
 memory  
     configurations 253  
     ECC 253  
     form factors 214  
     non-volatile 5  
     overview 5  
     ROM 269  
     settings 218  
     volatile 5  
 memory dump 650  
 memory module 252  
 metropolitan area network, *See* MAN  
 MFD  
     types 543  
 microATX 205  
 MicroDIMM 506  
 microprocessor 745  
 Microsoft Product Activation 304  
 Microsoft Windows  
     activation methods 305  
     common features 308  
     compatibility 294, 334  
     features 55  
     file sharing 479  
     gadgets 56  
     installation types 295  
     maintenance tools 352  
     migrating data between systems 335  
     networking 471  
     remote computing 481  
     system requirements 293  
     Upgrade OS Advisor 336  
     upgrading 334  
     versions 54, 293  
 Windows 7 editions 58, 310  
 Windows 8 editions 57, 310  
 Windows Vista 309  
     Windows Vista editions 58  
 mini-ATX 204  
 mini-HDMI 156  
 mini-ITX 206  
 MiniPCI 213  
 Mini-PCIe cards 508  
 mirroring, RAID 1 266  
 mobile carrier 520  
 mobile devices  
 common security symptoms 676  
 email 522  
 policies and procedures 637  
 security controls 598  
 security tools 678  
 synchronization 527  
 trusted sources 636  
 untrusted sources 636  
 vulnerabilities 598  
 mobile digital device 25  
 mobile memory specifications 507  
 mobile operating systems 63  
 Mobile OS  
     issues 661  
     tools 663  
 modems 93  
 motherboard  
     form factors 202  
 MSConfig  
     options 331  
     utility 648  
     vs. Services 332  
 MSDS  
     required information 134  
 MT-RJ connector 432  
 multiboot 296  
 multicast transmissions 436  
 multi-CPU motherboards 227  
 multi-factor authentication 106  
 multi-function device, *See* MFD  
 multimedia devices  
     common devices 176  
 multimeter 457  
 multitouch 62, 512  
 mutual authentication 106  
 My Computer, *See* Computer folder

## N

- Napier's Bones 741  
 NAT  
     dynamic NAT 477  
     implementations 476  
 native resolution 162  
 NET 460  
 NETSTAT 460  
 network  
     security measures 592  
 Network Address Translation, *See* NAT  
 network-based firewall 590  
 network-based printer 556  
 network cables

coaxial 425  
 fiber optic 428  
 FireWire 433  
 termination 428  
 twisted pair 422  
 network-connected printer 556  
 network connections  
     configuration options 460  
     types 433, 466  
 network connectivity  
     issues 665  
 network devices  
     legacy devices 90  
 network directory, *See* directory services  
 Network File Sharing, *See* NFS protocol  
 networking utilities 460  
 network interface card, *See* NIC  
 network locations 467  
 network models 84  
 network settings 466  
 network types  
     SOHO 484  
 NFS protocol 480  
 NIC  
     characteristics 420  
     configuring 467  
     status lights 420  
 nodes 84  
 non-compliant systems 581  
 Northbridge chipset 216  
 NSLOOKUP 460  
 NTFS 299, 617

## O

OLED 153  
 operating system  
     32-bit vs. 64-bit 227  
     boot methods 294  
     upgrade methods 334  
 optical discs 20  
 optical drive  
     overview 21  
     types 21  
 organic light emitting diode, *See* OLED  
 organizational policies  
     prohibited content 140  
     scope 140  
 orientation  
     landscape 558  
     portrait 558  
 OSHA 118

OS X  
     best practices 369  
     Boot Camp 61  
     Dock 61  
     features 364  
     file sharing 480  
     Finder 61  
     Gestures 61  
     hardware compatibility 362  
     iCloud 61  
     keychain 61  
     management tools 366  
     Mission Control 61, 364  
     operating system 61, 362  
     space 364  
     Spot Light 61  
     system requirements 362  
     user interface 363  
     versions 61  
 output devices 188  
 overclocking 240  
 overvoltage 245

