CompTIA A+ Master Cheat Sheet

How to Prepare for Questions about Hardware on the CompTIA A+ Core Series 1001 Test

General Information

Test 1001 of the CompTIA A+ Core Series contains questions about five topics and one of them is *Hardware*. These questions will occupy about 27% of the 1001 test and about two-thirds of them will begin with the description of a scenario you could encounter in real life. Then, you'll be asked to choose a solution. We've noted in which topics this might happen with the designation (of *scenario*) below.

Cables

You must be able to describe different cable types and their **characteristics** and **uses**.

Network Cables

Network cables **connect devices** to the network. The most common types are Ethernet, fiber, and coaxial cable.

Ethernet

Ethernet cables use **twisted pairs of copper wire**. It may be **shielded or unshielded**. Each category of cable has specific **physical characteristics** and a **maximum data rate**. Ethernet cables have a maximum length of 100 meters.

Cat 5—Category 5 cable supports data rates up to 100 Mbps.

Cat 5e—Category 5e cable supports data rates up to 1 Gbps.

Cat 6—Category 6 cable supports data rates up to 10 Gbps up to 55 meters and 1 Gbps up to 100 meters.

Plenum—Plenum cable is used in the plenum space of a building. **Any space that handles air circulation in an HVAC system** is **plenum space**, typically above a drop ceiling or below a raised floor. Plenum cable uses **low-smoke** and **low-flame materials** for fire prevention.

Shielded twisted pair—STP Ethernet cable uses **two or four pairs of copper wire**. It uses a foil or braided **shield** to reduce electromagnetic interference. Depending on the type of cable, each twisted pair may be shielded or a single shield covers all twisted pairs.

Unshielded twisted pair—UTP Ethernet cable uses **two or four pairs of copper wire**. The twist in the wires reduces electromagnetic interference.

568A/B—Ethernet cables are **terminated with RJ-45 connectors**. The pin-out (which wire connects to which pin) of those connectors is defined in the EIA/TIA 568A & 568B Standards. The difference between 568A and 568B is that the transmit and receive pairs are reversed. This allows for two types of cables, straight-through and crossover.

Straight-through is used to connect a device to the network via a **switch** or **hub**. It uses the same pin-out on both ends, whether 568A or 568B. A **crossover cable** is used to connect one device directly to another, such as two computers, without a switch or hub between them. **Crossover** cables use 568A on one end and 568B on the other.

Fiber

Fiber optic cable uses **light pulses** to transmit data through a glass or plastic core. The cable consists of **four layers**. The core is surrounded by a **cladding** that refracts light back into the core. The other two layers are the **outer sheath**, the part you see, and a strength member or buffer to protect the fiber.

Fiber is **not subject to electromagnetic interference**, since it uses light to transmit data. Transmission distances are longer and data rates are higher on fiber than they are on copper cable. There are two basic types of fiber, single-mode and multimode. **Single-mode fiber** carries only one light path, typically sourced by a laser. **Multimode** carries multiple light paths and is sourced by an LED. Single-mode has a much longer transmission distance than multimode.

Coaxial

Coaxial cable is used primarily for cable Internet service and audio/video applications such as cable TV. It has a **single copper conductor core** surrounded by a **dielectric insulator** and one or more layers of **shielding**. The shielding reduces electromagnetic interference. The two most common types of coaxial cable are **RG-6** for data and **RG-59** for audio/video.

Speed and Transmission Limitations

Each type of network has speed and distance limitations.

- **Category 5** cable supports data rates up to 100 Mbps.
- **Category 5e** cable supports data rates up to 1 Gbps.
- **Category 6** cable supports data rates up to 10 Gbps up to 55 meters and 1 Gbps up to 100 meters.
- The most commonly used fiber is **multimode** and supports data rates up to 100 Mbps up to 2000 meters, 1 Gbps up to 550 meters, and 10 Gbps up to 300 meters.

Video Cables

Video cables connect a specific type of video port on a computer to a display. Each has its own connector type and cable pin-out.

VGA— VGA cables connect older analog Video Graphics Adapters to a display. It uses a **15-pin connector** arranged in three rows of five pins.

HDMI—HDMI cables connect a High Definition Multimedia Interface to a display. It uses a **19-pin connector** arranged in two rows. There are **different types** of HDMI cables. The most commonly used is **type A** but is usually just referred to as an HDMI cable with no type designation.

Mini-HDMI—HDMI **type C** is usually referred to as mini-HDMI. It uses a 19-pin connector arranged in two rows, like the HDMI type A cable, but it is smaller and the pin-out is different.

DisplayPort—DisplayPort cables connect a DisplayPort interface to a display. It uses a **20-pin connector** arranged in two rows of ten pins.

DVI (DVI-D/DVI-I)—DVI cables connect a Digital Visual Interface interface to a display. DVI-D (-D for digital) supports only **digital signals**. DVI-I (-I for integrated) supports digital and analog signals. There are single-link and dual-link DVI cables. **Single-link** DVI supports 3.7 Gbps HDTV at 60 frames per second. **Dual-link** DVI supports 7.4 Gbps HDTV at 85 frames per second.

Multipurpose Cables

Connecting devices directly together without a network connection can be done with these cables.

Lightning—Lightning cables are proprietary to **Apple™**. They are used to connect Apple™ devices to USB ports. The cable has **eight wires** and is terminated with a USB connector on one end and a Lightning connector on the other. It can carry both data and power to charge the device. The Lightning connector is **reversible**, so it can be plugged into the device without regard to which side is up.

Thunderbolt—Thunderbolt is another **Apple™**-proprietary cable. It comes as either **copper or optical** cable. The **maximum length** is 3 meters for copper and 60 meters for optical cable. The connectors are based on the Mini DisplayPort standard, except Thunderbolt version 3 uses a USB-C connector on the peripheral end. It provides both data and power to peripheral devices, most commonly storage and display devices. There are **three versions** of Thunderbolt. Total throughput for Thunderbolt 1 and 2 is 20 Gbps and Thunderbolt 3 is 40 Gbps.

USB—**Universal Serial Bus** cables connect to a wide variety of **peripheral devices**. USB 1.1 was the first version in common use. It uses a type-A connector on the PC side and a type-B connector on the peripheral side. There are also mini and micro connectors for smaller devices such as cell phones and cameras. It supports **two speeds**. Low speed supports data transfer rate of 1.5 Mbps at lengths up to 3 meters. Full speed supports data transfer rates of 12 Mbps at lengths up to 5 meters. It **provides power**, as well.

USB-C—USB-C is a connector type that is used on **USB 3.0 and newer** cables.

USB 2.0—USB 2.0 maintains the characteristics of USB 1.1 and adds a **high-speed data transfer** rate of 480 Mbps at lengths up to 5 meters.

USB 3.0—USB 3.0 maintains the characteristics of USB 2.0 and adds **SuperSpeed data transfer rate** of 5 Gbps at lengths up to 3 meters. The connectors are a bit different, adding pins to some connectors to support the higher transfer rate, as well as adding the type-C connector.

Other Cable Types

Connections to serial ports and hard drives are done with specific cables discussed in this section. In some instances, **adapters** can be used to connect to devices.

Peripheral Cables

Peripheral cables are used **to connect a PC** to other devices.

Serial—While there are many types of serial cables, the term "serial cable" usually refers to a specific type of cable that confirms to the **RS-232 specification**. Serial cables are most often used to connect a laptop to the console or management port of a network device, such as a switch, router, or firewall.

Hard Drive Cables

Hard drive cables connect a hard drive to a **motherboard** or **controller card**. The same cables may also be used to connect optical drives and older floppy drives.

SATA—The Serial Advanced Technology Attachment (SATA) cable is the **most commonly used hard drive cable**. There are different SATA revisions. They all allow a maximum cable length of one meter. SATA revisions 1.0, 2.0, 3.0, and 3.2 support speeds of 1.5 Gbps, 3 Gbps, 6 Gbps, and 16 Gbps, respectively.

IDE—Integrated Drive Electronics is an **older interface**. The IDE cable is a 40-wire (34-wire for floppy drives) ribbon cable that is connected from the motherboard on one end to one or two drives on the other end.

SCSI—Small Computer System Interface was designed to support a wide variety of device types, so there are **different types** of SCSI cables. They may be ribbon cables or standard round cables of 50, 68, or 80 wires. Up to 16 devices, including the motherboard or SCSI controller card, may be connected to one SCSI cable or daisy-chained together.

Adapters

Adapters may be used to connect a device to a port that is different from the connector on the device. They are most often used to connect to a **display** or a **network**.

DVI to HDMI—This **connects a DVI port** to an HDMI display. DVI **does not carry audio**, so a separate connection is needed to carry audio to the display.

USB to Ethernet—This connects a USB port on a computer to an Ethernet port on a network device.

DVI to VGA—This connects a DVI port to a VGA display.

Connectors

You must be able to identify different connectors that are commonly **used to connect to computers, peripherals, and network devices**.

RJ-11—RJ-11 is the plain old telephone system connector. It is a single-row **6-pin** rectangular connector to connect to a phone system or modem.

RJ-45—Often referred to as an **Ethernet connector**, this single-row 8-pin rectangular connector is used for Ethernet connections.

RS-232—RS-232 is actually a specification for serial communications that uses either a DB-9 or DB-25 connector. It has a trapezoid shape. The **DB-9 is a 9-pin** connector arranged in two rows of four and five pins. The **DB-25 is a 25-pin** connector arranged in two rows of 12 and 13 pins. RS-232 is most commonly used to connect **to network devices' console or management ports**.

BNC—BNC connectors are used to **terminate DS3 coaxial cables**, used for wide area network connections. An older type of Ethernet network known as 10Base2 or Thinnet also used coaxial cable terminated with BNC connectors. It is a cylindrical connector with a twist-lock end to make a secure connection.

RG-59—**Cable TV coaxial cables** are **terminated** with RG-59 connectors, cylindrical connectors with a threaded end to make a secure connection.

RG-6—**Cable Internet coaxial cables are terminated** with RG-6 connectors, cylindrical connectors with a threaded end to make a secure connection.

USB—The **Type-A** USB connector is a rectangular **4-pin** connector that connects to a computer. The **Type-B** USB connector is a 4-pin connector that connects to a peripheral device. It is basically square, but two corners are cut at an angle.

Micro-USB—The micro-USB connector is a **5-pin** connector that connects to a peripheral device. It is basically rectangular, but two corners are cut at an angle.

Mini-USB—The mini-USB connector is a **5-pin** connector that connects to a peripheral device. It is basically rectangular, but two corners are cut at an angle on one side, and two tabs are on the other side.

USB-C—The USB-C connector is an **oval 24-pin** connector that connects to either a computer or peripheral device. It is **reversible**, meaning that it may be inserted with either side up. It has two rows of 12 pins. Each row carries the same set of signals.

DB-9—The DB-9 is a trapezoid-shaped **9-pin** connector arranged in two rows of four and five pins. It is used for serial connections to network devices' console or management ports.

Lightning—The Lightning connector is a rectangular **8-pin** connector that connects to either a peripheral device. It is **reversible**, meaning that it may be inserted with either side up. It has a single row of 8 pins that are exposed on both sides of the connector.

SCSI—There are **different types** of SCSI connectors. The most common are rectangular or trapezoidal with **50 or 68 pins** arranged in two rows.

eSATA—The external SATA (eSATA) connector is a **7-pin** connector that connects to an external SATA drive. It has basically a rectangular shape with tabs on the ends.

Molex—The most common Molex connector is a single-row **4-pin** connector used to provide power to disk drives. It has a basically rectangular shape with two corners cut at an angle.

RAM (*scenario*)

You need to understand the different types of random-access memory and how to install them.

RAM Types

SODIMM

Small Outline Dual Inline Memory Modules are commonly found in **laptops** and come in 100-, 144-, 200-, 204-, and 260-pin configurations. SODIMM defines the physical form factor of the module.

DDR2

Double data rate (DDR) refers to the **speed of data transfer**. DDR2 and has less power consumption and is faster than the original DDR RAM. It comes in 240-pin DIMM and 200-pin SODIMM.

DDR3

DDR3 is **faster** than DDR2 and has **30% less power consumption**. It comes in 240-pin DIMM and 204-pin SODIMM.

DDR4

DDR4 is **faster than DDR3** and has **less power consumption**. It comes in 288-pin DIMM and 260-pin SODIMM.

Single Channel

A single channel **RAM architecture** moves data on a single data bus, typically **64-bit**s at a time.

Dual Channel

A dual channel RAM architecture moves data on two data buses, typically **128-bits** at a time.

Triple Channel

A triple channel RAM architecture moves data on three data buses, typically **192-bits** at a time.

Error Correcting

Error Checking and Correcting (**ECC**) memory has logic built in to detect and **correct single-bit memory errors**. For each byte (eight bits) of memory, a parity bit is set that will allow the logic to detect and correct an error in a single bit of each byte. The logic would not correct an error in any byte with more than one bad bit.

Parity vs. Non-Parity

Memory with parity has **logic built in to detect single-bit memory errors**. For each byte (eight bits) of memory, a parity bit is set that will allow the logic to detect an error in a single bit of each byte. The logic may or may not detect an error in any byte with more than one bad bit. While parity allows for the detection of memory errors, it **does not correct those errors**. Additional logic, such as ECC, would be needed for error correction.

Storage Devices (*scenario*)

You should be well-versed with the various types of storage devices and be comfortable with the selection, installation, and configuration procedures for each.

Optical Drives

Optical drives use a laser to **read and/or write data** to an optical disk.

CD-ROM/CD-RW—**Compact disc-read only memory** (CD-ROM) stores data, but you cannot write to it. CD-RW is **rewritable**, so you can write data to it multiple times. CDs store up to 700 MB of data.

DVD-ROM/DVD-RW/DVD-RW DL—**Digital versatile disc-read only memory** (DVD-ROM) stores data, but you cannot write to it. **DVD-RW is rewritable**, so you can write data to it multiple times. DVD-ROM and DVD-RW have a capacity of 4.7 GB. **DVD-RW DL is a dual-layer** version of DVD-RW, nearly doubling the capacity to 8.5 GB.

BD-R—Blu-ray disc-recordable (BD-R) is a Blu-ray disc that you can **write to only once**. It has a capacity of 25 GB.

BD-RE—Blu-ray disc - rewritable (BD-RE) is a Blu-ray disc that you can **write to multiple times**. It has a capacity of 25 GB.

Solid-State Drives

Solid-state drives (SSD) use non-volatile RAM to store data. There is **no disk** and **no moving parts**, so SSD tends to be **more reliable** than disk drives. Access times are **faster** than disk drives.

M.2 drives—M.2 is a **form factor for SSD**. It is 22 mm wide and can vary in length. The most common lengths are 80 mm and 60 mm. It is referred to as **"gumstick memory"** because its size is similar to a stick of gum. M.2 drives plug into an M.2 slot on a motherboard.

NVME—**Non-volatile memory express** is a form of memory that uses the M.2 form factor. It is the **fastest** SSD available today.

SATA 2.5—The SATA 2.5 SSD is designed to** replace a 2.5-inch magnetic hard drive**. It is solid-state memory in the same size case as a 2.5 inch magnetic hard drive.

Magnetic Hard Drives

Magnetic hard drives use magnetic media on rotating platters to store data. **Speeds vary** among different drives, but generally, the faster the rpm, the faster response time in reading and retrieving data. Common speeds for hard drives are: * 5,400 rpm
* 7,200 rpm
* 10,000 rpm
* 15,000 rpm

Sizes—Magnetic hard drives come in different sizes, sometimes referred to as **form factor**. A 2.5-inch form factor means that the disc inside the drive has a diameter of 2.5 inches. The most common sizes are 2.5 and 3.5 inches.

Hybrid Drives

Hybrid drives **combine magnetic disk and SSD drives** in one hard drive case. It uses the disk for high capacity storage and the SSD for lower capacity fast access, providing the best of both storage types.

Flash

Flash memory is a form of **nonvolatile read/write memory**. Nonvolatile memory retains data when power is removed. Flash erases data in blocks, rather than at the byte level. This makes it **less expensive but slower** than other forms of nonvolatile memory.

SD card—Secure Digital cards are designed for use in **portable devices**. They are able to withstand higher impact without damage than other types of memory cards.

CompactFlash—CompactFlash or **CF** cards are primarily used in cameras, but are being replaced by SD cards.

Micro-SD card—Micro-SD is a **smaller** form factor SD card.

Mini-SD card—Mini-SD is a **smaller** form factor SD card that has been made **obsolete** by micro-SD.

xD—xD card, also referred to as xD-picture cards, is a **proprietary memory card** for Olympus and Fujifilm cameras. It is now **obsolete**, as both brands now use SD cards.

Configurations

Storage devices can be configured for high availability so that if one disk in an array of disks fails, data is not lost. The most common configuration is known as **Redundant Array of Inexpensive Disks (RAID)**.

RAID 0, 1, 5, 10—There are different RAID configurations that provide different levels of data protection. **Striping** is a method of storing part of the data on each drive in an array. **Mirroring** is keeping a full copy of a disk on another disk.

- **RAID 0:** offers striping of data only; no redundancy; good performance
- **RAID 1:** offers mirroring of data only; requires more storage space to store full copies of data
- **RAID 5:** offers striping with parity; minimum of three drives; ability to calculate missing data and rebuild
- **RAID 10:** offers striping and mirroring for full redundancy; minimum of four drives

HOT swappable—Hot swappable drives **can be inserted or removed in real time** while the system is powered on. A common type of drive of this type is a USB flash drive. Disks in a RAID array are often hot swappable.

Motherboards, CPUs, and Add-on Cards (*scenario*)

The motherboard provides the circuitry by which all parts of a computer communicate with each other, from the processor to the power supply. Every part of a computer interacts with the motherboard in some fashion. You should be able to install and configure motherboards, as well as the CPUs and add-on cards you plug into them, in a given scenario.

Motherboard Form Factor

The form factor describes the physical characteristics of the motherboard.

ATX—ATX stands for **Advanced Technology Extended**. Older ATX variants contain a 20-pin Molex power connection, while newer models contain the 24-pin Molex power connection.

mATX—Micro-ATX is a little bit **smaller than the ATX** and does not have as much expansion ability.

ITX—ITX is a series of **significantly smaller** form factor boards that were created by VIA Technologies™. The most common one is the mini-ITX.

mITX—Mini-ITX is the largest of the ITX form factors, with a size of 6.7 by 6.7 inches. It is also the **most popular**.

Motherboard Connector Types

Motherboards have a variety of connectors that determine what can be connected to it.

PCI—**Peripheral Component Interconnect** was introduced by **Intel™** in the 1990s. This replaced older 8- and 16-bit expansion slots with a 32-bit slot.

PCIe—**PCI express** sends data in a serial stream at **higher speeds** than conventional PCI. It has superseded PCI.

Riser card—A riser card plugs into an existing connector and contains more connectors of the same type. It increases the **number of cards** you can add. It also changes the **orientation** of the connectors 90 degrees so that cards can fit into a smaller case.

Socket types—CPUs plug into sockets. Two common socket types are **zero insertion force (ZIF)** and **land grid array (LGA)**. ZIF has holes that CPU pins slide into. LGA has pins that CPU contacts sit on top of. The CPU is held in place by a lever that keeps pressure on the CPU to hold it in place.

SATA—The **Serial ATA** connector is used to connect a hard drive or optical drive.

IDE—IDE connectors are another hard drive connection point. It has been largely **replaced** by SATA.

Front panel connector—The front panel has components on it that need to connect back to the **motherboard**. Each computer is different, but front panel components may include LEDs, USB ports, the power switch, a reset button, and audio connections. There may be multiple connections between the front panel and motherboard.

Internal USB connector—An internal USB connector allows you to **add USB ports**. They would typically be mounted in an open expansion slot.

BIOS/UEFI settings

The BIOS is, arguably, one of the **most important** aspects of a computer. You need to have a good understanding of system BIOS and how to modify the settings. Understand the importance of selecting the proper **boot sequence** and how BIOS provides low-level drivers that allow the operating system to interact with various hardware components. Comprehend the various stages in the boot sequence, the system **POST**, and the role BIOS plays in loading the operating system. The CompTIA A+ questions about BIOS require that you assess a scenario to be able to choose the best answer.

Boot Options

You can set the **sequence of devices to boot from** in the boot option settings. You usually boot from the hard drive, but you may want to boot from an optical drive or flash drive. The boot sequence tells the BIOS where to look to load the operating system. It will proceed down the list in the order configured until it finds an operating system to load.

Firmware Updates

Always **check the version of the BIOS** you are using before doing an upgrade. This can be found in your system information utility, or by typing `msinfo32` into the cmd prompt. Most manufacturers offer BIOS upgrades directly from their website, as a simple **download**, and it is a very straightforward process. Just download the correct file, based on the type of system you have, and run the update to begin the installation. This entire procedure is known as **flashing the BIOS**.

Security Settings

You are able to secure access to the BIOS, or to the operating system, by setting certain passwords from within the BIOS. These security measures require a password at startup to load the operating system or make changes to the BIOS.

Interface Configurations

This provides settings specific to interface categories or individual interfaces such as PCIe or SATA.

Security

Security settings control access to the BIOS and set security features.

Passwords—The supervisor or admin password, if enabled, requires a password to view and set all BIOS settings. The user or system password allows minor changes such as time and date or boot options to be set.

