เอกสารประกอบการฝึกอบรมและสอบมาตรฐานสากล

ระดับพื้นฐาน

หลักสูตรพื้นฐานระบบเทคโนโลยีสารสนเทศ (IT Fundamentals)

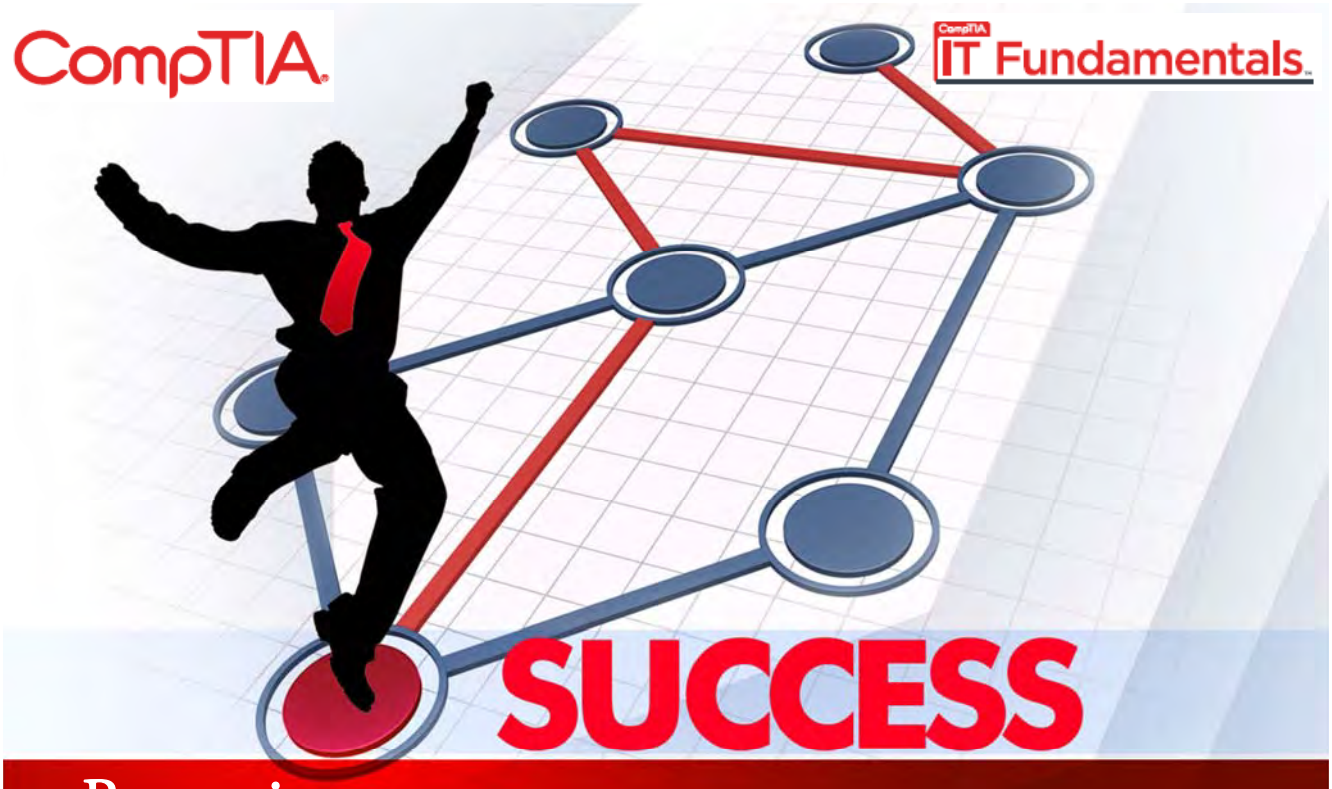
(Handouts)

บริษัท ดราก้อนส์ มู้ฟ จำกัด

94/389 ถนนคู้บอน แขวงบางชัน เขตคลองสามวา กรุงเทพฯ 10510

CompTIA

CompTIA IT Fundamentals



Becoming a CompTIA Certified IT Professional is Easy

Course Outline (Day 1)

- Identifying Computer Hardware
  - Identify Types of Computing Devices
  - Identify Internal Computer Components
  - Common Computer Connector Types
  - Identify Common Peripheral Devices
- Identifying Computer Software
  - Compare Functions and Features of Common Operating Systems
  - Identify Application Software

Course Outline (Day 2)

- Setting Up a Basic Workstation
  - Connect Hardware
  - Install and Configure Operating Systems
  - Install and Configure Applications
  - Configure Accessibility Options
- Configuring Network Access
  - Network Connection Types
  - Install and Configure a SOHO Router
  - Network and Alternative Technologies
  - Sharing and Storage Methods

Course Outline (Day 3)

- Working with Files, Folders, and Applications
  - Create Files
  - Navigate a File Structure
  - Manage Files and Folders
  - Compress and Extract Files
  - Create Screen Captures
- Configuring and Using Wireless Devices
  - Configure Wireless Devices
  - Use Wireless Devices

Course Outline (Day 4)

- Securing Computing Devices
  - Identify Security Threats
  - Apply Security Best Practices
  - Perform Secure Web Browsing
- Supporting Computers and Users
  - Environmental and Safety Concepts
  - Back Up and Restore Data
  - Manage Software
  - Implement Basic Support Measures

Course Outline (Day 5)

- Warp up and Discussion
  - Warp up IT Fundamentals
  - Practical Post Test : FC0-U51
  - Practical Post Test Review : FC0-U51

CompTIA IT Fundamentals

Lesson 1
Identifying Computer Hardware

CompTIA IT Fundamentals

Topic A :
Identify Types of Computing Devices

Computer Device

A computing device :

- ✓ is an electronic machine that uses binary data to automatically perform calculations.
  - Personal Computers
  - Desktop Computers
  - Laptop Computers
  - Tablets
  - Smartphones
  - Servers
  - Other Computing Devices

Personal Computer

Personal Computer

Desktop Computer

Desktop Computer

All-in-One Desktop Computer

All-in-One Desktop Computer

Laptop Computer

Laptop Computer

Smartphones

Smartphones

Server

Server

Other Computer Devices

Supercomputer

Mainframe

PDA

eBook reader

Multimedia Player

Other Computer Devices

Questions

CompTIA IT Fundamentals

Lesson 1

Identifying Computer Hardware

CompTIA IT Fundamentals

Topic B :

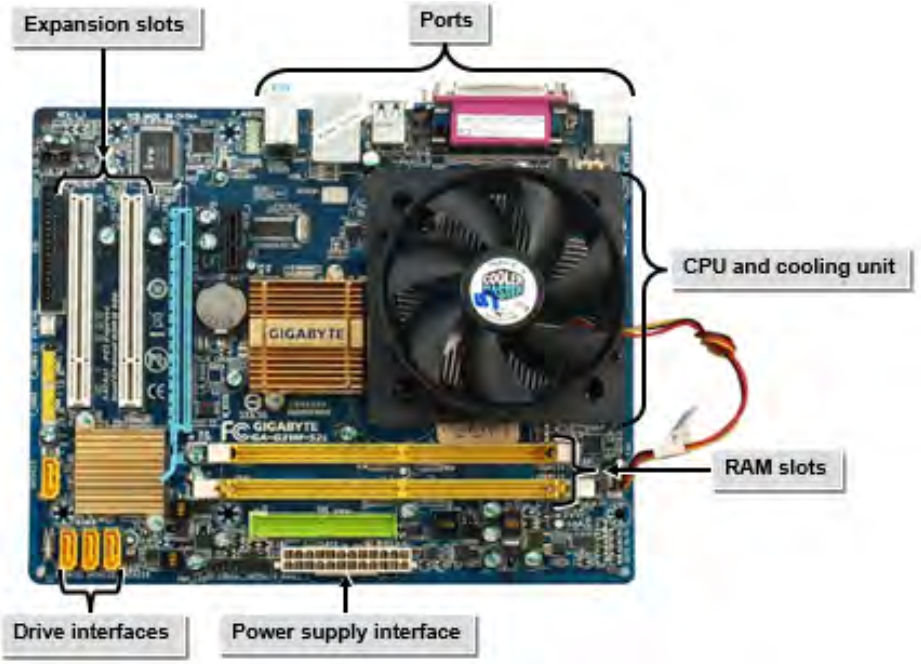
Identify Internal Computer Components

Identify Internal Computer Components

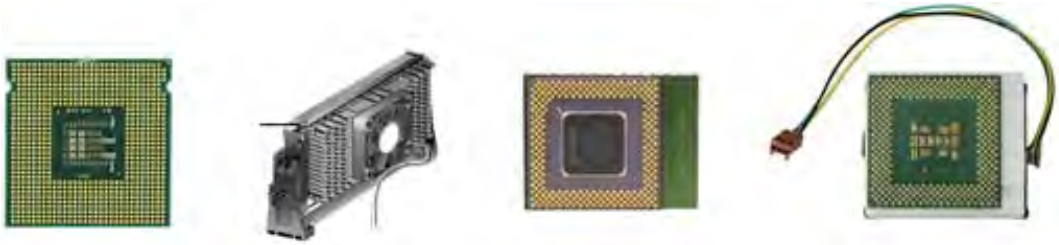
- ✓Motherboards
- ✓CPUs
- ✓Power Supplies
- ✓RAM
- ✓Storage
- ✓Expansion Cards
- ✓Cooling Systems

Motherboards

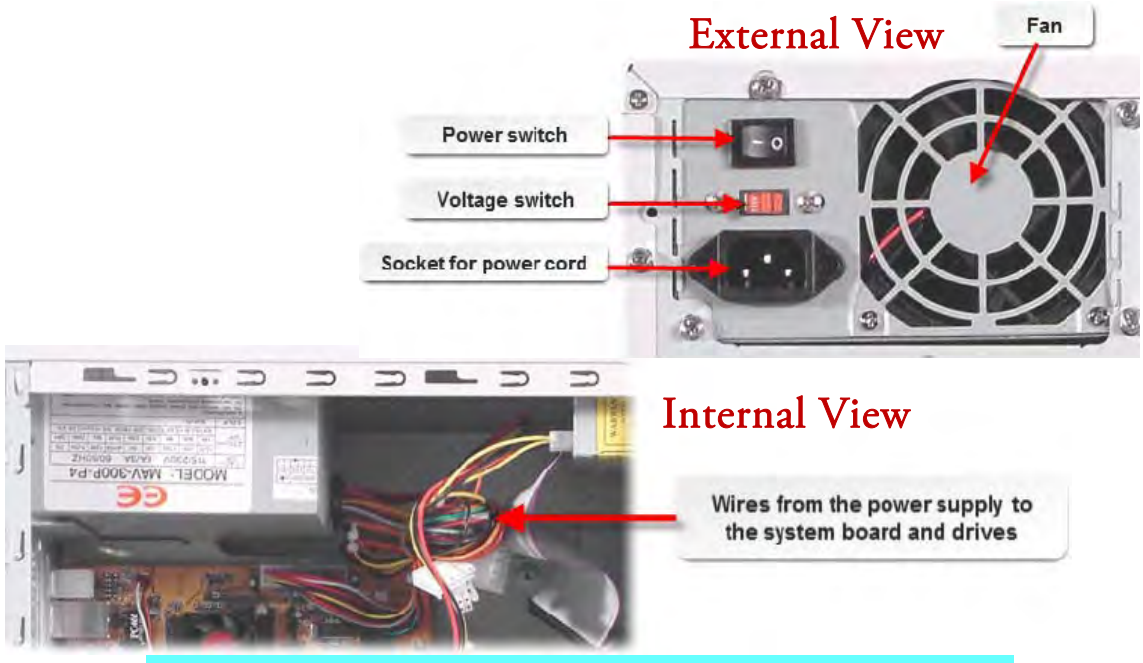
: *Sometimes called System Board or Mainboard*



Central processing unit (CPU)



Power Supplies



The power supply unit of a desktop computer

Random access memory (RAM)

Random access memory (RAM) :

- ✓is volatile memory.
- ✓measure larger amounts of memory

Memory Unit	*Description*
Byte	One character (a letter, number, space, or punctuation mark). A byte consists of 8 bits.
Kilobyte (KB)	1,024 bytes or 8,192 bits constitute 1 KB.
Megabyte (MB, Meg, or M)	1,048,576 bytes or 1,024 KB constitute 1 MB.
Gigabyte (GB)	1,073,741,824 bytes or 1,024 MB constitute 1 GB.
Terabyte (TB)	1,099,511,627,776 bytes or 1,024 GB constitute 1 TB.

DIMM vs. SODIMM

Dual in-line memory modules (DIMMS) :

- ✓are found in many systems, and they have a 64-bit data path.
- ✓DIMMs generally have 16 or 32 chips per module.

DIMM vs. SODIMM

Small outline dual in-line memory modules (SODIMMs) :

- ✓Small outline dual in-line memory modules (SODIMMs) are half the size of DIMMs .
- ✓have either 32- or 64-bit data paths.

Crucial 4GB SODIMM

Storage

Hard Drive

Solid state drive

Optical drive

Types of Optical Discs

- ✓ CD-ROM
- ✓ CD-R
- ✓ CD-RW
- ✓ DVD-ROM
- ✓ DVD-R
- ✓ DVD+R
- ✓ DVD+R DL
- ✓ DVD-RW
- ✓ DVD+RW
- ✓ DVD-RAM
- ✓ BD-ROM

USB Drive

Multi-card Readers and Writers

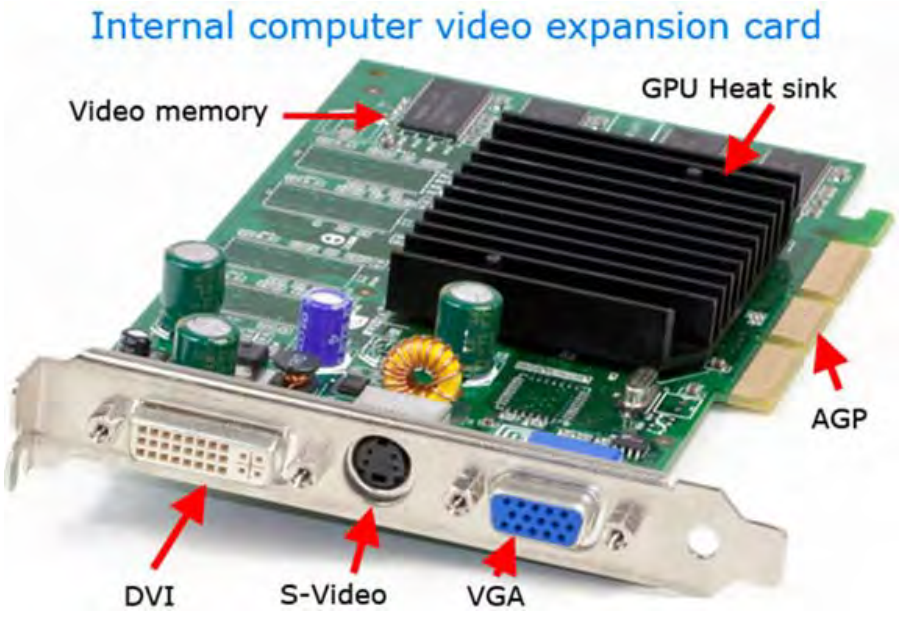
Mobile Media Devices

Expansion Cards

An expansion card :

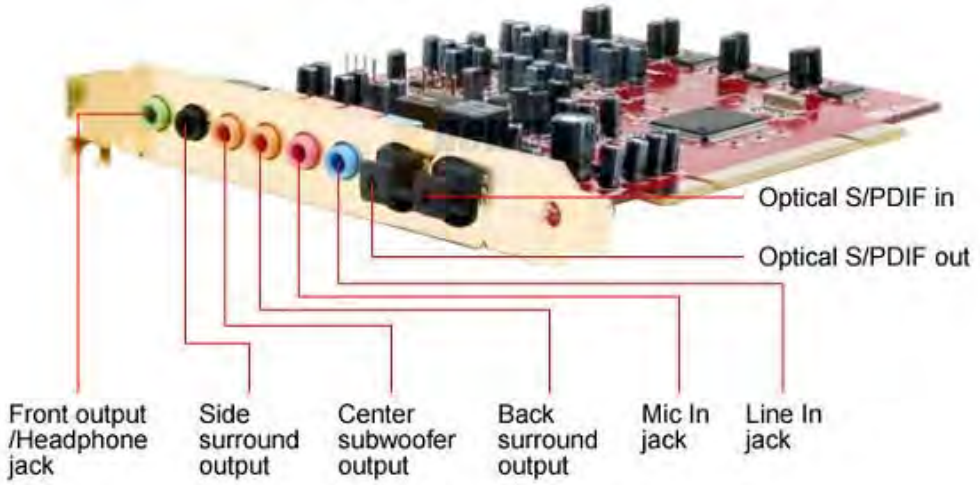
- ✓ is a printed circuit board that you install into a slot on the computer's system board to expand the functionality of the computer.
- ✓ Expansion card type :
  - Video card
  - Audio card
  - Network card
  - Modem