## P

pagefile 344  
 PAN 86  
 parity 253, 254  
 partitioning 297  
 partition management 392  
 partprobe program 393  
 Pascaline machine 742  
 password  
     authentication 678  
     best practices 621  
 patches 304, 355, 600, 624, 635  
 patch management  
     example 355, 624  
     policies 355, 624  
 patch panel 94  
 PC 745  
 PCI 210  
 PCIe  
     and DisplayPort 157  
     overview 212  
 PCI Express, *See* PCIe  
 PCI eXtended, *See* PCI-X  
 PCI-X 211  
 peer-to-peer networks 85  
 Performance Monitor 329  
 Peripheral Component Interconnect, *See* PCI

- Peripheral Component Interconnect Express,  
*See* PCIe
- peripheral devices 3
- permissions
- applying to subfolders 616
  - considerations when applying 614
  - for shared files and folders 612
  - inheritance 615
  - in Unix 592
  - NTFS, file 609
  - NTFS, folder 609
  - NTFS vs. share 479, 613
  - special 610
- Personal Area Network, *See* PAN
- Personal Computer, *See* PC
- personal firewall, *See* host firewall
- phablet 27, 513
- pharming 578
- phishing 578
- physical addresses 421
- physical security
- considerations 586
  - implementation 586
  - laptops 503
- physical security controls 586
- piconet 48
- PictBridge 543
- ping 460
- pixels 162
- plaintext 624
- plasma display 153
- plenum 425
- plenum cable 425
- Plug and Play, *See* PnP
- PnP 343
- PoE 91, 468
- polyvinyl chloride, *See* PVC
- POP3 523
- pop-ups 671
- port replicator 502
- ports
- characteristics 449
  - commonly used 450
  - filtering 593
  - forwarding and triggering 489
  - hardware 31
  - ranges 449
- POST
- beep error codes 654
  - card 239
  - errors during 277
- numeric error codes 655
- overview 11
- Post Office Protocol version 3, *See* POP3
- power connections 219
- power generator 132
- Power Management 240
- Power-On Self Test, *See* POST
- Power Options utility 325
- Power over Ethernet, *See* PoE
- Power Plans 325
- power protection systems 132
- power sag 132, 245
- power spike 132
- power supply
- connections 231, 232
  - issues with 245, 247
  - laptops 508
  - overview 7
  - safety recommendations 234
  - specifications 231
  - voltage switch safety 509
- power supply tester 239
- power surge 132
- Preboot Execution Environment, *See* PXE
- Preferred Roaming Index, *See* PRI
- Preferred Roaming List, *See* PRL
- prestaging 472
- PRI 519
- printer
- common issues 566
  - components 541
  - configuring 558
  - connection types 540
  - hardware vs. software terminology 540
  - impact 551, 562
  - inkjet 546, 562
  - installation 556
  - laser 544, 561
  - LED 545
  - maintenance kits 564
  - media types 555
  - paper trays 555, 558
  - ports 558
  - sharing methods 557
  - solid ink 548
  - supplies 555
  - thermal 549, 561
  - troubleshooting 564, 565
- Print Management 329
- print permissions 557
- print queue 556