Drive encryption—An encryption key can be set to access an encrypted hard drive. If set, that key must be used for decryption, even if the drive is moved to another computer.

- **TPM**—The **Trusted Platform Module** is a security chip that stores cryptographic keys.
- **LoJack**—A feature that enables a stolen device to be **tracked, locked, and/or wiped**.
- **Secure boot**—Secure boot ensures that the operating system and drivers are authorized versions **without malicious code** before loading them.

CMOS Battery

The CMOS (**complementary metal oxide semiconductor**) battery was originally used to maintain system settings stored in CMOS RAM since it was volatile. It is also used to power the systems real-time clock. Over the years, CMOS RAM has been replaced by flash memory that does not require a battery to maintain data; however, the real-time clock still requires a battery. As a preparation for this test, you should know how to locate and replace the CMOS battery.

CPU Features

There are several important features of CPUs that are important to consider. You need to understand the different features and their impact on performance.

Single-Core

A core is the part of the CPU that reads and executes instructions. As the name implies, a single-core CPU has **one core**. Most of today's CPUs have multiple cores.

Multicore

A core is the part of the CPU that reads and executes instructions. Multicore CPUs have more than one core. This allows **different threads** of instructions to be run **simultaneously**, with each core running one thread, resulting in **faster** performance. A dual-core processor will run faster than a single core, but not quite twice as fast. There are also quad-core, eight core, and other types of multicore processors.

Virtualization

Some CPUs have features to support **virtual machines (VMs)**, running multiple operating systems on a single machine. They offload some of the work that VM software would have to do, improving VM performance. Intel™ calls theirs Intel™ Virtualization Technology. AMD™ calls theirs AMD-V.

Hyperthreading

Hyperthreading, or **multithreading**, leverages virtual cores to run applications 15 to 30 percent faster.

Speeds

CPU speed, typically measured in**gigahertz**, is a measure of how fast a processor can read and execute instructions.

Overclocking

Overclocking is running the CPU at a speed higher than it was designed to operate. Some CPUs allow this while others do not. It will **improve the performance** of the CPU but generate more heat, so added cooling may be needed to prevent damage to the CPU.

Integrated GPU

An integrated GPU is a **graphics processing unit** embedded with the CPU. It is not as powerful as a stand-alone GPU, but it is commonly used in laptops to save space.

Compatibility

CPUs need to be installed in motherboards that have CPU sockets and chipsets that they are compatible with.

AMD

Specific AMD CPUs must run with specific AMD chipsets. The motherboard manufacturers may vary.

Intel™

Specific Intel™ CPUs must run with specific Intel™ chipsets. The motherboard manufacturers may vary.

Cooling Mechanism

Components on motherboards and add-on cards generate heat, especially CPUs and GPUs. There are several types of cooling mechanisms to remove heat from a computer.

Fans

Fans are used to **move air** through a computer to remove heat. Fans are positioned in the case to allow air to pass between the inside of the case and the outside. Fans are also used on individual components to provide **extra cooling**. They are sometimes integrated with a heat sink.

Heat Sink

Heat sinks are devices that conduct heat and have the effect of increasing the surface area of a component. This **removes heat** from the component more quickly than fans alone. Some heat sinks have fans built into them.

Liquid

For high-performance computers, air cooling may not be enough. Liquid cooling is more effective at transferring heat away from components. Distilled water is the most commonly used liquid. Liquid cooling systems include a tank for the liquid, a radiator, a water pump, and a cooling block that attaches to the component being cooled. These components may be in the computer or outside in a separate unit that connects to the computer.

Thermal Paste

The quality of contact between a component to be cooled and the heat sink used to cool it will impact how effectively it is cooled. Thermal paste conducts heat and is used **between the component and heat sink** to make the best thermal-conductive connection.

Expansion Cards

Expansion cards add additional functionality to your PC. You must use expansion cards that are **compatible** with the expansion slots available. You should understand how to install and configure expansion cards.

Video Cards

Video cards control the graphics that are displayed. This function may be provided by an add-on card or it may be on-board, meaning built into the motherboard.

On-board—On-board video cards typically provide good graphics features and specifications. It serves the purpose for **most users**, but some users, like gamers or graphic designers, may need better graphics.

Add-on card—Add-on video cards have their own GPU (graphics processing unit). They are used to **improve** the **graphics** capabilities beyond what the on-board video provides.

Sound Cards

Add-on sound cards are used to **improve the sound capabilities** beyond the motherboard's sound capabilities. A musician, composer, or audiophile may choose to upgrade their computer's sound with an add-on card.

Network Interface Card

A network interface card (**NIC**) is built into almost all motherboards today. An add-on card would typically only be necessary if you wanted a different interface or to connect to a second network.

USB Expansion Card

A USB expansion card is used to add USB ports to the computer. It may also be used to add newer version USB ports.

eSATA Card

An eSATA card is used to connect to external SATA storage devices.

Peripherals

The PC uses several peripheral devices to interact with other hardware, like a keyboard or mouse. You should understand the purpose and use of these peripherals.

Printer

Printers provide **hard copy** (paper) output. **All-in-one printers** include other functions such as fax, scanner, and copier. Printers may connect via WiFi, USB, Ethernet, Bluetooth, or infrared connections. Operating systems have generic printer drivers, but better printer control and features can usually be obtained by loading the printer's own drivers.

ADF/Flatbed Scanner

A scanner creates a digital image of a paper document and stores it in an image file or **Portable Document Format (PDF)** file. The original document can be input using a flatbed or an **automatic document feeder (ADF)**. **Flatbed** scanners provide a glass bed onto which you place the document. This allows you to scan either one-page documents or pages from a book. An ADF feeds paper, one sheet at a time, from a stack of separate sheets of paper.

Barcode Scanner/QR Scanner

Barcode and **quick response** (QR) code scanners read barcode and QR codes, often using the same application. Barcodes are usually used to represent a machine-readable number, such as a product's **universal price code (UPC)**. QR codes are most often used to represent a machine-readable link to a website that provides more information.

Monitors

Monitors, also called displays, allow users to see the video output of a computer. They connect through various types of video output, such as HDMI, DVI, or DisplayPort.

VR Headset

A **Virtual Reality (VR)** headset **completely blocks the user's view** of his or her actual surroundings and replaces it with what is on the screen in the headset. The **user can interact** with the virtual reality they are viewing and hearing in a number of ways with various input devices. Input devices range from simple game-controller-type devices to sensor-embedded suits and multi-directional treadmills. The most common use is currently **gaming**, but VR headsets are also used for training, design, architecture, medical applications, and more.

Optical Drive Types

Optical drives are used to read CDs, DVDs, and Blu-ray discs. They are often **built into** desktops and larger laptops. Slimmer laptops cannot accommodate an optical drive, so they use **peripheral** optical drives. They are typically connected via USB.

Mouse

A mouse is an input device that provides **point-and-click capability** for computers. Mouse devices connect to today's computers via **USB** or **Bluetooth**. Older computers used the PS/2 connector.

Keyboard

A keyboard is an input device used to enter alphanumeric characters and other symbols into the computer. Keyboards connect to today's computers via **USB** or **Bluetooth**. Older computers used the PS/2 connector.

Touchpad

A touchpad is an input device that provides point-and-click capabilities similar to a mouse. It is **built into laptops** but also available as a **peripheral device** that connects via **USB** or **Bluetooth**.

Signature Pad

A signature pad is an input device that has a **surface you can "write" on**, but rather than writing in ink, the pressure on the pad is detected, displayed on the screen and/or stored in a file. It is used to capture a signature during a transaction. It connects via **USB**.

Game Controllers

Game controllers are input devices that allow a user to **interact** with a video game. It is available in the form of a gamepad, joystick, steering wheel, gun, or anything to simulate whatever is used in the game.

Camera/Webcam

Cameras and webcams are **input devices** used to capture photos or videos. Webcams are also used for interactive communications such as video conferencing. **Webcams** may be **built into** devices or separate **peripheral** webcams are connected to the computer when in use.

Digital cameras are used when **disconnected from the computer** to take photos and videos that are stored as files in the camera. The camera can then be connected to a computer, usually via USB, to **transfer the files** to the computer.

Microphone

Microphones are **audio input** devices. They are used to **record** audio or for interactive communications such as Internet phone calls or video conferencing. Microphones may be built into a computer or connected as a peripheral via **USB**, **Bluetooth**, or a **tip/ring/sleeve (TSR)** audio input jack.

Speakers

Speakers are audio output devices. They are used to play audio or for interactive communications such as Internet phone calls or video conferencing. Speakers may be **built into** a computer or connected as a **peripheral** via **USB**, **Bluetooth**, or a **tip/ring/sleeve (TSR)** audio input jack.

Headset

A headset is a **microphone and headphones combined** in one unit. Like microphones and speakers, they are used to play audio or for interactive communications such as Internet phone calls or video conferencing. They connect via **USB, Bluetooth**, or **tip/ring/sleeve (TSR)** audio jacks. There may be **two audio jacks**, one for the microphone and another for the headphones, or it may be a single **combined jack**.

Projector

A projector is a video output device that projects the video output onto a screen or whatever you happen to point it at. It is most often used to do **presentations** or to show photos or videos. The projector must put out bright enough light so that the projected image is clearly visible.

How much brightness is needed is determined by distance and ambient light. Brightness is measured in **lumens (lm)**. The bulb in a projector will have a specific lumen value.

Projectors connect to computers using the same types of connections as any other display, such as **HDMI**, **DVI**, or **USB**.

External Storage Drives

External hard drives, solid state drives (SSD), and optical drives **store data** outside of the computer itself. They are usually not the primary drive but are used to **back up** data or increase overall **storage** capacity. They connect via **USB**, **eSATA**, or **Thunderbolt** connections.

KVM

Keyboard, **video**, **mouse (KVM)** switches are typically used in data centers with many servers. Rather than each server having its own keyboard, video monitor, and mouse, KVMs connect a single keyboard, monitor, and mouse, to **multiple servers**. The user at the KVM can then select which server they are controlling.

Magnetic Reader/Chip Reader

Credit cards and **debit cards** are read with either a magnetic reader or chip reader. The magnetic reader is what you swipe the card through, as it reads the data on the magnetic strip on the card. The chip reader is used to read the chip on newer cards. Aside from bank cards, they are used to read other types of cards as well. One example is **access cards** for opening doors to secure areas.

They often connect to **point-of-sale (POS)** systems. With the POS services available today, a POS system can be anything from a computer at a store checkout to a tablet to a mobile phone in a kiosk. So, there are many possible connection types, including **USB**, **Lightning**, and even the **headphone jack** on a phone.

NFC/Tap Pay Device

Near field communication (NFC) is a form of **contactless** communication. Two devices must be **within a few centimeters** of each other to communicate. It is most commonly used for **tap pay** systems that allow you to place a mobile phone or contactless credit card near the tap pay device to pay. NFC is also used for **transfer photos or files** between smartphones. There are other applications for NFC and more are being created.

Smart Card Reader

Smart cards are similar in form factor to credit cards, but their main purpose is to **securely store data**. Smart card readers come in **different forms**. They may be built into laptops that the card is inserted into. They may be contactless so that the card can be read if it is within a few centimeters of the reader.

The most common use for smart cards is to **authenticate a user** to a system. In addition to a username and password, it serves as a **second factor of authentication**.

Power Supplies

Power supplies **convert AC power to** the **DC power** that computer components run on. There are different types of power supplies to fit different types of computers. Each power supply has specific features related to **capacity** and **connectors**. You must be able to select the proper **power supply type** and **features** needed in any given scenario.

Input 115V vs. 220V

The input to a power supply is provided by the power company. This is the power available at a wall outlet. In North America and some other parts of the world, **110 volts AC - 120 volts AC** is supplied. Other countries supply **220 volts AC - 240 volts AC**. So, power supplies are designed to accept either or both of these inputs. You may find power supplies that accept only one or the other voltage, but most accept both. Some have a **switch** to set for the correct input. Others accept either input without having to set a switch.

Output 5V vs. 12V

The power supply **converts the AC power input to DC power** that supplies the computer's components. Most power supplies provide +5V and +12V. Others may also provide -12V, -5V, and +3.3V. You may see more than one connector for a specific output. For example, you may see two +12V outputs, each with its own connector. Each output is called a rail, so in this example, there would be two +12V rails.

24-Pin Motherboard Adapter

Most power supplies **provide DC output power** on a standard 24-pin connector, also called the **ATX power connector**, which plugs into the motherboard. The connector is keyed so that it can only plug in one way, ensuring that the proper voltages are supplied to the right pins. Specific pins are designated to supply +5V, +12V, -12V, and 3.3V.

Wattage Rating

Wattage rating, or **power rating**, is the **total capacity of the power supply**. This must be high enough to meet the total power demands of all components in the computer.

Number of Devices/Types of Devices to Be Powered

The number and types of devices or components in any given computer determine what **wattage rating** is **needed** for the power supply. It also determines what types of connectors are needed to ensure that you can connect the power supply to each device.

The type of case the computer is in also needs to be considered to ensure that the power supply physically fits properly.

To determine the wattage requirement of the power supply, add all of the wattage ratings of the individual components. Your power supply's wattage must meet or preferably exceed that total value. The connectors needed are determined by the connector types used on the devices to be powered. For example, if you have an older ATX motherboard, it has a 20-pin power connection, while newer models contain the 24-pin Molex power connection.

The power supply you select obviously must physically fit into the case. It also needs long enough cables from the power supply to reach the components.

Custom PC Configuration (*scenario*)

You should be able to select the proper components to configure a custom PC to meet the requirements for specific types of customers.

Graphic/CAD/DAM Design Workstation

Graphic design workstations require a lot of **fast memory** and **powerful graphics processing** capabilities.

SSD—A magnetic drive may be too slow to meet the demands of graphics design workstations. A **solid state drive** with faster access times should be selected.

High-end video—A powerful graphics card with a **dedicated graphics processing** unit is essential.

Maximum RAM—High-end graphics work with **large chunks of data** at a time. RAM is working memory, so the more you have, the better the performance will be.

Audio/Video Editing Workstation

Audio/video editing workstations perform best if they have an **expansion card** dedicated to editing. This may be in the form of two separate cards, a video card and a sound card, or one card that handles both video and sound. Editors work with large files, so a lot of **storage space** is needed. **Dual monitors** allow editors to do editing on one monitor and review the video on the other.

Specialized audio and video card—Editing requires more processing power than is available on some motherboard CPUs. Specialized video and/or audio cards provide added processing power.

Large, fast hard drive—Editing often involves working with large files, so a large, fast hard drive is needed. It is also helpful to have an additional solid state drive that can move large working files quickly.

Dual monitors—Video editing software has a lot of controls that are presented in separate Windows™. Dual monitors allow editors to spread these controls across different monitors. A separate monitor to review the edited video is another use of dual monitors.

Virtualization Workstation

Virtualization workstations are designed to run multiple virtual machines (VMs) on a single computer. Each VM needs CPU power and memory, so you need to **maximize CPU cores and RAM**. The more CPU cores and memory you have, the more VMs you will be able to run.

Gaming PC

Gaming PCs are among the **most demanding** custom PC types. They require the fastest audio and video processing, so a solid state drive (SSD), high-end graphical processing unit (GPU), and high-definition sound card are needed.

SSD—Video games cannot load completely into RAM, so they need to load from disk at times during game play. That can cause a momentary pause in the game if not done fast enough. To minimize the chances of such delays, SSD is preferred over a magnetic disk drive.

*High-end video/specialized GPU**—A **dedicated GPU** is required to provide the high-end video that gamers demand. The video is constantly being updated and even the slightest lag can take the enjoyment out of a game.

*High-definition sound card**—Sound plays a major role in some games, so a high-definition sound card is essential.

*High-end cooling**—Multiple high-end components, especially the GPUs and CPUs, generate a lot of heat, so high-end cooling is a must. In some cases, **liquid cooling** is necessary.

Network Attached Storage Device

Network attached storage (**NAS**) devices have a dedicated purpose of storing and providing access to files. Files can be stored on a NAS device so that they are available to all users on the network, without each user needing to have a local copy.

Media streaming—NAS devices provide streaming capabilities so that users can watch videos or listen to music without downloading files.

File sharing—NAS devices allow users to download files to their local PC or device.

Gigabit NIC—The throughput demand on a NAS server can be significant because multiple users may be streaming or transferring large files simultaneously. A gigabit network interface card (NIC) should be used to **minimize the risk of the NIC becoming a bottleneck**.

RAID array—NAS devices often store important files, whether business documents or treasured photos. So it is important to protect those files with redundancy. A redundant array of inexpensive disks (RAID) **provides redundancy** in NAS devices. RAID uses an array of disk drives that, depending on the configuration, may employ **parity checking and error correction** to ensure that data is not lost.

Hard drive—NAS devices usually store large quantities of files, so hard drives are used to meet the demand for high-capacity storage.

Standard Thick Client

A standard thick client is what most people think of (and use) as a **PC**. It stores and runs the operating system and applications locally.

Desktop applications—Thick clients store and run applications locally, so they need to meet all of the applications' requirements. This includes **storage space** for the applications' files, **processing power** to run the applications, and **working memory space**.

Meets recommended requirements for selected OS—Operating systems typically provide specifications to meet both minimum and recommended requirements. Thick clients do all processing locally, so they should **exceed the minimum requirements** for the operating system. They should have the processing power, memory, and other requirements to meet or exceed the recommended requirements.

Thin Client

Thin clients **rely on servers** to store applications and do some of the processing for them. So, they do not need as much processing power and memory as a thick client.

Basic Applications—The only applications run locally on thin clients are the basic applications needed to access the servers and remote applications they use.

Meets minimum requirements for selected OS—Operating systems typically provide specifications to meet both minimum and recommended requirements. Since thin clients rely on servers to store applications and do some of the processing for them, they need to only meet the minimum requirements for the operating system.

Network connectivity—Since thin clients rely on communications with servers, they need **high-speed** network connectivity.

Other Common Devices (*scenario*)

Common devices such as desktops and laptops are essential to any business or home user. In any given scenario, you must know how to install and configure desktops and laptops.

Desktop

Desktop computers fall into two categories: thin clients and thick clients. Installation and configuration will vary for each.

Thin Client

Thin client installation and configuration is a simple process, since thin clients do not run applications locally. They **connect to servers** that store and run applications. They often **do not store data** locally, using servers for storage as well. There is usually a **minimal operating system** pre-installed and a **network interface card** or **WiFi** to connect to the network.

Input/output devices such as the keyboard, mouse, and monitor may need to be configured. For example, you may configure language and keyboard layout settings. **Network parameters** may also need to be configured. **DHCP** may handle the network connection, but you may need to configure the initial server connection.

Thick Client

A thick client is a standard computer that** runs applications and stores data locally**. Thus, the operating system, applications, and peripherals need to be installed and configured. Network settings may be set by DHCP or need to be configured manually.

Account Setup/Settings

Account setup on a thin client is minimal. User accounts will typically be set up by an administrator on a directory server. The thin client can log in to an account previously configured on the network. Users **do not typically log in** to the thin client itself.

The thick client will have a **local login**, since it runs applications locally and stores data that needs to be protected. It should have a local **administrator account**, as well as a **user account**.

Laptop

Laptops share some of the items that need to be installed and configured with desktops, but they have additional items such as touchpads and touchscreens not typically found on desktops.

Touchpad Configuration

Touchpads usually work well with the default configuration but can be tuned to **user preferences** for sensitivity, multi-finger gestures, tapping, and clicking.

Touchscreen Configuration

The touchscreen may need to be **calibrated** to ensure that it properly recognizes the point being touched on the screen. This only needs to be done if accurately selecting objects on the screen is a problem.

Application Installations/Configurations

Laptops may not be as powerful as desktops, so you need to be sure that the laptop will **support the requirements** of an application before you install it. Check **CPU**, **RAM**, and storage requirements.

Synchronization Settings

Depending on the operating system, you can synchronize certain settings between devices. This gives you the same look and feel as you move from one device to another. You can also synchronize data, including files, photos, and music. The methods to do so vary for different operating systems and applications.

Account Setup/Settings

Laptops require **strong account settings**, since they are used in public spaces and more likely to be lost or stolen. A user account with minimal access should be set up as the default user account to minimize the risk if a malicious actor gets access to the laptop.

Wireless Settings

Laptops are mobile devices, so they often **connect to different networks**. To be able to join different networks, the wireless configuration should use **DHCP rather than a manual IP configuration**. This allows it to acquire its IP address and other settings from whatever access point it connects to.

SOHO Devices and Printers (*scenario*)

Multifunction devices and printers are suitable for **small office home office** (SOHO) use. They save cost and take up less space by combining multiple functions into a single device. You should be familiar with configuring these types of devices.

Use Appropriate Drivers for a Given Operating System

To get the most out of a multifunction device, the **proper drivers** for that device should be loaded. The device may work using the default drivers included with the operating system, but you may not get the **full functionality** that the device-specific driver provides. The drivers are specific not only to the device but to the operating system, as well. You also need to select the proper driver for either **32-bit or 64-bit systems**.

Duplex

Enabling duplex mode causes the printer to **print on both sides** of the paper.

Collate

Collate or collation settings determine the **order in which pages are printed**. If set to collate, the printer will print the complete document before printing the next copy.