Expansion Cards



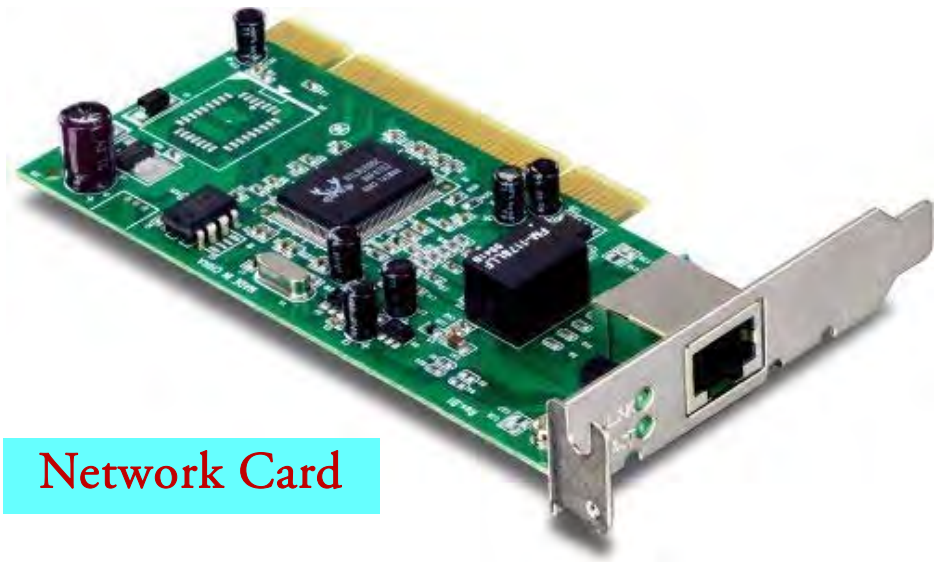
Video Card

Expansion Cards



Audio Card

Expansion Cards

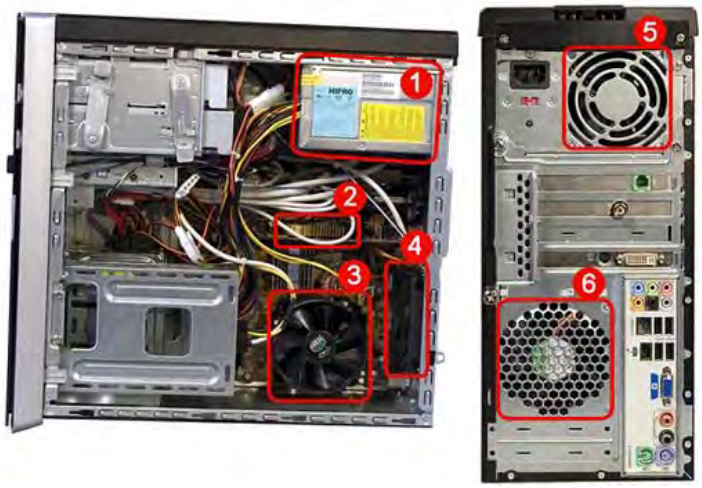


Network Card

Expansion Cards

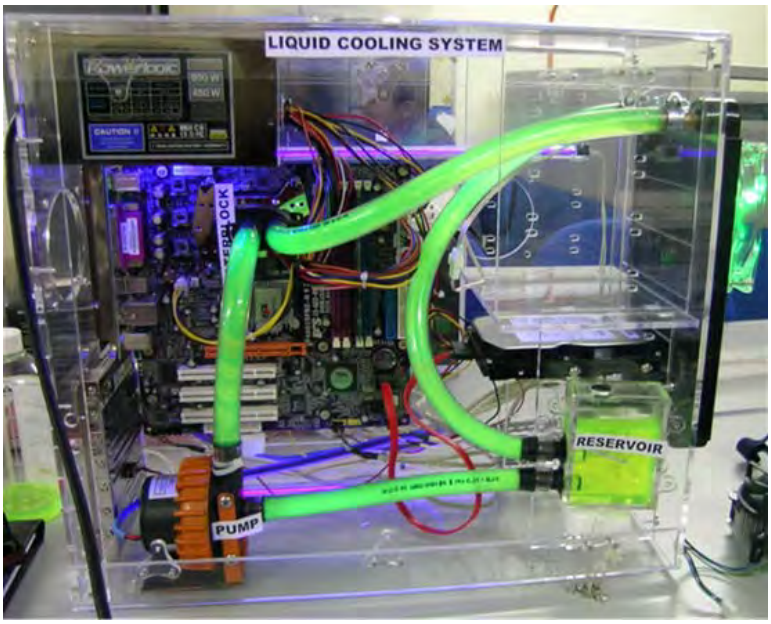
Modem

Cooling System



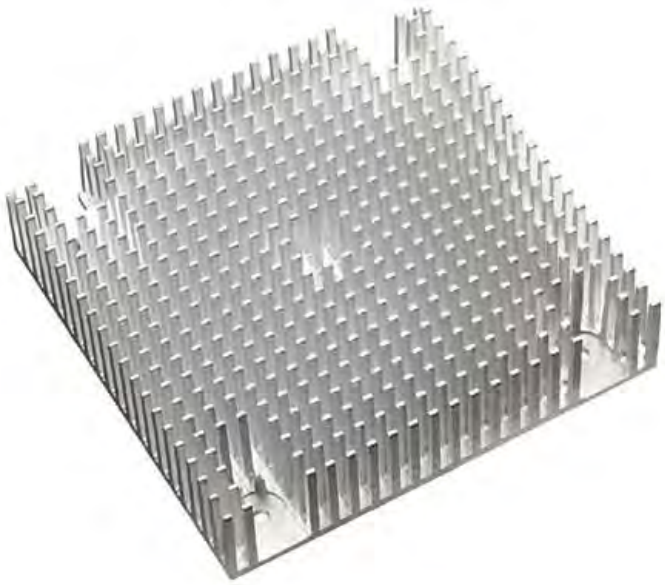
Fans

Cooling System



Liquid Cooling System

Cooling System



Heat sink

Questions

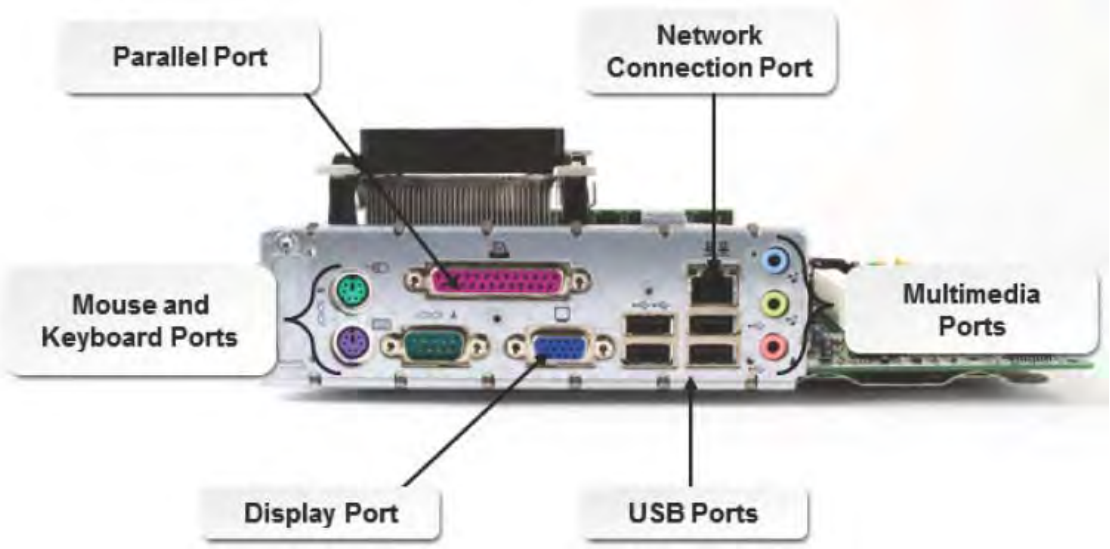
CompTIA IT Fundamentals

Lesson 1
Identifying Computer Hardware

CompTIA IT Fundamentals

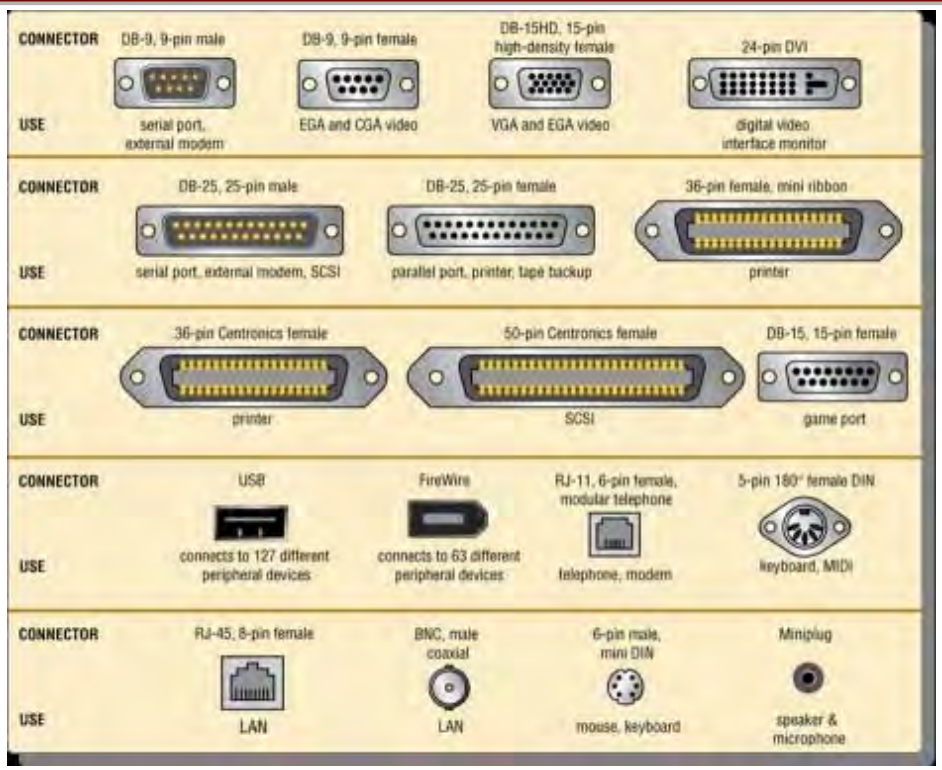
Topic C :
Common Computer Connector Types

Ports



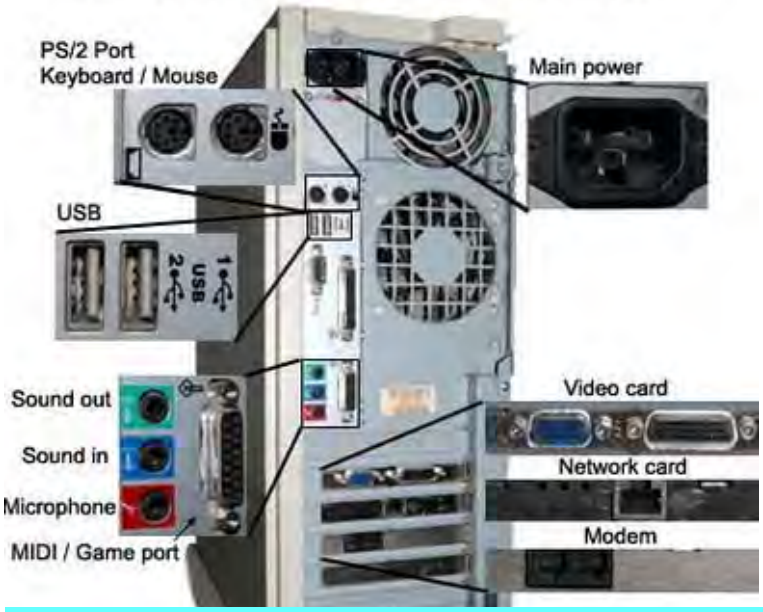
Ports on the personal computer

Genders / Port Shapes



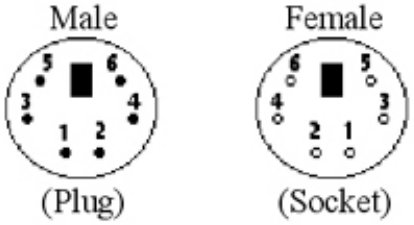
Connections

Back of computer case and each connection



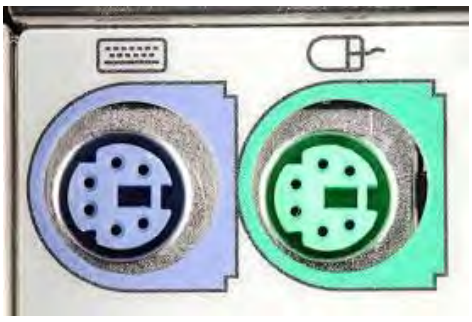
A personal computer connection

P/S2 Ports and Connectors

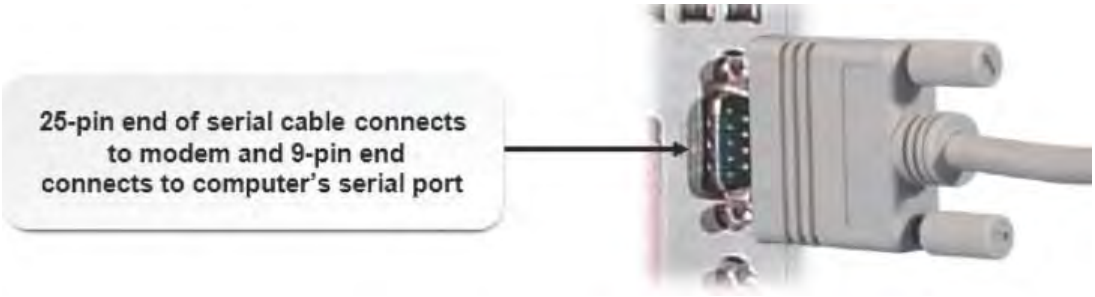


6-pin Mini-DIN (PS/2):

1 - Data
2 - Not Implemented
3 - Ground
4 - Vcc (+5V)
5 - Clock
6 - Not Implemented



Serial Ports and Connectors

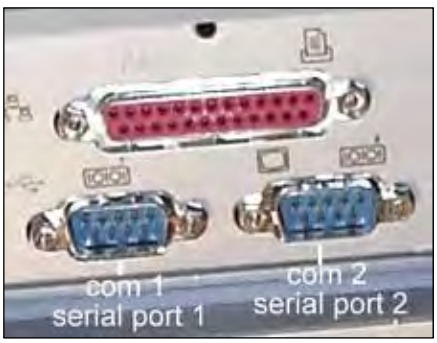


Serial Ports Naming

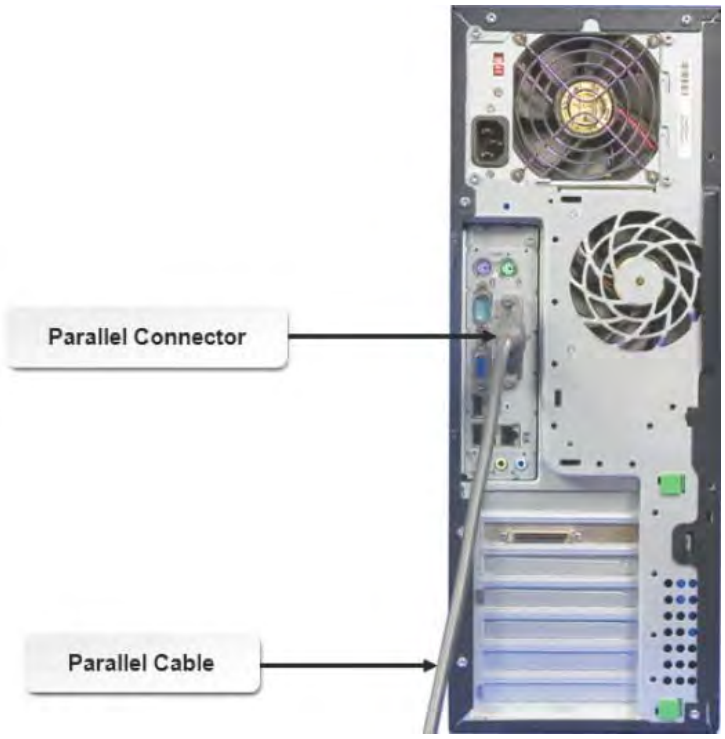
Serial port setting :

- ✓ 3F8/IRQ4 (COM1) : default the first serial port
- ✓ 2F8/IRQ3 (COM2) : default for the second serial port.
- ✓ 3E8/IRQ4 (COM3)
- ✓ 2E8/IRQ3 (COM4)

COM Port	Base Address	IRQ Setting
COM1	3f8	4
COM2	2f8	3
COM3	3e8	4
COM4	2e8	3

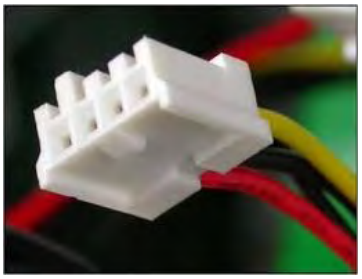


Parallel Ports and Connectors



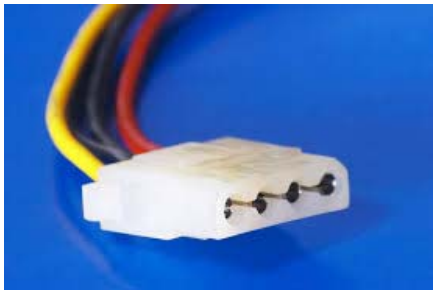
Power Connections & Connectors

Main power connector



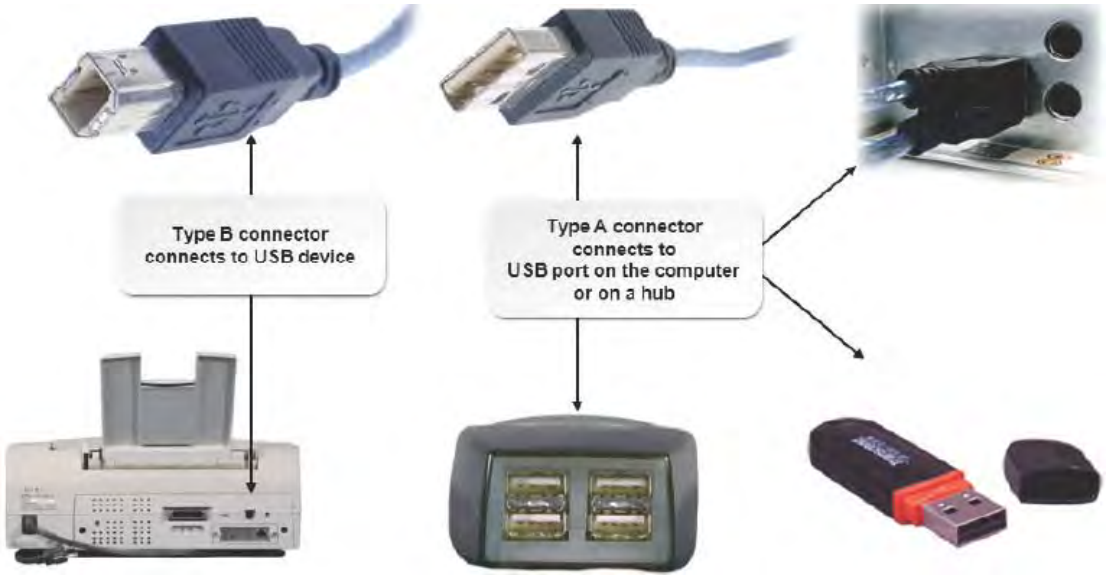
Berg connector

SATA power connector



Molex connector

USB Ports and Connectors



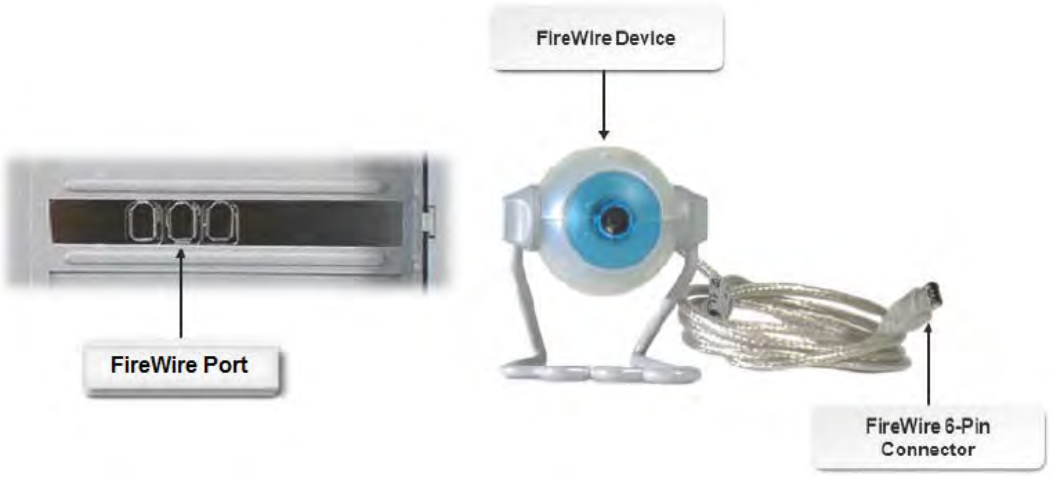
USB Connections

USB Standards

	Logo	Speed	Transmission	Power Supply	Cable Length
USB1.1		Low-speed(1.5Mbps) Full-speed(12Mbps)	Half-duplex two-wire differential signaling Unidirectional data flow with negotiated directional bus transitions	5V / 500mA	5M
USB2.0		Low-speed(1.5Mbps) Full-speed(12Mbps) High-speed(480Mbps)		5V / 500mA	5M
USB3.0		Low-speed(1.5Mbps) Full-speed(12Mbps) High-speed(480Mbps) Super-speed(5.0Gbps)	Dual-simplex, four wire differential signaling separate from USB2.0 signaling Simultaneous bi-directional data flows	5V / 900mA	5M

FireWire Terminology : IEEE 1394 Standard

FireWire Ports and Connectors



FireWire Terminology : IEEE 1394 Standard

FireWire vs. USB

Type	Transfer Rate	Number of Devices	Length
USB 1.1	12 Mbps	127	5 m
USB 2.0	480 Mbps	127	5 m
FireWire 1394a	400 Mbps	63	4.5 m
FireWire 1394b	800 Mbps	63	100 m

FireWire vs. USB

	Rate (bit/s)	Rate (byte/s)
USB 1.1	1.536 Mbit/s	0.192 MB/s
USB 2.0	12 Mbit/s	1.5 MB/s
USB 3.0	5000 Mbit/s	625 MB/s
FireWire 400	393.216 Mbit/s	49.152 MB/s
FireWire 800	786.432 Mbit/s	98.304 MB/s
FireWire 1600	1573 Mbit/s	196.6 MB/s
FireWire 3200	3145.7 Mbit/s	393.216 MB/s

Audio Ports and Connectors

Single-core/shielded cable

One pair/shielded cable

3-pin XLR connectors

TS and TRS connectors

Audio Ports and Connectors

Video Ports and Connectors

Video Graphics Array (VGA)

Digital Video Interface (DVI)

Video Ports and Connectors

Video Ports and Connectors

Mini-High Definition Multimedia Interface (Mini-HDMI)

High Definition Multimedia Interface (HDMI)

Video Ports and Connectors

Video Ports and Connectors

Separate Video (S-Video)

Component/RGB

Composite video

Coaxial

Video Ports and Connectors

Video Ports and Connectors

Radio Corporation of America (RCA)

DisplayPort

Bayonet Neill-Concelman (BNC)

Video Ports and Connectors

DVI Single Link vs. Dual Link

DVI Single Link :

- ✓ use a technology called Transition Minimized Differential Signaling (TMDS)
- ✓ to transmit serial data over a high-speed connection.

DVI Single Link vs. Dual Link

Dual Link :

- ✓ Single link cables use a single TMDS transmitter to carry data, while double-link uses two.
- ✓ can transmit larger images at higher speeds than single link.

Wireless A/V Connections

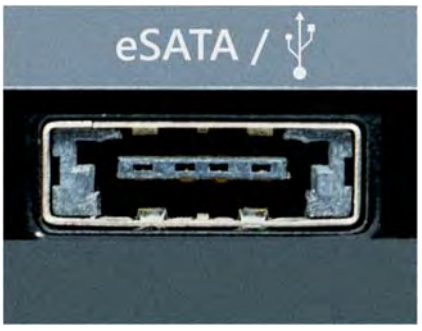
A wireless audio/visual adapter

- ✓ needs to be attached to the display monitor in order for the display to receive a signal from the device that is projecting to it.

eSATA Connectors

External SATA (eSATA) :

- ✓ is an external interface for SATA connections.
- ✓ provide fast data transfers without having to translate data between the device and the host computer.



eSATA and USB port

RJ-45 Ports and Connectors

The RJ-45 connector :

- ✓ used on twisted pair cable.
- ✓ eight-position connector that uses all four pairs of wires.
- ✓ The RJ in RJ-11 or RJ-45 is an abbreviation for "registered jack."

RJ-45 connector.

RJ-11 Ports and Connectors

The RJ-11 connector :

- ✓ used with Category 1 cables in telephone system connections
- ✓ is not suitable for network connectivity.
- ✓ smaller than RJ-45 connectors and have either four or six pins.

RJ-11 connector.

Questions

CompTIA IT Fundamentals

Lesson 1
Identifying Computer Hardware

CompTIA IT Fundamentals

Topic D :
Identify Common Peripheral Devices

Peripheral Devices

- ✓ is a external device that connects to a computer to expand the computer's functionality.
- ✓ examples : keyboards, mouse or other pointing devices, microphones, cameras, scanners, printers, and external drives.

Peripheral Devices

Input Devices

- ✓ is any hardware device that sends data to a computer, allowing you to interact with and control the computer.

Input Devices

Examples of Manual Input Devices

Keyboard 	Numeric Keypad 	Pointing Device 	Remote Control 
Joystick 	Touch Screen 	Scanner 	Graphics Tablet 
Microphone 	Digital Camera 	Webcams 	Light Pens 

Types of Input Devices

1. Keyboard

1.1 Standard keyboards

- ✓ rectangular in shape
- ✓ have 84, 101, or 104 keys.

Types of Input Devices

1.2 Ergonomic keyboard

- ✓ or natural keyboards
- ✓ split the keyboard in half so each hand can comfortably use its own set of keys.

Types of Input Devices

1.3 Dvorak keyboard

- ✓rearrange the keys into a more efficient arrangement
- ✓makes faster typing possible for users

Types of Input Devices

2. Pointing Device

Mouse

Trackball mouse

Touch pad

Trackpoint

Stylus pen

Joystick

Types of Input Devices

3. Other Input Device

Scanner

Microphone

Webcam

Graphics tablet

Output Devices

- ✓ enable the user to get information and data out of the computer.
- ✓ Typical examples include printers, speakers, and displays.

Types of Output Devices

1. Printer

1.1 Laser Printer

- ✓ is a printer that uses a laser beam to form images and toner to print the images on a printing medium

Types of Output Devices

1.2 Inkjet Printer

- ✓ is a printer that forms images by spraying liquid ink from an ink cartridge out of nozzles aimed carefully on the printer.

Types of Output Devices

1.3 Thermal Printer

- ✓ 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.

Types of Output Devices

2. Display Device

2.1 CRT (Cathode ray tube)

- ✓ displays use electron beams within a vacuum tube to create images on a fluorescent screen.

Types of Output Devices

2.2 LCD (Liquid crystal display)

- ✓ displays are a compact, lightweight alternative to traditional CRT displays.

Types of Output Devices

2.3 LED (Light-emitting diode)

- ✓ displays utilize the same screen as an LCD display, but use a different backlighting technique/technology.

Types of Output Devices

2.4 OLED (Organic light emitting diode)

- ✓ used in a larger variety of dimensions than LED screens, and are currently utilized in computer monitors, television screens, tablets, and mobile phones.

Types of Output Devices

2.5 Plasma (Plasma displays)

- ✓ 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.

Types of Output Devices

2.6 Projector

- ✓ used to display the video output onto a whiteboard or other surface so that a larger audience can see it.

Devices that Perform Both Input and Output Functions

Flash drive

External hard drive

Mobile media

Smartphone

Memory card

Optical discs and drives

Network attached storage

Touchscreen

Questions

CompTIA IT Fundamentals

Lesson 2

Identifying Computer Software

CompTIA IT Fundamentals

Topic A :

Compare Functions and Features of Common Operating Systems

Operating Systems

- ✓ is a software package that enables a computer to function.

Operating System Software

Operating System Functions

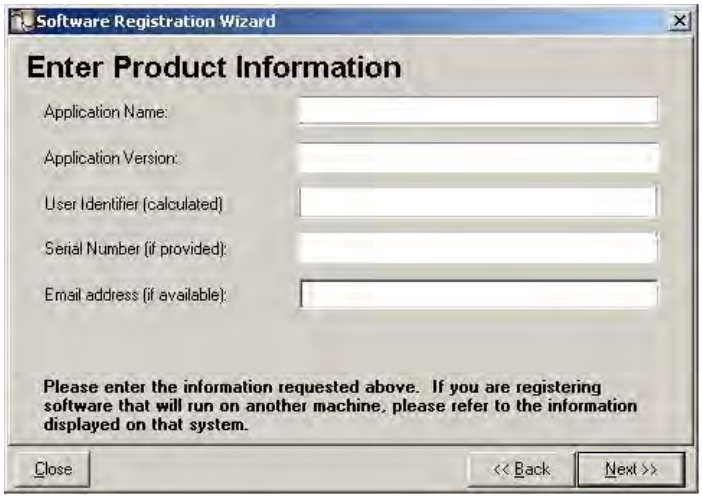
- ✓ Provides the user-friendly environment to work with system features and applications.
- ✓ Converts a user's input and sends it to the monitor or other display device.
- ✓ Controls peripheral devices such as disk drives and printers.
- ✓ Provides the structure for files and folders.
- ✓ Monitors the operating system's health and functionality.