- print server [96](#), [556](#), [557](#)  
 privacy [143](#)  
 PRL [519](#)  
 procedural security controls [586](#)  
 processor connections  
     socket types, AMD [225](#)  
     socket types, Intel [223](#)  
 process table [402](#)  
 PROM [269](#)  
 proxy server [96](#)  
 proxy settings [474](#)  
 PSTN [446](#)  
 PSU [7](#)  
     *See also* power supply  
 Public Switched Telephone Network, *See* PSTN  
 punch down tool [459](#)  
 PVC [425](#)  
 PXE [294](#)
- Q**
- QoS [468](#), [485](#)  
 quality of service, *See* QoS
- R**
- Radio Corporation of America, *See* RCA  
 radio firmware [519](#)  
 radio frequency, *See* RF  
 radio-frequency interference, *See* RFI  
 radio networking [48](#)  
 RAID  
     overview [265](#)  
     standards [265](#)  
 RAM  
     buffered [254](#)  
     compatibility [254](#)  
     configurations [253](#)  
     form factors [214](#)  
     issues with [258](#)  
     non-buffered [254](#)  
     not recognized [258](#)  
     overview [5](#)  
     single- vs. double-sided [253](#)  
     types [252](#)  
 Rambus Inline Memory Module, *See* RIMM  
 RAM chip [745](#)  
 RAM module, *See* memory module  
 Random Access Memory, *See* RAM  
 rapid elasticity [101](#)  
 RCA [158](#)
- Read-Only Memory, *See* ROM  
 ReadyBoost [57](#)  
 Recovery Console [329](#)  
 recovery image [349](#)  
 Redundant Array of Independent Disks, *See* RAID  
 refresh rate [162](#)  
 REGEDIT utility [648](#)  
 Registry  
     editing [343](#)  
     errors [658](#)  
     files [342](#)  
     overview [342](#)  
     subtrees [343](#)  
     value entries [342](#)  
 Registry Editor [330](#), [343](#)  
 REGSVR32 utility [648](#)  
 regulatory security controls [586](#)  
 remote backup [600](#)  
 Remote Desktop [322](#), [481](#), [649](#)  
 remote printing [559](#)  
 repair disks [647](#)  
 repair tools [112](#)  
 repeaters [92](#)  
 resistors [744](#)  
 restore [349](#)  
 RF  
     spectrum allocation [49](#)  
 RFI [531](#)  
 RIMM [214](#)  
 riser card [9](#)  
 ROM  
     overview [5](#)  
     types [269](#)  
 rootkit [576](#)  
 rotation method [350](#)  
 routers  
     configuring [489](#)  
     firmware [490](#)  
     overview [92](#)  
 RPM  
     overview [401](#)  
 RPM Package Manager, *See* RPM  
 RS-232 interfaces [433](#)  
 Run line  
     accessing [330](#)  
     opening management consoles with [331](#)
- S**
- Safe Mode  
     options [649](#)

- SATA  
 connection 37  
 installation considerations 260  
 troubleshooting 279  
 satellite communications 446  
 SC connector 431  
 scheduled tasks 350  
 screen 500  
 screen lock 599, 634  
 screen resolution 319  
 Screen Resolution utility 167  
 SDTV 156  
 Search 330  
 Secure Boot 271  
 Secure Shell, *See* SSH  
 Secure Sockets Layer, *See* SSL  
 security  
   controls 586  
   incidents 583  
   permissions 608  
   shared files and folders 615  
   system files and folders 616  
 security cards 588  
 Security Center utility 309  
 security compliance 103–105, 582, 591, 622  
 security issues 671  
 security policy  
   digital data 589  
   educating users 104, 582, 675  
   user practices 105  
 Server Message Block, *See* SMB  
 servers  
   functions 84  
   home 416  
   roles 96  
 Service Level Agreements, *See* SLAs  
 Service Packs 304  
 Services  
   vs. MSConfig 332  
 Services console 330  
 Service Set Identifier, *See* SSID  
 set-top box 193  
 sfC 647  
 Shadow Copy 56  
 shares  
   administrative 480, 612  
   characteristics 612  
   local 612  
   permissions for 612  
 shell commands 395  
 shells 393  
 shielded twisted pair, *See* STP  
 shoulder surfing 577  
 Sidebar 56  
 signal loss 676  
 Simple Network Management Protocol, *See* SNMP  
 single sign-on, *See* SSO  
 SLAs 485  
 Sleep 325  
 SMA connector 431  
 smart camera 28, 514  
 smart cards 106, 595  
 smartphone  
   devices 27, 512  
   network connectivity 520  
 smart watch 28  
 SMB 452, 453  
 snapshot printer 550  
 sniffing  
   attack 579  
 SNMP 451  
 social engineering attacks  
   types 577  
 SODIMM 507  
 software  
   diagnostic tools 114  
   trusted sources 595  
   upgrading 334  
 software diagnostic tests  
   examples 115  
 software license 144  
 software updates 303  
 SOHO MFD, *See* MFD types  
 SOHO networks  
   characteristics 484  
   QoS in 485  
   securing 627, 629  
   size 484  
 soldered 4  
 solid ink printer 548  
 solid state drives, *See* SSD  
 solid state storage  
   characteristics 15  
   types 15  
 Southbridge chipset 216  
 spam 577, 578, 580, 672  
 SPDIF 44  
 speakers 498  
 spear phishing 578  
 spectrum analyzers 459  
 speed light 421