Orientation

There are two options for orientation, **portrait or landscape**. In portrait mode, the top of the page is the shorter dimension. This is how pages are typically printed. In landscape mode, the top of the page is the longer dimension. Spreadsheets and slides are often printed in landscape mode.

Quality

Print quality settings control resolution and color. **Resolution** is expressed dots per inch. Higher resolutions provide better quality printouts. **Color** settings control how vivid the color output is.

Device Sharing

Devices can be shared by multiple users, over wired or wireless connections. Users can **connect directly** to a printer or through a **print server** or **cloud** printing service.

Wired

Wired connections to printers may be made via USB, serial, or Ethernet.

USB—USB is the **most common** way to connect a printer to a computer. When connected, that computer can be configured to make that printer shareable.

Serial—Serial is an **older** connection method using a **serial cable** with a DB-9 or DB-25 connector. It is unlikely that you would see this type of connection today.

Ethernet—Printers that are designed to work on a **network** will have an RJ-45 Ethernet connector. They connect to the network with an Ethernet cable, just as a computer would. They are **easily shared**, since the are connected directly to the network.

Wireless

Wireless connections to printers may be made via Bluetooth, 802.11, or a direct ad hoc connection.

Bluetooth—Bluetooth connections can be used to print from devices within 10 meters (about 30 feet) of the printer. Mobile devices can use Bluetooth to send documents directly to a printer.

802.11 (a, b, g, n, ac)—Printers may use the 802.11 wireless protocol to make **WiFi** connections to networks. Any device on the network can then use that printer. A device may also **connect directly** to a printer using 802.11.

** Infrastructure vs. ad hoc**—When the device and the printer use the network** **WiFi** infrastructure to communicate, it is referred to as **infrastructure mode**. Another mode of 802.11 communications is ad hoc mode. In **ad hoc mode**, a device **connects directly** to the printer over 802.11.

Integrated Print Server (Hardware)

A print server sits on the network and handles printing requests from users. It can **spool** (temporarily store) requests for printers that are busy, allow **prioritization** of print jobs, and **delete** jobs after they've been sent. Print servers may be separate devices or integrated into the printer.

Cloud Printing/Remote Printing

Cloud printing is a service that allows you to **print from anywhere** you have Internet access to a printer that has been configured for use with that service. Not all printers are compatible with all cloud print services, so you must check for **compatibility**.

Public/Shared Devices

SOHO devices can be made available and shared with anyone on a network. This is true for devices that are connected directly to the network or connected to a computer. If a printer is connected to a computer, then the operating system must be **configured** to make the printer available to users on the network.

Giving access to users over the network raises concerns over **data privacy**. Steps must be taken to ensure that users cannot read other users' print jobs.

Sharing Local/Networked Device

Different operating systems have their own mechanisms for sharing printers.

Windows™ provides a means to configure printers with **Control Panel**, where it may be set as shareable. Users can then access the printer over transmission control protocol (TCP) and user datagram protocol (UDP) by identifying the IP address of the computer and the TCP/UDP ports. The ports used for network printing are TCP 139, TCP 445, UDP 137, and UDP 138.

Apple™ computers share printers using the **Bonjour™** protocol. Any Apple™ device can discover printers connected via Bonjour™. Windows™ users would have to install **iTunes™** to access Bonjour™ printers. Apple™ mobile devices running iOS™ use **AirPrint™** to print to shared printers over WiFi.

Data Privacy

To ensure data privacy of print jobs, you need to manage user authentication and hard drive **caching** of print jobs, also known as spooling.

User authentication—Users can be required to **authenticate** to print servers. They typically authenticate at one of two security levels: **user** or **administrator**. Users are limited to printing and managing their own print jobs. This prevents other users from seeing or interfering with other users' print jobs. Administrators can manage all print jobs.

Hard drive caching—Hard drive caching of print jobs is called spooling. It allows print jobs to be stored on a hard drive or other storage device until the printer is ready to print it. The print job sits in a file until it is printed, and then it **should be automatically deleted**. However, automatic deletion may fail. In that case, the file can be manually deleted by an administrator.

Other Print Technologies (*scenario*)

There is a variety of print technologies such as laser, inkjet, thermal, impact, and 3D printers. There are also virtual print options to print to a text, PDF, XPS, or image file. You need to be able to install and maintain each of these print technologies for any given scenario.

Laser

Laser printers create high quality printouts using a complex process. The component that actually “draws” the image is a laser. It works with other components to transfer that image to the paper.

** Imaging drum, fuser assembly, transfer belt, transfer roller, pickup rollers, separate pads, duplexing assembly**—

- **Imaging drum:** The laser “draws” the page image onto the imaging drum.
- **Fuser assembly:** The fuser assembly applies pressure and heat to bond the toner to the paper.
- **Transfer belt:** Used in color laser printers, the transfer belt transfers the page image from the imaging drum to the paper.
- **Transfer roller:** Used in black-and-white laser printers, the transfer roller transfers the page image from the imaging drum to the paper.
- **Pickup rollers:** Rubber pickup rollers feed paper from the paper tray through the printer.
- **Separate pads:** To ensure that only one page is fed at a time, separate pads separate the page begin fed from the pages underneath it.
- **Duplexing assembly:** To print on both sides of the paper, the duplexing assembly will flip the paper over.

** Imaging process: processing, charging, exposing, developing, transferring, fusing, and cleaning**—

- **Processing:** Before any actual printing is done, the image of the full page in placed into memory.
- **Charging:** A high negative charge is applied to the imaging drum.
- **Exposing:** The laser “draws” the image of the page onto the imaging drum by exposing it to the laser light. The tightly focused laser light removes the negative charge from (neutralizes) the imaging drum, leaving the rest of the drum negatively charged.
- **Developing:** The negatively charged toner is transferred to the imaging drum. Since the drum is also negatively charged, the toner will only stick to the areas that have been neutralized by the laser.
- **Transferring:** The transfer roller or transfer belt transfers the toner from the drum to the paper.
- **Fusing:** A fusing roller users heat and pressure to bond the toner to the paper.
- **Cleaning:** Any residual toner is cleaned off of the imaging drum.

Maintenance: Replace toner, apply maintenance kit, calibrate, clean— Laser printers tend to be **expensive**, so **regular maintenance** must be done to keep them running well for a long time. Manufacturers make this fairly easy for common maintenance tasks like replacing toner. Other tasks require more knowledge and skill.

- **Replace toner:** Toner is used for each print job, so it must periodically be replaced. Toner comes in a toner cartridge that is easily replaced by the user.
- **Apply maintenance kit:** Printer manufacturers recommend replacing certain parts periodically. They provide these parts in maintenance kits. They may include the fuser assembly, transfer belt, transfer roller, pickup rollers, and/or separate pads.
- **Calibrate:** Calibration is done to keep the page image sharp and accurate. This may be done on a periodic basis and when parts are replaced. Each printer will have its own calibration process.
- **Clean:** Toner is a fine powder that will leave residue in the printer. Keeping the inside of the printer clean will keep it running well and prevent loose toner from showing up on printouts.

Inkjet

Inkjet printers create high-quality printouts, though the **resolution can be less** than that of laser printers. They are also much **less expensive**. They create the page image by spraying ink dots onto precise points on the paper. Several components work together to transfer the page image to the paper.

** Ink cartridge, print head, roller, feeder, duplexing assembly, carriage, and belt**—

- **Ink cartridge:** Ink is stored in ink cartridges that supply ink to the print heads. There may be a separate cartridge for each of the standard colors used — cyan, magenta, yellow, and black. Some inkjet printers use a combined color cartridge with cyan, magenta, yellow ink plus a black ink cartridge.
- **Print head:** The print head draws the ink from the cartridge and ejects it onto the paper. Some printers combine the ink cartridge and print head into a single unit.
- **Roller:** Paper is fed through the printer by the roller.
- **Feeder:** Paper may be fed from either a simple paper tray or a feeder. Most feeders have adjustments to allow you to feed papers of varied sizes.
- **Duplexing assembly:** The duplexing assembly flips the paper over so that you can print on both sides. It is not found on all inkjet printers.
- **Carriage:** The carriage holds the print heads and gets moved into position so the print heads can eject the ink onto the proper spot on the paper.
- **Belt:** The belt moves the carriage into position so the print heads can eject the ink onto the proper spot on the paper.

Calibrate—Calibration is done to keep the page **image sharp** and accurate. This may be done on a periodic basis and when parts are replaced. The printer should be calibrated whenever a print head or ink cartridge is replaced. Each printer will have its own calibration process.

Maintenance: Clean heads, replace cartridges, calibrate, clear jams—Inkjet printers require minimal maintenance that is easily done using features available using the printer's menus or software. To determine if maintenance is needed, **test pages** specifically designed to point out flaws can be printed from the printer's menus or software.

- **Clean heads:** Printer heads can get clogged over time. Cleaning the heads can be done by selecting a menu option or through the printer's software. When initiated, the printer will run through a head cleaning process.
- **Replace cartridges:** When the ink in a cartridge has been used up, the cartridge must be replaced. A calibration should be done after replacing a cartridge.
- **Calibrate:** Calibration is done to keep the page image sharp and accurate. This may be done on a periodic basis and when parts are replaced. The printer should be calibrated whenever a print head or ink cartridge is replaced. Each printer will have its own calibration process.
- **Clear jams:** Paper may get jammed in the printer as it is fed through. It may be cleared manually by simply pulling it out. Some printers provide a way to run just the feeder, either manually by turning a wheel or by running the feed motor.

Thermal

Thermal printers use chemically treated **thermal paper** that changes color when heated. It is the **heat**, rather than ink, that transfers the image to the paper. They are **simple** and **inexpensive**. Common uses are for receipts and shipping labels. The image printed is sensitive to light and heat, so it **will fade** over time.

Feed assembly, heating element—

- **Feed assembly:** The feed assembly feeds the thermal paper through the printer.
- **Heating element:** The heating element heats specific areas of the thermal paper as it scrolls by. The heated areas darken to create the image.

Special thermal paper—Thermal paper is chemically treated paper that changes color when heated.

Maintenance: Replace paper, clean heating element, remove debris—Maintaining thermal printers is simpler than other types of printers. There are fewer moving parts and no ink.

- **Replace paper:** Thermal paper comes in rolls of various sizes. Replacing the paper is a simple matter of removing the empty roll and inserting the new roll. There is a button or wheel that can be used to feed the paper into the printer after the new roll is inserted.
- **Clean heating element:** The heating element should be cleaned periodically to ensure proper heat transfer to the paper. Isopropyl alcohol is typically used as the cleaning agent. Some printers come with a pen or pad to make it easier to access the heating element for cleaning.
- **Remove debris:** Paper fragments and dust will accumulate in the printer over time. This debris should be removed as needed. A commonly used method is to blow out the debris with compressed air.

Impact

Impact printers use a **matrix of pins** to strike an **ink ribbon** to transfer ink to the paper. The most common type is the **dot-matrix** printers. A unique feature of impact printers as compared to other printers is that they can print **multiple copies simultaneously** using carbonless or NCR (no carbon required) paper.

** Print head, ribbon, tractor feed**—

- **Print head:** The print head is a row or rectangular matrix of metal pins. The pins that strike the ink ribbon form the character to be printed.
- **Ribbon:** The ribbon holds the ink that is transferred to the paper by the print head during printing.
- **Tractor feed:** The tractor feed feeds the paper through the printer.

** Impact paper**—Impact paper is simply paper made for impact printers. It may come on a **roll** or as **fanfold** paper in single-ply, **duplicate**, or **triplicate**. Duplicate and triplicate paper transfers the image through to all copies simultaneously.

Maintenance: Replace ribbon, replace print head, replace paper—There is **little maintenance** required on impact printers. In most printers, these items can all be replaced by the user.

- **Replace ribbon:** Ribbon replacement is usually a simple task. The new ribbon should be taught, leaving no slack.

- **Replace print head:** The pins in a print head can get bent or broken. So the print head will eventually need to be replaced. The print head does get hot due to the friction or rapidly moving parts, so care must be taken to ensure it cools down before touching it. It is held in by a lever that must be released to remove the old print head.
- **Replace paper:** Paper replacement requires a bit more effort than in other types of printers. The paper has holes along the side that are placed into the tractor feed. These must be aligned so that the paper feeds properly. Also, since the paper is continuous, as opposed to separate sheets, the top of the page must be lined up properly.

Virtual

A virtual printer is a printer drive that creates a file rather than a paper copy. The file can take the form of a printer file (PRN), portable document format file (PDF), XML Paper Specification file (XPS), or image file.

Print to file—Print to file is an option in the **Windows™ print dialog**. When a file is sent to a printer, the printer driver sends instructions to the printer to control printer functions. The Windows™ print to file option **embeds** the printer instructions you would select in the print dialog in a file with a .prn extension. The .prn file can then be used to print to that model of printer, even if the application that created the original file and the printer driver are not available.

Print to PDF—A **Portable Document Format** file stores an image of a file that is identical to a printout of that file. This allows it to be shared with other people or computers to be printed **regardless of** what **operating system** and **application** created it.

Print to XPS—An **XML** Paper Specification file is a **Microsoft™** file format that, like PDF files, stores an image of a file that is identical to a printout of that file. Microsoft™ provides an **XPS Document Writer** printer driver to create XPS files. To view or print XPS files, Microsoft™ provides an **XPS Viewer**.

Print to image—Operating systems and graphics applications each have ways to **save a file** or screen capture to an image file. For example, **Windows™ 10** includes a **Snipping Tool™** that captures a screen or portion of it and save it as a **PNG**, **GIF**, **JPEG**, or **HTML** image file.

3D Printers

3D printers create three-dimensional objects from a digital file. 3D printing is also known as **additive manufacturing**. The model represented in the file is divided into horizontal **cross-sections** or slices. The bottom slice is laid down using precisely positioned **melted plastic**. Then the next slice is laid on top of it. This repeats until the full object is formed.

Plastic filament—The plastic used for 3D printing comes in the form of plastic filament. The filament is fed from spools through a heated nozzle that melts and positions the plastic. It then **cools to a solid** to form the object.

How to Prepare for Questions about Hardware and Network Troubleshooting on the CompTIA A+ Core Series 1001 Test

General Information

Over one-fourth (27%) of the CompTIA A+ Core Series 1001 test is devoted to questions about this topic, so you'll need to know the content well. In addition, *all* of these questions will relate to a scenario given in the question introduction. So, you'll need to decide what *you* would do in that situation, relying on your knowledge of proper procedures and hardware and network concepts.

Methodology (*scenario*)

Consider this situation:

"After arriving at work and logging in to your system, you start looking over the trouble tickets that are in your queue. While triaging them, you receive a phone call from Mary in accounting. She cannot log in to the system and has a meeting in 15 minutes. She is very irate that she **cannot access her files** for this meeting and is unable to finish her preparations."

What's the first thing you tell her? How do you go about troubleshooting this? Ensure that you **consider all corporate policies, procedures, and impacts** prior to implementing *any* changes to *any* system.

Identify the Problem

While there are numerous avenues that can be taken for the situation above, the onus is on you, the technician, to identify the problem. Always remember, users don't always tell you everything, especially when emotions are involved and the possibility of not being prepared for their supervisor is a looming possibility. Simply calming the user down a little can move the conversation in the right direction.

User

Be calm and ask questions to the user while attempting to **identify any changes** to the computer that might have been performed such as security patches, physical movement, etc. These can be simple to correct and have the user back online in moments. (for example, if the cleaning company physically moved the computer while cleaning, Mary's network cable might have come unattached and she is no longer physically connected to the network.). Be sure to **make a backup** of her files prior to attempting any changes on the computer itself just in case there is a larger issue and her system cannot be recovered.

Changes

Consider all the changes that could affect the user (network, computer, power issues, external connection, user account, etc.) and how those changes can be involved in the problem. As an example, let's say the Network team worked over the weekend performing an upgrade to the infrastructure (switch replacement) and neglected to plug all the cabling back into the switch (as simple as a cable falling behind the wiring channel and being missed). Mary might have been the one missed and now she cannot authenticate to the network, cannot access her files, cannot print to the network printer, and therefore cannot perform her morning functions prior to her meeting. These things happen daily and other teams can be conducting changes without regard to the effect on employees.

Logs

If Mary's system is on the network but she cannot authenticate, then there are a variety of methods that can be used to **verify and/or troubleshoot her issue remotely** (possibly faster than getting to her work space). Obtaining her computer name and opening up her **event viewer** from your workstation can give a wealth of knowledge into why she cannot authenticate. Obviously, this will not work if she is physically disconnected from the network (first thing that should be checked). By opening the *Event Viewer* or *Computer Management* on your workstation, you can choose to "Connect to Another Computer" and enter her computer name (or IP address, if known) to open her event log. From there, choose *Windows Logs* and peruse the list of log files given. Starting with the *Application*, look for any errors (noted with a red circle around an exclamation point) or a warning (noted with a yellow triangle around an exclamation point). These are indicators that something is amiss and should be investigated further.

Develop a Theory

Keep it simple. Always **question the obvious** and don't think something isn't relevant. You might think it is common sense to be plugged into the network, but the user might not know this. Using your questioning ability, develop a theory (or two) regarding what the problem might be. Another point to remember when developing your theory is that someone, somewhere has possibly run into this issue already. The Internet can be your friend or your worst enemy and the ability to decipher what you glean from **the Internet is a valuable resource**.

Test the Theory

When you have your theory developed, you need to test it. On a time-sensitive issue, or if you know 100% that the theory is valid, then you can implement it based upon corporate policies and/or procedures. In a perfect world, you would be able to replicate the issue within a testing (or laboratory) environment for verification. This isn't always the case and you should be ready to test your theory at a moment's notice.

If Theory Is Confirmed

Only **test one possible solution at a time** and only **make one change at a time**. Sounds like a lengthy process? Yes, but if you implement multiple changes in one process how do you know which one worked and which one didn't? Remember, keep it simple. If your theory is confirmed, then you can skip to the plan of action to implement your theory. If not, then it's back to testing again. No worries, proper troubleshooting is an art.

If Theory Is Not Confirmed

You've tested your theory and the problem still exists. Step back and take a look at your theory to see what other avenues are available and develop a working theory regarding the next possible solution.

Plan of Action

Always remember: **Your company's policies and procedures take precedence** and should be in the forefront prior to acting on any plan. The conclusion that you make might possibly affect the whole company, but that might also be needed depending on the breath of the issue. Does correcting the issue require downtime for the company or just a computer? Can that be scheduled around the users workday? Does it need to happen immediately? These are all questions that should be included in your plan of action.

Verify

When implemented, does your solution **fully rectify the problem** and return all systems to functionality? Does the user have **access** to all documents and functions? Is there any way to **prevent** these issues from arising again?

Document

Documentation! We can't express how **important** it is for issues to be fully documented. Everything that you have done from the moment the user contacted you to the moment the user was back online such as **indications, findings, actions, outcomes, scenarios**, etc. Your company should have a repository (also known as a *knowledge base*) to keep this information safe. It should also be possible to share among your peers in the event the same type of issue arises in the future.

Motherboards, RAM, CPUs, and Power (*scenario*)

Listed below are some of the more **common symptoms** of issues in this area. There are many different situations that can arise when these types of hardware components start failing. For example, let's say Jim from the mailroom calls the help desk and states that his computer is running slow. What are some of the **first questions** you should ask him? Starting with the specifications of his workstation might be good. If he only has 2 Gb of Random Access Memory installed and is using a memory-intensive program, then that might be a cause for his slowness.

- **Unexpected shutdowns**—These can be caused by hardware that's failing or by adding new hardware that's incompatible.

- **System lockups**—They can be caused by something freezing up the operating system, such as a bad system or application process, or by using old software or driver versions. Maxed-out RAM can also cause a lockup.
- **POST code beeps**—Errors in the *Power On Self Test* are associated with hardware components required to successfully boot the system. The cause of these could be problems with BIOS configuration or hardware.
- **Blank screen on bootup**—BIOS or CMOS battery issues can be the root of this problem. Also check video signals.
- **BIOS time and setting resets**—These indicate a problem with the BIOS CMOS battery.
- **Attempts to boot to incorrect device**—This can be caused by a problem with the boot settings within the BIOS.
- **Continuous reboots**—These could be related to BIOS problems or OS problems. Problems with a bad driver may also be responsible.
- **No power**—Power outlet or power supply issues are usually the cause of this.
- **Overheating**—Problems with the fan, heat sink, dust accumulation, or something blocking the air circulation can all cause a device to overheat.
- **Loud noise**—This can be a result of loose hardware or issues with the hard drive.
- **Intermittent device failure**—Hardware is usually responsible for this, in the form of a bad hardware installation, overheated components, hardware going bad, or hardware not fully connected to motherboard.
- **Fans spin—no power to other devices**—This can be caused by a problem with the motherboard. Also check the power supply.
- **Indicator lights**—Indicator lights can inform you of certain problems going on with computer hardware or tell if there is activity or power coming from a certain connection point. Consult the computer's documentation for more information about this.
- **Smoke**—Smoke can indicate a blown capacitor.
- **Burning smell**—Again, a bad capacitor or a burned-out hardware piece can be the culprit.
- **Proprietary crash screens**—This could be caused by faults in the OS system files.
- **Distended capacitors**—There could be a defective capacitor from manufacturer or overheating inside the case (bad fan)
- **Log entries and error messages**—Can indicate a variety of issues from improper credentials to failing hardware.