Licensing

- ✓ *Open source :* software enables users to access its source code and gives them the right to modify it .
- ✓ *Freeware :* applications can be downloaded from the Internet directly and used without any restrictions .
- ✓ *Commercial :* software application is sold to users .
- ✓ *Copyleft :* is used to define a concept that is essentially the opposite of “copyright .”
- ✓ *Shareware :* free applications that a user can download from the Internet directly .

Software Registration

- ✓ By registering the software, a user becomes eligible to receive regular updates, upgrades, and technical support.



Types of Operating Systems for Workstations

Microsoft Windows

Google Chrome OS

Mac OS X

LINUX

Types of Operating Systems for Mobile Devices

RIM BlackBerry

Blackberry OS 6

iOS

ANDROID

Windows phone

Operating System Compatibility Issues

- ✓ **Hardware :** The 32-bit and 64-bit OS architectures have different hardware requirements.
- ✓ **Applications :** designed to run on 64-bit operating systems are not compatible with 32-bit OSs.
- ✓ **Drivers :** is specialized software that controls a device attached to a computer.

Questions

CompTIA IT Fundamentals

Lesson 2

Identifying Computer Software

CompTIA IT Fundamentals

Topic B :

Identify Application Software

Application Software

- ✓ is a program that provides specific functionality such as word processing, graphics creation, or database management.

Software applications that run on a Windows operating system.

Types of Productivity Software

- ✓ **Word processing**
  : used to create and work with typed documents.
- ✓ **Spreadsheet**
  : used to calculate and analyze tables of numbers.
- ✓ **Email**
  : used to communicate with others.
- ✓ **Basic database**
  : used to manage large volumes of lists and records.
- ✓ **PDF**
  : used to view, create, and work with PDF documents.

Types of Productivity Software

- ✓ **Presentation**
  : used to create and work with slide shows.
- ✓ **Desktop publishing**
  : used to work with page layouts and typography in documents and publications.
- ✓ **Personal information managers (PIM)**
  : used to manage your contacts and schedules.
- ✓ **Remote desktop**
  : used to access another desktop to provide troubleshooting assistance.

Collaboration software

Collaboration software :

- ✓ is designed to facilitate sharing data and resources between users in a variety of locations
- ✓ and using a variety of computing devices.

Types of Collaboration Software

Common types of collaboration software

- ✓ **Online workspace**
  - : enables users to work with common files in a shared space on the web.
  - : Example Microsoft SharePoint.
- ✓ **Document storage / sharing**
  - : provides a repository to store and share files between users in various locations.
  - : Example OneDrive and Dropbox.

Types of Collaboration Software

Common types of collaboration software

- ✓ **Screen sharing**
  - : enables users to see each other's desktops from remote locations.
  - : Example - Windows Remote Assistance and TeamViewer.
- ✓ **Video conferencing**
  - : enables users to communicate with audio and video functionality from diverse locations.
  - : Example - Skype and Google Hangouts.

Types of Collaboration Software

Common types of collaboration software

- ✓ Instant messaging
  - : enables users to work with common files in a shared space on the web.
  - : Example - Microsoft Lync and AOL Instant Messenger (AIM).
- ✓ Email
  - : allows users to share contact and calendar information.
  - : Example - OneDrive and Dropbox.

Types of Utility Software

- ✓ Antimalware
  - : detects and eliminates malicious software that resides on a computer.
  - : Example - Windows Defender and Malwarebytes Anti-Malware.
- ✓ Software firewalls
  - : filter incoming or outgoing network traffic depending on how they are configured.
  - : Example - ZoneAlarm and Comodo Internet Security (CIS).

Types of Utility Software

- ✓ Diagnostic/maintenance
  : software reports on any problems or issues that a computer may be experiencing.
  : Example - Windows Action Center and PC-Doctor.
- ✓ Compression
  : software reduces the size of files so that they can be stored and transmitted more easily.
  : Example - WinZip and 7-Zip.

Types of Specialized Software

- ✓ Computer-aided design (CAD)
  : used to create design specifications for electronics, mechanical objects, animation, and other products.
  : Example - AutoCAD and SketchUp.
- ✓ Graphic design
  : used to create visual representations of concepts and ideas.
  : Example - Adobe Illustrator and CorelDRAW.

Types of Specialized Software

- ✓ Medical
  - : used to collect, analyze, and present data related to medical information.
  - : Example - AutoCAD and SketchUp.
- ✓ Scientific
  - : used to collect, analyze, and present data used in experiments.
  - : Example - LISREL and Sage.

Types of Specialized Software

- ✓ Financial
  - : used to keep track of expenses, maintain a budget, file taxes, and manage other financial information.
  - : Example - Quicken and Microsoft Dynamics.
- ✓ Gaming
  - : software enables you to purchase, collect, and play video games on a computer.
  - : Example - Steam and Origin.

Types of Specialized Software

- ✓ **Entertainment**
  : software enables you to purchase, collect, and experience entertainment media such as music and movies on a computer.
  : Example - Google Play and iTunes.

Common File Types and Extensions

Types of Files	File Extensions
Documents	.txt
	.rtf
	.doc / .docx
	.xls / .xlsx
	.ppt / .pptx
	.pdf
Audio	.aac
	.flac
	.m4a
	.mp3
	.wav

Types of Files	File Extensions
Images	.bmp
	.gif
	.jpg / .jpeg
	.png
	.tif / .tiff
Video	.avi
	.flv
	.mp4
	.mpg / .mpeg
	.wmv

Common File Types and Extensions

Types of Files	File Extensions
Executables	.app
	.bat
	.com
	.exe
	.msi
	.scexe
Compression formats	.iso
	.dmg
	.gzip/.gz
	.jar

Types of Files	File Extensions
Compression formats	.rar
	.7zip/.7z
	.tar
	.zip

Questions

CompTIA IT Fundamentals

Lesson 3

Setting Up a Basic Workstation

CompTIA IT Fundamentals

Topic A :

Connect Hardware

Workstation Setup Process

To set up a basic workstation :-

1. Gather and connect hardware components.
2. Power on the computer.
3. If necessary, run the operating system setup utility.
4. If necessary, configure the peripherals.
5. Configure and verify the Internet connection.

Workstation Setup Process

To set up a basic workstation :

6. Install security software.
7. Identify applications should be on the workstation, and install / uninstall applications as necessary.
8. Update operating system, security, and application software as needed to ensure that all software is up to date.
9. Configure user accounts as needed.
10. Perform basic cable management to reduce clutter and enhance physical safety.

Cable Management

Tips for managing cables :

- ✓ recommend cord protectors be used to shield the cords and cables must traverse a floor area
- ✓ use Velcro® strips, twist ties, or large binder clips to gather a computer's cables together.

Questions

CompTIA IT Fundamentals

Lesson 3

Setting Up a Basic Workstation

CompTIA IT Fundamentals

Topic B :

Install and Configure Operating Systems

Install and Configure Operating Systems

- ✓ Operating System Hardware Requirements :
  - ✓ Each operating system (OS) requires specific minimum hardware.
- ✓ Operating System Installation Programs :
  - ✓ Types of installation programs
    - A Windows setup wizard
    - A system image (ISO file)

Install and Configure Operating Systems

- ✓ Common Operating System Configuration Parameters
  - Date
  - Time zone
  - Language
  - Keyboard type
  - Screen resolution
  - Audio settings

* * Note : Parameters such as date, time zone, and language are commonly referred to as localization settings.

Multiple User Accounts

- ✓ A user account is an information profile that uniquely identifies a user on a computer.
- ✓ Every user account on a computer needs to have a unique user name / password.
- ✓ Users can set their own passwords.
- ✓ Different users on the same computer may have different rights and permissions

User Account Information

User Account Characteristics :

- ✓ **User name**
  : a unique name identifying a user on a computer.
- ✓ **Password**
  : a strong password is a combination of both upper and lowercase letters, numbers, and special characters.
- ✓ **Permissions and rights**
  : allowed to do on a computer and what resources the user can access.

Peripheral Configuration

For example, in Windows 8.1,
: Use Control Panel utilities to configure peripheral devices.

- ✓ Use Devices and Printers : Device Manager -> scan for hardware.
- ✓ Use Display : configure display devices, adjust screen resolution, a second monitor, and adjust screen brightness.

Peripheral Configuration

- ✓ Use Keyboard : configure the keyboard properties.
- ✓ Use Mouse : configure mouse and pointer properties, such as primary button, double-click speed, and pointer options.
- ✓ Use Sound : configure audio devices, speakers and microphones.
- ✓ Use Speech Recognition : configure the microphone and computer for voice input.

OS Updates

- ✓ Software updates
  - are software programs or code intended to address security flaws and performance issues in an existing version of software.
- ✓ Versioning
  - are information about the iteration of the software.
  - Software versions are changed every time the software is upgraded or newer features

OS Updates

OS Update Category	Description
Patch	small units of supplemental code meant to address either a security problem or a functionality flaw in a software package or OS.
Hotfix	is a patch that is often issued on an emergency basis to address a specific security flaw.

OS Updates

OS Update Category	Description
Service Pack	is a larger compilation of system updates (include functionality enhancements, new features, and typically all patches, updates, and hotfixes issued up to the point of the service pack release.
Rollup	is a collection of previously issued patches and hotfixes, usually meant to be applied to one component of a system, such as the web browser or a particular service.

OS Updates

OS Update Category	Description
* Remark * Automatic updates	is a feature of an operating system or a software application that enables updates to be downloaded and installed automatically on a system at a scheduled time.

Questions

CompTIA IT Fundamentals

Lesson 3

Setting Up a Basic Workstation

CompTIA IT Fundamentals

Topic C :

Install and Configure Applications

Install and Configure Applications

- ✓ **Bundled Applications**
  : are software programs that are sold together as a set or suite or that are sold with an OS or with a new computer.
- ✓ **Software Inventory**
  : is a listing of the applications that are available on a computer.

Install and Configure Applications

- ✓ **Desired Applications**
  - A web browser.
  - An email client.
  - Word processing software.
  - Security software.
  - Software updates, including OS updates.
- ✓ **Bloatware**
  : is a slang term that describes software that has lots of features and requires considerable disk space and RAM to install and run.

Install and Configure Applications

- ✓ **Application Sharing**
  : application will be available to only your account or shared with all users on the computer.

Install and Configure Applications

Guidelines for Ensuring a Computer Contains Only the Necessary Applications :

- ✓ Conduct a manual inventory or purchase an inventory utility to identify the applications currently on the computer.
- ✓ Identify one application for each of the following :
  - A web browser
  - An email client
  - Word processing software
  - Security software
  - Software updates, including OS updates

Install and Configure Applications

- ✓ Guidelines for Ensuring a Computer Contains Only the Necessary Applications
  - Remove any unnecessary applications.
  - Install any other necessary applications.

Questions

CompTIA IT Fundamentals

Lesson 3

Setting Up a Basic Workstation

CompTIA IT Fundamentals

Topic D :

Configure Accessibility Options

Accessibility

Accessibility :

- ✓ is the use of assistive technology to make computers available and easier to use.
- ✓ Accessibility features can be built-into the operating system or provided through specially designed applications and software.

Windows 8.1 Accessibility Options

Ease of Access Menu Choice :

- ✓ Narrator
- ✓ Magnifier
- ✓ On-Screen Keyboard
- ✓ High Contrast
- ✓ Sticky Keys
- ✓ Filter Keys

Windows 8.1 Accessibility Options

Narrator :

- ✓ use the commands category to define the specific keyboard shortcuts to start, stop, and repeat the reading; navigate to read different items on the screen; and adjust the voice volume.

Windows 8.1 Accessibility Options

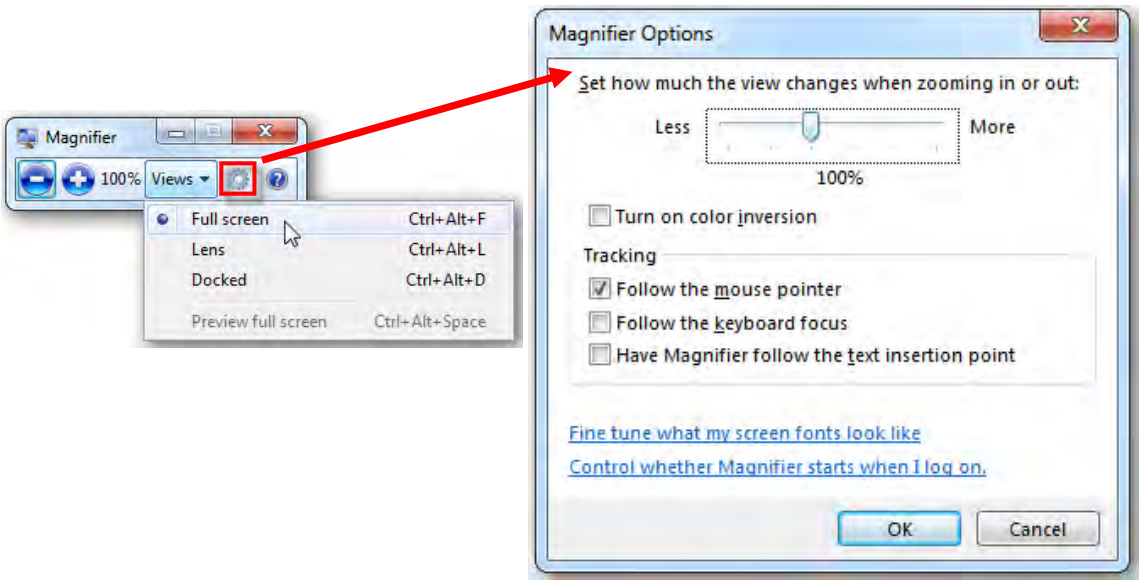
The Narrator Settings dialog box.

Windows 8.1 Accessibility Options

Magnifier :

✓ will enlarge the whole screen, or portions of the screen, to make viewing easier.

Windows 8.1 Accessibility Options



Magnifier Toolbar and Options.

Basic Accessibility Options in Other OSs

Operating System	Accessibility Features
Mac OS X	VoiceOver
	Zoom and Cursor Size
	Dictation
	Closed Captions
	Screen Flash
	Mono Audio
	Switch Control
	Slow Keys
	Sticky Keys

Basic Accessibility Options in Other OSs

Operating System	Accessibility Features
Mac OS X	Speakable Items
	Simple Finder
	Text to Speech
Chrome OS	ChromeVOX
	Accessibility settings
Android OS	TalkBack
	Explore by Touch
	Accessibility settings

Other Adaptive Technologies

Adaptive technology :

- ✓ tools that are designed to ensure that people with disabilities are able to use the software.
- ✓ Examples
  - Braille translation
  - Eye-tracking devices
  - Tobii EyeMobile

Questions

CompTIA IT Fundamentals

Lesson 4

Configuring Network Access

CompTIA IT Fundamentals

Topic A :

Network Connection Types

Computer Networks

A computer network :

- ✓ is a group of computers that are connected together to communicate and share network resources such as files, applications, and devices.

Computers connect to communicate and share resources

Computer Networks

A computer network :

- ✓ components that make up a computer network

Network Component	Description
Device	Hardware such as computers, servers, printers, fax machines, switches, and routers.
Physical media	Media that connects devices to a network and transmits data between the devices.
Network adapter	Hardware that translates data between the network and a device.
Network operating system	Software that controls network traffic and access to common network resources.

Network Types

Different between LANs and WANs :

- ✓ A local area network (LAN)
  - is a group of computers and associated devices that share the resources of a single processor or server within a small geographic area.
  - A LAN may serve as few as two or three users or as many as thousands of users.
  - A network set up between the computers in a home would be an example of a LAN.

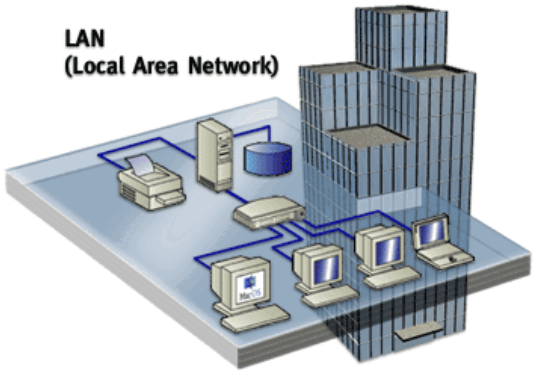
Network Types

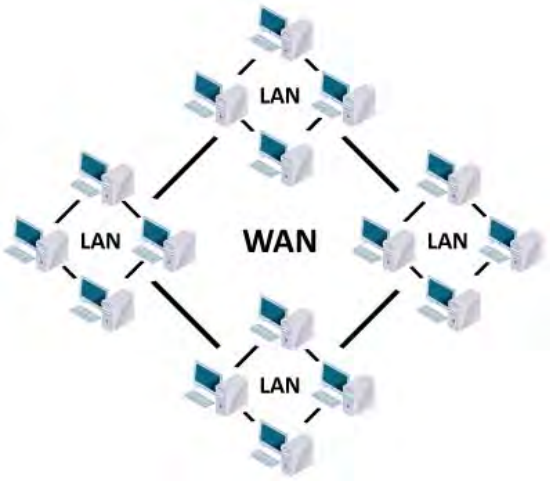
Different between LANs and WANs :

- ✓ A wide area network (WAN)
  - is a network of computers that are spread across a large geographic area.
  - An example of a WAN would be a company that has offices in several different cities or nations; the company's computers would be connected by a WAN.

Network Types

Different between LANs and WANs :





LAN

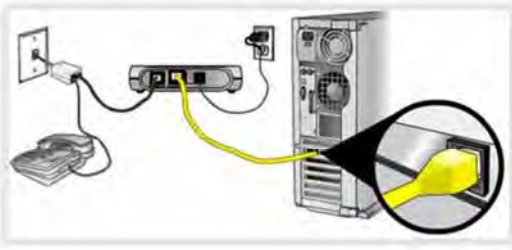
WAN

Network Connection Methods

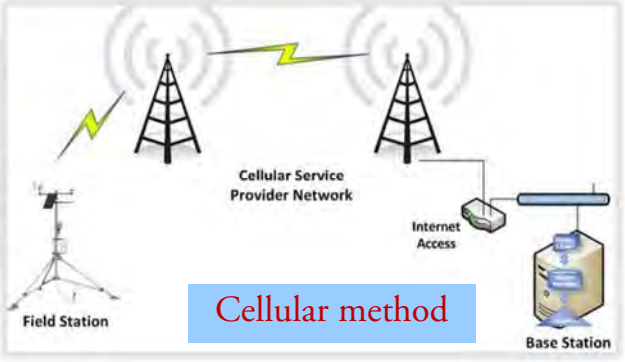
Network connection methods :

- ✓ Wireless
- ✓ Wired
- ✓ Cellular

Wireless method



Wired method



Cellular method

Network Connection Methods

Important characteristics in networking :

- ✓ Mobility
- ✓ Availability
- ✓ Throughput
- ✓ Bandwidth
- ✓ Reliability
- ✓ Concurrent connections
- ✓ Security

Wired Network Connections

Wired computer networks :

- ✓ use a technology called Ethernet
- ✓ allows computers to communicate over small distances using a wired medium
- ✓ use Ethernet to provide both backbone and end-user services

Remark : Ethernet is a set of networking technologies and media access methods specified for LANs

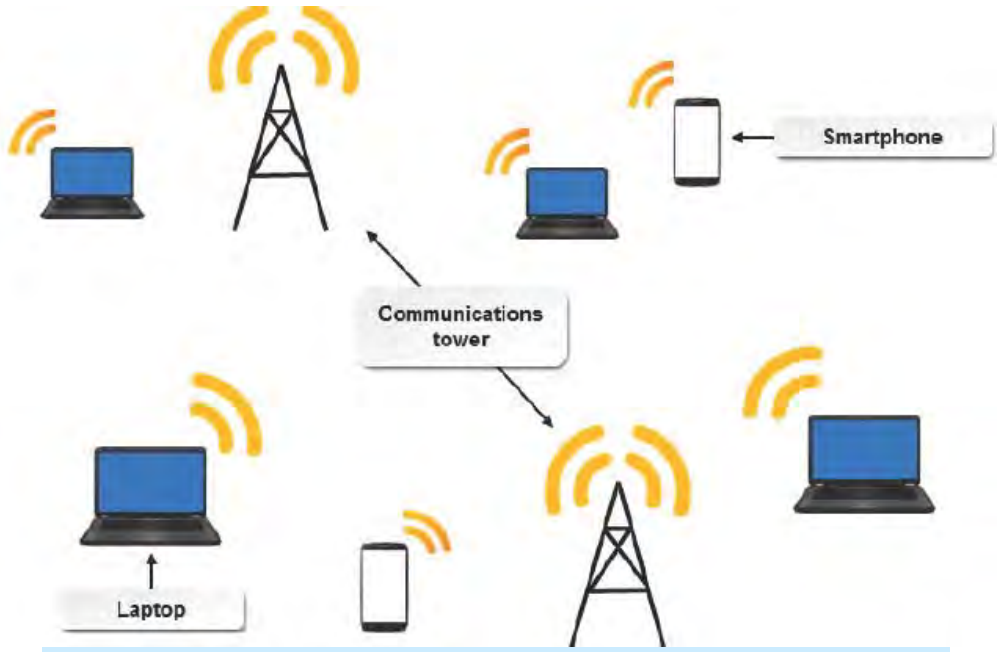
Wired Network Connections

Wireless computer network :

- ✓ is a network in which computers use wireless connections to link with other computers
- ✓ can connect a few devices over short distances, within a home or an office, or can be set up to connect computers over large distances through the Internet.
- ✓ networking protocol is Wi-Fi,
- ✓ wireless devices called wireless access points (WAPs) or wireless routers

Remark : Wireless connections transmit data by using radio frequency waves.