- spim 578
- spoofing 577, 593
- spyware 576
- SSD
  - in tablets 512
  - overview 15
  - troubleshooting 279
- SSH 453
- SSID 488
- SSL 523
- SSO 616
  - standard client workstation 408
- Standard Connector, *See* SC connector
- Standard Definition TV, *See* SDTV
- standard formatting, *See* high-level formatting
- Standby 325
- startup errors 652
- static addressing 440
- static electricity
  - sources 120
  - voltage 120
- ST connector 431
- Stepped Reckoner 742
- stop error 278
- storage devices
  - characteristics 6
  - disk partition 297
  - external, considerations 261
  - internal, considerations 260
  - solid state storage 15
- STP 423
- Straight Tip connector, *See* ST connector
- striping, RAID 0 265
- striping plus mirroring, RAID 10 266
- striping with parity across drives, RAID 5 266
- strong passwords 104, 591, 599, 634
- stuck pixels 167
- Sub Miniature type A connector, *See* SMA connector
- Sub Multi Assembly connector, *See* SMA connector
- subnet masks
  - CIDR 438
  - overview 437
- Subscriber Connector, *See* SC connector
- surge suppressor 132
- surround sound 188
- Suspend 325
- switches 91
- system BIOS 9
- system boards
- chipsets 215
- connections, components 219
- connections, fans 219
- expansion slots 209
- issues with 242
- laptops 505
- preventing problems 242
- repairs 243
- system bus 6
- System Configuration 329
- System File Checker, *See* sfc
- system files 71
- system firmware
  - component settings 269
  - monitoring functions 272
  - upgrades 269
- system image 350
- System Information utility 330
- System Restore 57, 322, 349, 352
- system restore point 57
- systems
  - embedded 97
  - legacy 97
- system unit 2
- System utility 322

## T

- tablet PC
  - devices 26, 511
  - vs. laptop 511
- tape drive 22
- Task Manager 311, 656
- Task Scheduler 329
- TCP
  - common ports 450
  - vs. UDP 449
- TCP/IP 435, 460
- technical security controls 586
- Telecommunications Industry Association, *See* TIA
- Telnet 453
- Temporal Key Integrity Protocol, *See* TKIP
- thermal dye transfer printer 550
- thermal paper 549
- thermal paste 228
- thermal printer
  - characteristics 549
  - maintenance 561
  - types 549
- thermal wax transfer printer 550
- thick clients 408

- thin clients 408  
 threats and vulnerabilities  
     protecting against 582, 583, 586, 589, 590  
     sociological 577  
     software 576  
 TIA 425  
 TKIP 488  
 TLS 523  
 TN 152  
 tokens  
     RSA 588  
 tone generators and locators 458  
 toner 544, 555  
 toner vacuums 564  
 tools  
     cable tester 456  
     for file encryption 617  
     punch down 459  
     wire crimpers 457  
     wire stripper 457  
 touchpad 498  
 tower 2  
 TRACERT 460  
 traces 6  
 trackpoint 175  
 transistors 5, 744  
 Transmission Control Protocol, *See* TCP  
 Transmission Control Protocol/Internet Protocol, *See* TCP/IP  
 Transport Layer Security, *See* TLS  
 triboelectric generation 120  
 Trojan horse 576  
 troubleshooting  
     app issues 663  
     boot process 645  
     cooling system issues 241  
     CPU issues 239  
     external power sources 244  
     hard drive issues 276, 277  
     hardware 239  
     helpful documentation for 117  
     network connectivity 460, 665–668  
     operating system issues 646, 656  
     power supply issues 245, 247  
     printers 564, 565  
     process for 146  
     RAID issues 276, 279, 656  
     RAM issues 258  
     SATA drives 279  
     security issues 671  
     SSD issues 279  
 system board issues 242  
 tools 147, 646, 668  
 video and display issues 166, 651  
 wireless connectivity 535  
 twisted nematic, *See* TN  
 twisted pair cable  
     types 423
- ## U
- UAC 69  
 UDP  
     common ports 450  
     vs. TCP 449  
 UEFI 10  
 unattended installation 295  
 unicast transmissions 436  
 Unified Extensible Firmware Interface 10  
 Unified Threat Management, *See* UTM  
 uninterruptible power supply, *See* UPS  
 UNIVAC 743  
 Universal Automatic Computer, *See* UNIVAC  
 Universal Plug and Play, *See* UPnP  
 universal serial bus, *See* USB  
 UNIX  
     file sharing 480  
     operating system 59  
 unshielded twisted pair, *See* UTP  
 updates 355  
 UPS  
     characteristics 132  
     safety recommendations 234  
     types 133  
     uses 115  
 USB  
     booting from 294  
     for network connections 433  
     speeds 261  
 USB connection 33  
 User Account Control, *See* UAC  
 user accounts  
     group accounts 70  
     types 69, 608  
 User Accounts utility 320  
 user authentication 616  
 User Datagram Protocol, *See* UDP  
 user groups  
     creating 609  
 user interfaces  
     types 76  
 users  
     local 68