Hard Drives and RAID Arrays (*scenario*)

Clicking, grinding, whining, whirring—these are all **indications of failing hard drives**. You won't hear much from a **Solid State Drive (SSD)**, but you may on a **conventional hard disk drive** that spins at an amazing speed (5400 rpm, 7200 rpm, 10000 rpm, and beyond). Below is a small list of indications of a hard drive beginning to fail (or having failed, in some cases). **Server hard drives** are a little more difficult to detect, as they are normally in a server room with other servers. These rooms can be very noisy. A good practice for server rooms is to turn off the overhead lights and watch the hard drive indicators. If you see an amber light, troubleshoot this server a little further. There are various **software platforms** that will notify the operator (regarding servers) of the "health" of the hard drive, but nothing compares to **physically checking** periodically.

- **Read/write failure**— This indicates a dying hard drive and could happen if the read/write head crashes.
- **Slow performance**— This can indicate that a drive has already failed or that there are errors on the drive files. There may also be issues with virtual memory.
- **Loud clicking noise**— This can be caused by a mechanical failure within the drive itself.
- **Failure to boot**— This failure could be a hardware or software issue, depending on what stage the boot process gets to before it happens. Check in BIOS settings for removable devices such as USB drive. Cables and connectors can also cause the problem.
- **Drive not recognized**— Typically, this indicates a hardware issue with one of the drives. This could be a failed component, a data corruption issue, or an error in BIOS settings.
- **OS not found**— This message indicates a software issue with loading the operating system.
- **RAID not found**— This problem could be caused by issues with the RAID controller or the management software.
- **RAID stops working**— This can happen in any RAID array that does not mirror data. It is usually caused by one of the drives failing.
- **Proprietary crash screens (BSLO/pin wheel)**— This is known as the "blue screen of death." On Windows, this is a stop error, and on Apple, you will get a continuous pinwheel on the screen. This typically indicates a fatal failure, such as a CPU dying or a burned-out part.
- **S.M.A.R.T. errors**— This stands for Self Monitoring Analysis and Reporting Technology, and it includes multiple error categories known as SMART statistics. These can proactively see issues before a drive fails completely.

Video, Projector, and Display (*scenario*)

Consider this situation:

A call comes in to the help desk, the Chief Financial Officer (CFO) has started a meeting with the "C" level officers (including the Chief Executive Officer, CEO) in your company and the projector won't power on. This has happened before and will happen again. What's the next step?

Below are some of the more **common symptoms** to look for. Watch out, those projector bulbs can be hot!

- **VGA mode**— This mode is similar to Safe Mode but for display issues. The PC boots with the minimum video drivers in use, which is helpful for troubleshooting.
- **No image on screen**— This can happen if there is a cabling issue, or a connection is not seated properly.
- **Overheat shutdown**— A shutdown of this sort could be due to problems with the video card or blocked airways for ventilation.
- **Dead pixels**— This issue is typically related to the hardware, or the monitor itself. Replacement of the display is usually necessary to correct it.
- **Artifacts**— These could be caused by problems with the adapter or video drivers.
- **Incorrect color patterns**— Damaged cables or a damaged connection port on the PC may be responsible for this malfunction.
- **Dim image**— This irregularity often has something to do with brightness settings on the display or with adapter issues.
- **Flickering image**— This happens when there are damaged cables or a damaged connection port on the PC.
- **Distorted image**— The system settings on your OS may be responsible for a distorted image. The refresh rate or resolution may be at fault.
- **Distorted geometry**— This variance could be caused by display settings, video card issues, or magnetic interference.
- **Burn-in**— This is caused when images stick on the screen and become permanent parts of the display. It could be caused by stuck pixels.
- **Oversized images and icons**— If the resolution of the monitor does not match the system settings, this can be the result.

Common Mobile Devices (*scenario*)

Mobile devices are here to stay and are computers just like laptops, desktops, etc. Only difference is they are smaller, much smaller. Compact and portable, mobile devices can be much **tougher to troubleshoot** than conventional devices. Your **company policy** will dictate the level of repair you will be required to perform on these. If the device is personally owned, you might not be required to touch it.

Common Symptoms

Below are some fairly common symptoms and corresponding questions you should ask with regard to mobile devices. Ensure you have a very **clean workspace** and **sufficient lighting** prior to undertaking a major repair.

- **No display**— Was the device dropped? Does the device power on (as evidenced by the power indicator, if equipped). Is the device charged?

- **Dim display**— Verify display settings are at factory settings prior to attempting to diagnose this symptom.
- **Flickering display**— Perform a “Hard Reset” (based on the equipment manufacturer). Is the device warm to the touch? Has it been in the sun for an extended period of time?
- **Sticking keys**— Verify that no liquid or sticky food products have come in contact with the device.
- **Intermittent wireless**— Where is this occurring? It could be spotting signals based upon your distance from the tower (or antenna).
- **Battery not charging**— Is it plugged in to a proper power receptacle? Is the cable frayed or damaged any other way? Is it an original manufacturer cable or aftermarket cable?
- **Ghost cursor/pointer drift**— Is cursor drifting when you’re not controlling it? Is there another pointing device connected, like a wireless mouse? Is your mouse or trackpad dirty or physically damaged?
- **No power**— Is the battery charged? Does it work when connected to an AC power supply? Is it stuck in hibernation? Does it respond to a hard reset procedure?
- **Num lock indicator lights**— Is it a problem or a desired function by the user, trying to use the additional number keys? Some portable devices that don’t have full keyboard combine key functions. If you can’t find the *Num Lock* key, check if there’s a *FN* key that would allow engaging the *Num Lock* light.
  Is *Num Lock* enabled by default in BIOS settings?
- **No wireless connectivity**— Is the wireless network available and working with another wireless device? Is Wi-Fi enabled on the device? Is Wi-Fi network configured with the right password?
- **No Bluetooth connectivity**— Is Bluetooth enabled on the device? Is Bluetooth set to *discoverable* mode? Are the devices within range? Is the device paired with the right code? Is the Bluetooth device on and is the battery charged?
- **Cannot display to external monitor**— Is it connecting to the monitor with the cable or wirelessly? Is it a good known cable? Is the external monitor set to show the right source of signal? If it is a wireless connection, are devices paired? If they cannot pair, do devices support the same wireless casting protocols and technologies?
- **Touchscreen non-responsive**— Is the screen dry and clean? Are you using clean, dry fingers, with no gloves on the screen? Does the device react to any other hardware inputs or frozen?
- **Apps not loading**— Are there any error messages when loading the app? Are there enough free system resources to run the app? Is it the latest version of the app? Does reinstalling the app help?
- **Slow performance**— Are there many apps or processes that run at the same time? Are there enough free system resources? Does the hardware meet the system requirements of the software running?

- **Unable to decrypt email**— Is S/MIME enabled on the device? Can this email be successfully decrypted on another device?
- **Extremely short battery life**— Is the battery swollen or very hot? Is the battery old? Is the right charged being used to charge the battery? Are there many apps and processes running on the device?
- **Overheating**— Are there many apps and processes running on the device? Is there dust or debris blocking the cooling vents? Is the device in direct sunlight?
- **Frozen System**— Are there many apps and processes running on the device? Is it low on battery? Is it very hot? Does it respond to a hard reset procedure?
- **No sound from speakers**— Is the volume level set not too low and not muted? Is there a hardware *mute* switch on the device? Is it paired with a Bluetooth speaker or have headphones connected?
- **GPS not functioning**— Are you located outside a building with a clear view of the sky? Does restarting the device help? Are location services enabled in the device settings?
- **Swollen battery**— Is it an old or low quality replacement battery? Was the right charger used to charge it?

To Disassemble

Disassembling computer systems, large and small, should be a **meticulous undertaking**. **Documentation** is key. Each part has a specific purpose and can be disastrous if not placed back in its original function. The manufacturer normally has diagrams to refer to online.

- **Document and label**— It is important to document what you are doing as you are taking apart a mobile device. You should include locations of all parts, and label any pieces that you remove. These tiny parts are typically very easy to remove, but get complex and confusing when it comes to reassembling everything. You could even take pictures, if it will help you remember exactly where a part goes. When handling small screws, it is best to be on a workbench with a raised lip and part particular attention to screw sizes, as the wrong screw size could crack a display screen.
- **Organize**— Many professionals make use of organization bins to sort and store all of the various parts when disassembling a mobile device. This is another way to help keep you organized and help you remember the location of each part.
- **Refer to resources**— If you have trouble knowing exactly what to take apart, or you would just like some extra information, always feel free to consult the manufacturer’s documentation. This can be paper documentation or gleaned online from their website.
- **Tools**— Mobile devices often have their own specialized set of tools with which to work. These tools are especially important, as they are made specifically for the mobile equipment. Standard tools may not work or they may damage the delicate mobile parts.

Printers (*scenario*)

Given a scenario, you'll need to be able to troubleshoot printers. Although a lot of information is being passed digitally, printers still have their uses in offices and IT professionals need to know their way around troubleshooting and maintaining them. **Inkjet** and **laser** are the **most common** printer types in offices. Other **less common** printer types are **impact** and **thermal**. Printers can be either directly connected to a computer for local use, or shared over a network.

Common Symptoms

Below are some fairly common symptoms, corresponding **troubleshooting steps**, and **questions** you should ask with regard to printers and printing issues.

- **Streaks**— These are usually caused by ink residue. Follow the printer's cleaning procedure. This may include physical cleaning of internal parts of a printer, or a cleaning process that can be triggered by the printer's software. Try printing a test page—are there streaks, too? Sometimes streaks may be caused by the scanning part of a copier, not being a printing problem.
- **Faded prints**— Check toner or ink levels. Try replacing the cartridges with new ones, of known good quality. Check printing settings. Are there any *ink saving* settings enabled that may reduce the amount of ink or toner used?
- *Ghost images*— This may happen only on laser printers due to self-cleaning problem. Try replacing the drum.
- **Toner not fused to the paper**— This may only happen on laser printers due to a fuser problem. Try replacing the fusing roller or the fuser lamp.
- **Creased paper**— Paper gets creased due to a feeding problem. Follow the same troubleshooting steps as for a *paper jam*.
- **Paper not feeding**— Follow the same troubleshooting steps as for a *paper jam*.
- **Paper jam**— There are many reasons to frequent or sporadic paper jams. The reasons can be categorized as related to the paper or to the printer hardware. Ensure that the **paper size and weight** used are as recommended by the printer's manufacturer. Try using a new, dry pack of good quality paper. Don't load too much paper at once. Bend the stack of paper to separate sheets before loading. If the problem is not with the paper, then the **printer hardware** needs to be checked. Check to see if the printer has been maintained per the manufacturer's recommendations. Some printers have a page counter and recommendations on replacing specific internal parts to prevent paper jams. If the jams are very frequent, check for broken parts in the feeding path.
- **No connectivity**— For a printer that is **directly connected** to the computer you're using to print: is it turned on? Is it connected correctly with a good cable? Have the drivers been installed? For a printer **on a network**: follow network troubleshooting steps. Is the printer connected to the network, can it be reached by other computers on the same network? Have the drivers been installed on the computer?

- **Garbled characters on paper**— This may mean a software or connection issue. Are correct drivers installed? Is the printer connected firmly with a good cable? Is there enough RAM free on the printer?
- **Vertical lines on page**— Similar to *streaks* troubleshooting, these may be caused by toner or ink residue. Ensure that the internals are clean and the cartridge is not leaking.
- **Backed-up print queue**— Is the printer jammed or doesn't have paper or ink to print? This may be a *spooler* issue. Does restarting the printer or the printing computer clear the queue?
- **Low memory errors**— Printer has internal memory to store and manage the print jobs. Is the printing document very large, has a lot of pages, or high-resolution graphics? Try reducing the source file. Some printers may allow increasing memory by adding the hardware RAM internally.
- **Access denied**— Does the computer user have the system permissions to print? Try printing as a different user, and modify the user permissions to allow printing.
- **Printer will not print**— Check printer power, status messages, connectivity. If everything seems right, but it wouldn't print, check the *spooler* service on the printing computer. Does restarting the spooler service help? Disable the spooler to print directly to printer.
- **Color prints in wrong color**— Color printers use base colors to create shades of all other colors. Wrong color is usually due to one of the ink or toner cartridges being empty or malfunctioning. Print a test page to rule out software configuration issue. Replace the cartridges with known good ones.
- **Unable to install printer**— Are you using the correct drivers for your operating system? Consult with the printer's documentation or support website to check for current, compatible drivers.
- **Error codes**— Error codes would direct you to the issue, usually with paper, ink or toner, or memory. Troubleshoot these errors accordingly.
- **Printing blank pages**— This is usually an ink or toner quantity or quality issue. Rule out a software configuration issue by printing a test page. Check if the cartridges are not empty and not dried out due to lack of use. Replace with new, good cartridges.
- **No image on printer display**— Is the printed connected to a good power source and turned on? Try reconnecting the power. If there's still no display on the printer's LCD screen, the screen or the printer may be malfunctioning.
- **Multiple failed jobs in logs**— Are there specific errors on these jobs that can direct to the troubleshooting steps (such as toner, paper, access issues)? This may be due to *spooler* issues. Restart the *spooler* service. Try disabling *spooler* and print directly to the printer, with no queueing.

Wired and Wireless Networks (*scenario*)

Given a scenario, you will need to troubleshoot common wired and wireless network problems. Networks are in the heart of today's computing. A failure in network access has a good chance of preventing users from doing their work, or information from being accessed. It needs to be addressed effectively.

Common Symptoms

Below are some fairly common symptoms and corresponding troubleshooting steps and questions you should ask with regard to networking and connectivity issues.

Limited Connectivity

Limited connectivity is a state when a device is connected to the network, but can’t reach outside of the local network. Even some local resources may be not reachable.

For Wi-Fi networks, this is frequently caused by incorrect password. Try reconfiguring the Wi-Fi connection with the correct password.

For wired Ethernet networks, the issue is usually due to the device not getting an IP address from the DHCP server. Or if it has a static IP address that doesn’t match the router network configuration. Does the device have IP address configured manually? Is the default gateway configured correctly and matches the IP address of the router on the network? For dynamic IP addresses, does the device get an IP address assigned? Is it in valid range on the same network as the router on the network?

Unavailable Resources

Sometimes you can access some resources on the network, but not others. For example, you can print to your office printer, but can’t access the Internet. Or you can access the web pages, but not your email.

Internet

When a device can reach local resources, but not the Internet, the first thing to check is the **router** that provides the Internet access. Is the router reachable on the network with a **ping test**? Is the router connected to the Internet or is there an Internet service interruption?

Local Resources

These are issues with accessing network resources locally and troubleshooting steps and questions.

- **Shares**— File sharing service requires network access to the file server and correct sharing configuration. Is the file server accessible with a ping test? Is there an error message when trying to access the shares? Is it an authentication or access error?
- **Printers**— Is the printer connected to the network? Can it be reached by other computers on the same network? Have the correct drivers have been installed on the computer?

- **Email**— If the Internet connectivity works, but the email application doesn't, it's possibly due to misconfigured settings. Verify the email settings. Check to see if the email service has a Web interface that can be reached to verify that the service is operational.
- **No connectivity**— If you can't access a local resource, check that the server you're trying to reach is connected and working. Can you reach this resource from another computer on the network? Can you reach the network from this server or is it disconnected?
- **APIPA/link local address**— APIPA are special addresses that can be used when there's no DHCP service on the network. In most cases, if the device tries to connect to the network but gets an APIPA (169.254.x.x IP address), that means that there's no working DHCP server on the network. Is the DHCP server working and configured correctly? Is DHCP running out of available addresses? Alternatively, configure IP address, subnet mask, and default gateway manually, accordingly to your network and router addresses. On wireless networks, it may be caused by wrong Wi-Fi password. Reconfigure the network with the correct password.
- **Intermittent connectivity**— On wireless networks, this may be caused by weak signal or radio interference. Are you too far from the Wi-Fi access point? Is connectivity more stable when you're closer to the access point?
  To avoid interference, access points can change the used radio channel frequency. Try restarting the access point to allow it re-select the channel. Try manually reconfiguring the channel. On wired networks, it may mean wiring problem or intermittent power issues in the network equipment.
- **IP conflict**— This can happen when you're configuring an IP address manually, and this address already exists on the network. Configure the device to get an IP address automatically if there's a DHCP server on the network. If there's no DHCP server, configure a different address manually.
- **Slow transfer speeds**— On wireless networks, this may be caused by weak signal or radio interference. Are you too far from the Wi-Fi access point? Is transfer speed higher when you're closer to the access point? On both wireless and wired networks, number of other concurrent transfers may be causing the slowness. The network is usually shared between multiple devices that share the available bandwidth.
- **Low RF Signal**— On wireless networks, this may be caused by weak signal or radio interference. Are you too far from the Wi-Fi access point? Is connectivity more stable when you're closer to the access point? To avoid interference, access points can change the used radio channel frequency. Try restarting the access point to allow it re-select the channel. Try manually reconfiguring the channel.
- **SSID not found**— If you have previously configured a Wi-Fi network, but now the SSID is not working, you're either out of range of the access point with this network or the access point configuration has been changed and the SSID is no longer available. Reconfigure the Wi-Fi connection to an existing SSID.

How to Prepare for Questions about Mobile Devices on the CompTIA A+ Core Series 1001 Test

General Information

This topic is assessed in the CompTIA A+ Core Series test that is numbered 220-1001 and about 14% of the questions on this test concern mobile devices. That's not a huge percentage when you consider that there are five major topics covered in this test, but it's enough of an emphasis that you'll want to know the material in this study guide.

Note that in all of our CompTIA A+ Core Series study guides, the notation (*scenario*) indicates that questions about that topic will contain a description of a situation and then a question that asks you what to do about it.

Laptop Hardware Installation and Configuration (*scenario*)

You must be able to install and configure the hardware and components of a laptop in a given scenario. You should be aware of the following hardware and be comfortable replacing it.

Keyboard

The keyboard on a mobile device is smaller sized and typically has certain keys removed or in different locations than a full-sized keyboard.

Hard Drive

These come in three main types: **SSD**, **Hybrid**, and **Magnetic**.

SSD vs. hybrid vs. magnetic disk

- *SSD* uses flash memory for fastest response times possible.
- *Magnetic* is a traditional drive that spins and reads, using specialized equipment.
- *Hybrid* is a combination of both drives and typically more cost effective than a full SSD.

1.8 in vs. 2.5 in

These are the diameters of the magnetic platters inside a hard disk. SSDs do not have magnetic platters, so the dimension represents a size equivalent to a magnetic drive.

Memory

Laptop memory typically comes in the smaller **SO-DIMM** and **Micro-DIMM** form factors. SO-DIMM is Small Outline Dual In-line Memory Module. The "SO" tells you the memory module has a smaller outline (length and width) than the original **DIMM**. It is also thinner. As the name Micro-DIMM implies, its outline and thickness is even smaller than SO-DIMM.

Smart Card Reader

Many laptops come with this reader built in, which provides an authentication mechanism. External readers that connect via USB are also available.

Optical Drive

Smaller model laptops will not include an optical drive for **DVD**s or **CD**s and, instead, may use an external drive that connects via USB.

Wireless Card/Bluetooth Module

A wireless or WiFi card connects the laptop to a WiFi network. Most laptops include this card to allow for connecting to a wireless network. It can also be added directly to the motherboard. A Bluetooth module connects the laptop to a personal area network or a Bluetooth device.

Cellular Card

A cellular card connects the laptop to a cellular network (**3G**, **4G**, **LTE**). It is rare for laptops to include this card, but it can be added.

Video Card

Laptop video adapters are most often built into the motherboard or the processor, but some laptops use a separate card that connects to the motherboard. This allows for replacing or upgrading the video adapter without replacing the entire motherboard.

Mini PCIe

Mini PCI Express (PCIe) is a small form-factor for adapter cards such as wireless, Bluetooth, or SSD cards. It is smaller than the older **PCI** and **Mini PCI** cards.

Screen

The screen displays are similar to desktop displays, but they will typically be smaller. Take steps to protect these screens with cases or other equipment, as they are fragile. Laptops typically use **high-resolution LCD** screens.

DC Jack

Laptop chargers will come with an AC-DC power converter that is a part of the charger. This takes the AC power from the wall outlet and converts it to DC power that the laptop can use. This is plugged into the DC jack port on your laptop.

Battery

Lithium Ion is the most popular laptop battery in use today. It does degrade over time and will eventually need to be replaced in order to maintain a charge.

Touchpad

This is an input device found on laptops that allows you to move the cursor around on the screen with your finger(s) and click to select items, similar in function to a separate mouse on a desktop.

Plastics/Frames

Many laptops have durable plastic frames that are light to carry around. These are inexpensive to replace.

Speaker

Speakers are usually found **integrated** in the laptop. Typically, these are not of the best quality, but they do allow you to hear audio, when needed.

System Board

These boards are proprietary to the laptop make and model, and the replacement process is often a bit complex.

CPU

Laptop **Central Processing Units** are designed to consume less power and generate less heat than desktop CPUs. Since laptops often run on battery power, components are designed to limit power consumption. Due to the smaller, more tightly packed form factor of laptops, it is difficult to dissipate heat that builds up inside the laptop case. They may also integrate features with the CPU, such as the video controller.

Laptop Display Installation (*scenario*)

When working on laptop displays, you must be able to install components in a given scenario. In addition to the display itself, the full display assembly may also include a **WiFi antenna**, **webcam**, **microphone**, **inverter**, and **digitizer/touch screen**.