Wired Network Connections



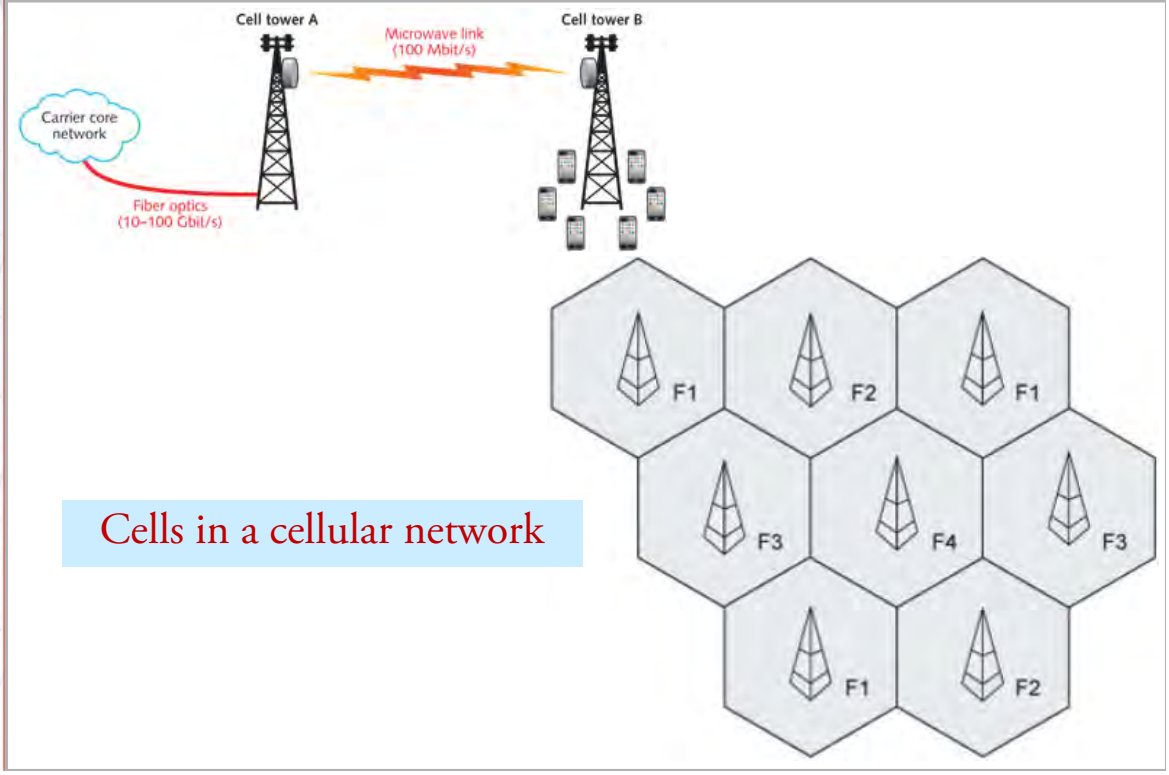
A wireless network connects devices by using radio waves

Cellular Network Connections

Cellular Network Connections :

- ✓ otherwise known as a mobile network, is a radio network.
- ✓ consists of different areas called cells
- ✓ each cell has a transceiver, known as a base station (BS) or a cell site

Cellular Network Connections



Cells in a cellular network

Mobility

Table compares the level of mobility available to users based on the network connection method :

Network	Mobility Level	Explanation
Wired	Little to none	By definition, a wired network requires computers and other devices to be physically attached to the network. Network devices are mobile only within the reach of the cables.
Wireless	Medium	With the use of a wireless router, network devices can travel outside of the reach of a cable but must stay within reach of the router signal. Some router signal strength requires the devices to be within the same building (such as a home router), whereas other routers are strong enough to broadcast across a university campus.
Cellular	High	The mobility of devices on a cellular network are limited only by their proximity to a cellular tower, as long as the device can receive a signal from the base station.

Availability

Table compares the level of availability afforded to users for the different network connection methods.

Network	Availability Level	Explanation
Wired	Medium to high	A wired network's availability depends upon the health of its network devices and its cabling infrastructure.
Wireless	Medium to high	A wireless network's availability depends upon the health of its network devices.
Cellular	High	Large telecommunications companies have many backups in place to ensure that their networks are always up and running.

Bandwidth and Throughput

Table compares the level of bandwidth and throughput available to users for different network connection methods.

Network	*Bandwidth/ Throughput Level*	*Explanation*
Wired	High	Ethernet technology provides bandwidth up to 100 Gb/s, but is more commonly provided at 10 Gb/s and 1 Gb/s for enterprise LANs.
Wireless	Medium	Wi-Fi technology provides bandwidth up to 7 Gb/s, but is more commonly provided at 1.3 Gb/s and 600 Mb/s for enterprises LANs.
Cellular	Low	4G networks typically deliver bandwidth up to 100 Mb/s.

Reliability

Table compares the level of reliability between the different network connection methods.

Network	*Reliability Level*	*Explanation*
Wired	High	Wired connections do not suffer from the interference issues that wireless connections do. As long as the physical cable is healthy, the connection should stay highly reliable.
Wireless	Medium	Wireless connections are susceptible to interference from other devices and phenomena that operate in the electromagnetic spectrum, which can interrupt connectivity and cause corruption of data in transit.
Cellular	Low	Cellular networks are also susceptible to interference. Additionally, despite their wide coverage, cellular networks often see a degradation in performance or a complete lack of connection in certain locations.

Concurrent Connections

Table compares the amount of concurrent connections that each network connection method can have.

Network	*Concurrent Connection Level*	*Explanation*
Wired	Medium	The high bandwidth of Ethernet connections means that more people can connect at once without losing significant performance. However, the number of people connected simultaneously is physically limited by the cabling infrastructure of the network.
Wireless	Medium	The lower bandwidth and small coverage of wireless networks means that few users and devices can connect to a single access point. For example, a 600 Mb/s Wi-Fi signal shared among 100 people would reduce each person's bandwidth to 6 Mb/s. Some wireless routers have a built-in limit to the amount of connections they can handle.
Cellular	High	Although they offer low bandwidth, cellular networks are intended to support millions of connections at once.

Security Levels

Table compares the level of security inherent in each network connection method.

Network	*Security Level*	*Explanation*
Wired	High	Because a wired LAN isolated from other networks requires physical access, it is much more secure from a remote breach into the network. Without this physical connection, an attacker will be unable to intercept communications.
Wireless	Medium	Attackers can intercept wireless communications without needing to be physically plugged in. The attacker just needs to be within range of the wireless network in order to monitor its transmissions. To protect against this, most modern Wi-Fi transmissions are encrypted. However, some older or poorly implemented technology may use weak encryption or none at all.
Cellular	Low	Like wireless networks, cellular transmissions are susceptible to attackers monitoring and intercepting data remotely. This is compounded by the large coverage of cellular networks and their high mobility. Many carriers implement some form of encryption, but this encryption may not be suitably strong.

Network Connection Method Comparison

Table is an overview of the strengths and weaknesses of each network connection method.

Characteristic	*Wired*	*Wireless*	*Cellular*
Mobility	Little to none	Medium	High
Availability	Medium to high	Medium to high	High
Bandwidth/throughput	High	Medium	Low
Reliability	High	Medium	Low
Concurrent connections	Medium	Medium	High
Security	High	Medium	Low

Questions

CompTIA IT Fundamentals

Lesson 4
Configuring Network Access

CompTIA IT Fundamentals

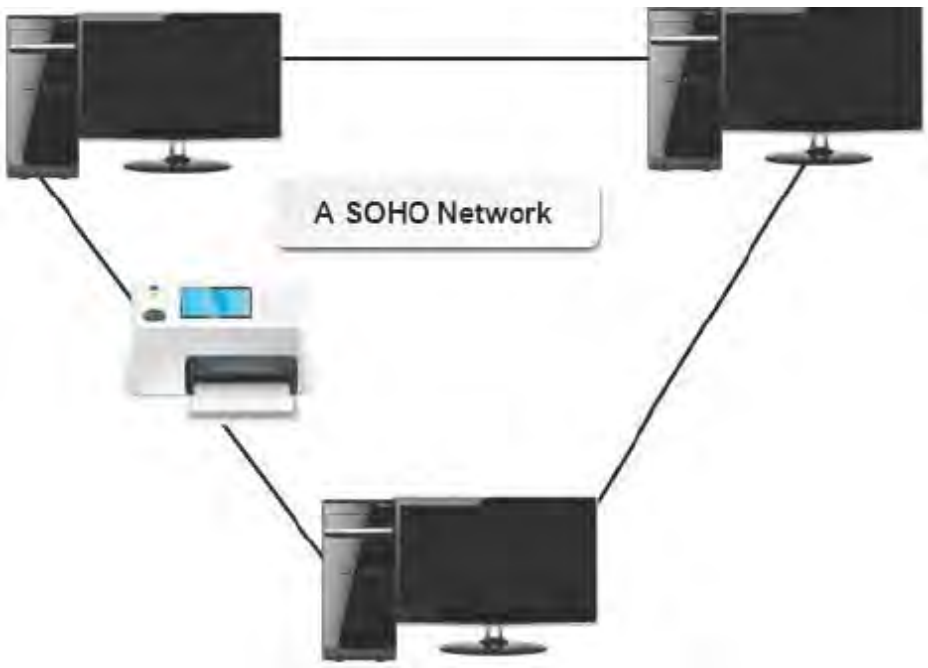
Topic B :
Install and Configure a SOHO Router

SOHO Networks

A SOHO network :

- ✓ is a network that provides connectivity and resource sharing for a small office or home office.
- ✓ limited to fewer than 20 computers or nodes
- ✓ facilitates sharing of files and printers
- ✓ contain a combination of wired and wireless computer connections

SOHO Networks



SOHO Routers

A wireless router :

- ✓ connects a computer to multiple networks through a wireless connection
- ✓ performs the functions of a wireless access point (WAP) and a router
- ✓ allow multiple users to be connected to a network at the same time
- ✓ Some wireless routers have a firewall built into them

SOHO Routers

A wireless router connects a computer to multiple networks.

SOHO Routers

Table compares the level of availability afforded to users for the different network connection methods.

Network Device	*Description*
Hub	A *hub* is a networking device that connects multiple computers to form a LAN. The hub broadcasts data in the form of signals to all connected computers. Hubs support transmission speeds of 10 Mbps, 100 Mbps, or both.
Switch	A *switch* is a small network hardware device that joins multiple computers together within the same LAN. Like hubs, switches also have multiple ports and are responsible for forwarding data from a source to a destination. However, switches forward data packets to only the nodes or segments they are addressed to and reduce the chances of collisions among data packets.
Router	A *router* is a networking device used to send data among multiple networks that use the same protocol. A protocol is a set of rules used to establish communication between two computers on a network. Routers send data among networks by examining the network addresses contained in the packets they process. A router can be a dedicated device or can be implemented as software running on a node. Although the functions of a router are similar to that of a switch, a router has a comparatively higher data handling capacity and is mainly used in WANs.

Encryption

File encryption :

- ✓ is a type of file protection that disguises the data within a file or message so that the specific information included within the file or message cannot be read or understood by unauthorized users.
- ✓ A key is used to encode the data, and neither the file nor the key contents can be read by anyone who does not have the key.

Encryption

A message being encrypted.

Wireless Encryption Standards

Wireless encryption protocols :

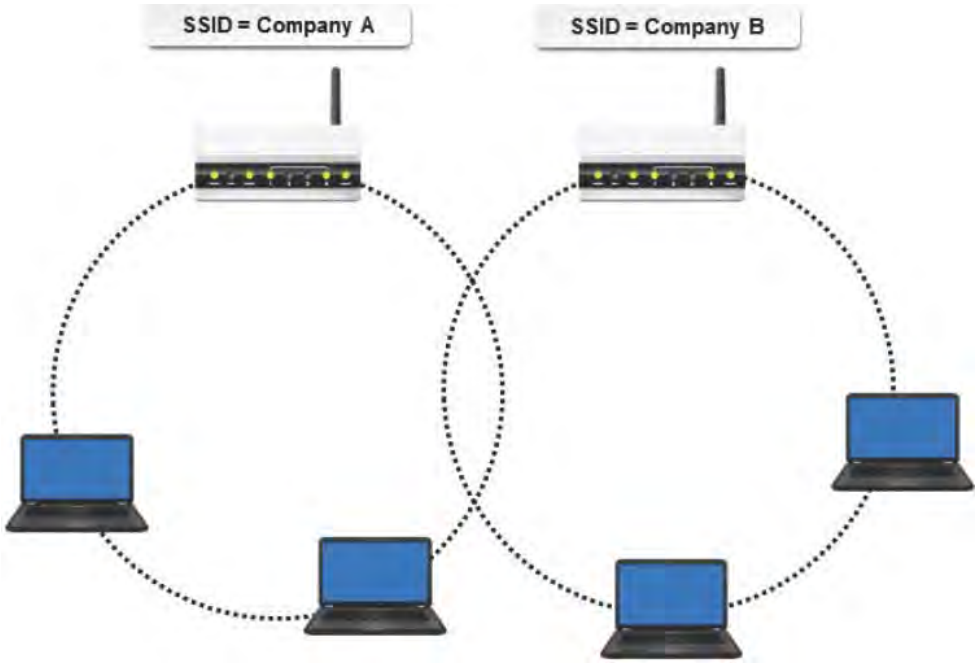
Wireless Encryption Method	*Description*
WEP	*Wired Equivalent Privacy (WEP)* is a security protocol for wireless local area networks (WLANs). WEP does not use strong encryption and is therefore considered obsolete. However, some legacy devices may only support WEP.
WPA	*Wi-Fi Protected Access (WPA)* provides a significantly stronger encryption scheme than WEP, and can use a shared private key, which are unique keys assigned to each user.
WPA2	*Wireless Protected Access 2 (WPA2)* replaced WPA encryption in 2006 and is based on the IEEE 802.11i standards. The Institute of Electrical and Electronics Engineers (IEEE) *802.11i* standard is the most recent encryption standard that provides improved encryption for wireless networking. The 802.11i standard requires strong encryption key protocols, known as *Temporal Key Integrity Protocol (TKIP)* and *Advanced Encryption Standard (AES)*. WPA2/802.11i encryption is considered to be the strongest available method of wireless security.

Service Set Identifiers (SSIDs)

A Service Set Identifier (SSID) :

- ✓ is a unique ID that consists of 32 characters and is used for naming wireless networks.
- ✓ When multiple wireless networks overlap in a certain location, SSIDs make sure that data gets sent to the correct destination.
- ✓ The SSID is different than the name that is assigned to a wireless router.

Service Set Identifiers (SSIDs)



The SSIDs of two different WAPs.

SOHO Router Configuration Options

Setting	*Description*
Basics	Basic settings apply to both wired and wireless routers and can include the ability to: • Secure your router or access point administration interface. • Change default administrator passwords (and user names). • Disable remote administration. • Secure/disable the reset switch/function. • Change the default SNMP parameter. • Regularly upgrade the Wi-Fi router firmware to ensure you have the latest security patches and critical fixes.
SSID	When installing a wireless router, change the default Service Set Identifier (SSID) and verify that you are not broadcasting out to the 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, you can use one of the 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.

Firmware

- ✓ Firmware is specialized software that is stored on a hardware device's read-only memory (ROM)
- ✓ Router firmware may need an upgrade from time to time depending on manufacturer updates.
- ✓ These updates contain security patches, updates to performance, and updates to address any known issues.

Note: Overwriting existing firmware, often through updating, is called *flashing*.

Router Setup Process

The basic setup and configuration process for a SOHO router includes :

1. Verify the wired connection, if applicable.
2. Configure encryption standard (WEP, WPA, or WPA2).
3. Change SSID from default.
4. Apply a new wireless password.
5. Change the admin password for the router.
6. Connect to the new network.
7. Verify the Internet connectivity.
8. Update firmware, if necessary.

Questions

CompTIA IT Fundamentals

Lesson 4
Configuring Network Access

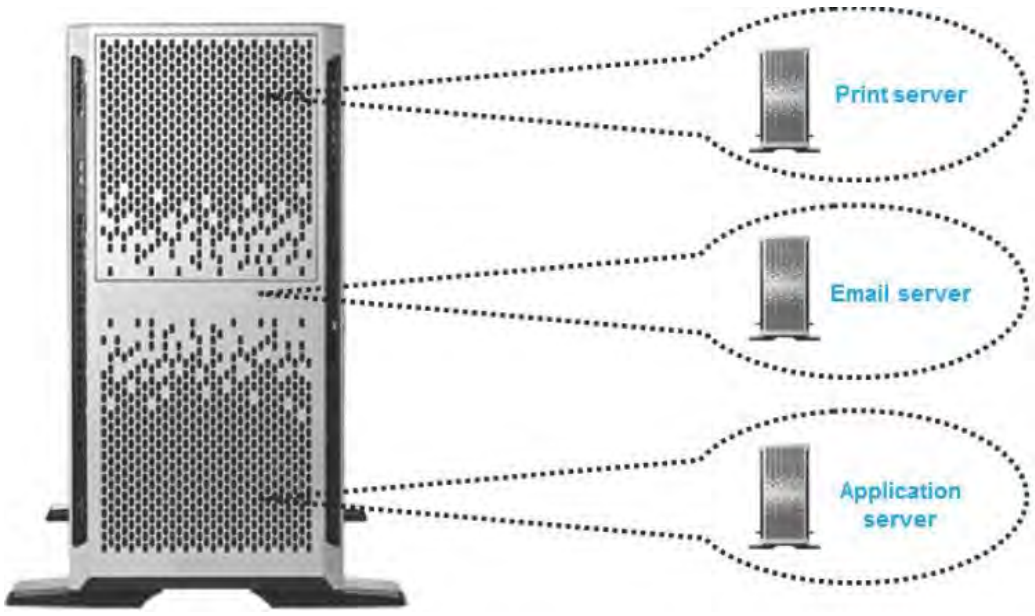
CompTIA IT Fundamentals

Topic C :
Network and Alternative Technologies

Virtualization

- ✓ virtualization software allows for one physical device, such as a server operating system, to host multiple logical operating systems.
- ✓ These logical systems are called virtual machines.
- ✓ A single physical server can host several virtual servers using one hardware platform.

Virtualization

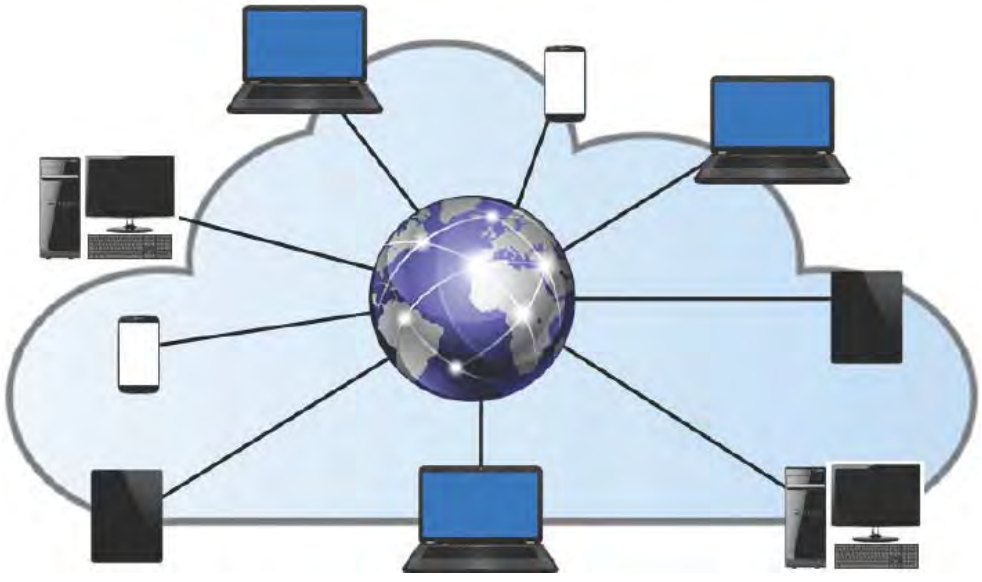


Several servers virtualized into one

Cloud Computing

- ✓ *Cloud computing* is a computing infrastructure in which resources, such as storage and applications, are hosted in a distributed fashion by a third party over the Internet.
- ✓ The "cloud" is a metaphor for the Internet and the complexity of its infrastructure.
- ✓ A major concern with cloud computing is the security of data.

Cloud Computing



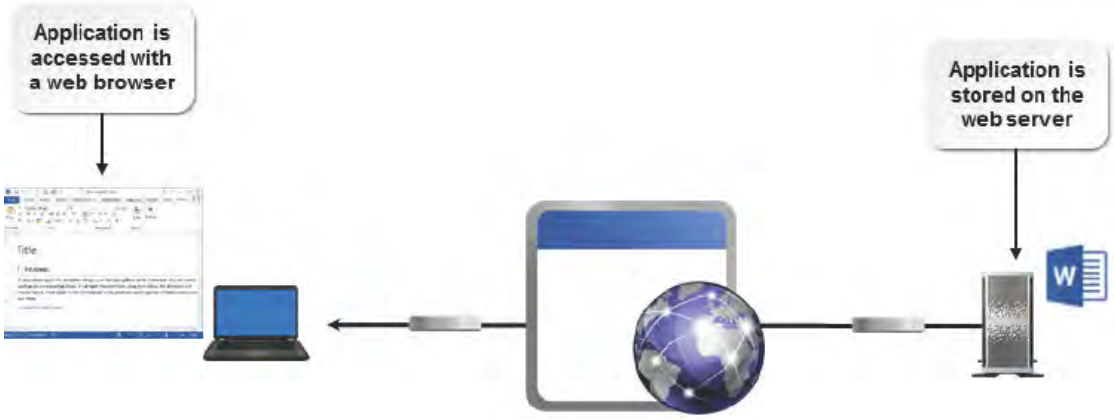
Cloud computing hosts applications over the Internet.

Web Applications

Web applications

- ✓ are software applications that are installed on web servers and delivered to users through the Internet.
- ✓ End users interact with these applications through their web browsers.
- ✓ This allows them to work with applications without having to install them on their systems.
- ✓ Such services depend on network bandwidth for efficient use as the data transfer happens in real time.

Web Applications



Web-delivered services deliver applications through the web.

VoIP

Voice over IP (VoIP) :

- ✓ is the transmission of voice communications over IP networks, such as the Internet.
- ✓ VoIP can help a business save money as well as energy and resources for the following reasons:
  - Training sessions can be done remotely; no travel is needed.
  - Remote offices can collaborate without being in the same physical location.
  - VoIP is very cost efficient and bypasses long-distance charges.

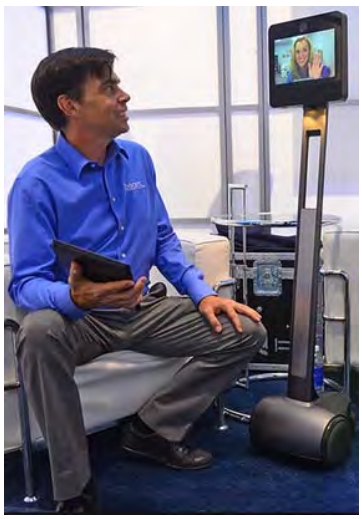
VoIP

Telepresence

- ✓ *Telepresence* is the latest generation of video conference technology. It gives users the experience of a "life-like," "face-to-face" meeting remotely, enabling them to interact as if they were in the same room.
- ✓ Telepresence equipment requires video, audio, and manipulation capabilities.
- ✓ Automated robots *(Telepresence robot)* with a connected mobile computing device (tablet, laptop, or iPad) can move around freely to simulate an absent person's presence.

Telepresence

Telepresence



A telepresence robot

Questions

CompTIA IT Fundamentals

Lesson 4
Configuring Network Access

CompTIA IT Fundamentals

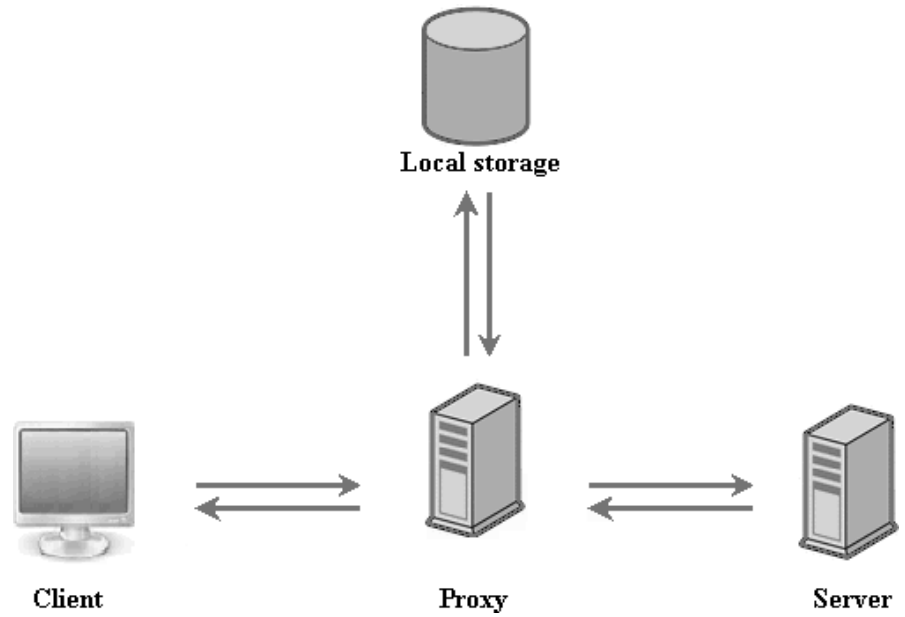
Topic D :
Sharing and Storage Methods

Local vs. Hosted Storage

Local storage :

- ✓ refers to any storage media that is directly attached to the computer that uses it.
- ✓ This can include direct-attached storage such as hard drives over Serial ATA (SATA) connections, as well as external hard drives that use ports such as USB to plug in to computers.
- ✓ Local storage often has the advantage of speed and accessibility.
- ✓ Local storage media offer security guarantees that networked storage does not.