User State Migration Tool, *See* USMT  
 USMT 335  
 UTM 97  
 UTP 423

## V

vacuum tubes 743  
 VGA 154  
 video  
   adapters 159  
   converters 159  
 video card troubleshooting 167  
 Video Graphics Array, *See* VGA  
 virtual desktops 376  
 virtualization  
   benefits 286  
   client-side 286  
   network requirements 289  
   purposes of 287  
   requirements 409  
   resource requirements 288  
   server-side 286  
   software products 409  
 virtual memory  
   page 345  
   page fault 345  
   paging 345  
   process 345  
   swapping 345  
 Virtual Memory Manager 344  
 Virtual Network Computing, *See* VNC  
 virus  
   characteristics 576  
   signatures and definitions 356, 590  
 vishing 578  
 visitor access logs 588  
 visual artifacts 168  
 VM 409  
 VNC 378  
 voice phishing, *See* vishing  
 volt-ohm meter, *See* multimeter  
 Volume Activation 304  
 Volume License Product Key 305

## W

WAIK 647  
 Wake-on-LAN, *See* WOL  
 WAN 86  
 WAP 488  
 weak signal 676

wearable devices 513  
 wearable technology 28  
 web server 96  
 WEP 487  
 whaling 578  
 Wide Area Network, *See* WAN  
 Wi-Fi  
   connectivity 432, 520  
   IEEE standard 802.11b 485  
   laptop antenna 508  
   vulnerabilities 677  
 Wi-Fi locators 667  
 Wi-Fi Protected Access, *See* WPA  
 Wi-Fi-Protected Setup, *See* WPS  
 Wi-Fi tester 459  
 Windows  
*See also* Microsoft Windows  
 tools 77  
*See also* Microsoft Windows  
 Windows 7  
   editions 58, 310  
   features 310  
 Windows 8  
   editions 57  
   features 310  
 Windows Aero 56  
 Windows Automated Installation kit, *See* WAIK  
 Windows Defender 57, 308  
 Windows Error Reporting 658  
 Windows Explorer 72  
 Windows Firewall  
   configuration 591  
   features 475, 628  
   with Advanced Security 330  
 Windows Genuine Advantage Notifications 304  
 Windows Memory Diagnostic 329  
 Windows operating system  
   custom settings 302  
 Windows PowerShell 329  
 Windows pre-installation environment, *See* WinPE  
 Windows security policies 581, 582  
 Windows Update 309  
 Windows updates 303  
 Windows Vista  
   editions 58  
   features 309  
 Windows XP  
   power user 608

WinPE 647  
WinRE 647  
Wired Equivalent Privacy, *See* WEP  
Wireless Access Point, *See* WAP  
wireless channels 486  
wireless communication  
    signal strength 432  
wireless connectivity issues 535  
wireless device connections 47  
wireless encryption types 487  
Wireless Network Connection status 460  
Wireless Personal Area Network, *See* WPAN  
wireless security 628, 631  
wireless tester 459  
Wireless WAN, *See* WWAN  
wire stripper 456  
WOL 468  
workgroups 300, 471  
workstations  
    audio/video editing 412, 413  
    media design 411  
    standard client 408  
worm 576  
WPA 487  
WPA2, *See* 802.11i  
WPAN 86  
WPS 630  
WWAN 447

## X

X forwarding 378  
xfs tools 393  
XP mode 57

## Z

zero day attack 578  
zombie 580