Types

The two types of displays that you should be familiar with are LCD (liquid crystal display) and OLED (organic light emitting diode). The vast majority of laptops use LCD displays. OLED was introduced a few years ago but is still not found on many laptops. However, with a new generation of OLED displays being introduced, you can expect to see more.

LCD

LED technology uses backlighting, where light shines through liquid crystals to create images. The light passes through color filters to create the color image. This type can be TN or IPS:

- **TN**: twisted nematic LCD; fast response times.
- **IPS**: in-plane switching LCD; good for mobile devices, but more expensive.

LCD technology can feature either CCFL or LED backlighting:

- **CCFL**: cold cathode fluorescent lamps: older technology; needs more power than backlighting.
- **LED**: brighter and more energy efficient than CCFL.

OLED

As the name implies, organic light emitting diodes *do* emit light, so no backlighting is needed. When the element is off, it is completely black, whereas LCD elements cannot be completely black. OLED displays look sharper than the LCD.

WiFi Antenna Connector/Placement

It is important that antenna wiring be placed **as high as possible** to get the best signal from within your laptop case. Typically, these wires wrap around the outside edges of your display. This is also done to get the best signal possible.

Webcam

Most laptops include a webcam that allows you to record **audio** and **video**. This is usually integrated into the top area, around your display.

Microphone

There is also a microphone built into most laptops that allows you to record sound. This can be found in numerous locations, with some being a part of the display and others found along the edges of your keyboard.

Inverter

An inverter is used with older display technology using **CCFL** (cold cathode fluorescent) lamps. CCFL runs on AC power. This allows the DC power of the laptop to be converted into the AC power needed for these display types.

Digitizer/Touch Screen

This technology enables you to write directly on the display screen. You can also **emulate mouse and touchpad actions** such as click, drag, and touchpad gestures directly on the screen. This can be found mostly in devices that can act as a hybrid laptop-tablet device.

Laptop Features (*scenario*)

There are many features on a laptop that are not found on desktop computers. You must know how to use appropriate features of the laptop in a given scenario. This section covers those, as well as some features shared with desktops.

Special Function Keys

There are several special keys related to a laptop. For example, there is one to quickly turn your wireless adapter on or off and one to adjust screen brightness. Other special functions that you should be aware of for this exam include: dual displays, cellular (on/off), volume settings, Bluetooth (on/off), keyboard backlight, touchpad (on/off), screen orientation, media options (fast forward/rewind), GPS (on/off), and Airplane mode.

Dual Displays

Most of today's laptops have an external display connector, such as an **HDMI** connector. The dual display function key is used to select which display (laptop/external/both) to send the image to.

Wireless

The wireless function key toggles on/off the WiFi connection.

Cellular

The cellular function key toggles on/off the cellular connection.

Volume Settings

Most laptops have two function keys for volume, one for volume down and one for volume up. Some have a separate **mute** function key.

Screen Brightness

Most laptops have two function keys for brightness, one for dimmer and one brighter.

Bluetooth

The Bluetooth function key toggles on/off the Bluetooth connection.

Keyboard Backlight

Some keyboards include a backlight. The keyboard backlight function key toggles it on/off.

Touchpad

The touchpad function key toggles the touchpad on/off.

Screen Orientation

Many laptops have the option of viewing the screen in landscape or portrait mode. The screen orientation key selects the orientation of the screen.

Media options

Media function keys are used to **control audio and video playback**. They vary from one laptop to the next, but typically include play/pause, fast forward, and rewind keys.

GPS

The GPS function key toggles the GPS location service on/off.

Airplane Mode

The Airplane mode function key toggles WiFi, Bluetooth, and cellular on/off, simultaneously.

Docking Station

This is a device to which you can connect a laptop. It will handle the external functions needed, like displays, power, and USB ports. It is normally seen in a **business environment** setup. All of your connections are plugged into the docking station. To access it, slide the laptop down on the docking connectors. It effectively turns your laptop into a desktop with external display, external keyboard, external mouse, Ethernet LAN, USB devices, and power supply all connected by just sliding your laptop into the docking station. It may also add functionality with adapter cards.

Port Replicator

A port replicator is similar to a docking station, but more limited. It is typically smaller and does not have a power supply or slots for adapter cards. It just provides a way to connect an external display, keyboard, and mouse with one connection.

Locks

To protect your laptop from theft, you can use a **physical laptop lock** and **cable lock**. One end of the cable lock loops around a fixed object such as part of a desk that the loop cannot be slipped off of. The other end plugs into a security slot in the laptop and locks with a combination or key.

Many other physical laptop locks may be used for laptops that do not have a security slot. These typically hook around the laptop where the keyboard meets the display and are tied to a fixed object with a cable lock, as previously described.

Special Screens

Some laptops have rotating and/or removable screens. These screen types allow you to turn your laptop into a tablet-like device. When locked into position, you will be able to use the laptop as if it were a tablet, including the use of a touch screen and stylus pen.

Other Mobile Device Features

Various types of mobile devices other than laptops are gaining in popularity. Each has its own set of characteristics that you must be able to compare and contrast.

Tablets

This is a popular touch-screen device, usually 7 to 10 inches diagonally in size, that usually runs an Android or Apple operating system.

Smartphones

A smartphone is a cell phone that offers advanced communication abilities, such as e-mail, video messaging, and document viewing. They provide WiFi connectivity in addition to cellular.

Wearable Technology Devices

You should be familiar with the types of technology devices that can be worn, such as smart watches, fitness monitors, and headsets.

Smart Watches

These watches are typically connected to your smart phone and provide similar communication abilities, such as text messaging or phone calls.

Fitness Monitors

This device is able to calculate certain fitness information for you, such as your heart rate, distance traveled, or steps taken.

VR/AR Headsets

Virtual reality (VR) and **augmented reality** (AR) headsets allow the user to see and interact with different surroundings. A virtual reality headset completely blocks the user's view of his or her actual surroundings and replaces it with what is on the screen in the headset. The user can interact with the virtual reality they are viewing and hearing in a number of ways with various input devices. Input devices range from simple game-controller-type devices to sensor-embedded suits and multi-directional treadmills.

Augmented reality allows the user to interact with the real world, but with objects or information added to their view, through either a headset, tablet, or smartphone. For example, information can be added about a street you are walking down or a building you are looking at.

E-readers

These devices provide you the ability to read **e-books**, or books in electronic format. Reading material can be downloaded directly to the e-reader and you may start reading instantly.

GPS

These are small devices used solely to provide GPS functionality. They can typically be used anytime you want navigation ability to a destination, or want to look at surrounding places in a certain area.

Mobile Device Accessories and Ports (*scenario*)

You must be familiar with the different connection types and the accessories or devices that use them. You should be able to connect accessories to the appropriate ports of other mobile devices and configure them to work correctly in a given scenario.

Connection Types

Connection types are either wired or wireless.

Wired

You should know these wired connection types before you take the CompTIA A+ Core Series exam.

Micro-USB/Mini-USB/USB-C— Mini-USB, micro-USB, and USB-C connect to smaller mobile devices, such as cell phones or tablets. They can be used for **data transfer** and/or **charging the battery**. Mini-USB and micro-USB have a top and bottom, so they must be inserted in a specific way, while USB-C can be inserted either way.

Lightning— proprietary connector for **Apple devices**; more durable and simpler than USB standard.

Tethering— Tethering uses your phone’s cellular network to provide service to another device.

Proprietary vendor-specific ports— Apple uses a proprietary communication/power connection, known as Lightning. This allows faster charging, and the connector can be inserted in any way, unlike older USB connectors, which have a top and a bottom.

Wireless

You should know these wireless connection types before you take the CompTIA A+ exam.

NFC— short-range technology; speeds of 106, 212, or 424 kbps; distance around 10 centimeters.

Bluetooth— **Class 1** is for industrial use, with a maximum distance of 100 meters. **Class 2** is for mobile use, with a maximum distance of 10 meters. **Class 3** is for special usage, with a maximum distance of 1 meter.

IR— **infrared technology**, uses up to 4 mbps; line of sight needed; maximum distance is 3 feet.

Hotspot— A mobile hotspot allows wireless connections to your phone for the purpose of tethering.

Accessories

You should be familiar with these accessories for mobile devices and be comfortable identifying them.

Headsets

These come in wired and wireless versions and allow you to use your cell phone for voice calls or audio. The advantage is that you can be **hands-free** when using a headset.

Speakers

Speakers are often wireless and are used for playing sound while on a mobile device. They are usually powered by batteries.

Game Pads

These are often wireless and allow you to play games on your mobile device by using a separate, dedicated controller.

Extra Battery Packs/Battery Chargers

Extra batteries allow you to keep power on your phone throughout the day, even when there is no charger accessible. Mobile battery chargers allow you to **pre-charge** a small device, then connect it to your phone later as a mobile charging source.

Protective Covers

Protective covers typically stick on the display of your screen to avoid scratching. You can also use cases that cover your entire phone to help prevent further damage, such as cracks or water damage. Some covers provide water resistance while other provide waterproofing

Credit Card Readers

These readers can connect to the audio port on your mobile device and allow you to accept credit cards through the reader in real time.

Memory

This is a common feature found on most Android devices. It allows you to add an extra memory card to increase the storage space of your device. Memory cards come in different physical form factors and sizes. **MicroSD memory** is used in smartphones and other mobile devices.

Mobile Device Connectivity and Applications (*scenario*)

You must be able to connect mobile devices to a network and configure applications supporting the connection in a given scenario.

Wireless/Cellular Data Network

Mobile devices have become a common link to the rest of the world. You must know how to enable and disable network services, explain how tethering sets up hotspots to share data and connections, and understand Airplane mode when traveling.

Hotspot

A mobile hotspot allows wireless connections to your phone for the purpose of tethering.

Tethering

Tethering uses your phone’s cellular network to provide service to another device.

Airplane Mode

The Airplane mode function key toggles WiFi, Bluetooth, and cellular on/off, simultaneously.

Bluetooth

When enabled on a mobile device, a Bluetooth connection allows you to create your own personal area network having a range of approximately 10 meters. To use Bluetooth, both devices must be within range and must be paired by entering the correct pin code. Understand how to enable Bluetooth, set up **pairing**, and **locate** other Bluetooth devices.

Enable Bluetooth

Mobile devices typically have a Bluetooth item within the Settings menu. From there, you can enable Bluetooth. Most device also have shortcuts to enable Bluetooth, but they vary from device to device.

Enable Pairing

The Bluetooth item in the Settings menu is also where you will enable pairing. Depending on the device, you enable pairing by selecting **Scan for devices**, **add a Bluetooth device**, or **air**. The accessory you are trying to pair should be in discoverable mode. Each accessory has its own method of enabling discoverable mode, so you will have to read the instructions.

Find a Device for Pairing

When pairing is enabled, the Bluetooth setting screen shows list of devices that are in discoverable mode. Select the device to pair.

Pin Code

Some accessories require that a pin code be entered to pair with it. Each accessory has its own method of discovering the pin code, so you must read the instructions. At a point during the pairing process, you will have to enter the appropriate pin code.

Test Connectivity

When paired, you can test connectivity simply by using the accessory as intended to see if it works.

Corporate and ISP E-mail Configuration

You need to understand the difference between a corporate e-mail server using Exchange and an e-mail server provided by a local ISP, as well as how to make basic configurations to connect to each. Review the functions POP3 (port 110) and IMAP (port 143) protocols provided when retrieving e-mail and the use of SSL and S/MIME in providing security.

POP3

Post Office Protocol 3 (POP3) is a protocol used to receive mail from a mail server. Messages are deleted from the server by default after being retrieved from the server. This is a problem if you use multiple devices to receive mail. Most POP3 implementations allow you to change this default behavior. The standard port for POP3 is 110.

IMAP

Internet Message Access Protocol (IMAP) is another protocol used to receive mail. It allows more control of the e-mail server with options to save messages, create folders, and organize messages. The standard port for IMAP is 143.

Port and SSL Settings

In configuring the client/server connection, you must configure the ports and security settings. Most e-mail servers use the standard ports. Connection security is set by selecting the SSL type.

S/MIME

Secure Multipurpose Internet Mail Extensions (S/MIME) provides a means to send encrypted and digitally signed e-mail. This is done in corporate environments.

Commercial Provider

Mobile devices include integration with other e-mail services such as *iCloud*, *Yahoo*, or *Google*. Yahoo Mail supports POP3 and IMAP, as does *Outlook.com* and *Google Gmail*. *Apple iCloud* only supports IMAP. The integrated commercial provider e-mail configuration to use these services varies based on the specific provider.

iCloud

E-mail is one component of iCloud, so when you sign in to iCloud using your *Apple ID*, you can configure e-mail there. In most cases, the default settings will work, so you may not have to do any manual configuration. It is, of course, the default mail app in iPhones.

Google/Inbox

As was the case with Apple and iCloud, Google makes it easy to configure Google mail, or Gmail. When you sign in to your Google account, the default settings should work without additional configuration. If not, you can manually configure it. Gmail is the default e-mail app on **Android** devices.

Note: Since the exam objectives were written, Google shut down Inbox. It is not yet known how that will impact the exam.

Exchange Online

Known better as *Outlook* or outlook.com, formerly *Hotmail*, it is the default mail app on *Windows* devices. A *wizard* is provided to guide you through configuration.

Yahoo

Unlike the others, Yahoo is not the default mail app on any mobile device. However, there is a Yahoo Mail app for just about any device. The app setup will walk you through the configuration.

Updates

PRI (Product Release Instruction) has the settings for device configurations specific to the cell network to which you are currently connected. **PRL** (Preferred Roaming List) refers to which cell towers to use while in roaming mode. Both are typically updated when the operating system of the mobile device is updated. Certain carriers support updating the PRL by dialing a certain sequence of numbers. The baseband operating system on a mobile device is needed to communicate with the radio hardware, which is similar to the hardware abstraction layer in Windows occasionally required updating.

Radio Firmware

The baseband operating system is the interface between the mobile phone and the radio and is often referred to as radio firmware.

IMEI vs. IMSI

IMEI is the International Mobile Equipment Identifier, a 15-digit number that uniquely identifies a mobile device, similar to a **MAC** address on a **NIC** (Network Interface Card). If a device is lost or stolen, this allows it to be deactivated. *IMSI* is the International Mobile Subscriber Identity, a 15-digit number that describes the user and the network.

VPN

VPN is a Virtual Private Network setup using a public network, providing security on an otherwise insecure network.

Mobile Device Synchronization (*scenario*)

Push synchronization automatically syncs data between mobile devices and desktop devices. An example is when entries made on your *desktop calendar* or *contact list* are automatically synchronized with your mobile device. You must be able to synchronize mobile devices using various methods in a given scenario.

Synchronization Methods

You have the option to synchronize data to the cloud or to your desktop. **IOS** devices allow you to synchronize to the desktop using *Apple iTunes* on Windows or MAC OS. **Android** synchronizes nearly everything online. If you use a **Windows Phone**, the Windows Phone app can synchronize your media. Lately, most synchronization has been moving to cloud-based systems.

To the Cloud

Android, Apple, and Windows devices all have options to synchronize data to the cloud. Android syncs to **Google Drive**, Apple to **iCloud**, and Windows to **OneDrive**.

To the Desktop

Synchronizing a mobile device to the desktop is typically initiated by simply connecting the device to the desktop USB port. That will, in most cases, open a dialog to start the sync. Synchronization can also be done through a WiFi connection.

To the Automobile

With cars now providing connectivity to cell phones, synchronizing contact data is very helpful. Music players and connections to smartphones in cars also invites synchronization of music. Bluetooth and USB connections may be used to synchronize phones and cars.

Types of Data to Synchronize

The key to the success of mobile devices is the ability to synchronize data across many varied devices. For example, new contacts added on your tablet device will automatically synchronize with your cell phone, so you are able to communicate with that contact when needed, no matter what device you are using. Similarly, adding a business meeting to your desktop calendar can synchronize with your tablet device, so that, when you are away from your desk, you still can view your schedule for planning. Other popular items to synchronize include the following: programs, e-mail, pictures, music, videos, bookmarks, documents, location data, social media data, and e-Books.

Contacts

Contacts are one of the most important types of data to synchronize.We rely on it for phone calls and e-mail messages. With many people having hundreds of contacts with frequent additions, updates, and deletions, it would be quite cumbersome to make changes on our phones, desktops, laptops, tablets, and even our cars. Synchronizing contacts between these devices saves a lot of time and trouble.

Applications

Synchronizing application data is more common in **commercial applications**. When a device and server need to share data but may not always be connected, synchronization keeps the data alike in both places. Delivery applications in which a driver is updating tracking information on a package is one example.

E-mail

E-mail is probably on the top of most people's list of essential applications. Viewing your e-mail on your laptop and then having it available on your phone when you are on the road is a great feature of e-mail synchronization.

Pictures

People fear losing pictures, as some can never be replaced. Synchronizing pictures provides the added advantage of serving as a quick, if temporary, backup of pictures. It also allows you to show off pictures on your phone, while being able to view it in higher resolution on your desktop.

Music

Synchronizing music files allows them to be played wherever you are on whichever device works best at the time. Music files tend to be quite large, so you need to be selective to avoid running out of memory on any given device.

Videos

Similar to music, synchronization allows you to view videos on whatever device best serves you at the moment. The same memory concern applies here as it does for music.

Calendar

Creating a calendar on a desktop and then being able to access and update it on your phone when out on the road is one of the best synchronization features.

Bookmarks

Most browsers allow you to automatically synchronize bookmarks between devices, so that you have the same bookmarks available on all of your devices.

Documents

Synchronization to the cloud is commonly used to synchronize documents. It allows you to start working on a document on your desktop at work and then continue working on it on your phone on your train commute home.

Location Data

Synchronizing location data is useful for applications like tracking packages or even tracking a runner for safety or "cheering" purposes.

Social Media Data

Being able to post to multiple accounts at once is possible through synchronization. This is especially for companies that use various social media as part of their business strategy.

E-books

The ability to start reading an e-book on a desktop and then continuing where you left off on your e-reader is a very handy use of synchronization.

Passwords

Passwords may be synchronized when using a **password manager**. This allows you to access your encrypted passwords from whichever device you are using. If you change or add a password on one device, that change will be effective on the other devices as well. Passwords stored in browsers may also be synchronized.

Mutual authentication

SSO (Single Sign On) is a feature used by Microsoft, Google, and Apple to allow a single login to provide access for multiple services.

Software Requirements

Synchronizing between devices with different operating systems, such as Android, iPhone, and a Windows PC may require specific software. You need to understand the specific software requirements to install an application on the PC.

Connection Types

You need to know how to enable synchronization **to the cloud** as well as **to the desktop**. The various connection types you can use between devices include: USB, Bluetooth, WIFI, or utilizing cloud storage as a two-step process. Copy from mobile device to cloud storage, then from cloud to desktop.

How to Prepare for Questions about Networking on the CompTIA A+ Core Series 1001 Test

General Information

There are five major topics covered on the 220-1001 CompTIA A+ Core Series exam, *Networking* is one of them, and about **20% of the questions** cover networking concepts and procedures. If you see the notation (*scenario*) beside a heading below, it means that questions regarding the information in that section will begin with a situation or "**scenario**" and conclude by asking you for a recommended action or further knowledge about it.

Ports, Protocols, and Purposes

For this exam, you should know the following TCP/UDP port numbers, the protocols that run over those ports, and the primary use for each.

Ports and Protocols

Port numbers are used to **distinguish different protocols and services** that run over a network.

21 – FTP—**File Transfer Protocol**; used to **transfer files** to and from a server

22 – SSH—**Secure Shell**; used to access remote devices with added **encryption**

23 – Telnet—used to access remote devices with **no encryption**

25 – SMTP—**Simple Mail Transfer Protocol**; used for sending **email**

53 – DNS—**Domain Name System**; translates **domain names to IP addresse**

80 – HTTP—**Hypertext Transfer Protocol**; standard for communication on the web, used to render pages in web browsers

110 – POP3—**Post Office Protocol 3**; used for receiving **email**

143 – IMAP—**Internet Message Access Protocol**; used for receiving **email**.

443 – HTTPS—**Secure Hypertext Transfer Protocol**; **secured communication** on the web

3389 – RDP—**Remote Desktop Protocol**; used to connect to remote computers

137-139 – NetBIOS/NetBT—**Network Basic Input Output System**; used for **LAN** communication

445 – SMB/CIFS—**Server Message Block/Common Internet File System**; used for **shared access** on a network

427 – SLP—**Service Location Protocol**; used for **local service discovery**

548 – AFP—**Apple Filing Protocol**; used for **Apple file services**

67/68 – DHCP—**Dynamic Host Configuration Protocol**; used to assign **IP addresses** to network hosts

389 – LDAP—**Lightweight Directory Access Protocol**; used to **access a directory** on network objects

161/162 – SNMP—**Simple Network Management Protocol**; used to send and receive **network management messages**

TCP vs. UDP

Transmission Control Protocol (TCP) is a connection-oriented protocol used to **send and receive data** over a network. Before data is sent, a connection is established with the receiving host. It is considered a **reliable protocol** because the receiving host acknowledges that it received the data. TCP is used in cases where receiving the **proper data is more important than speed**.