Local vs. Hosted Storage



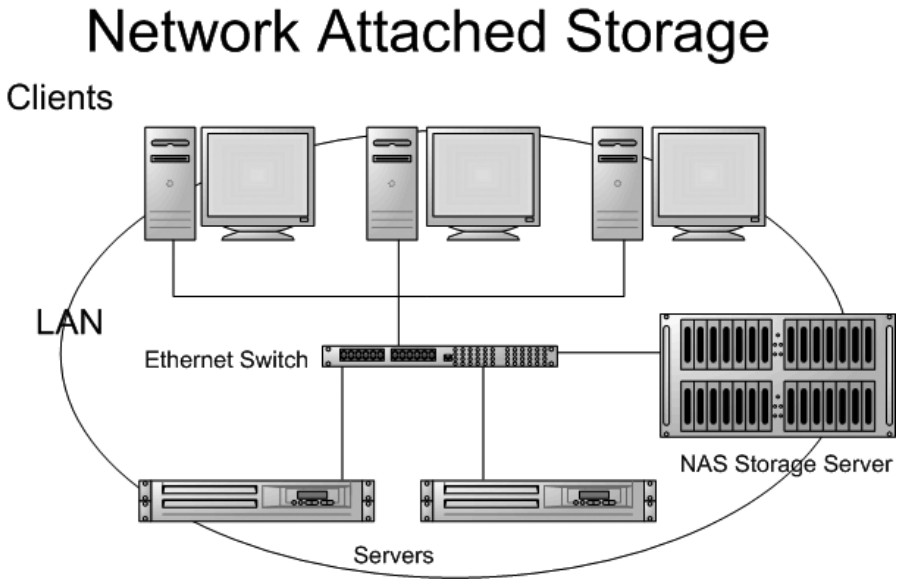
Local Storage

Local vs. Hosted Storage

Hosted storage :

- ✓ or networked storage, places data on specialized devices that serve files to clients in a network based on each client's need.
- ✓ Networked drives are available to groups of users who share access.
- ✓ One solution that uses networked drives is a network-attached storage (NAS) device.
- ✓ NAS devices are ideal for small-to-mid-size companies because they can combine multiple drives into one storage pool for easy access over the network.

Local vs. Hosted Storage



Network-Attached Storage (NAS)

Peer-to-Peer Networking

A peer-to-peer network :

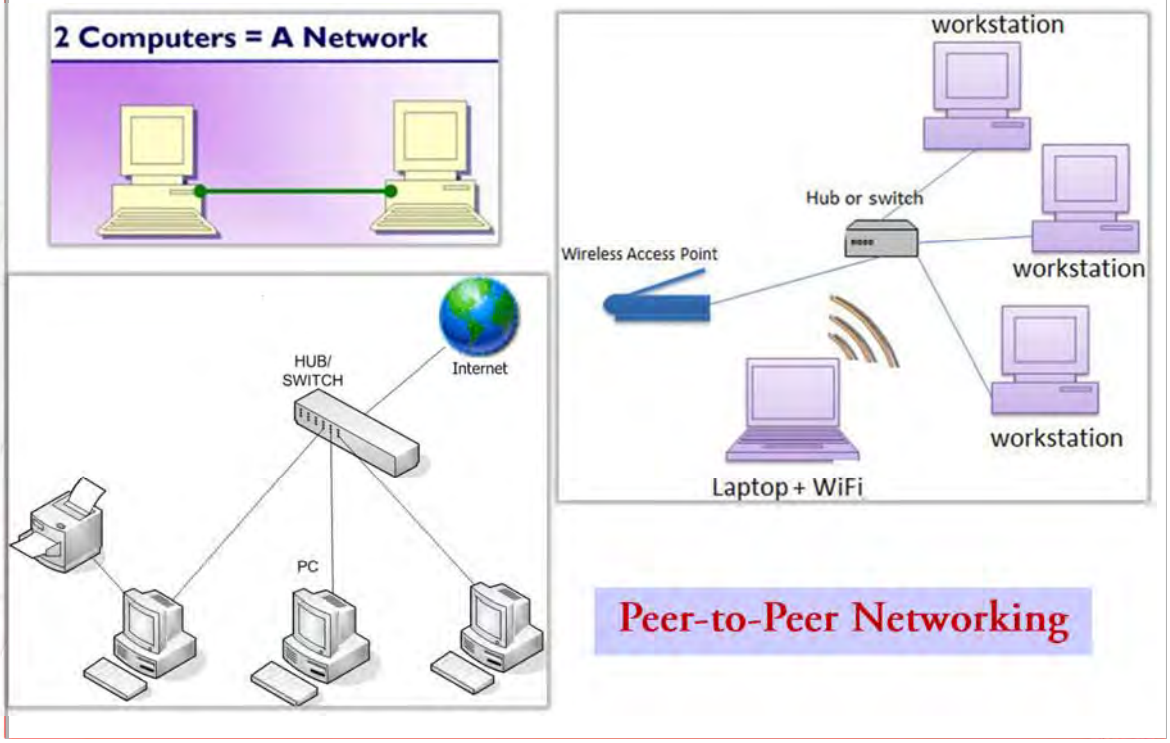
- ✓ is a network in which resource sharing, processing, and communications control are completely decentralized.
- ✓ All clients on the network are equal in terms of providing and using resources, and users are authenticated by each individual workstation.
- ✓ user accounts must be duplicated on every workstation from which a user accesses resources.
- ✓ peer-to-peer networks should not exceed 10 computers.

Peer-to-Peer Networking

You can set up and use peer-to-peer networks by using several different methods :

- ✓ *Direct link* allows you to physically connect each PC to every other PC to form the peer-to-peer network.
- ✓ *Local ad hoc networks* allow peers to connect to each other and share files without needing to set up routers or access points. (using standards such as Wi-Fi and Bluetooth.)
- ✓ *Online networks* allow clients to connect to other peers over the Internet. (using BitTorrent enables peer-to-peer file sharing over the Internet)

Peer-to-Peer Networking



HTTP and HTTPS

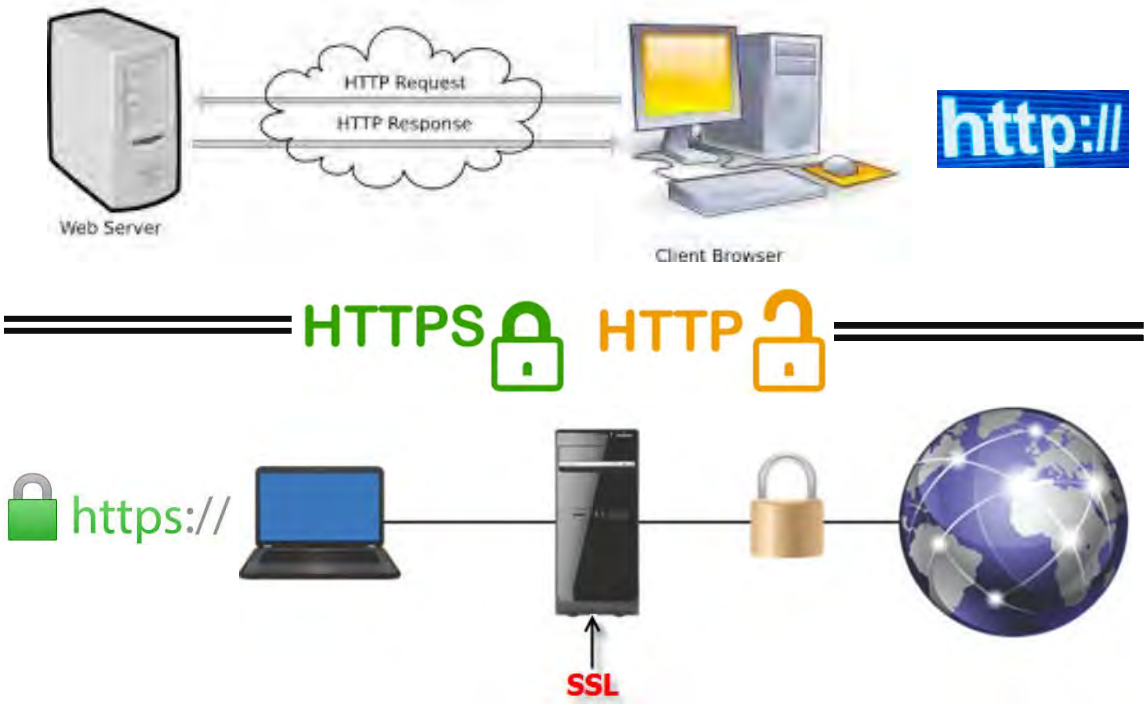
HyperText Transfer Protocol (HTTP)

- ✓ is the TCP/IP service that enables clients, such as a web browser application, to connect and interact with websites.

HyperText Transfer Protocol Secure (HTTPS)

- ✓ is a secure version of HTTP that supports web commerce by providing a secure connection between web browsers and servers.
- ✓ HTTPS uses Secure Sockets Layer/Transport Layer Security (SSL/TLS) to encrypt data.

HTTP and HTTPS



FTP

File Transfer Protocol (FTP) :

- ✓ is used to transfer files across a TCP/IP network, such as the Internet.
- ✓ FTP is intended to enable file transfers, independent of the operating system.
- ✓ FTP is the protocol that web developers use to upload web pages to a remote server.
- ✓ Other common uses of FTP include uploading images to photo sites, and audio and video files to media sites.

FTP

FTP is used to transfer files across a network

FTP

In addition to standard FTP, there are other, similar file transfer protocols :

Protocol	*Description*
Simple File Transfer Protocol (SFTP)	This protocol was an early unsecured file transfer protocol that has since been declared obsolete.
FTP over SSH	Also called *Secure FTP*, FTP over SSH is a secure version of FTP that uses an SSH tunnel as an encryption method to transfer, access, and manage files. Secure FTP is used primarily on Windows systems.
File Transfer Protocol Secure (FTPS)	This protocol, also known as *FTP-SSL*, combines the use of FTP with additional support for SSL/TLS.

Printing

A network printer :

- ✓ is a shared printing device that can be used simultaneously by multiple users on a network.
- ✓ can be wired over Ethernet, but more commonly network printers offer wireless capabilities that allow users to print without being physically connected to the device.
- ✓ are much more useful than local printers if used in an office setting, but multiple users printing from the same device may cause delays.

Printing

Local Printer

Network Printer

A local printer and a network printer.

Questions

CompTIA IT Fundamentals

Lesson 5

Working with Files, Folders, and Applications

CompTIA IT Fundamentals

Topic A :

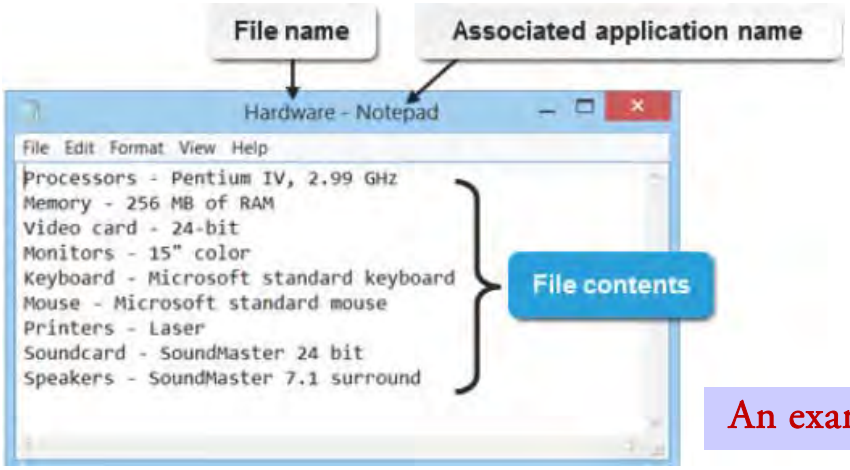
Create Files

Files & File Type

A file :

- ✓ is an object that stores information on a computer.
- ✓ Each file has a name and usually has an extension.
- ✓ Files are classified as system files and user files.
- ✓ The operating system and other applications run using system files; user files are created and managed by users.
- ✓ File Types : documents, audio files, image files, and video files, executable file, compressed file.

Files



An example of a file

Note: - User files can be deleted or modified; however,
- do not delete or modify system files
- because any modification or deletion of an application's system files can affect its functionality.

File Extensions

File extensions :

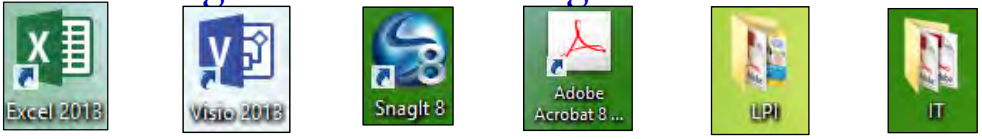
- ✓ indicate a file's type.
- ✓ The file extension is the last three or
- ✓ four characters that appear at the end of the name to the right of the period.
- ✓ For example, the file extension .docx identifies "qtr_report.docx" as a Word document.

Note : When you try to open a file, it is opened in the associated application. File extensions are not always visible within applications or utilities in Windows. You can customize various settings so that you can see file extensions.

Shortcuts

A shortcut :

- ✓ is a link or pointer to a program, file, or folder that is represented by a small icon.
- ✓ shortcuts are placed on the Desktop.
- ✓ Instead of needing to traverse the file structure to locate an item.
- ✓ Some applications create shortcuts when the application is installed.
- ✓ You can also create a shortcut yourself by right-clicking a file and selecting Create Shortcut.

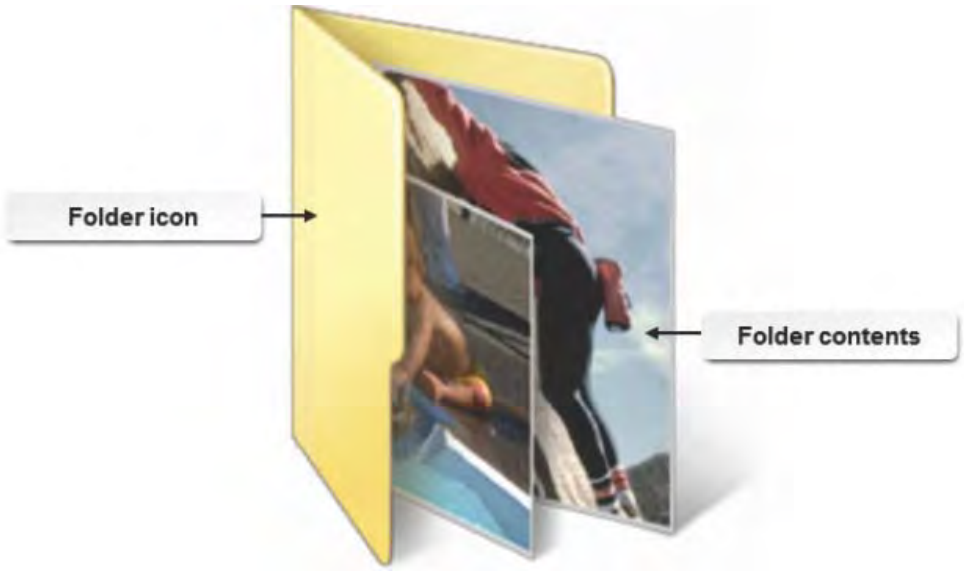


Folders

A folder :

- ✓ is a container object that can store your files in an organized manner.
- ✓ a folder is represented by a folder icon.
- ✓ Folders can be of different types and can contain any number of other folders and files, including pictures, music, videos, documents, or any combination of these types.
- ✓ A folder is also referred to as a directory.
- ✓ A folder within a folder is called a subfolder.

Folders



A folder

File and Folder Naming Conventions

File and Folder Naming, be sure to :

- ✓ Use a name that indicates the content or purpose of the document, project, or task it is related to.
- ✓ Limit the length of the name; although 260 characters can be used, file names of this length are impractical.
- ✓ Avoid special characters. (\ ), (/), (|), (:), (*), (?), ("), (<),(>) are not permitted.

File and Folder Permissions

File and Folder Permissions :

- ✓ You can manage user access to file and folder objects on a computer by modifying their permissions.
- ✓ You can also deny access to a file for a user or group of users.

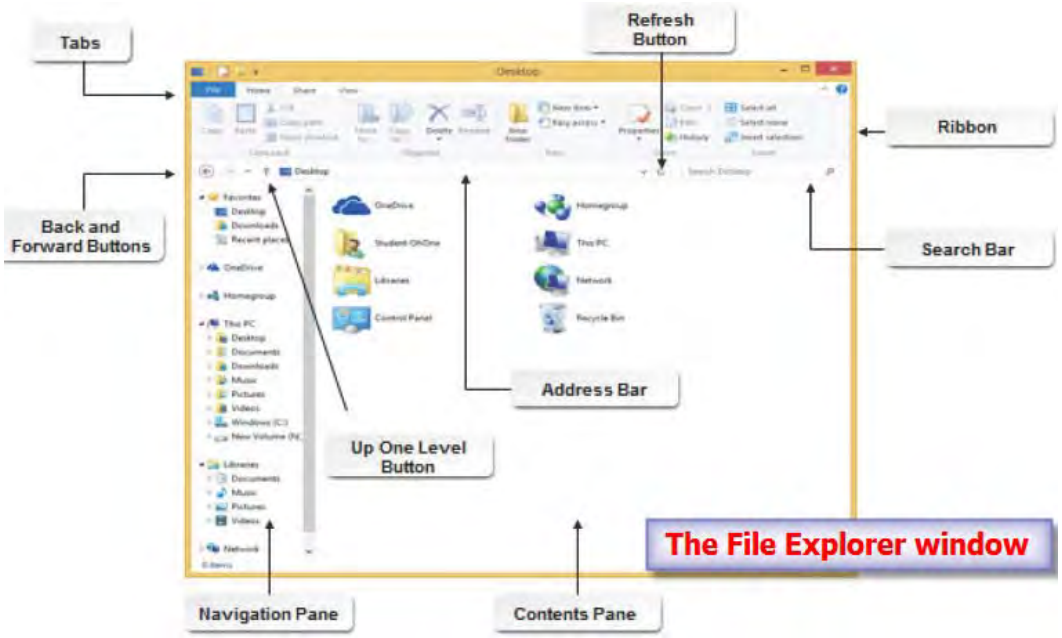
File Explorer

File Explorer :

- ✓ is a Windows utility application that offers a single view of all the resources and information that you can access from a computer.
- ✓ You can also use File Explorer to manage the information on your computer by copying and moving files.

File Explorer Components

The components of File Explorer can help you explore the Windows folder hierarchy and work with data.



File Explorer Components

Table lists and defines the components of the File Explorer.

Component	*Description*
Address bar	The *Address bar* displays the address of an object. It is located below the Ribbon.
Navigation pane	The *Navigation pane* is located in the left pane of the window; it enables you to scroll and directly access folders on your PC, your OneDrive files and folders, drives and devices connected to your computer, or other computers on the network.
Ribbon	The *ribbon* is displayed below the title bar. It can show a list of common tasks depending upon the selected object or objects. It can be collapsed to give you more room to view files and folder, a useful feature on smaller screens.
Contents pane	The *Contents pane* displays a list of files and subfolders within a folder. It consists of column headings that help in arranging the contents in various categories such as name, size, and type of file.
Preview pane	The *Preview pane* displays a preview of files such as documents, presentation slides, and images without opening them in an application. It displays the actual file contents rather than a thumbnail or an icon. This pane is not displayed by default, but when shown it appears to the right of the Contents pane.

File Explorer Components

Table lists and defines the components of the File Explorer.

Component	*Description*
Details pane	The *Details pane* displays the file properties such as file name, file type, author, last modified, size, and other properties. Like the Preview pane, the Details pane is not displayed by default, but when displayed, it shares the Preview pane's location. You can display only the Preview pane or the Details pane, but not both at the same time.
Status bar	The Status bar displays the number of items in the selected location. If you have multiple items selected in the file list section, the number of items selected is displayed along with the total size of the selected items.
Navigation buttons	Above the Navigation pane are four buttons. The **Back** button returns you to the last location you viewed or the last search results you viewed. The **Forward** buttons returns you to the next location or search results you viewed. The **Recent locations** button shows a list of the most recent locations you visited. The **Up** button opens the location one level up from the current folder.
Search bar	The Search bar enables you to locate documents within the file structure. You can search from the current location, including any folders contained in the current folder. As you begin to type the search, any files matching what you type will be displayed in the search results list.

The Navigation and Refresh Buttons

The Navigation button :

- ✓ allows you to move back and forward through the folder views in the order of their display.

The Refresh button:

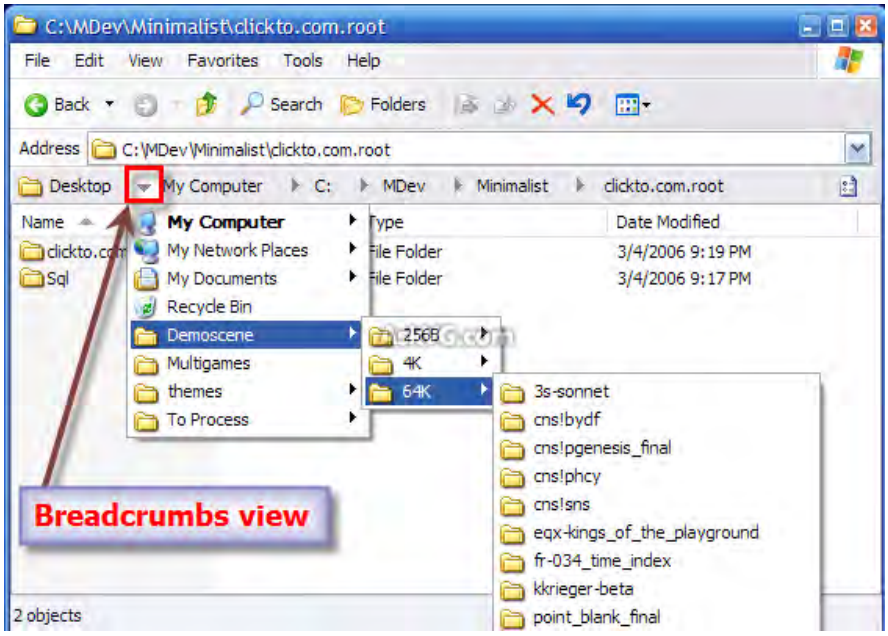
- ✓ allows you to see the latest changes in the folder window.
- ✓ Any changes to the folder or file structure done outside of File Explorer will be displayed by clicking the Refresh button.