User Datagram Protocol (UDP) is a **connectionless protocol**. Data is sent without any assurance that the receiving host is actually receiving the data. For that reason, it is considered an **unreliable protocol**. The advantage of UDP over TCP is that it is **faster**.

Hardware Devices

For this exam, you should understand the basic purpose of network hardware devices and the similarities and differences between them.

Routers

These are **Layer 3** (network layer) devices that **determine the best route** for traffic between networks.

Switches

Switches are **Layer 2** (data link layer) devices that **interconnect hosts** on a local area network using the MAC address of each host to make decisions about forwarding traffic.

Managed

Managed switches are **configurable** and have features that allow a network administrator to **optimize and customize** the switch. They typically have better monitoring options than unmanaged switches.

Unmanaged

Unmanaged switches are **not configurable**, sometimes referred to as **plug-and-play**. Since they cannot be configured, they are designed to allow hosts to connect automatically when plugged into the switch, but that can come at the expense of performance.

Access Points

An access point is technically any device to which a host can connect in order to access a network. So, while an access point may be a switch, the term usually refers to a wireless access point that **allows WiFi devices to connect to the network**.

Cloud-Based Network Controller

This is a network appliance that acts as a **management console** for multiple network access points. It also allows connection of access points to the network without configuring each one individually.

Firewall

This security appliance filters traffic, **permitting or blocking traffic** through it based on a configured set of rules and inspection of network traffic.

Network Interface Card

This is an adapter card used to **connect a host to the network**.

Other Devices

Repeater— a device used to **extend a signal** being sent to provide additional coverage

Hub— an older technology **Layer 1** (physical layer) device that simply **connects hosts** together. Hubs have **no intelligence** and do not recognize MAC addresses, so they just send traffic coming in on one port out on every other port

Cable/DSL Modem— a device used to **connect to an Internet Service Provider (ISP)**

Bridge— a **Layer 2** (data link layer) device that **connects two network segments** and controls traffic moving between them

Patch Panel— a physical panel with multiple connection points used as a central location to **interconnect devices and ports** on a network. This allows for an organized cabling structure to manage dozens or hundreds of interconnections.

Power over Ethernet (PoE)— a technology, usually incorporated into switches, that delivers **power to devices over data lines** (Ethernet) rather than having a separate power cord

- **Injectors:** A PoE injector is used to **add power** to a data cable going to a PoE device like an IP phone or IP camera.
- **Switch:** A PoE switch is a network switch that **supplies power** to its Ethernet ports to power PoE devices.

Ethernet over Power (EoP)— a technology that uses **standard electrical wiring** to interconnect Ethernet devices

Network Installation and Configuration (*scenario*)

You should be able to install and configure **small-office/home-office (SOHO)** network using wired and wireless devices in a given scenario.

Router/Switch Functionality

Routers and switches **provide connectivity** and **control traffic** on the network. **Switches** are **Layer 2** (data link layer) devices that endpoint devices connect to. **Routers** are **Layer 3** (network layer) devices that interconnect different networks.

In a SOHO network, there is typically one router provided by the Internet Service Provider (ISP) that connects the local area network to the Internet. SOH routers often have other integrated features, such as a **cable modem** or **DSL modem**, **switch ports**, and/or a **wireless access point**.

The switch, whether integrated into the router or as a separate device, is what the local computers and other devices connect to via physical Ethernet ports on the switch. The switch interconnects devices on the local area network.

Access Point Settings

The wireless access point built into the router requires some configuration. At a minimum, you should configure the **Service Set Identifier (SSID)**, **encryption method**, and pre-shared key (also called **WiFi password**).

IP Addressing

The router is configured with default IP address settings that get you up and running quickly. In most cases, you can leave the settings at the default values. The router's DHCP feature assigns IP addresses to devices when they connect to the network. Again, the default settings will work in most cases, but you can **change DHCP settings** or turn it off altogether.

NIC Configuration

Computer connect to the network through a **network interface card (NIC)**. It is here that you configure the IP address of the computer. If you enable DHCP, the NIC will get assigned an IP address by the DHCP server that is typically integrated into the router. Otherwise, you can manually configure the IP address, subnet mask, and default gateway.

Wired

For NICs that **connect via an Ethernet cable** to the router, they will get the configuration from DHCP, unless you disable DHCP. Then you need to manually configure the IP address, subnet mask, and default gateway.

Wireless

For wireless NICs, it is the same as wired, plus you need to configure it to **connect to the wireless access point**. The settings for that include the SSID, encryption method, and pre-shared key or WiFi password.

End-User Device Configuration

Other types of end-user devices, such as smartphones and tablets, typically use WiFi to connect to the network. So, the configuration is the same as you would do for a wireless NIC. You need to configure it to connect to the wireless access point by setting the SSID, encryption method, and pre-shared key or WiFi password. Then you will get an IP address from DHCP or you need to manually configure the IP address, subnet mask, and default gateway.

IoT Device Configuration

Internet of Things (IoT) devices are essentially **anything that connects to the Internet**. Some examples are:

- Thermostats
- Light switches
- Security cameras
- Door locks
- Voice-enabled, smart speaker/digital assistant

They connect via WiFi, so the configuration settings are the same as an end-user device. However, the way you access those settings will be different. Depending on the device, it may be a **control panel** on the device or it may be done using a **mobile app**.

Cable/DSL Modem Configuration

A cable modem or **digital subscriber line (DSL)** modem connects your premises to the Internet. More specifically, it **connects you to you Internet Service Provider (ISP)**. So, the basic configuration will typically be done by the ISP, either remotely or by an onsite technician. The physical connection depends upon which type of service you have.

A DSL modem connects to a traditional copper wire **Plain Old Telephone System (POTS)** line. POTS is also referred to as the **Public Switched Telephone Network (PSTN)**. It uses an RJ-11 connector to **connect to a standard phone jack**. A cable modem is **connected to a cable TV** line using **coaxial cable**.

Firewall Settings

A firewall **protects your network** by blocking traffic that may be used for malicious purposes. Most SOHO networks do not run servers that need to be accessed from the Internet, so any traffic would be initiated from inside the network. That means the firewall can be configured to simply deny any traffic initiated from the Internet. That is the default configuration for many firewalls, especially those integrated into a router. While that will work in most situations, there are a few settings that may need to be configured, as described below.

DMZ

A **demilitarized zone** is a separate network behind your firewall where you place hosts that may be accessed from the Internet, such as a web server. First, you configure the network by assigning the IP address range for the network. Then, you specify which IP addresses are allowed to access which hosts on the DMZ. Lastly, you can specify which services or ports may be used.

Port Forwarding

Port forwarding is another way to allow access to your network from the Internet. It is similar to a DMZ but **allows traffic to a single host**. You specify the host and the port allowed to access it.

NAT

Network Address Translation is used to **translate** all of your network's **internal IP addresses** to a single external IP address that will be used on the Internet. The ISP assigns this address, and it is configured on the router by the ISP.

UPnP

Universal Plug and Play is an **alternative to manually configuring** port forwarding. If enabled, UPnP allows devices inside your network to automatically allow access from the Internet by opening access through the router to that device on a specified port.

Whitelist/Blacklist

Content filtering is a feature of routers and firewalls that **control what URLs can be accessed from your network**. There are **two methods** to use, whitelist or blacklist. Most routers use blacklist by default. That allows access to any URL except those specified on a blacklist that you configure. Conversely, whitelisting blocks all URLs by default. Only URLs that you configure in the whitelist can be accessed.

MAC Filtering

Every device that connects to the network has a **Media Access Control (MAC)** address. MAC filtering allows you to **specify which MAC addresses** are allowed to connect to your router. Anyone trying to connect with a MAC address not listed in your MAC filtering table will be denied access.

QoS

Quality of Service allows you to **prioritize** different types of **traffic** on your network. This is helpful for applications that need real-time communications, such as voice, video, and gaming. You can give these services priority over others that are less sensitive to delays, like email.

Wireless Settings

Most wireless settings on a router run well at their default settings, but there are a few that you may want to configure, as described below.

Encryption

Encryption is configured to **control communications** between the end-user device and the wireless access point. If not encrypted, all of your traffic can be read by a simple network monitoring tool. There are three types of encryption available: **Wired Equivalent Privacy (WEP)**, **WiFi Protected Access (WPA)**, and **WPA2**. WEP and WPA both have vulnerabilities that make it easy to break the encryption, so you should **set this to WPA2**. It uses the **AES** encryption algorithm.

Channels

Channels are **different frequencies** that are used for communications between the end-user device and the wireless access point. This will be selected automatically, but you can manually set it as well. It may be helpful if there are other nearby access points and you can set it to a less crowded channel.

Wireless Networking Protocols

You need to understand the different wireless networking protocols, what they have in common, and where they differ.

802.11 WiFi Specification

The WiFi specification 802.11 is part of the **IEEE 802** wireless networking standards. It is used for WiFi communications. They all use the Ethernet protocol and **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)** media access method. The main characteristics that differentiate them are their operating frequencies, theoretical maximum data speed or throughput.

802.11a—5 Ghz frequency, maximum speed of **54 Mbps**, not much in use today

802.11b—2.4 GHz frequency, maximum speed of **11 Mbps**

802.11g—2.4 GHz frequency, maximum speed of **54 Mbps**

802.11n—2.4 and 5 GHz frequencies, maximum speed of 600 Mbps. The **boost in throughput** is due to the use of multiple-input multiple-output (MIMO) technology. It transmits and receives multiple signals that can overcome interference and combine for greater throughput.

802.11ac—5 GHz frequency, maximum speed of 7 Gbps. A variation of MIMO, multi-user MIMO (MU-MIMO), provides greater throughput.

Frequencies

The two operating frequencies for WiFi are 2.4 GHz and 5 GHz. The frequency has an impact on **transmission range** and **data throughput**.

2.4Ghz—This **relatively low frequency** (compared with 5 GHz) has a greater transmission range because it passes through objects such as walls and floors better. On the negative side, **throughput is lower** and it is an **open frequency range** that other devices use. Devices like cordless phones and microwave ovens can interfere with it.

5Ghz—At this higher frequency, **throughput is faster**. On the negative side, the **transmission range is shorter**, as the signal gets attenuated by objects such as walls and floors.

Channels 1–11

Channels are different frequencies that are used for communications between the end-user device and the wireless access point. The 2.4 GHz range has 14 channels, but the top 3 cannot be used in North America, so we have 11 available channels. Devices will automatically select a channel, but if there seems to be interference, we can manually select another channel. The 5 GHz range also has channels, but there is more room in the RF spectrum at that range, so we never have to set those channels.

Other Wireless Networking Protocols

There are a number of wireless networking protocols beyond just the WiFi protocols. Each has its own purpose and characteristics.

Bluetooth—Bluetooth allows devices to communicate over short distances (10 meters) in a **Personal Area Network (PAN)**. It is typically used to **connect peripherals** such as headphones to a laptop or smartphone. It is the IEEE 802.15.1 standard.

NFC—**Near field communication** has a very short range of a few inches. It is used for **contactless communications** of devices that are right next to one another. The most common use today is for contactless payment systems.

RFID—**Radio frequency identification** uses a **radio signal** to send information from an RFID tag with identifying information. This is commonly used to streamline inventory of tracking applications.

Zigbee—Zigbee is one of two **wireless protocols** (Z-Wave being the other) focused on home automation and other Internet of Things (IoT) devices. It is a personal area network (PAN) protocol. It uses **128-bit AES encryption**. It is designed for **low power**, **low speed**, and **low cost**. It operates at **2.4 GHz** with 250 kbps throughput and **915 MHz** with 40 kbps throughput in North America. Transmission range is **10 meters**. IT supports **up to 65,000 nodes**. It is the **IEEE 802.15.4 standard**.

Z-Wave—Z-Wave is one of two **wireless protocols** (Zigbee being the other) focused on home automation and other Internet of Things (IoT) devices. It is a personal area network (PAN) protocol. It uses **128-bit AES encryption**. It is designed for **low power**, **low speed**, and **low cost**. It operates at **908 MHz** with 40 kbps and 9.6 kbps throughput in North America. Transmission range is **30 meters**. IT supports **up to 232 nodes**.

3G—3G refers to the **third generation** of cellular phone service. It was introduced in 1998. Mobile broadband and the ability to use the Internet over cellular was first introduced with 3G.

4G—4G, introduced in 2008 was a **significant throughput improvement** over 3G.

5G—5G is the **next generation of cellular technology**. The infrastructure for 5G is still being deployed. It is expected to bring much greater speeds and improved features.

LTE—**Long Term Evolution** is an enhancement to 4G, providing higher speeds and some improvements to features like voice and streaming.

Network Host Services

You need to have a working understanding of the properties and purpose of network-delivered services in a client-server environment and know how to summarize them. Know the difference between a **client application** and a **server application**. Client applications request services from a server application.

Server Roles

You are expected to have a working understanding of the following network services. A server is not necessarily a stand-alone piece of hardware. A server is usually a **process running in memory on a networked system** that **responds to requests from a remote client system**.

Web server—a web-based server that typically uses **HTTP (hypertext transfer protocol)**, or possibly **FTP (file transfer protocol)**, to respond to requests from a client

File server—the repository of **shared data files** in a client-server model

Print server—a network attached device that **manages print requests**

DHCP server—**dynamic host configuration protocol** server used to assign the necessary network parameters to hosts on a network, such as IP address and subnet information

DNS server—**domain name system** server used to resolve a domain name into an IP address

Proxy server—an intermediary device between the Internet and users; a dedicated system that **locally stores often used Internet sites**; improves response time and provides security

Mail server—an application that acts as a **message transfer agent (MTA)** to send and receive email on a network

Authentication server—an application that **provides authentication** to users attempting to log in to a network

syslog—a syslog server receives and stores syslog messages from network devices. Syslog messages indicate **events of different severities** that may be used for monitoring and troubleshooting.

Internet Appliance

An Internet appliance is a physical device on the network that is purpose-built to serve a single purpose. The most commonly used Internet appliances are **security devices**.

UTM—**Unified threat management** is an all-inclusive network security appliance that typically provides intrusion detection, anti-malware, firewall, and content filtering.

IDS—An **intrusion detection system** appliance monitors network traffic to detect and alert on the presence of malicious traffic. IT uses signatures and heuristics (analyzing traffic to determine abnormal behavior) to determine if traffic is malicious.

IPS—An **intrusion prevention system** appliance works like an IDS, but rather than just alerting on malicious traffic, it will also **block** it.

End-point management server—an appliance that provides a management console that can monitor and control end-point devices. It is used to **deploy and update software** on end-points. It may also **monitor security settings and software** such as checking to see that antivirus is running and up to date on each end-point.

Legacy/Embedded Systems

Legacy systems are **older systems** that for one reason or another have not been updated. It is usually due to essential applications that will not run on the updated platform. Embedded systems are **devices other than computers** that have computer technology running within. Like legacy systems, these may not be able to stay updated.

Configuration Concepts

For this exam, you should be familiar with the properties and characteristics of several features of the TCP/IP protocol suite related to addressing on an IP network and be able to explain them.

IP Addressing

IP addresses are numbers assigned to identify devices on a TCP/IP network. There are **several types** of addresses described in this section.

Static IP address—A static address is one that is **set manually** by a user or administrator. A device that is assigned a static address will keep that address until someone changes the configuration.

Dynamic IP address—A dynamic address is one that is **automatically assigned**, typically by a router or DHCP server. The next time a device that was dynamically assigned an IP address joins the network, it may be assigned a different IP address.

APIPA—**Automatic private IP addressing** **assigns an IP address** to a device that was not assigned a static or dynamic IP address. The address will be in the 169.254.0.0 network. This is generally not useful, other than being an indication that the device failed to get an IP address through normal means. These addresses are also referred to as **link local** addresses.

Link local—Link local addresses are a **specific set of automatically assigned addresses**. In IPv4, it is the APIPA address block of the 169.254.0.0 network. In IPv6, it is the block of addresses that begin with 1111111010 (FE80). IPv6 link local addresses remain in place even after another IP address is assigned manually. IPv4 handles this differently, removing the link local address if another is assigned.

Other Concepts

There are other network configuration concepts associated with IP addressing. These impact how your network handles IP traffic.

DNS—**Domain Name System** settings are usually given out via DHCP along with IP address information, but this can be done manually as well. This allows the user (client) to resolve domain names to IP addresses in order to **perform searches or lookups**. These are usually given out in a primary and secondary fashion for redundancy purposes.

DHCP—**Dynamic Host Configuration Protocol** automatically assigns all of the settings needed to access resources on your LAN or the Internet. It can provide IP address, subnet, gateway, and DNS information. If you want to ensure that a device gets a specific IP address, you can configure a DHCP reservation in the DHCP server.

IPv4 vs. IPv6—**IPv4** is the original **32-bit** addressing scheme for IP. It allows for over 4 billion addresses. IPv4 addresses are formatted as four decimal number octets separated by periods; for example, 192.168.1.1. When it became apparent that IPv4 was running out of addresses, **IPv6** was created with **128-bit addressing**. IPv6 addresses are formatted as eight hexadecimal quartets separated by colons; for example, fe80:5e:9acd:a725:5496:aecd:2256:1b98.

Subnet mask—IPv4 addresses are divided into two sections: network and host. The subnet mask **defines which bits are part of the network** (or subnet) address.

Gateway—A gateway is a **router that connects your network to another network**, typically the Internet. When configuring a device on the network, you specify the internal IP address of the gateway as a default destination to send traffic.

VPN—A **virtual private network** is an **encrypted connection** between two networks or between a host and a network. When a host connects to a network over a VPN, it is assigned a separate IP address that is in the network's address range.

VLAN—A **virtual local area network** is a logical subnet, typically configured on a switch, that **acts as a separate subnet**. Without VLANs, every device connected to a switch would be on the same subnet. By configuring VLANs on the switch, you can have devices on that one switch in different subnets or VLANs.

NAT—**Network address translation** is used on a router to **translate an IP address** as it passes through the router. It is most often used to translate private IP address to a public address.

Connection and Network Types

For this exam, you should understand the specific networks and Internet connections listed below and understand the differences between them.

Internet Connection Types

There are a number of ways that you can connect to the Internet.

Cable—uses **coaxial lines** paired with a **cable modem** to bring in Internet service

DSL—uses existing phone lines paired with a **digital subscriber line (DSL)** modem to bring in Internet service

Dial-up—old technology that connected to the Internet over **phone lines** using **analog modems**

Fiber—uses **fiber optic lines** to connect to the Internet

Satellite—a high-latency service, useful for **remote destinations**, that connects to the Internet via satellite

ISDN—**Integrated Services Digital Network** that had been used in business communication over **T1 lines** but is being replaced with other services

Cellular—uses a mobile service provider's **cellular network** to connect to the Internet

- **Tethering**—Tethering uses your phone's cellular network to provide service to another device.
- **Mobile hotspot**—Setting up a phone or other device as a hotspot allows other devices to use the phone's cellular Internet connection. The other devices can connect to the hotspot using WiFi or by tethering the phone to the device.

Line-of-Sight Wireless Internet Service

Line-of-Sight **(LOS)** wireless Internet service, also known as **fixed wireless Internet**, uses low-power radio frequency signals to connect to a service provider's antenna. There must be a **clear path** between your antenna and the provider's antenna.

Network Types

Networks types define the general area that is covered by a network

LAN—**local area network**; typically within one site; does not traverse routers

WAN—**wide area network**; comprises multiple LANs across several sites with no geographical limitations; may be a private corporate WAN; the Internet is a WAN

PAN—**personal area network**; connects personal or IoT devices such as a smartphone to a headset; Bluetooth, Zigbee, and Z-Wave are used to form PANs

MAN—**metropolitan area network**; A type of WAN that is confined to a small region

WMN—**wireless mesh network**; allows individual wireless access points to connect in a mesh network so that any network needs only to connect as far as the next access point

Networking Tools (*scenario*)

For this exam, you should be able to evaluate a set of network requirements in a given scenario and select the best network tool for the job.

Crimper

A crimper is used to **connect a connector to a cable**. It is not usually practical to use cables of a fixed length. It is also easier to run cable without the connectors on it. So, cable is run and cut to the desired length and then the connector is crimped on using a crimper. There are **different types** of crimpers for Ethernet, coaxial, and fiber optic cables.

Cable Stripper

Cable strippers are used to **remove the insulation** from the end of a cable before the connector is crimped onto it.

Multimeter

A multimeter is a tool to **measure voltage, current, and resistance** at a minimum and sometimes has other features.

Tone Generator and Probe

These devices are used to **locate cables** in a wiring closet. The tone generator is typically placed at the user end, and a probe is waved around in the wiring closet to locate the connection. It will make a distinctive noise when it is near the correct cable.

Cable Tester

This device is used to **certify that the cable meets the standards** of the wiring code used and ensure it can be used for communication. It will identify broken wires or missing pin connections.

Loopback Plug

This tool is a special cable that is wired to **transmit and receive on a single connector**. There are loopback plugs for different types of connectors like USB or Ethernet for testing **network interface cards (NICs)**.

Punchdown Tool

Cabling within a building usually goes through patch panels or punch down blocks that serve as a central location, often in a room called a wiring closet, for all cabling. A punchdown tool is used to **connect the cables** to the patch panel or punch down block.

WiFi Analyzer

A WiFi analyzer is used to **design, optimize, or troubleshoot** a WiFi network. This device is used to show strong and weak spots in wireless coverage. It is a way to visualize WiFi network coverage.

How to Prepare for Questions About Virtualization and Cloud Computing on the CompTIA A+ Core Series 1001 Test

General Information

The previous edition of the CompTIA A+ test only considered these topics within other concept areas in sort of a cursory manner. The current test, however, devotes **a whole section** of its content outline to virtualization and cloud computing, so they have definitely become more important in today's computing environment. About **12%** of the questions on the 1001 test assess your knowledge and skills in these two areas. The questions about virtualization will be presented based on a given "scenario."

Cloud Computing

For this exam, it is important to understand cloud computing and the different types of cloud computing offerings that exist. Before cloud computing, **scalability** was difficult, as users were always restricted by their local resources. A common example of cloud computing includes online **file storage**. Online file storage allows users to store documents, photos, and videos "in the cloud" without needing to take up storage on their local hard drive. However, cloud computing covers far more than just file storage. It's now possible to move **an entire organization's infrastructure** (everything from servers to networking equipment) to the cloud.

Cloud Models

As mentioned in the previous section, cloud computing encompasses many different aspects of computing. We call these aspects *cloud models*. For this exam, you will need to know the three most common types of cloud models: IaaS, SaaS, and PaaS.

IaaS

Infrastructure-as-a-Service (IaaS) can be thought of as a **virtual data center**. As its name suggests, Infrastructure-as-a-Service (IaaS) providers allow clients to build their entire infrastructure in the cloud. Infrastructure includes items such as servers, firewalls, routers, and switches. In an IaaS environment, **clients are entirely responsible** for managing, maintaining, and patching operating systems and applications. Examples of IaaS providers include DigitalOcean® and Rackspace®.

SaaS

In recent years, there has been a major shift from locally installed software to Web-based software. Software-as-a-Service (SaaS) has become a popular choice for organizations because it allows them to access their programs anywhere an Internet connection is available. SaaS can be described as any program that is **accessed via the Web** and **not locally installed**. Examples of SaaS providers include Google Apps® and Dropbox®.

PaaS

Platform-as-a-Service (PaaS) provides a **platform for developers to build their own applications**. PaaS providers will handle everything on the back-end, including servers, operating systems, and development tools. This allows developers to focus on creating, building, and managing their applications. Examples of PaaS providers include Google App Engine® and AWS Elastic Beanstalk®.

Other Considerations

- **Public cloud—**When you hear people use the term *the cloud*, they are typically speaking of the public cloud. The public cloud refers to anything that is **delivered across the open Internet**. When you interact with applications such as Dropbox®, you are accessing that program via the public cloud.
- **Community cloud—**It can be easy to get the terms *community* and *public* confused, but in a discussion about cloud technologies, they mean different things. A community cloud is **not available to everyone in the public** in the way a public cloud is, rather it should be thought of as a **shared cloud** being used by multiple organizations. Private clouds are very costly to implement and maintain, but some organizations are not comfortable using a cloud that is available to the entire public. In these scenarios, a community cloud is a great option.
- **Private cloud—**Private clouds are certainly the **most secure** cloud option, but they come at a **high price**. Private clouds give organizations flexibility while ensuring that they still have 100% ownership of their data and infrastructure.

- **Hybrid clouds—**Private, community, and public clouds can be combined to create a hybrid cloud. Hybrid clouds can be beneficial when some data need to be kept in a private cloud, but the **cost to implement** a private cloud for all of the data may be too high.

Shared Resources

A major upside to **virtualization** is that it provides **flexibility**. An example of this flexibility is *shared resources*. If there is a need for more resources, **hardware can be combined** and shared. One physical host machine with a lot of resources (memory, storage capacity) can have its resources shared among multiple virtual machines. This resource sharing can occur both **internally and externally**.

Rapid Elasticity

It's not always clear how much of a particular resource you are going to need when setting up a new environment. It's entirely possible (and quite common) for your resource needs to grow as the organization grows. An organization that started with five servers might triple their server needs in several years. Virtualization makes it possible to **quickly add new servers** as you need them without the hassle of purchasing new hardware each time. This is known as rapid elasticity.

On-Demand

Just as a company may see its need for servers to increase, they may also see it decrease. Some companies may require additional Web servers to handle traffic around Christmas time when they are the busiest. However, when traffic decreases the rest of the year, it doesn't make financial sense to keep paying for these additional resources. Virtualization can provide on-demand access to resources so organizations can simply **pay for the resources they need** as they need them.

Resource Pooling

Resource pooling is the concept of combining the resources of physical servers and making them available in a *pool*. When this is done on a large scale (imagine Amazon®) it allows customers to use and **pay for only the resources they need** from the pool at a given time.

Measured Service

When purchasing services from a cloud provider, you may be billed based on measurements such as **Web traffic** or **uptime**. This type of billing process is known as a *measured service*.

Metered

A *metered service* differs from a *measured service* because rather than being interested in how long your Web application has been running or some other service measurement, they base the pricing off of the **amount of processing resources** you require.

Off-Site Email Applications

For many years, organizations had to have an on-premise email server to send and receive email messages. Thanks to cloud computing, this is no longer a requirement. While there are still plenty of organizations that prefer to use an on-premise solution, many organizations are not following the trend and moving their email services to the cloud. There are numerous options when it comes to off-site email applications, but one common example is Microsoft making Outlook® available in the cloud.

Cloud File Storage Services

Cloud file storage has made accessing files much easier than in the past. This is because many cloud file storage services use *synchronization apps*, which allow users to access the same version of their files on all of their **multiple devices**.

Virtual Application Streaming/Cloud-Based Applications

Having the ability to **access your applications from anywhere** you have an Internet connection has become an absolute must for most people. Virtual application streaming and cloud-based applications have made this possible. A cable provider is no longer required to watch television, as it can be streamed through a cloud streaming service like Neflix® or Hulu®.

Applications for Cell Phones/Tablets

Cloud-based applications are not just for computers; they can also be accessed on cell phones. One example of this is Spotify®. It’s not necessary to use all of your cell phone or tablet’s storage to store hundreds of songs because they can now be **streamed** directly from the cloud.

Applications for Laptops/Desktops

While many people still choose to download and install programs like Microsoft Word®, Powerpoint®, and Excel® locally on their laptop or desktop, it’s no longer required. Many applications are now available for use from the cloud in a **SaaS**-based model. The entire suite of Microsoft Office products, for example, be used entirely via the Web with Office 365®.

Virtual Desktop

Thanks to virtualization, it’s possible to have multiple virtual desktops running on one physical machine. These machines operate similar to a physical desktop, but all of the hardware is virtualized. For example, just as a physical computer needs a network interface card (NIC) to connect to a network, a virtual desktop uses a virtual NIC. The virtual NIC performs the same functions that a physical NIC, but it’s **software-based** rather than hardware-based.

Virtualization (*scenario*)

At times, it is necessary to configure a virtual machine to run on your local desktop. This process is known as *client-side virtualization*. In order to set up and configure client-side virtualization, you'll need to first **verify** that your **physical system's hardware** can meet the resource requirements needed for a virtual machine. Next, you'll need to install a **hypervisor** on your local machine. After the hypervisor is installed, you can **create a virtual machine** and **configure** the proper virtualized hardware for the guest operating system you'd like to use. After all of these steps are complete, you may **install the operating system** the same way that you install an operating system on a physical machine.

Purpose

Virtual machines are useful because they allow for the use of **multiple desktops** without the need to purchase expensive hardware for every single machine. One use for a virtual desktop is the need for multiple operating systems. Imagine a user that has a Windows® desktop, but needs to perform a specific task on a Linux® machine. Rather than needing to purchase an entirely new computer to run Linux®, the user could simply create a virtual machine on her Windows® machine that would run Linux®.

Requirements

Before being able to create a virtual machine, there are requirements to satisfy. A **hypervisor** is required in order to run a virtual machine. It's also important to ensure that the physical hardware CPU has *hardware virtualization support*. The majority of new computers today will have hardware virtualization support as both AMD and Intel added it to all of their CPUs over a decade ago.

Resource

Not all virtual machines are created equal. This is because the individual that is building the virtual machine determines what resources to provide to the virtual machine. This means determining the amount of **hard drive space** and the amount of **memory** that your local machine can afford to give the virtual machine. If your physical machine doesn't have a lot of RAM, then you will not be able to provide enough RAM for your virtual machine to run smoothly.

Emulator

It's easy to confuse the terms emulation and virtualization, but while they may go hand-in-hand, they are two different concepts. During virtualization, the virtual desktop creates a completely new simulated environment. Emulators are used to **mimic or imitate the behavior of another device**. One common use for emulators is in the **video game industry**. Gamers are able to emulate a Super Nintendo® on their computer, this allows them to play old games like Super Mario Bros® on their computer without the need for the Super Nintendo® hardware.

Security

Just as security is vital in physical computing, it's also important to think of security when working with virtual machines. This means implementing the same types of security controls on your virtual desktops as you would on your physical ones such as strong passwords, account lock out policies, and even multi-factor authentication.

Network

Virtual networking is a bit different than standard networking, and there are few options that you should be aware of.

- **Internal networking—**This function allows a VM to communicate with other VMs that you specify, but not access the Internet or any other computers on your network.
- **Bridged mode—**In bridge mode, the VM is able to communicate directly through the network to which the physical machine is connected.
- **NAT mode—**Having a VM network in NAT mode allows the VM to make outbound connections only.

Hypervisor

Full virtualization is not possible without the use of a *hypervisor*. A hypervisor handles all of the interactions during virtualization and makes it possible for one host to run multiple guest operating systems at the same time. VMware ESXi® and Microsoft Hyper-V® are two examples of popular hypervisors.

How to Prepare for Questions About Operating Systems on the CompTIA A+ Core Series 1002 Test

General Information

The emphasis on each of the content areas tested on the CompTIA A+ Core Series 1002 test is roughly equal, with *Operating Systems* being the subject assessed by 27% of the questions. A little over half of these questions begin with a scenario, and those concept areas are indicated below by (*scenario*) notation.

Operating System Types

An operating system controls and coordinates all the elements of a computer. It controls many functions that are necessary to use the computer, such as **hardware management**, **file system**, and **user interface**.

The **workstation operating systems** in the scope of the exam are:

- Windows

- MacOS
- Linux

Cell phones and other mobile devices also have **operating systems**. The scope of the exam is:

- Windows
- Android
- iOS
- Chrome OS

32-bit vs. 64-bit

Operating systems need to manage the hardware, and there are different operating system versions for different hardware. One important difference is **CPU architecture** that differs in *bits*. Historically, there were **8-bit** and **16-bit** computers. Currently, **32-bit** and **64-bit** computers are widely used.

The bit length refers to the number of bits that is used for **memory** addresses. For instance, 64-bit computers use 64 bits for memory address.

RAM Limitations

Computer architectures with different numbers of bits can support different amounts of memory. For instance, when using 32 bits for memory addresses, the highest number would be:

1111 1111 1111 1111 1111 1111 1111 1111 = 4,294,967,295

That means that the maximum size of memory a 32-bit computer can use is 4 **gigabytes**.

With 64 bits, the highest address in memory would be 18,446,744,073,709,551,616, and the maximum size of memory this architecture can use is 16 **exabytes**. This number is way beyond memory addressing needs for the foreseeable future. In practice, the most memory supported by a Windows workstation operating system is 2 **terabytes**.

Software Compatibility

Most operating systems will have a 32 and 64-bit version. The 32-bit version may be referred to as *x86*, and the 64-bit version as *x64*. In most cases, the hardware is **backward compatible**, meaning that you can install a 32-bit OS on 64-bit hardware, but not vice-versa.

Applications can also come in different **versions**. You will need a 64-bit OS on a 64-bit CPU to run a 64-bit application.

Workstation Operating Systems

Workstation operating systems are designed to be used on a desktop or a laptop computer by one person at a time. These operating systems provide a convenient graphical user interface (GUI) and access to files and applications on the computer.

Microsoft Windows

Microsoft Windows is the most widely used workstation operating system. It can be installed on a wide variety of compatible hardware from many manufacturers and it is commonly used in homes, schools, and offices.

Apple Macintosh OS

Apple MacOS is the operating system designed to run on Apple workstations. It is included with every Macintosh computer and is the second most widely used workstation OS.

Linux

Linux is a **kernel**, the core of the operating system. Interfaces and applications can be added to the kernel. These pre-configured combinations are known as *distributions*. This flexibility allows users to create various flavors of systems for different cases. A distribution can have an extensive **graphical user interface (GUI)**, like **Ubuntu**, or be better adapted to high performance server tasks, like **Red Hat**.

Cell Phone/Tablet Operating Systems

Phones and tablets are widely used, growing in hardware and performance, and raise the need for complex, powerful, yet convenient operating systems.

Microsoft Windows

Microsoft has discontinued its operating system for mobile phones. Tablets from different hardware manufacturers support Windows, and they run the full version of **Windows 10**.

Android

Android is an operating system developed by **Google** specifically for mobile devices. It is based on the Linux kernel and is **free and open source**. Many devices from different manufacturers around the world make phones and tablets that run the Android operating system. It is the **most used** mobile OS.

iOS

iOS is the operating system on **Apple's iPhones and iPads**. It cannot be installed on devices not manufactured by Apple.

Chrome OS

Chrome OS is not widely used on tablets, but mostly on **netbooks**. These are lightweight laptops that are intended mostly for using services over the Internet and for web browsing.

Vendor-Specific Limitations

Once an operating system is installed, it can continue running. But there are some limitations that you need to keep in mind and consider updating.

End-of-Life

When an operating system reaches the end-of-life phase by its developer, there will be no more updates, patches, or technical support. There will probably be no more applications developed or supported for this OS version.

Update Limitations

When the OS developer stops supporting the version, there will be no more security patches released for that OS version. As new vulnerabilities get discovered, this may leave the computer with an outdated operating system exposed to security risks.

Compatibility

Applications that are available for one operating system may be not available for others. The developer of the application may limit its efforts to only one operating system. Some applications may be available for MacOS and Windows (for example, **Microsoft Office**). Some applications may be available for MacOS, Windows, and Linux (for example, **Google Chrome**). In any case, these are different installation files of similar software.

Another compatibility concern may be caused when updating an operating system to a newer version. **New versions** of operating systems may cause issues with previously installed hardware and applications. Many large organizations choose not to update their operating systems without thorough testing of the new version with the existing hardware and business-critical software.

Microsoft Windows

Versions

Windows 7, 8, 8.1, and 10 have many elements in common, but there are also some differences in what each provides.

Windows 7

File management—Windows Explorer is the utility to manage the files on the computer.

Libraries—Libraries showed files of a specific type in one place, even though they were stored in different locations on the computer. Default libraries are **Documents**, **Pictures**, **Videos**, and **Music**. This is the **default location for Windows Explorer** on Windows 7.

Aero—Provides visual enhancements to the desktop and GUI experience. Requires a **video card** with enough performance for full support.

Windows 8

Start screen—The *Start Menu* has been replaced with the *Start Screen*. This is a screen with tiles for installed applications and system menus.

Windows Store—This is an online store for downloading and purchasing new software.

Microsoft Accounts for sign-in—In addition to *local accounts*, a Microsoft online account can be used to login. This allows transferring appearance and system settings between computers.

Settings—The most-used user settings became available in a separate Settings menu.

Control Panel—This allows more system configuration and is still available.

Recommended multi-touch display screen—To emphasize that the operating system can be used on tablets and allow advanced **GUI interaction**, Microsoft has recommended that a multi-touch display be used with Windows 8.

Libraries—Introduced in Windows 7, libraries are still available, but not enabled by default. Instead, the folders *Documents*, *Pictures*, *Videos*, and *Music* are now normal folders that are created for each user.

Windows 8.1

Refinements—Windows 8.1 is a more refined version of Windows 8, with no fundamental changes. Most enhancements are related to the user interface, making it easier to use, especially on computers without touch displays.

Windows 10

Cortana— This is a personal assistant you can talk to by voice or typing, and get a response in text or speech. It can set reminders, calendar appointments, and answer questions using the Bing search engine.

Start menu—It combines the start menu of Windows 7 with a panel similar to the Windows 8 start screen, and doesn’t obstruct the whole screen and the desktop.

Corporate vs. Personal Needs

Microsoft Windows is the most popular workstation OS for both personal and corporate use. Although they have a very similar look and feel, the *Professional Editions* allow more efficient and secure use in corporate environments and offer additional features.

Domain Access

This allows access to the network domain. The computer will be registered on the domain and domain users can be used to log in.

BitLocker

This is a **drive encryption utility**. All data on a disk is encrypted to prevent unauthorized access, which may be especially useful on laptops that may leave the protected office environment and may be lost or stolen.

Media Center

Available on Windows 7 Home Premium, *Windows Media Center* is **a player** for slideshows, videos, and music from files, optical drives, local networks, and selected streaming services.

BranchCache

Beneficial in corporate environments with multiple branch offices, this creates a local cache of files from file servers and web servers for **quicker access**.

EFS

Standing for **Encrypting File System**, this is a file system feature that can be configured to encrypt volumes, folders, and files. This protects data from an attacker with physical access to the computer.

Desktop Styles/User Interface

Windows versions in the scope of the exam, between Windows 7 and Windows 10, provide a **similar user experience**. The important differences are Aero, Start Menu and Start Screen differences, and the Settings menu.

Windows also offers **different interfaces**: keyboard and mouse entry, touch screen, and Cortana voice recognition.

Installation and Upgrades

To start using an operating system, it needs to be installed on the computer first. To start the installation process, the computer needs to be **booted with the installation media**.

Boot Methods

A boot method allows the user to select how to boot a computer and what media to use. There are **multiple ways to boot** a computer.

Optical Disc (CD-ROM, DVD, Blu-ray)

A computer may have a **built-in drive** to read optical discs. A computer can be booted from this device with an installation disc inserted. This is a very common way to install an operating system on a computer.

External Drive/Flash Drive (USB/eSATA)

An external device may be connected to a computer from which to boot. There are many types of external devices, for example: external optical drive, external hard disk, and external flash drive.

Common interfaces used to connect the external drives are USB and eSATA. A USB flash drive is a very common way to install an operating system.

Network Boot (PXE)

Preboot eXecution Environment (PXE) allows the user to boot from network resources. The computer that boots will need to be connected to a network. The network and the remote server that hosts the bootable image need to be configured.

This is a common way to install an operating system in a corporate environment, where network and server resources are available, and it allows a user to quickly set up many computers similarly.

Internal Fixed Disk (HDD/SSD)

An internally connected hard disk may be used from which to boot. The disk may include the operating system installation image or have the operating system installed. This is the most common way to boot a computer after the operating system installation was completed.

Internal Hard Drive (Partition)

It's important to **distinguish between a hard disk and a partition**. In many simple configurations, there is one bootable partition on a disk. But one disk can have more than one partition, as it may be useful to have different operating systems on the same computer (multiboot). Also, one logical partition can span across multiple physical hard disks.

Installation Types

Depending on the current state of the computer, available hardware and environment, and desired setup, there are multiple ways to install an operating system.

Unattended installation—This requires preparation ahead of time and best suited for cases where **many computers** need to be installed with the same configuration. Requires a special server with the installation image and the installation script.

In-place upgrade—This is an installation method that **installs a newer operating system over an older one**. Depending on the OS and versions, it may preserve the settings, files, and applications.

Clean install—This installation **disregards previous data at the destination**. It can be used if the computer doesn't have any operating system installed or if the intent is to completely delete the previous operating system, files, applications, and settings.

Repair installation—Some operating systems provide this option. It is usually initiated by booting with the installation media of the same version of operating system that was previously installed, then selecting the *repair* option from the menu. It **rewrites system files**

and settings, while keeping the user files. This mode may be useful for repair purposes, if the installed operating system is not bootable, or shows serious issues that can't be fixed otherwise.

Multiboot—This method uses a **boot manager** to **install multiple operating systems** on a single computer. The boot manager maintains the boot configurations and lets the user select what operating system to boot when starting the computer. It's recommended to install separate operating systems on separate hard disks, or at least separate logical partitions.

Remote network installation—PXE network boot can use a remote server with the operating system's installation files to install the OS on the computer. Depending on the configuration of the server, the installation process may require **selecting installation options**, just like booting from a CD, or be an **unattended installation**.

Image deployment—If many computers have **identical hardware** and **need identical operating systems, settings, and applications** installed, it can be accomplished with image deployment. There are different software tools for this task, but usually the process involves the following steps:

1. Select one computer.
2. Perform a clean installation of the desired operating system, configure, and install applications.
3. Create the image from this computer.
4. Make this image available on the network or portable media.
5. Copy the image to other computers.

Recovery partition—Some operating systems provide an option to create a *recovery partition* during the installation. It will be a **bootable partition** that can later be used and **contains diagnostic and repair tools**, or may be used for a **repair installation**.

Refresh/restore—If configured beforehand, it may be possible to restore the operating system to a **restore point**. It is recommended to create a restore point before significant configuration changes and software installations. If something unexpected happens, the **settings may be reverted**.

Partitioning

Partitioning creates **one or more logical drives** on a physical disk. Each partition can be **separately formatted** and have a **separate file system**. In Windows, each partition can have a separate drive letter.

Dynamic—This is a disk with a **more complex configuration** that doesn't have the limitations of a *basic* disk. It allows creating partitions that can span multiple physical hard disks (software RAID).

Basic—This is the **most common** disk type, separated into logical partitions.