Types of Views in the Address Bar

In the Address bar, the path of a folder or file can be displayed in

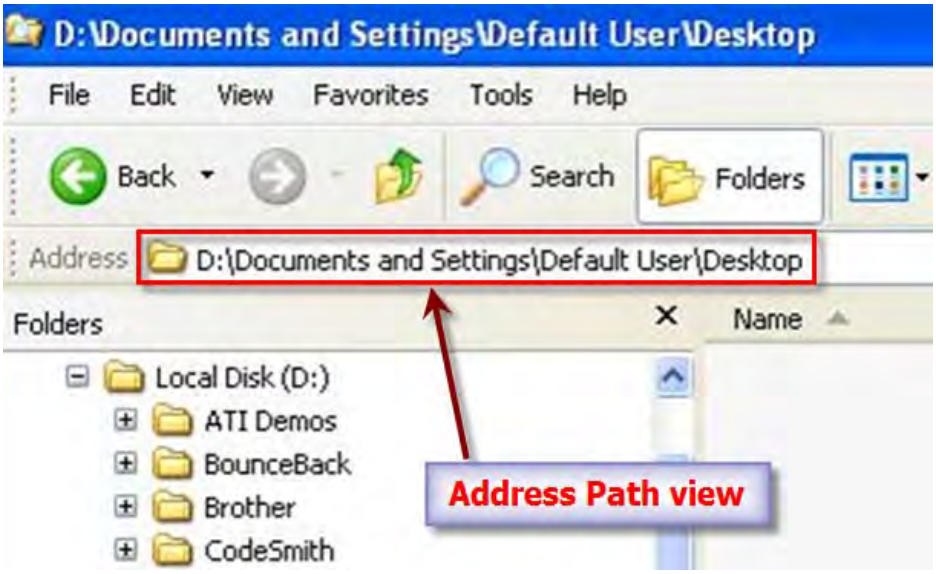
- ✓ Breadcrumbs view
  - is enabled by default and makes it easier to navigate through files and folders. (click the small arrow next to a folder to list the subfolders)
- ✓ Address Path view
  - enables you to type an object's address to access it.

Types of Views in the Address Bar



Breadcrumbs view

Types of Views in the Address Bar



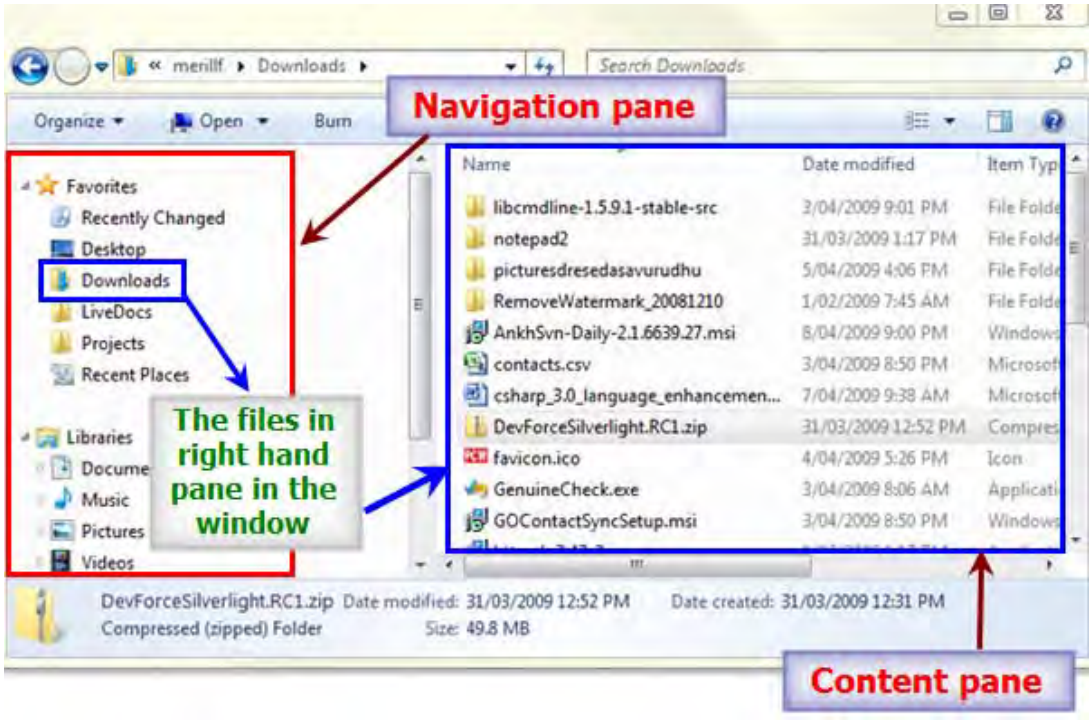
Address Path view

Expanding and Collapsing the Windows Hierarchical Structure

File and Folder Permissions :

- ✓ can also navigate by expanding and collapsing the Windows hierarchical structure.
- ✓ In the Navigation pane, a right-pointing arrow displayed in front of a folder indicates that the folder has other folders stored inside it.

Expanding and Collapsing the Windows Hierarchical Structure



Questions

CompTIA IT Fundamentals

Lesson 5

Working with Files, Folders, and Applications

CompTIA IT Fundamentals

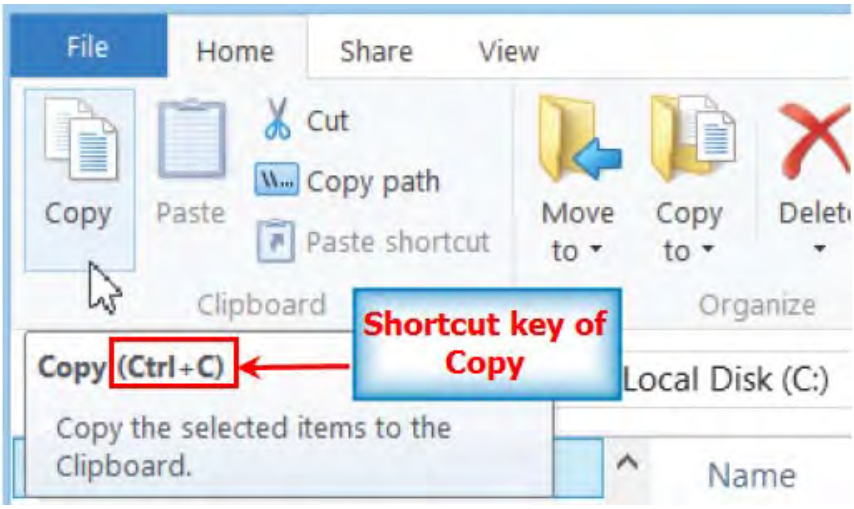
Topic B :

Navigate a File Structure

Shortcut Keys

Shortcut keys :

- ✓ are sometimes referred to as hot keys or hot key combinations.



Common Windows Shortcut Keys

Table lists some of the most common Windows shortcut key combinations :

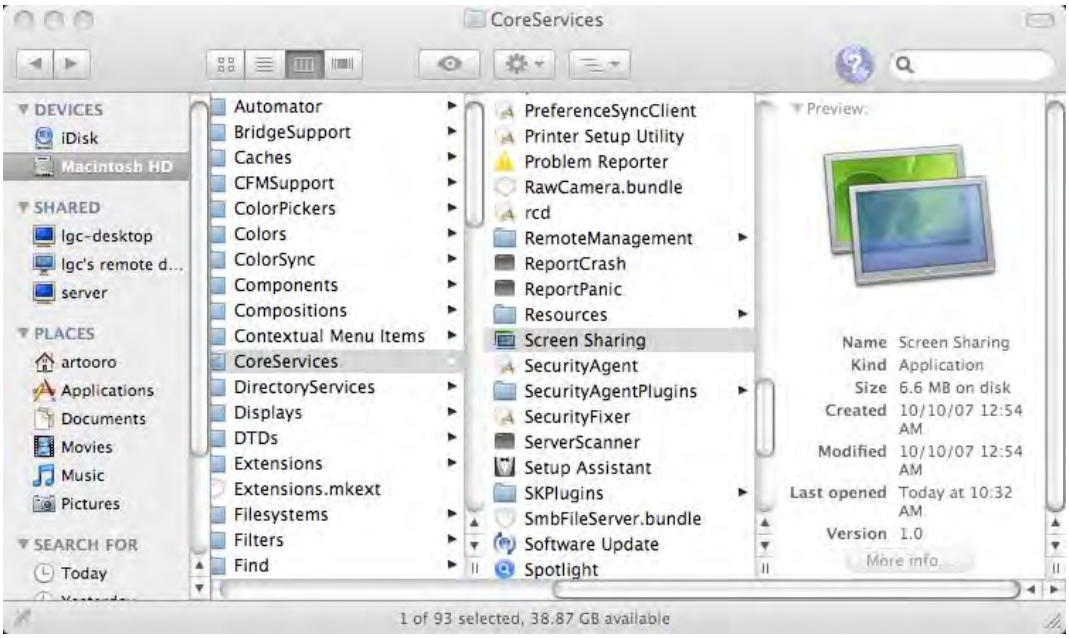
Key Combination	*Used to Perform*
Ctrl+C	Copy the selected file or folder.
Ctrl+X	Cut the selected file or folder.
Ctrl+V	Paste the selected file or folder.
Ctrl+D	Delete and send object to the Recycle Bin.
Ctrl+S	Save the file from within a Windows application.
F1	Display the application's Help window.
F2	Rename the selected file or folder.
Alt+Enter	Display properties for the selected file or folder.
Ctrl+A	Select all of the contents of the current folder or all of the text within a document.

File Structure Navigation on Non-Windows Devices

On non-Windows devices :

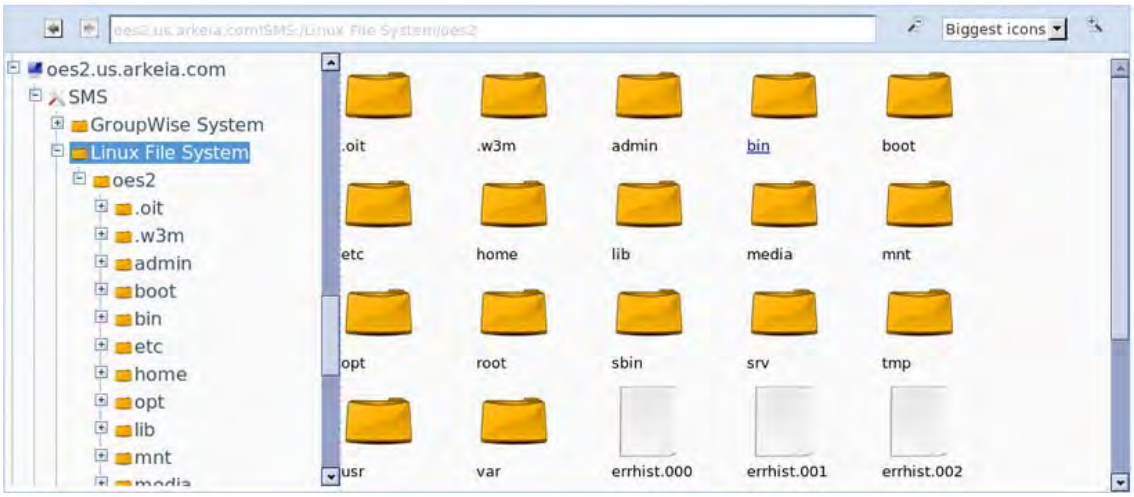
- ✓ such as Mac, Linux, and Android™ devices, the file structure is still hierarchical.
- ✓ They each have their own file management system.
- ✓ Mac computers use an application called Finder.
- ✓ Most Android devices do not have a default file management application, but there are many free file management apps available to download.

File Structure Navigation on Non-Windows Devices



Mac File System

File Structure Navigation on Non-Windows Devices



Linux File System

Questions

CompTIA IT Fundamentals

Lesson 5

Working with Files, Folders, and Applications

CompTIA IT Fundamentals

Topic C :

Manage Files and Folders

Basic File and Folder Management Techniques

Basic folder & file management actions in any File Explorer window :

- ✓ Create objects
- ✓ Select multiple objects
- ✓ Open files
- ✓ Edit files
- ✓ Save files
- ✓ Rename objects
- ✓ Copy objects
- ✓ Move objects
- ✓ Delete objects
- ✓ Undo last action

The Recycle Bin

The Recycle Bin :

- ✓ is a container object located on the desktop that temporarily stores deleted files.
- ✓ called the Recycle Bin because you can restore deleted files and folders from it.
- ✓ does not store files that are deleted from removable media such as USB drives or network drives - they are always deleted permanently.

The Recycle Bin

The Recycle Bin is a repository for deleted items such as files and folders

File Attributes

Standard Attributes 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 Archive 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 such as File Explorer, Computer in Windows 8, or My Computer in Windows XP.
Read-Only (R)	Enables users to read the contents of a file or execute it (if 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 Indexing Service to create an index of the file to speed up the Search function.

Display Options

Common modifications to the File Explorer layout include :

- ✓ Changing the layout for the display of folder contents.
- ✓ Changing the order in which items are displayed.
- ✓ Changing how libraries are displayed.
- ✓ Displaying file sizes.

Note : The Details pane displays the Date modified, Size, Date created, and Availability information for the selected file.

Questions

CompTIA IT Fundamentals

Lesson 5

Working with Files, Folders, and Applications

CompTIA IT Fundamentals

Topic D :

Compress and Extract Files

File Compression and Extraction

Compressing a file :

- ✓ is the process of reducing the size of a file.
- ✓ The major advantage of a compressed file is that it makes it easier to transfer files from one location to another.
- ✓ You can compress a single file to make it smaller and compress multiple files and folders into a single compressed file, making it easier to move the group of files to another location.
- ✓ Restoring a compressed file to its original size is called extracting.

File Compression and Extraction

The compression and extraction process

Questions

CompTIA IT Fundamentals

Lesson 5

Working with Files, Folders, and Applications

CompTIA IT Fundamentals

Topic E :

Create Screen Captures

Screen Captures

A screen capture :

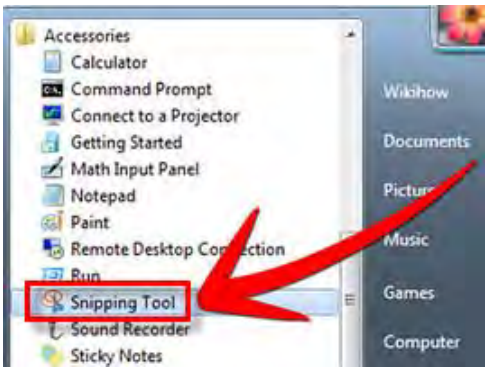
- ✓ is a picture, or image, of what is displayed on your computer monitor.
- ✓ It is also known as a screenshot, screen grab, or screen dump.
- ✓ Full screen captures with :Windows+Print Screen → saved to a Screenshots folder in your Pictures folder →saved as PNG files.
- ✓ You can also purchase third-party screen capture applications.

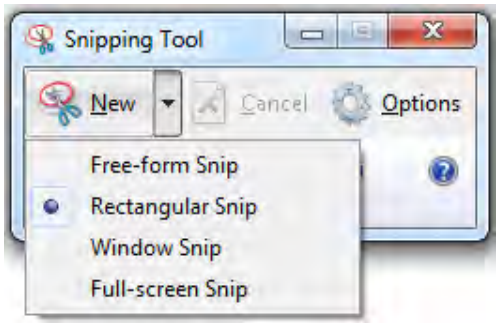
The Snipping Tool

The Snipping Tool desktop application :

- ✓ was introduced in Windows 7 and is still available in Windows 8/8.1/RT.
- ✓ enables you to capture rectangular areas, freeform areas, a specific window, or the full screen.
- ✓ The captured image is then displayed in the Snipping Tool application window.
- ✓ can use the Pen or the Highlighter tool to annotate the image before saving, copying, or sending it.
- ✓ You can also save it as PNG, GIF, JPG, or MHT file types.

The Snipping Tool





Questions

CompTIA IT Fundamentals

Lesson 6

Configuring and Using Wireless Devices

CompTIA IT Fundamentals

Topic A :

Configure Wireless Devices

Wireless Device Configuration Options

Configure on a typical wireless device :

- ✓ Security
- ✓ Sharing
- ✓ Communication
- ✓ Data management

Basic Security Configuration Settings

Configure on a typical wireless device :

- ✓ Securing a mobile device is a necessary task that should be required and enforced by any employer or user.

Operating System	Accessibility Features
Enable screen lock and passcode settings	• Using a numeric PIN or a password is considered more secure.
Configure device encryption	• Device encryption can also be a requirement in an organizational security policy.
Require remote wipes	• administrators will have rights to remotely connect to any device that is supported by the organization.

Basic Security Configuration Settings

Operating System	Accessibility Features
Enable location services and applications	• GPS tracking service functionality is available on most mobile devices
Enable remote backup	▪ Apple offers remote backup services to its iCloud® through the General Settings of the device. ▪ Android™ offers remote backup using Google Drive. Both of these services offer the first 5 GB of data for free ; then you can purchase more backup space as needed.

Basic Security Configuration Settings

Operating System	Accessibility Features
Install antivirus software	Available solutions include : • BullGuard Mobile Security • Kaspersky Mobile Security • ESET Mobile Security • Lookout Premium • Trend Micro Mobile Security • Webroot SecureAnywhere Mobile
Install updates and patches	• Verify that devices are set up to automatically install updates from the manufacturer.

Bluetooth

Bluetooth® :

- ✓ is a wireless technology that facilitates short-range wireless communication between devices.
- ✓ Both voice and data information are exchanged among these devices at 2.4 GHz within a range of approximately 30 feet.
- ✓ this connection of two to eight Bluetooth-enabled devices is known as a piconet.
- ✓ Bluetooth devices operate at very low power levels of approximately 1 milliwatt (mW).

Bluetooth

Other common uses include :

- ✓ In mobile headsets for hands-free communication with mobile phones.
- ✓ For computer peripherals such as the mouse, keyboard, and printer.
- ✓ For Bluetooth-enabled devices such as gaming consoles and global positioning system (GPS) receivers.

Bluetooth Pairing

- ✓ By using Bluetooth technology, mobile devices can establish a connection through a process called pairing.
- ✓ When two devices pair, they share a secret key to establish a wireless connection and then begin data transfer.

Bluetooth Pairing

Bluetooth pairing.

Bluetooth Pairing

The basic steps in this process include :

1. Enable Bluetooth on the mobile device through system settings.
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 it 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.

Near Field Communication

Near Field Communication (NFC) :

- ✓ is a standard of communication for mobile devices, such as smartphones and tablets, that are in very close proximity.
- ✓ is most often used for in-person transactions or data exchange.
- ✓ cannot transfer as much data as Bluetooth.
- ✓ allows for data exchange between two devices that are within inches of each other.

The Wireless Connection Setup Process

General process to set up wireless connections :

1. Verify that wireless capabilities are available.
2. If necessary, turn on Wi-Fi on the wireless device.
3. Locate and select the SSID for the WAP.
4. If necessary, enter the password for the wireless network.
5. Verify that your wireless device can connect to the Internet.

Email Configuration

On a mobile device, you can access email in one of two ways :

- Web-based access, install the email provider's app in the mobile device's app store. (enter your user name and password to access)
- Client-based email access is a bit more complicated and requires more information to access email services.

Note : Microsoft Exchange is a client-based email system that allows mobile devices to sync with the server.

Email Protocols

Protocol	Description
POP3	*Post Office Protocol version 3 (POP3)* 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.
IMAP	*Internet Mail Access Protocol version 4 (IMAP4)* 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.
SMTP	*Simple Mail Transfer Protocol (SMTP)* is used to send email from a client to a server or between servers. It uses a store-and-forward process, in which the sender starts the transfer. An SMTP server can store a message until the receiving device comes online. At that point, it contacts the device and forwards the message. If all devices are online, the message is sent quickly.

Synchronization of Wireless and Other Devices

Data synchronization :

- ✓ is the process of automatically merging and updating common data that is stored on multiple devices.
- ✓ The types of data that you can synchronize include :
  - Contacts
  - Programs
  - Email
  - Pictures
  - Music
  - Videos

Synchronization of Wireless and Other Devices

Data synchronization

Exchange ActiveSync

- ✓ Microsoft has its own synchronization protocol called Exchange ActiveSync (EAS)
- ✓ Exchange administrators can limit what devices can connect and synchronize with the server and can control which ones are blocked.

Synchronization Requirements

Factors to consider when enabling data synchronization on a mobile device include :

1. Verify that wireless capabilities are available.
2. If necessary, turn on Wi-Fi on the wireless device.
3. Locate and select the SSID for the WAP.
4. If necessary, enter the password for the wireless network.
5. Verify that your wireless device can connect to the Internet.

Questions

CompTIA IT Fundamentals

Lesson 6

Configuring and Using Wireless Devices

CompTIA IT Fundamentals

Topic B :

Use Wireless Devices

Gesture-Based Interactions

Table describes gestures that are universally recognized on devices that have Touchscreens :

Gesture	*Description*
Tap	Tap an item, such as a button or link, to select it or tap an app to launch it. Starting with your finger off the screen, touch the screen on the item you wish to activate. Then immediately pull your finger away from the screen. This is comparable to clicking an item with a mouse.
Tap & Hold	Tap an item and continue to hold your finger steady until a shortcut menu appears or the app icons jiggle.
Double-Tap	Tap an item twice in rapid succession. Double-tap the **Home** button to display the multitasking bar.
Pinch	Pinch an item to zoom out or make it smaller. Starting with your index finger and thumb apart from each other, touch both to the screen on the item you want to pinch. Without releasing the screen, move your fingers together, and then release the screen.
5-Point Pinch	With all five fingers making contact with the screen, pinch to quickly return to the **Home** screen.

Gesture-Based Interactions

Gesture	*Description*
Spread	Stretch an item to zoom in or make it larger. Starting with your index finger and thumb together, touch both to the screen on the item you want to stretch. Without releasing the screen, move your fingers apart, and then release the screen.
Swipe	Swipe an item to reveal a setting or change the screen display. Starting with your finger off the screen, touch the screen on the item you wish to swipe. Without releasing the screen, drag your finger across the screen. You can slide a control by swiping the button to the left or right.
Drag	Tap and hold an item and then move the item to drag it to a new location.
Flick	Flick your finger up or down on the screen to scroll through the items displayed on the screen. This gesture uses the concept of *kinetics* to emulate the feeling of sliding sheets of paper. A flick is quicker than a swipe.
Slide	Slide controls by swiping left or right to change the setting.

Screen Orientation

- ✓ On most mobile devices, the screen orientation changes automatically with the position of the device.
- ✓ Advanced mobile OS technology includes :
  - An accelerometer
  - A gyroscope
- ✓ The accelerometer reads and measures the orientation of the device by using a sensor.
- ✓ The gyroscope changes the orientation of the device by reading the x and y coordinates.

Screen Orientation

Change Orientation

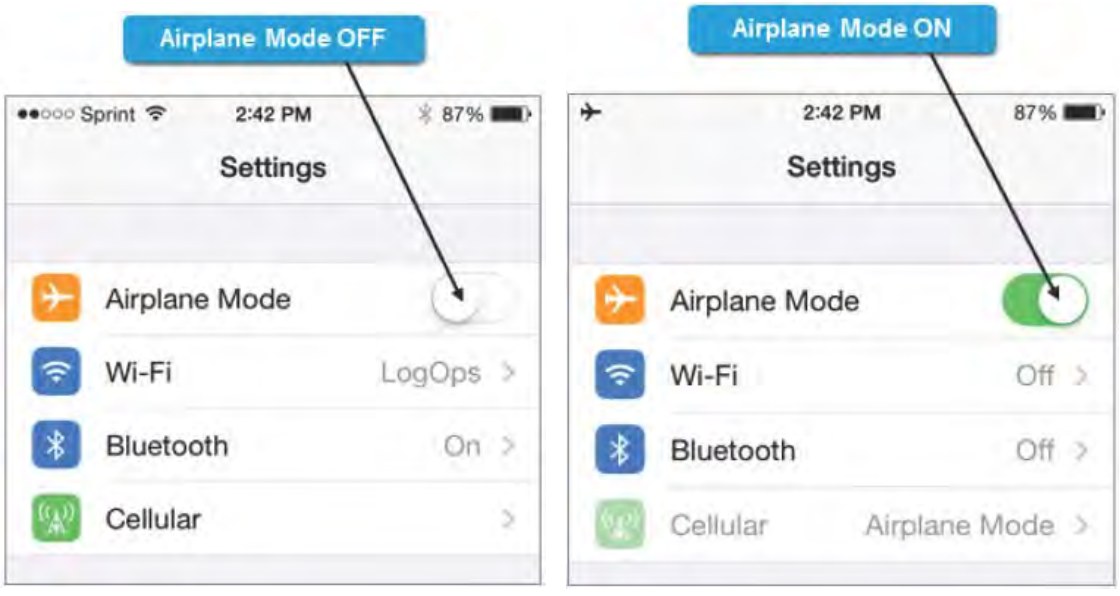
Tablet screen orientation adjusting to rotation.

Airplane Mode

the airplane mode setting :

- ✓ to quickly disconnect a mobile device from Wi-Fi and cellular connections, disabling the ability to send and receive calls, email, and text messages.
- ✓ You might also decide to use airplane mode to conserve battery life or avoid roaming charges when traveling abroad.

Airplane Mode



Mobile App Stores

Mobile apps :

- ✓ are compact software programs that are developed to perform a predefined function.
- ✓ can be downloaded for free or for a small fee from the following stores:
  - The App Store contains apps for Apple iOS devices.
  - Google Play™ store and Amazon Appstore contain apps for Android devices.
  - The Windows® Store contains apps for Windows devices.
  - Company app stores contain proprietary apps created by in-house developers.

Mobile App Stores

Questions

CompTIA IT Fundamentals

Lesson 7
Securing Computing Devices

CompTIA IT Fundamentals

Topic A :
Identify Security Threats

Hackers and Attackers

Hacker :

- ✓ is a neutral term for a user who excelled at computer programming and computer system administration.

Attacker :

- ✓ is a term that always represents a malicious system intruder.

Note : The term cracker refers to an individual who breaks encryption codes, defeats software copy protections, or specializes in breaking into systems.

Hackers and Attackers

A white hat :

- ✓ is a hacker who discovers and exposes security flaws in applications and operating systems so that manufacturers can fix them before they become widespread problems.

A black hat :

- ✓ is a hacker who discovers and exposes security vulnerabilities for financial gain or for some malicious purpose.

Malware

Malware :

- ✓ is any unwanted software that has the potential to damage a system, impede performance, or create a nuisance condition.

Types of Malware

Malware Type :

- ✓ Virus
- ✓ Worm
- ✓ Trojan horse
- ✓ Logic bomb
- ✓ Spyware
- ✓ Adware
- ✓ Rootkit
- ✓ Spam
- ✓ Ransomware

Types of Malware

Malware Type	Description
Virus	A piece of code that spreads from one computer 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.
Worm	A piece of code that spreads from one computer 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.
Trojan horse	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.
Logic bomb	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 programed to do. Often, this includes erasing and corrupting data on the target system.

Types of Malware

Malware Type	Description
Spyware	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.
Adware	Software that automatically displays or downloads advertisements when it is used. Although 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.
Rootkit	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.

Types of Malware

Malware Type	Description
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.
Ransomware	Ransomware is malicious software that prevents you from using your computer. It usually displays a message stating that you must pay a fee or face some other penalty before you can access your files and computer again. Paying the ransom doesn't necessarily mean that you will regain access to your files or computer.

Social Engineering Attacks

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.
- ✓ can come in a variety of methods: in person, through email, or over the phone.
- ✓ can be prevented with effective user education.

Types of Social Engineering Attacks

Social Engineering Type	Description
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.
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.
Hoax	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.

Types of Social Engineering Attacks

Social Engineering Type	Description
Phishing	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.
Vishing	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*.
Whaling	This is a form of phishing that targets individuals who are known to possess a good deal of wealth. It is also known as *spear phishing*. Whaling targets individuals that work in Fortune 500 companies or financial institutions whose salaries are expected to be high.

Types of Social Engineering Attacks

Social Engineering Type	Description
Spam and *spim*	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. 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.
Dumpster diving	By properly disposing of paper and hardware, you can protect your organization from Dumpster divers.

Password Cracking

A password attack :

- ✓ is any type of attack in which the attacker attempts to obtain and make use of passwords illegitimately.
- ✓ The attacker can guess or steal passwords or crack encrypted password files.
- ✓ A password attack can show up in audit logs as repeatedly failed logons and then a successful logon, or it can show as several successful logon attempts at unusual times or locations.

Password Cracking

Attacker guesses the password to gain network access

Types of Password Attacks

- ✓ Hackers use several common categories of password attacks. Creating complex passwords can
- ✓ increase the amount of time it takes for an attack to succeed.

Password Attack Type	*Description*
Guessing	A *guessing attack* is the simplest type of password attack and involves an individual making repeated attempts to guess a password by entering different common password values, such as the user's name, a spouse's name, or a significant date. Most systems have a feature that will lock out an account after a specified number of incorrect password attempts.
Stealing	Passwords can be stolen by various means, including sniffing network communications, reading handwritten password notes, or observing a user in the act of entering the password.

Types of Password Attacks

Password Attack Type	Description
Dictionary attack	A *dictionary attack* 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.
Brute force attack	In a *brute force attack*, the attacker uses password-cracking software to attempt every possible alphanumeric password combination.
Hybrid password attack	A *hybrid password attack* utilizes multiple attack vectors including dictionary, brute-force, and other attack methodologies when trying to crack a password.

Physical Security Issues

Threat/Vulnerability	Description
Internal	It is important to always consider what is happening inside an organization, especially when physical security is concerned. For example, disgruntled employees may be a source of physical sabotage of important network security-related resources.
External	It is impossible for any organization to fully control external security threats. For example, an external power failure is usually beyond a network technician's control because most organizations use a local power company as their source of electrical power. However, risks posed by external power failures may be mitigated by implementing devices such as an uninterruptible power supply (UPS) or a generator.
Natural	Although natural threats are easy to overlook, they can pose a significant risk to the physical security of a facility. Buildings and rooms that contain important computing assets should be protected against likely weather-related problems including tornadoes, hurricanes, snow storms, and floods.
Man-made	Whether intentional or accidental, people can cause a number of physical threats. Man-made threats can be internal or external. For example, a backhoe operator may accidentally dig up fiber optic cables and disable external network access. Alternatively, a disgruntled employee may choose to exact revenge by deliberately cutting fiber optic cables.

Physical Security Issues

Threat/Vulnerability	*Description*
Internal	It is important to always consider what is happening inside an organization, especially when physical security is concerned. For example, disgruntled employees may be a source of physical sabotage of important network security-related resources.
External	It is impossible for any organization to fully control external security threats. For example, an external power failure is usually beyond a network technician's control because most organizations use a local power company as their source of electrical power. However, risks posed by external power failures may be mitigated by implementing devices such as an uninterruptible power supply (UPS) or a generator.
Natural	Although natural threats are easy to overlook, they can pose a significant risk to the physical security of a facility. Buildings and rooms that contain important computing assets should be protected against likely weather-related problems including tornadoes, hurricanes, snow storms, and floods.

Environmental Threats and Vulnerabilities

Environment Threat	Effects and Mitigations
Fire	-Fire is a serious network environment security threat -It can destroy hardware and the data, and it is hazardous to people and systems. -key systems are installed in a fireresistant facility, and that there are high-quality fire detection and suppression systems on-site.
Hurricanes & tornadoes	-Hurricanes and Tornadoes are major network security threats -It can destroy hardware and the data -your information systems are well-contained and that your physical plant is built to appropriate codes and standards.

Environmental Threats and Vulnerabilities

Environment Threat	Effects and Mitigations
Flood	-A flood is another major network security threat -Your organization should check the history of an area to see if you are in a flood plain before constructing your physical plant, and follow appropriate building codes as well as purchase flood insurance. - Construct the building so that the lowest floor is above flood level.
Extreme temperature	-Extreme temperatures, heat can cause some sensitive hardware components to melt and degrade, resulting in data loss. -You can avoid this threat by implementing controls that keep the temperature in your data center within acceptable ranges.

Environmental Threats and Vulnerabilities

Environment Threat	Effects and Mitigations
Extreme humidity	-Extreme humidity can cause computer components, data storage media, and other devices to rust, deteriorate, and degrade, resulting in data loss. -You can avoid this threat by ensuring that there is enough ventilation in your data centers and storage locations, and by using temperature and humidity controls and monitors.

Theft

Theft of both data and hardware :

- ✓ You can physically secure laptops and tablets by using a cable, but determined thieves will cut through a cable.
- ✓ You can install software and encrypt the information on all of these portable devices to make it more difficult for the thieves to access the information contained on the devices.

Theft

Theft of software and licensing :

- ✓ 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.

Questions

CompTIA IT Fundamentals

Lesson 7
Securing Computing Devices

CompTIA IT Fundamentals

Topic B :
Apply Security Best Practices

Types of User Accounts

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

User Account	*Provides*
Administrator	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.
Standard User	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.
Guest	Limited computer access to individuals without a user account. By default, the **Guest** 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.

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.
- ✓ Three phases in the user access process :
  - Identification : when entering a user name and password.
  - Authentication : The verification of that claim.
  - Authorization : The action taken as a result of verifying the claim.

Authentication Factors

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.

Authentication Factors

Multifactor authentication :

- ✓ is any authentication scheme that requires validation of two or more authentication factors.
- ✓ Requiring a physical ID card along with a secret password is an example of multi-factor authentication.
- ✓ Example : A bank ATM card

Single Sign-On

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.
- ✓ Different systems may use different mechanisms for user authentication.
- ✓ SSO has to use different credentials to perform authentication.
- ✓ 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.

Password Management Best Practices

A Password :

- ✓ is your access to your computer, and your computer is safe and inaccessible to others.
- ✓ You should always change any default passwords to strong passwords to protect your computer and data.
- ✓ A strong password is one that cannot be easily guessed by others and is often referred to as a complex password.

Password Management Best Practices

To create a strong password :

- Use at least seven characters.
- Use a combination of uppercase letters, lowercase letters, numbers, and symbols.
- If you are replacing a previously created password, make sure that your new password is significantly different from the last one.
- Do not use common words, your name, your user name, or other words that people might associate with you, such as a pet's name.

Password Management Best Practices

To protect your password, make sure that you :

- Do not write it down or share it with others.
- Do not use your network password for other purposes.
- If you are a computer administrator, create a new administrator account other than the normal login for security purposes.
- Do not re-use passwords.
- Change your password at least every 60 to 90 days, especially if your account is not configured so that the password expires automatically.
- Always use password protection whenever you're given the option.
- Change your password if you suspect that it has been compromised.
- Do not save your password on the computer.

Password-Protected Screen Savers

- ✓ Setting a password to your screen saver is a security measure that
- ✓ prevents unauthorized access to confidential information and passwords associated with your user account.
- ✓ can be enabled by checking the On resume, display logon screen check box in the Screen Saver Settings dialog box.

Device Hardening Best Practices

Device hardening :

- ✓ Device hardening is a collection of security tasks used to reduce the scope of the device's vulnerability and attack surface.
- ✓ Table summarizes some device hardening techniques.

Device Hardening Technique	*Description*
Timeouts and lockouts	User accounts should be configured so that after a specified number of incorrect login attempts, the account is locked. The lockouts and timeouts are a common method used to prevent attackers from breaching a user account by trying to guess the user's password.

Device Hardening Best Practices

Device Hardening Technique	*Description*
Software firewall	*Firewalls* use administrator-defined rules to inspect traffic flowing in and out of a device. Firewall rules can be based around any of the following criteria: • IP addresses • Domain names • Protocols • Ports • Keywords/phrases • Types of files (such as executables or images) A good firewall should offer the following services: • Packet filtering: • Stateful inspection • Content filtering: • Proxying:

Device Hardening Best Practices

Device Hardening Technique	*Description*
Antimalware	In addition, you might install ad blocking software. Be sure to use antivirus software on desktop, laptop, tablet, and smartphone devices.
Disable Bluetooth	Bluetooth technology connects headsets and audio headphones, keyboards, and even printers to computing devices, especially mobile devices. It is rarely secured. If you don't use Bluetooth devices, or only use them occasionally, you should consider disabling the service so it isn't used to compromise your system.
Disable NFC	*Near Field Communications (NFC)* is used on smartphones and other mobile devices to enable radio communication when the devices touch each other or are a few centimeters apart. Any time you don't need to use this feature, turn it off to prevent intruders from accessing your phone or mobile device.

Device Hardening Best Practices

Device Hardening Technique	*Description*
Encryption options	*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.

Wireless Networking and Security

- ✓ use a secured wireless network rather than an open wireless network.
- ✓ Open wireless networks are a major security risk when accessed directly that they are insecure.
- ✓ The protocols used on a secure wireless network help protect your data from attack.

Wireless Networking and Security

Open Wi-Fi vs. secure Wi-Fi

Email Best Practices

Suspicious email issues to be aware of include :

- Spam
  - ✓ is an email-based threat where the user's inbox is flooded with emails that act as vehicles carrying advertising material for products or promotions for get-rich-quick schemes and can sometimes deliver viruses or malware.
- Hijacked email
  - ✓ is an account that has been accessed by an attacker and is being used by the attacker to send and receive emails.

Email Best Practices

Suspicious email issues to be aware of include :

Note

- ✓ Avoid selecting links in emails whenever possible.
- ✓ If you discover that your email account has been compromised ,
  - o the first thing to do is change your password
  - o alert the network administrator.
  - o perform a complete scan of your system with antivirus software to locate and remove any malware onto your system.

Cloud Storage Best Practices

Some things to consider when deciding to use cloud storage include :

- ✓ Which data do you feel comfortable storing in the cloud?
- ✓ How much encryption will you place on content stored in the cloud?
- ✓ Will the cloud be your primary backup location?
- ✓ What other backup locations will you need?

Note : As with any other service that has user names and passwords, make sure not to share your credentials.

Security Software Alerts

In some organizations,

- ✓ users are not allowed to install the updates themselves. because the IT department needs to test the patch before deploying it throughout the organization.
- ✓ The patch might cause issues with features that you use in the software or with how the application interacts with other applications on your system.
- ✓ If you see such an alert for an application that you don't have installed, but sure not to select the link for the update. Having conflicting antivirus software applications on your system can prevent either of them from trapping attacks on your system.

Guidelines for Applying Security Best Practices

- ✓ Disable or rename default user accounts.
- ✓ Use the Administrator account only when necessary, and use a regular user account the rest of the time.
- ✓ Safeguard your authentication credentials by not sharing them with anyone or posting them where they are visible.
- ✓ Consider using SSO so that signing in to the device
- ✓ Passwords are not dictionary words.
- ✓ Avoid connecting to unsecured wireless networks.
- ✓ When using cloud storage, be sure the data is encrypted.
- ✓ Be aware of suspicious email messages.

Guidelines for Applying Security Best Practices

- ✓ Harden devices by :
  - Implementing lockouts and timeouts when the wrong password is entered after a specified number of times.
  - Configuring a software firewall to protect mobile device data.
  - Disabling Bluetooth and NFC when not in use.
  - Installing antivirus software and keeping it up to date.
  - Encrypting data.
- ✓ You change your password if your account has been compromised.
- ✓ Install patches and updates to applications as soon as possible to address security alerts.

Questions

CompTIA IT Fundamentals

Lesson 7
Securing Computing Devices

CompTIA IT Fundamentals

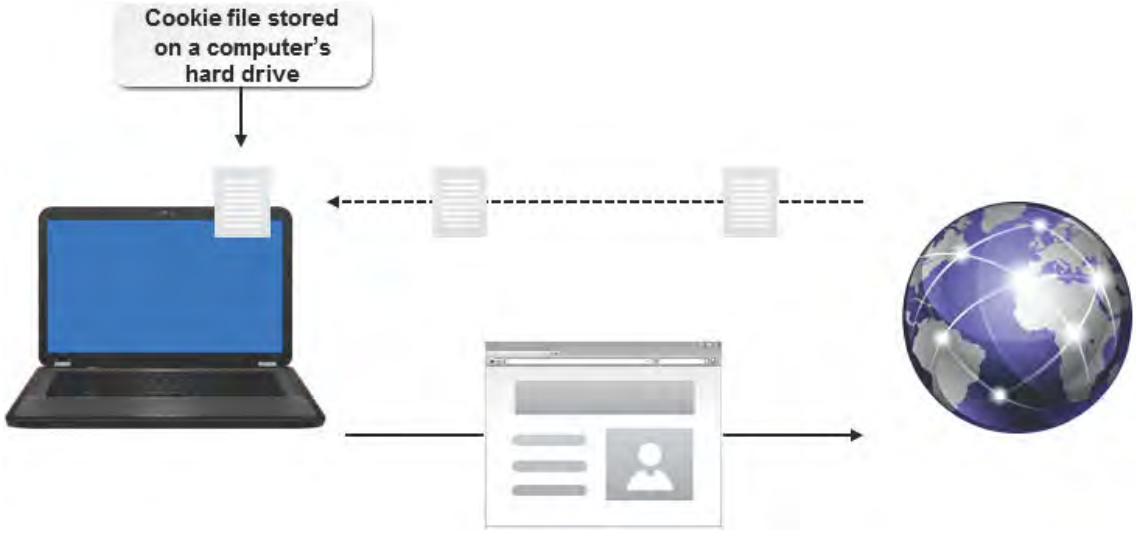
Topic C :
Perform Secure Web Browsing

Cookies

A cookie :

- ✓ is a text file that is created by a website and placed on a computer's hard drive to store information that is used to identify users and technical information about the user's actions at a website, the links the user clicked, to prepare customized web pages for them.
- ✓ Cookies can be temporary or persistent.
  - Temporary cookies, which are also referred to as session cookies, are stored on a computer only for the duration of the web session.
  - Persistent cookies are saved on the hard drive and remain there even after the browsing session ends.

Cookies



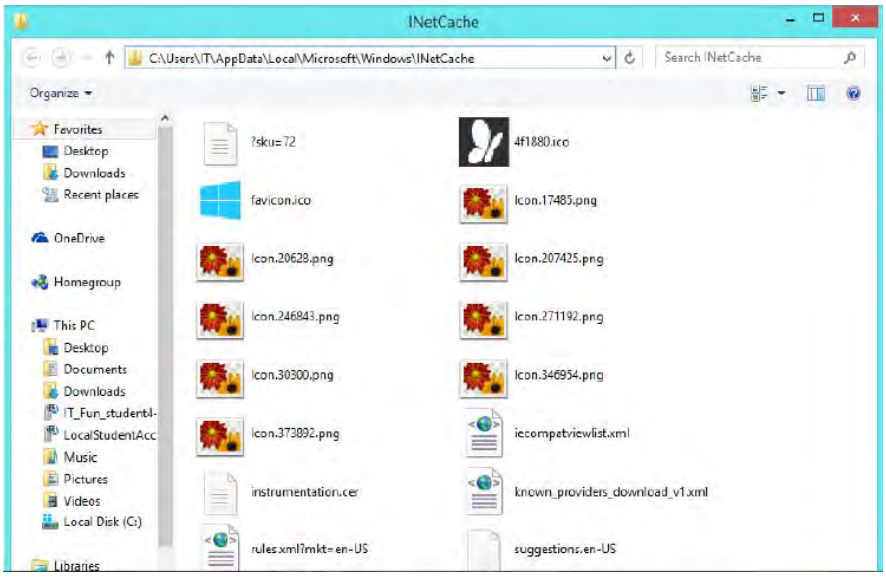
A cookie file with user information

Internet Cache

An Internet cache :

- ✓ is a local storage area that holds the files saved by a web browser to decrease the time it takes to reload a web page.
- ✓ The browser cache includes all the text, image, and script files necessary to create and display a given web page when you first access it.
- ✓ If you visit secure websites on a shared computer, clearing the browser cache can help keep your personal information safe.

Internet Cache



Web pages stored in a local folder.

Browser Enhancements

Browser enhancements include :

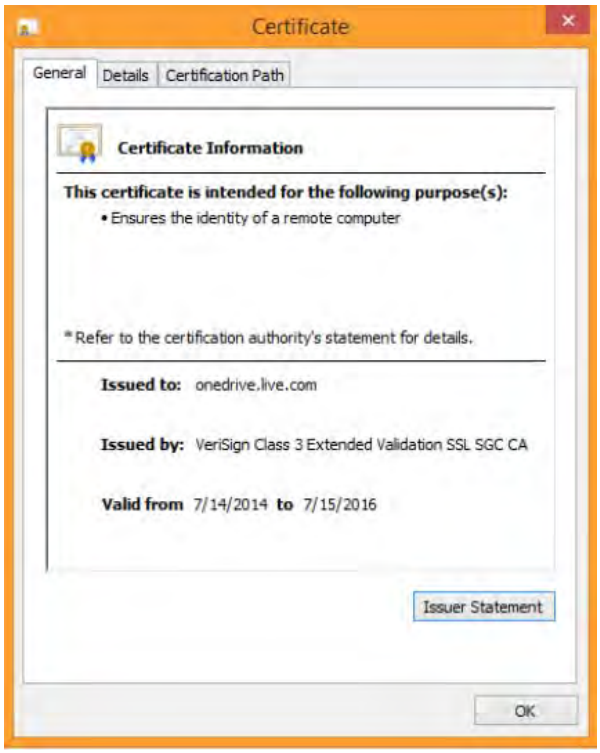
- ✓ Plug-ins: A plug-in enables the browser to process specific types of content.
  - For example, the Adobe® Flash® player plug-in enables you to view Flash files.
- ✓ Extensions: An extension adds additional features to the browser and becomes part of the browser application.

Digital Certificates

A digital certificate :

- ✓ is an electronic document that provides for the secure exchange of information over a network.
- ✓ A certificate can verify the validity of a website, the identity of a person, or the integrity of a file.
- ✓ Certificates are digitally signed by the issuing authority and can be issued to users, computers, services, or files.

Digital Certificates



Certificates ensure the security of information exchanged

Invalid Certificates

When you attempt to access a site, you might receive a warning that the digital certificate is invalid :

- ✓ you should check to see if there is a browser update
- ✓ available or try a different web browser.
- ✓ You should also check that your date and time are correct on your computer.

Secure Web Connections

A Password :

- ✓ is your access to your computer, and your computer is safe and inaccessible to others.
- ✓ You should always change any default passwords to strong passwords to protect your computer and data.
- ✓ A strong password is one that cannot be easily guessed by others and is often referred to as a complex password.

Adware Symptoms

Symptoms of adware include :

- ✓ Resets your Homepage
- ✓ Changes Search Results
- ✓ Pop Up Ads Displayed
- ✓ Installs Unwanted Software
- ✓ Slow Browsers
- ✓ Toolbars Added to your Browser

Untrusted Sources

- ✓ You might get a dialog box with a warning, or you might see a message displayed under the menu or toolbar.
- ✓ You will be given the option to continue to load the content or to close the page.

Personal Identifying Information

Personal identifying information (PII)

- ✓ is any information that can be used to determine who a person is.
- ✓ This information includes a person's Social Security number, financial account information, or driver's license number.

Automated Forms

Personal identifying information (PII)

- ✓ Avoid using the autofill feature of web browsers.
- ✓ Use the Settings feature of your browser to disable autofill of forms.

Browsing on Public Workstations

Steps to take include :

- ✓ Log out of sites rather than just closing the web page.
- ✓ Log out of the computer as well as any sites to which you are logged in whenever you step away from the computer.
- ✓ Be aware of your surroundings and of other people who might be attempting to shoulder surf.
- ✓ Avoid entering sensitive information such as credit card numbers, financial institution logins, or any other private data.

Browsing on Public Workstations

Steps to take include :

- ✓ Be sure that the browser is not set up to remember your user name or password.
- ✓ Delete the temporary Internet files.
- ✓ Delete your browsing history.
- ✓ If your browser has a private browsing feature, use it.

Browsing on Public Workstations

Using your device in a public location include :

- ✓ Be aware of anyone attempting to shoulder surf.
- ✓ Install or apply a screen shield to prevent people from easily seeing what is on your screen.
- ✓ Connect only to secure wireless networks
- ✓ Turn off Bluetooth to prevent people from connecting to your device.
- ✓ Never leave your device unattended.

Guidelines for Performing Secure Web Browsing

To protect your own information and your organization's information, be sure to follow these guidelines :

- ✓ your browser is up to date. Security patches and updates fix any security holes.
- ✓ Disable cookies and clear the browser cache and history.
- ✓ Disable any plug-ins, toolbars, and extensions that you are not using.
- ✓ Avoid selecting suspicious links or banner ads.
- ✓ Be aware of spoofed web pages that appear to be the web page of another company.

Guidelines for Performing Secure Web Browsing

- ✓ If your browser has been infected with adware, be sure to clear the cache and cookies, reset passwords, and use your antivirus software to try to eradicate the infection.
- ✓ Be careful to protect your personally identifiable information including your Social Security number, driver's license number, financial account numbers, and log in credentials.

Questions

CompTIA IT Fundamentals

Lesson 8
Supporting Computers and Users

CompTIA IT Fundamentals

Topic A :
Environmental and Safety Concepts

Ergonomics

Ergonomics :

- ✓ is the study of a person's efficiency at the workplace as it relates to his or her health, safety, and productivity.
- ✓ guidelines for office situations.
  - Chairs, workstations, keyboards, monitors, and other peripheral equipment (mouse, document holder, and so on) need to be adjustable so that they can be properly aligned or the individual users.

Ergonomics

An ergonomically correct workstation

Ergonomic Best Practices

keyboard and mouse :

- ✓ should be directly in front of the person and within a comfortable reach.
- ✓ Keyboard trays can be used to place the keyboard at the
- ✓ correct height. Wrist rests can provide additional support while typing.
- ✓ mouse should be at same level as keyboard and close enough to prevent over extended reaches.

Ergonomic Best Practices

Office furniture :

- ✓ The height of the chair and the desk is critical for proper posture.
- ✓ Adjustable chairs are a must and should also provide lower-back support.
- ✓ Footstools might be necessary.
- ✓ Another alternative to the standard office chair is balance ball chairs.

Ergonomic Best Practices

Monitor :

- ✓ The top of the monitor needs to be at eye level to reduce eye and neck strain.
- ✓ Monitors should be adjustable both in angle and height. If necessary, place them on top of a stand to elevate them.

RoHS Guidelines

Restriction of Use of Hazardous Substances (RoHS) :

- ✓ is a compliance directive launched in 2006 and enforced by the European Union that aims to restrict certain dangerous substances commonly used in electronic devices.

RoHS Guidelines

Table outlines the permitted amounts of materials restricted by RoHS guidelines :

Material	*Allowable Amount*
Lead	0.1% by weight at raw homogeneous materials level
Cadmium	< 0.01% by weight at raw homogeneous materials level
Mercury	100 parts per million (ppm) or less; not intentionally added
Hexavalent chromium	< 0.01% by weight at raw homogeneous materials level
Polybrominated biphenyls	0.1% by weight at raw homogeneous materials level
Polybrominated diphenyl ethers	0.1% by weight at raw homogeneous materials level

WEEE Directive

The Waste Electrical and Electronic Equipment (WEEE) :

- ✓ is a directive launched in 2003 in Europe that serves a very similar purpose as the RoHS.
- ✓ It imposes the responsibility for the disposal of waste electrical and electronic equipment on the manufacturers of such equipment

Device Disposal Options

Disposal Option :

- ✓ Donating : to a local school or nonprofit organization.
- ✓ Selling : to employees, at a garage sale or online auction site.
- ✓ Bringing to recycling center
- ✓ Shipping to vendors : recycling and/or trade-in programs.

Disposing of Certain Devices

Device :

- ✓ CRT monitors
- ✓ Scanners
- ✓ Batteries
- ✓ Ink/toner
- ✓ Hard drives

Device Placement

Environmental Hazards :

- ✓ Temperature
- ✓ Humidity : Computers function best in a relative humidity of 50 to 60 percent.
- ✓ Dust
- ✓ Electromagnetic interference (EMI) : EMI occurs when sources that output electromagnetic radiation interfere with your electronic devices.

Ventilation Components

Ventilation components are essential to protect any electronic device from heat and dust :

Ventilation Component	*Used To*
Fans	Cool the internal components of a computer.
Ozone filters	Filter the ozone that is generated inside printers during the printing process.
Dust filters	Prevent dust from entering the critical components of a computer.

Ventilation Components

Power and Energy Efficiency :

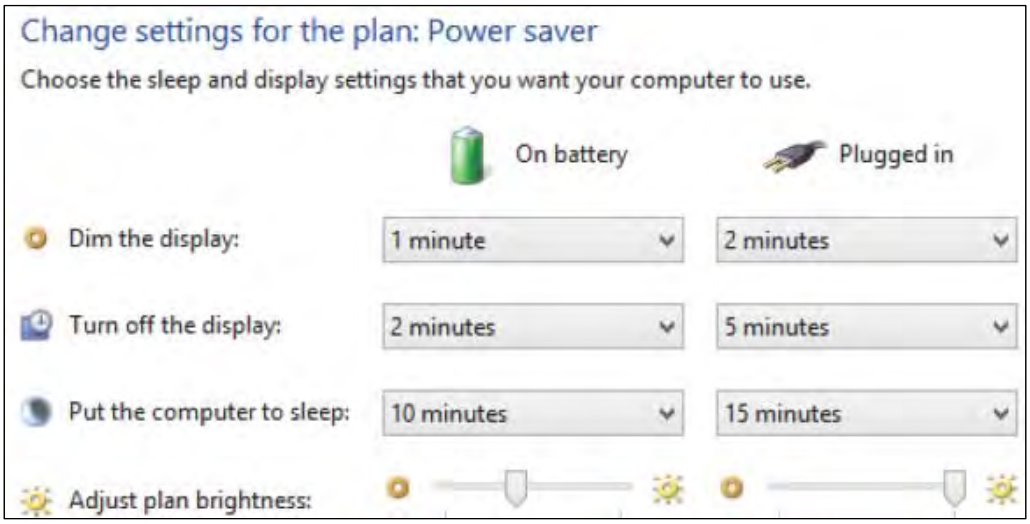
- ✓ As the technology used in computer devices evolves, the newer devices tend to be more efficient than their predecessors. For example :
  - Liquid crystal display (LCD)
  - A solid state drive (SSD)
  - Green Parallel Advanced Technology Attachment (PATA)
  - A network-attached storage (NAS) device
  - A Bluetooth version 4.0 wireless mouse or keyboard battery can last up to 5 or 10 years

Power Profiles

Standard recommendations for power management settings :

Function	*Setting*
Monitor/display sleep	After 15 minutes or less
Turn off hard drives/hard disk sleep	After 15 minutes or less
System standby/sleep	After 30 minutes or less

Power Profiles



Power Saver plan options

Power Supply Options

Use proper power devices :

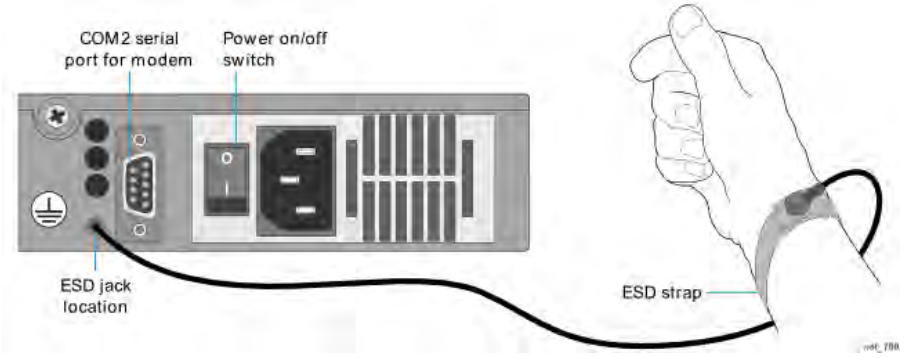
- ✓ A power strip
- ✓ A surge protector
- ✓ An uninterruptible power supply (UPS)

Power connectors connected to a UPS

Electrostatic Discharge

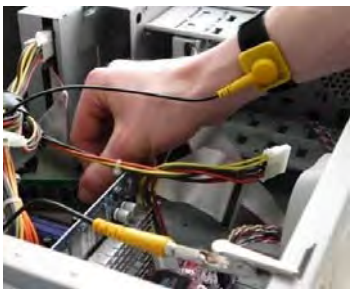
Electrostatic discharge (ESD) :

- ✓ ESD can cause damage to people as well as sensitive computer equipment.
- ✓ 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.



Antistatic Tools

Tools used in preventing ESD :



Antistatic strap

Antistatic mat

Antistatic Tools

Tools used in preventing ESD :

Antistatic bag

ESD smock

Guidelines for Protecting Against ESD

To ensure safety from electrical hazards :

- ✓ Unplug the device from its power supply before you start servicing it.
- ✓ Do not wear jewelry that could accidentally contact circuitry and conduct current.
- ✓ Plug wires and connectors into the appropriate sockets.
- ✓ Suspend work during an electrical storm.
- ✓ Do not handle electrical equipment when your hands or feet are wet or when you are standing on a wet surface.

Guidelines for Protecting Against ESD

To ensure safety from electrical hazards :

- ✓ Stand on a totally insulated rubber mat to increase the resistance of the path to ground and provide some protection for yourself.
- ✓ Ensure that power cables and network connections are routed properly.
- ✓ Avoid powering the device from an overloaded circuit.
- ✓ Take special care when handling high voltage components.

Questions

CompTIA IT Fundamentals

Lesson 8

Supporting Computers and Users

CompTIA IT Fundamentals

Topic B :

Back Up and Restore Data

Data Backups

A data backup :

- ✓ is a type of information protection scheme that enables you to store copies of critical files and folders on another medium for safekeeping.

Data backup stores copies of files on another storage medium

Importance of Data Backups

A data backup :

- ✓ Backups protect against data loss due to disasters such as file corruption or hardware failure.
- ✓ you can still have your information intact if you have a backup of your files.
- ✓ You can recover the files without having to recreate them, thereby saving time and effort.

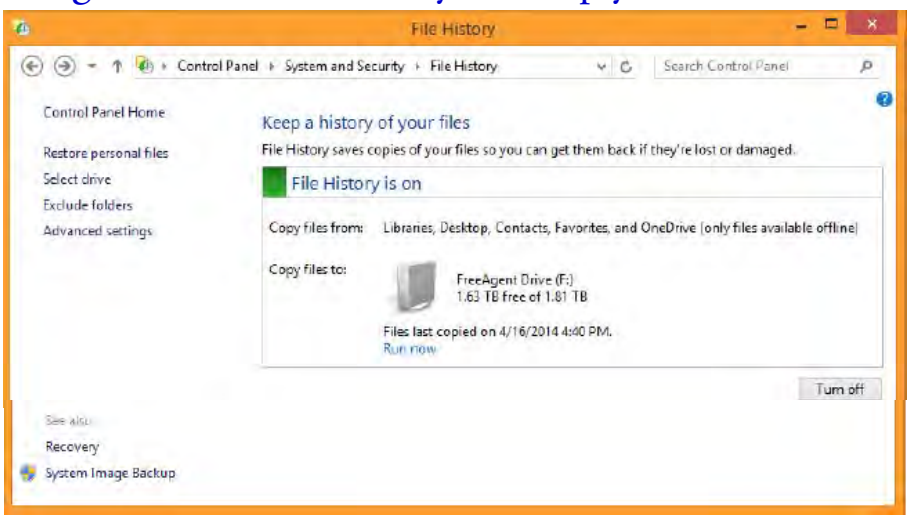
Backup Methods

Data backups can be accomplished in several ways :

- Manually copying individual files and folders to another location, such as a CD-ROM.
- using software specifically designed to assist you in backing up your data.

Backup Methods

✓ Windows 8.1 comes with File History, which can be configured to automatically back up your files.



Using File History from the Desktop to back up data.

Backup Frequency and Schedules

The actual scheduling frequency will depend on :

- ✓ the total size of your data,
- ✓ the number of files in that data,
- ✓ how sensitive that data is,
- ✓ how often the data changes, and
- ✓ how available and accessible that data must be to yourself and others.

Backup Storage Media

Storage media including: :

- ✓ Locally attached storage
  - refers to drives attached directly to workstations and servers through a connection such as Serial ATA (SATA).
  - use for home or small-office
- ✓ Offsite/cloud-based
  - ✓ in which you offload storage to a third party that takes over the burden of storing and maintaining your backups.

Backup Storage Media

Storage media including: :

- ✓ Network-attached storage (NAS)
  - which is a popular solution for small-to-mid-size companies that need to share network storage with dozens of employees in an efficient manner.

Note : Verification and testing your backups is an important part of protecting your data from loss.

Guidelines for Backing Up Data

- ✓ When you are determining what files to back up and how often to back them up, consider the
  - costs of re-creating or replacing the information, and
  - balance those costs against the costs of backing up data.
- ✓ Consider backing up your data or the entire system prior to installing new hardware or software, in case the installation does not proceed as smoothly as planned.

Guidelines for Backing Up Data

- ✓ Consult your organizational policies to determine if rules or guidelines for backups are included in them.
- ✓ Consider implementing a regular schedule for backups to protect your files.
- ✓ Consistently test your backups to verify that your data is intact and not corrupted.

Data Restoration

Data restoration :

- ✓ is a type of information protection scheme that enables you to recover stored copies of critical files and folders from another medium.
- ✓ Data restoration can be local or network-based.

Data restoration restores backed up files

Restoration Methods

Data restoration can be accomplished in several ways :

- ✓ manually copying individual files and folders from another location.
- ✓ using software specifically designed to assist you in restoring data.

Note : Microsoft® Windows® operating systems provide a variety of recovery tools.
For example, Windows 8.1 includes File History, System Restore, and Recovery.

Questions

CompTIA IT Fundamentals

Lesson 8

Supporting Computers and Users

CompTIA IT Fundamentals

Topic C :

Manage Software

Software Management

Questions for considering what software to add or remove :

- ✓ What applications do end users absolutely need to get their jobs done?
- ✓ What are the best products to fulfill this need?
- ✓ Can this product be easily uninstalled if necessary?
- ✓ What OS features might be helpful to the end user?
- ✓ What OS features might be beyond the scope of the end user's duties?

Software Management

Questions for considering what software to add or remove :

- ✓ Are these features easy to add and remove, if necessary?
- ✓ What drivers are available for the hardware that an end user uses?
- ✓ Are these drivers necessary, or are they optional?
- ✓ Will it be easy for you to roll back these drivers in case of incompatibility or other issues?

Software Versions

Versioning :

- ✓ provides information about the iteration of the software you are using.
- ✓ Software versions are changed every time the software is upgraded or newer features have been added to it.
- ✓ Before installing software, you must consider compatibility issues to ensure that it works properly.

Software Versions

Versioning :

- ✓ provides information about the iteration of the software you are using.
- ✓ Software versions are changed every time the software is upgraded or newer features have been added to it.

Software Updates

A software update :

- ✓ is the process of replacing a software application completely with a newer version.
- ✓ It can be done in two ways :
  - by replacing a few selected files only
  - by completely overwriting the software

Software Updates

Automatic updates :

- ✓ is a feature of an operating system or a software application that enables updates to be downloaded and installed automatically on a system at a scheduled time or a certain frequency.

Note : By identifying the risks associated with upgrading, you will consider before you make an upgrade to your system.

Software Licensing

This license can extend to

- ✓ individual users on individual computers or
- ✓ a multi-license (volume) form for enterprises

Note :

- o Licenses entitle the licensee to a product or activation key.
- o Unactivated software may not function, or it may have limited functionality.

Guidelines for Managing Software

- ✓ Identify which applications, OS features, and drivers your users absolutely need to get their jobs done.
- ✓ Identify how easy it is to uninstall any of these pieces of software should issues arise.
- ✓ Identify the version numbers of the software you are looking to download.
- ✓ Identify any compatibility issues that these versions have with your hardware or OS.

Guidelines for Managing Software

- ✓ Schedule a check for updates, such as through automatic updates, to keep your software at the most current version at all times.
- ✓ Obtain the necessary licenses and product keys for each piece of proprietary software.
- ✓ Manage and keep track of all licenses and product keys, mapping them to specific users and machines they are deployed to.

Questions

CompTIA IT Fundamentals

Lesson 8

Supporting Computers and Users

CompTIA IT Fundamentals

Topic D :

Implement Basic Support Measures

General Troubleshooting Tips

Basic troubleshooting steps when you face a device Problem :

- ✓ Use common sense
- ✓ Check the physicalconnections
- ✓ Check external issues
- ✓ Check the adapter to which the device is connected
- ✓ Check Device Manager
- ✓ Use the Help and Support Center
- ✓ Check for a number of causes

Common Operational Problems

You might encounter several problems when troubleshooting PC hardware :

- ✓ No input is sent when keys are pressed on a keyboard
- ✓ Mouse is not working
- ✓ Local network connection but no Internet connection
- ✓ Unable to print
- ✓ No network connectivity or connection lost
- ✓ Hardware device not working properly

Boot Issues

There are several errors that can occur during the boot process or Windows startup :

- ✓ POST errors
- ✓ Invalid boot disk
- ✓ Failure to boot
- ✓ Missing operating system
- ✓ Missing dll message
- ✓ System files fail to open or are missing
- ✓ Device or service fails to start
- ✓ Boots to safe mode
- ✓ Device, or program in Registry, not found

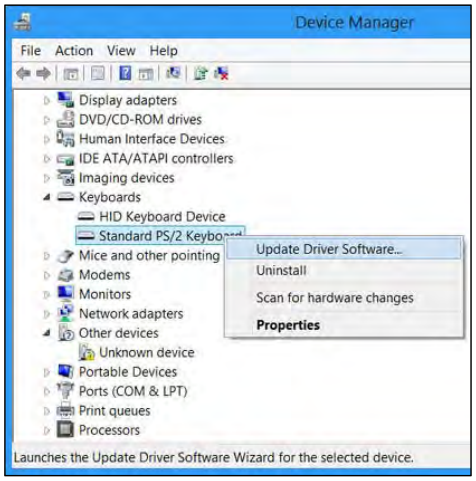
CMOS Error Codes

CMOS 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 CMOS do not match.

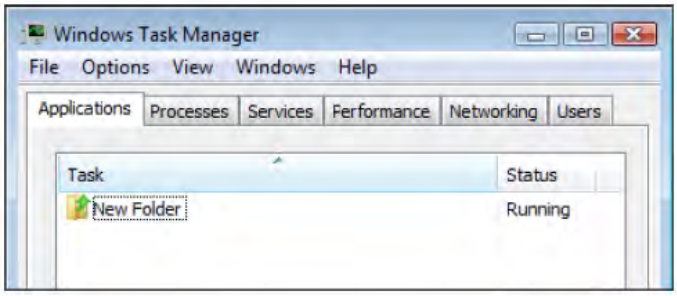
System Management Tools

Tools will help you troubleshoot the issues and maintain the operating system :

System Management Tool	*Description*
Device Manager	

System Management Tools

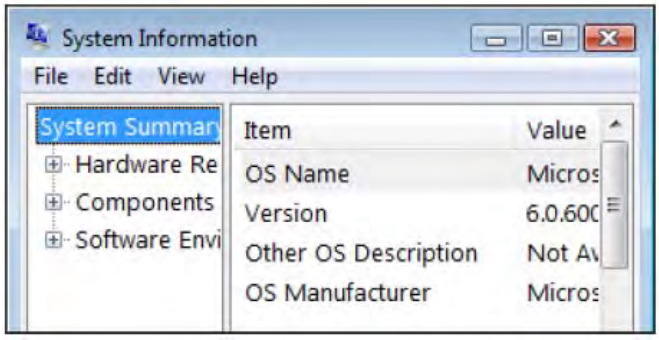
Tools will help you troubleshoot the issues and maintain the operating system :

System Management Tool	*Description*
Windows Task Manager	

System Management Tools

Tools will help you troubleshoot the issues and maintain the operating system :

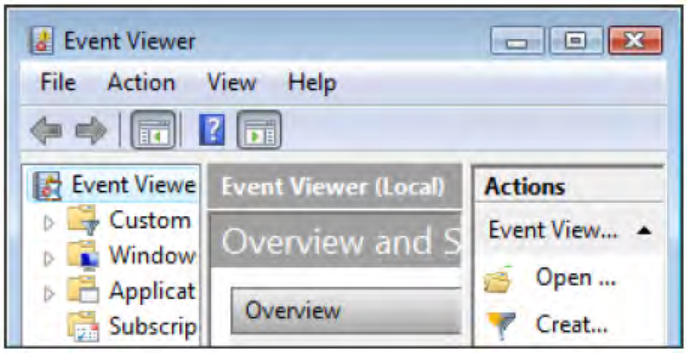
System Management Tool	*Description*
System Information utility	



System Management Tools

Tools will help you troubleshoot the issues and maintain the operating system :

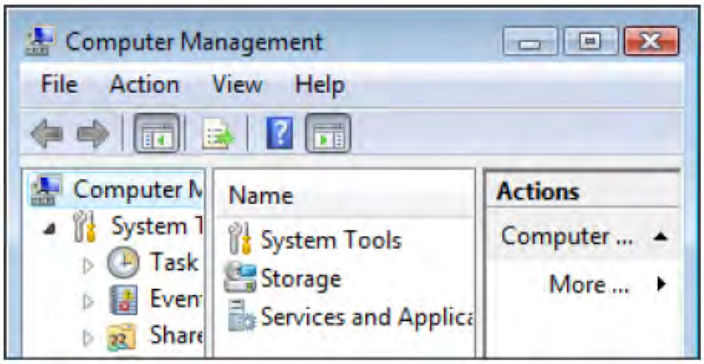
System Management Tool	*Description*
Event Viewer	



System Management Tools

Tools will help you troubleshoot the issues and maintain the operating system :

System Management Tool	*Description*
Computer Management	



Support Resources

As an IT technician, you cannot know everything, but your knowledge of available resources can go a long way :

- ✓ manufacturer's documentation.
- ✓ manufacturer's websites.
- ✓ online technical user groups and
- ✓ communities.
- ✓ Internet search engine
- ✓ technical support

Questions