Primary—You can have **only one logical drive**. Windows can only boot from a primary partition, so at least one is required.

Extended—You can have **more than one logical drive**.

Logical—A logical drive is represented by a drive letter in Windows. Make sure you distinguish between disk, partition, and logical drive. These can be assigned one-to-one in the simplest configuration, but are not limited to one.

GPT—A **GUID Partition Table** contains information on how the disk is partitioned. Compared to MBR, it supports larger drives, and more partitions per drive.

File System Types/Formatting

The file system allows storing, managing, and accessing files on a partition. An operating system usually supports different file systems, and a partition needs to be *formatted* with a specific file system before usage.

ExFAT—This is designed for small flash and SSD drives, optimized for performance and media file storage.

FAT32—Providing very basic features, it is supported by many operating systems. Supports partitions up to 2 TB in size.

NTFS—This is much more advanced than FAT32, supported by all modern Windows versions. NTFS allows users to set and manage *permissions* for files and folders for specific users and groups, making it very useful for secure network file sharing. Additionally, it provides indexing (for faster file search), compression, and encryption on the file system level.

CDFS—This is a file system for CDs and DVDs.

NFS—This stands for Network File System, used for file access over a network between systems. Mostly used in servers, and less in workstations.

ext3, ext4—These are used by Linux. Ext4 is an updated version that supports larger partitions, a larger number of files, and improves performance.

HFS—This is used natively by MacOS.

Swap partition—Swap is a Linux partition that is used when the computer runs out of physical RAM. Data from RAM overflows to the swap partition. It reduces the performance, but allows more applications to run at once.

Quick format vs. full format—These are two ways of formatting a partition. Quick format only changes the file system records, so the disk appears empty. Full format also rewrites the previous files, making it harder to restore previous files, and may detect some surface errors on the disk.

Other Considerations

Here are some other considerations to keep in mind when installing and configuring the operating system.

Alternate Third-Party Drivers

Drivers used in Windows installations that have been tested and approved by Microsoft are referred to as **signed drivers**. When installing device drivers, signed drivers should always be used; however, you may find situations where the driver is an unsigned driver (third-party driver). Before installing an unsigned driver, verify the source to ensure that it is valid.

Workgroup vs. Domain Setup

You will need to know how to set up a workgroup and set up a system as part of a domain. A workgroup could be a small department in a larger organization, or more likely a home user. Setting up a home workgroup is an easy way to allow printer sharing and file sharing with family. Businesses would more than likely use a **domain controller** that would provide secure, centralized logins to a very large group. This centralized facility simplifies managing a large network.

Time/Date/Region/Language Settings

During the installation of the operating system, some *regional settings* can be changed. These include local time and time zone, region, and language. Most of these settings can be changed later, after the installation, but not all operating systems will allow changing the interface language without reinstalling.

Driver Installation, Software, and Windows Updates

Understand the importance of keeping your system up to date, specifically relating to **security**. Know the procedures for installing drivers, using 32-bit drivers on x86 systems and 64-bit drivers on x64 systems. Be familiar with the function of the **Device Manager** and how it relates to drivers.

Windows Updates are performed by running the **Check for updates** utility. These updates will frequently cover other installed Microsoft software, like Office, and development tools. Other software updates need to be checked for and installed separately. Windows updates can be configured to run automatically.

Factory Recovery Partition

For computers that come with a recovery partition, you are expected to know how to use this to implement a system recovery. Also understand how partitions can be hidden.

Boot Drive

For each operating system, understand the procedure for partitioning and formatting drives. Know how to determine which partition is the active partition.

Hardware Compatibility

Ensure that the system's hardware is supported to install and configure the desired operating system. The essential **BIOS**, **CPU**, and **RAM** need to support the installation. The hardware should have **supported drivers** to be used optimally by the OS.

Application Compatibility

Between 32-bit and 64-bit, and also the versions of operating systems, verify that the desired applications are compatible and will run successfully. Understand the **compatibility mode**.

OS Compatibility

To upgrade the OS version, there must be an **upgrade path**. When a new OS is released, there is a lot of effort put in to allow upgrades from previous versions. There may be some limitations that won't allow an upgrade. For instance. a 32-bit OS can't be upgraded to 64-bit. There are cases of fundamental feature changes; for instance, a new version may not support the file system used by the previous operating system. In these cases, only a clean install would allow you to use the newer operating system instead of the old one.

Microsoft Command Line Tools (*scenario*)

You are expected to have a working knowledge of basic command line tools listed below and be able to recommend their use when given a scenario.

Navigation

These commands are used to navigate the file system.

`dir` —gives a listing of a directory.

`cd` —change directory used.

`cd ..` —move one level up in the directory structure.

Other Tools

These are some other commands and command line utilities for networking, file, system, and disk management.

`ipconfig` —displays configuration of network adapters.

`ping` —tests reachability of a remote computer over the network.

`tracert` —displays what network devices a packet goes through to reach a remote computer.

`netstat` —displays network statistics on data transfers, ports, and applications.

`nslookup` —resolves name to IP address, for DNS troubleshooting.

`shutdown` —shut down or restart the computer. Allows options like delayed restart.

`dism` —Deployment Image Servicing and Management tool to mount and service Windows image files.

sfc —System File Checker tool checks the status and versions of system files.

chkdsk —will verify the file system of a volume and fix logical file system corruption.

diskpart —tool for managing disks, partitions, and volumes.

taskkill —used to kill system processes given the process ID number **PID**.

gpupdate —manually refresh the domain *group policies* applied to the computer or the user.

gpresult —displays the current *group policies* and their status.

format —create a file system on a storage device.

copy —make a copy of one or more files.

xcopy —copy command with numerous options.

robocopy —replaces **xcopy**, has numerous options.

net use —connect or map a network share.

net user —manage users.

[command name]/? —adding the */?* parameter at the end of a CLI command will display the list of command options and parameters, with their short descriptions.

Command Availability

Just like system utilities in the GUI, the CLI commands need to be run with the right privileges. Usually, displaying the information can be done with standard privileges, but changes to the system require that you run the CLI as administrator first.

Microsoft OS Features and Tools (*scenario*)

Make sure you can apply the following features and tools when given typical user scenarios. Microsoft puts all the various tools needed to manage a system on a single screen to simplify the process.

On Windows Vista, to load the administrative tools, right-click **Taskbar** and then select the **Start Menu tab > Custom > System Administrative Tools**.

On Windows 7, to load the administrative tools, click **Control Panel > System Security > Administrative Tools**. The Windows 8 and 8.1 administrative tools can be found in **Settings > Tiles > Show Administrative Tools**. Familiarize yourself with all the applications available in the administrative tools. In Windows 10, you can access the administrative tools by clicking on the Start button on the taskbar, then scrolling down your apps and clicking on Windows Administrative Tools.

Administrative

Windows comes with a set of utilities for administration.

Computer Management

Computer Management, located in **Administrative Tools**, contains a variety of tools used to manage the operating system found under the heading **System Tools**. Review the function of these tools and be familiar with: *Device Manager*, *Performance Monitor*, *Services*, *System Configuration*, *Task Scheduler*, *Print Manager*, *Memory Diagnostics*, *Windows Firewall*, and *Advanced Security*.

Device Manager

Device Manager allows you to view the status of devices, view the properties, and modify the configuration parameters.

Local Users and Groups

As a system administrator, you need to know how to create and delete users and maintain their accounts, as well as how to establish secure passwords.

Local Security Policy

This can be run by command `secpol.msc` and allows changes to local security policies, permissions, and rules.

Performance Monitor

This can be run by command `perfmon` and displays in real time how the computer uses memory, disk, CPU, and the network, to help diagnose performance issues.

Services

These can be run by command `services.msc`. They display the installed services and their status. They allow the user to configure how the services start with the computer and let you stop, start, and restart a service. Services are background processes that are used by applications and don’t have their own interfaces.

System Configuration

This can be run by command `msconfig`. It allows you to change how Windows boots and what programs start with Windows.

Task Scheduler

The task scheduler can be run by command `taskschd.msc`. It allows you to configure automated tasks that will run on a schedule, at specified times.

Component Services

These can be run by command `compexp.msc`. Components, or COM apps, is a model for apps to share components and libraries. The component services modification may be needed if you need to troubleshoot a COM or DLL error when trying to start an application.

Data Sources

These can be run by command `odbcad32.exe`. Data sources allow local applications to connect to remote databases, over the network. If the application requires the ODBC connection, that *data source* needs to be configured in Windows.

Print Management

Part of the Microsoft Management Console (MMC) that can be run by command `mmc.exe`. It allows you to view the status and manage local and network printers.

Windows Memory Diagnostics

These can be run by command `mdsched.exe` tool to test RAM for errors. It requires the user to restart the computer.

Windows Firewall

The firewall is included with all versions of Windows. Be sure you are familiar with all of the features here.

Advanced Security

Advanced Security is a more detailed way to configure the Windows Firewall. It allows you to block and allow specific applications and network ports.

Event Viewer

This can be run by command `eventvwr.msc`. It shows system, application, and security logs and error messages.

User Account Management

As a system administrator, you need to know how to create and delete users and maintain their accounts, as well as how to establish secure passwords.

MSConfig

This can be run by command `msconfig` and allows you to change how Windows boots and what programs start with Windows. The utility’s functions are presented in five tabs:

General

The *General* tab shows the mode of Windows startup.

Boot

The *Boot* tab allows configuration of multi-boot when multiple operating systems are installed, and how to boot into these operating systems, mostly for troubleshooting (safe mode).

Services

The *Services* tab allows the user to manage services for troubleshooting. A restart will be required after making a change.

Startup

In Windows 7, the *Startup* tab showed applications that started with Windows. Since Windows 8, the tab only contains a link to the *Startup* tab in the *Task Manager* utility for the same functionality.

Tools

The *Tools* tab lists and launches other administrative and troubleshooting tools.

Task Manager

The *Task Manager* is a utility that shows and manages running applications and services, logged in users, and system performance.

Applications

Lists the running applications. The *Applications* tab is only available in Windows 7 and was dropped in Windows 8 and beyond.

Processes

This tab lists the current running processes and resources consumption. Since Windows 8, it also lists the running applications.

Performance

This tab shows how CPU, Memory, Disk I/O, and network resources are utilized. It can be very helpful in identifying the bottleneck in a slow-running computer.

Networking

This tab in Windows 7 shows the networking performance. In Windows 8 and later, this information has been moved to the *Performance* tab.

Users

This tab shows currently logged in users, their status, and applications run by these users.

Disk Management

Windows provides a disk management utility that can be run with the `diskmgmt.msc` command. The utility shows information and allows changing the disks, partitions, and volumes configuration.

Drive Status

The *Status* column shows the status information for each volume. It includes health and availability, volume type, and content type.

Mounting

Mounting applies to NTFS and allows the user to mount a drive to a folder, not a drive letter.

Initializing

After adding a new disk to a Windows computer, the drive may need to be initialized. This erases all data and prepares the disk to be used in Windows.

Extending Partitions

You can increase the size of a partition by extending it. It requires free space adjacent to the partition. Depending on the type and the file system, this task may or may not require erasing the data.

Splitting Partitions

Splitting partitions means creating two partitions in place of one. Windows Disk Management tools don’t allow splitting, but the same can be achieved by shrinking a partition, then creating another one.

Shrink Partitions

Shrinking is reducing the size of a partition. Of course, the resulting partition size should be able to fit all existing data. Depending on the type and the file system, doing this may require erasing the data.

Assigning/Changing Drive Letters

To access the file system and start using the disk for file storage, a disk needs to be assigned to a drive letter (e.g., C:, D:, E:, etc.). Once assigned, the files can be accessed through this drive. A drive letter can be changed for the disk. Be aware that it may change how the system, applications, and users' shortcuts reference the files and break some functionality if not done correctly.

Adding Drives

To add a drive, install the hardware, initialize, format, assign a letter, or mount the NTFS drive to a folder.

Adding Arrays

An array is a set of disks configured for improved performance and reliability. Software arrays are created and managed by Windows and can be created in the *Disk Management* utility after adding more than one disk. Hardware arrays use a special controller, configured separately before Windows boots. The array of disks then appears as a single disk to the operating system.

Storage Spaces

Storage spaces are created in a separate dedicated utility in Control Panel. This allows you to create different types of disk arrays, even across different types and sizes of disks.

System Utilities

Windows includes system utilities useful in maintenance, configuration, and troubleshooting.

Regedit—**Registry Editor** allows the user to view and change the Windows registry. The registry contains some operating system and application settings that may need to be changed in advanced troubleshooting.

Command—Command line interface, a prompt to enter commands in text format.

Services.msc—Command to open the *Services* utility to view and manage the system services.

MMC—**Microsoft Management Console** is a graphical interface used by many system utilities, for instance the *Device Manager*. Running MMC separately allows the user to open all the utilities that use that interface in the console.

MSTSC—Client for remote desktop, also known as **terminal service**, to connect to a remote Windows computer

Notepad—Simple text editor.

Explorer—File explorer to browse and manage files.

Msinfo32—Displays advanced hardware and drivers information.

DxDiag—**DirectX Diagnostic Tool** is for troubleshooting DirectX, display, audio, and input devices drivers.

Disk Defragmenter—Relocates pieces of large files to continuous space on a disk for optimized performance.

System Restore—Creates, manages, and restores the system using **restore points**.

Windows Update—Checks, installs, and manages Windows and other Microsoft updates.

Microsoft Windows Control Panel Utilities (*scenario*)

The *Control Panel* includes tools and utilities to view, change, and troubleshoot system settings.

Internet Options

Internet Options is a utility to manage network settings beyond basic IP connectivity. The settings are separated into multiple tabs.

Connections—Add and manage dial-up and VPN connections; configure proxy settings for web browsing.

Security—Define security settings for different *zones*. Websites can be added to the list of *trusted* or *restricted* sites, and different settings may be applied to these lists. The settings control what types of scripts will be run on the sites in the different lists and by default.

General—Configure what is shown when *Internet Explorer* is started, home page, tabs behavior, and interface appearance

Privacy—Allow and block sites, choose if you want to send your location to websites, and configure pop-up blocking.

Programs—Set default applications for Internet browsing, HTML editing, and email; manage and configure Internet Explorer add-ons.

Advanced—Lists advanced settings of accessibility, web browsing behavior and protocols, and security.

Display/Display Settings

This is the means to change the video output settings.

Resolution

Resolution is the **number of vertical and horizontal pixels** on the monitor. Windows usually recommends the highest resolution that your monitor supports for a crisper view, but this can be changed if needed.

Color Depth

Color depth is a measurement of **how many bits are used to represent color**. Higher depth would result in more accurate color representation on the monitor, but requires more hardware and software resources to do so.

Refresh Rate

Refresh rate is **how frequently the image on the monitor changes**. A higher rate provides smoother motion for graphics, videos, and games, but requires more hardware and software resources.

User Accounts

You can add, manage, and remove local users and their roles for the computer. Each user will have his or her own **profile** with different settings and user folders.

Folder Options

Folder options change how files are shown and searched.

View Hidden Files

Hidden is a file flag that signifies that users don't usually need to see these files, like system and configuration files. Windows settings can be changed to show these files if they need to be accessed.

Hide Extensions

In Windows, files have extensions at the end of the file name, after a period (e.g., .txt, .docx, and .exe). To make the file names cleaner and prevent users from making accidental changes to the extensions, these are usually hidden. This behavior can be changed with this setting.

General Options

The *General* tab of the *File Options* utility allows you to change the general behavior of the file browsing interface.

View Options

The *View* tab allows you to change many appearance options, including showing hidden files and file extensions.

System

System is the utility of *Control Panel* that shows hardware overview, and some other settings, as noted below.

Performance (Virtual Memory)

Virtual memory is space reserved on a hard disk for a paging file. A **paging file** allows you to run more concurrent applications while reducing the need in RAM size.

Remote Settings

Options on this tab configure whether this computer can be controlled remotely with **Remote Desktop** and what users will have that permission.

System Protection

Manage and create system restore points or revert to previously created restore points. **Restore points** save the system configuration and are useful if a change needs to be reverted.

Windows Firewall

An important security addition to Windows, the **Windows Firewall** protects the computer by controlling what applications can access the network from this computer, and also how this computer can be accessed over the network.

Power Options

You can choose what pressing the **power button** on the computer should do and configure the monitor and computer power to be reduced after some time of not being used.

Hibernate

Hibernation is a mode that **saves the current state of the computer and shuts it down**. When started again, it restores to the same state, but without consuming power in the meantime.

Power Plans

There are three power plans that can be configured and selected depending on the current need: **Power Saver**, **Balanced**, and **High Performance**.

Sleep/Suspend

The *Sleep* mode **doesn't shut down the computer** like *Hibernation* does, but instead significantly reduces the power to the components for a quick restart of work where you left it.

Standby

The term *Standby* is sometimes used interchangeably with *Sleep*, but is not used in the current Windows versions.

Other Utilities

Credential Manager

Credential Manager is a tool to manage Windows and web credentials in the corresponding vaults; for example, internet and remote desktop passwords.

Programs and Features

You can **uninstall and modify** applications (programs) and add or remove operating system features.

HomeGroup

HomeGroup is a feature that allows you to easily share files and printers in a small network. It is only available when you connect to a network and categorize it as the **Home network**, and disable it for work and public networks.

Devices and Printers

This screen lists printers, scanners, cameras, monitors, and other connected peripheral devices, and the settings of these devices can also be accessed.

Sound

You can manage devices to play and record sounds and configure sounds that the operating system produces on startup, shutdown, alerts, and prompts.

Troubleshooting

The Troubleshooting screen of the Control Panel provides a list of wizards to diagnose and troubleshoot some common issues with hardware and software.

Network and Sharing Center

Here, you can configure network adapters, create new network and dial-up connections, and configure network file and printer sharing.

Device Manager

This tab lists all hardware connected to the computer, and provides management for drivers of the devices.

BitLocker

You can **enable or disable** BitLocker encryption for fixes and portable disks.

Sync Center

Sync Center is a utility to configure **offline files**. Offline files is a feature that allows the user to continue working on network files when there is no current network connection, and synchronize the changes once connected again.

Application Installation and Configuration

There are multiple methods to install new applications and software. Some things need to be taken into consideration for successful installation and use of the applications.

System Requirements

The system needs to have enough resources to allow installation of new applications. The specific requirements depend on the application and can be usually found in the supporting documentation for the application.

Drive Space

Before running an application, its files need to be stored on the computer's disk. There should be enough **free disk space** to copy and use the program's files.

RAM

To run an application, it needs to be loaded into memory. There should be sufficient RAM available or the application will run slowly, slowing down other processes too, or not be able to run at all.

OS Requirements

An application expects to work with a specific operating system. The installation of the software should be compatible with the operating system. Refer to the application's documentation to find out what operating systems are supported.

Methods of Installation and Deployment

There are multiple ways to distribute software installation files.

Local (CD/USB)

The only method to install new software on a computer that is **not connected to any network** is to have the application on a portable media, CD or USB disk. This can also be useful for large applications or slow networks. The installation files can be run directly from the media or copied to the hard disk first and then installed.

Network-Based

On computers connected to a network, applications can be installed over the network and not from portable media or local files. If the application is acquired from the Internet, the files are first copied to the local disk, then installed. Operating systems also include forms of application stores and repositories that make it easy to find and install new software.

Local User Permissions

There are permissions considerations when adding new applications. The user installing the application needs to have the permissions to write the application's files to the installation directory. For some applications, the operating system's settings need to be modified for it to run.

The user running the application needs to have sufficient permissions to **run the application** and possibly **modify files and OS settings** when using the software.

Security Considerations

Any new software installed on a computer may cause effects that may compromise the security of the computer and the network it is connected to.

Impact to Device

Installing a new application may allow it access to other files on the computer. Some software may be **malicious** and may need to be researched before installing. Even if there are no bad intentions, some functions of the software may be not suitable for protected corporate environments with sensitive information.

Impact to Network

If a new application is installed on a computer that is connected to the network, it will effectively get access to the network and may be compromising the security of other computers on the same network.

Microsoft Windows Networking (*scenario*)

Windows comes with many abilities to effectively use network resources.

HomeGroup vs. Workgroup

- *HomeGroup* doesn't require a lot of configuration and is best suited for small home networks to share files and printers.
- *Workgroup* allows better flexibility and extended functionality and is best suited for small business networks.

Domain Setup

Windows Domain is a solution for larger organizations and scales very well. It allows many security features to limit access to resources to specific groups. It requires **proper configuration** of domain controller servers. The computers and the users on the domain need to be configured to use the domain as well.

Network Shares/Administrative Shares/Mapping Drives

Windows allows sharing of files and folders over the network, allowing a shared space for network users. For convenience, *network shares* can be mapped to a drive letter. For the users and applications, the network share appears like a local disk.

Administrative shares are created automatically to allow remote administrators to configure the computer. These shares are not shown and are not accessible to non-administrative users.

Printer Sharing vs. Network Printer Mapping

You can use the *printer sharing* functionality to allow printing from other computers to the printer connected locally. To print using a shared printer on a remote computer, it needs to be *mapped* first, installing the drivers for the printer.

Establish Networking Connections

There are multiple ways to connect a Windows computer to a local or remote network.

VPN

VPN is a **Virtual Private Network** and uses another underlying network, usually the internet. It allows secure access to a remote location over public infrastructure.

Dial-ups

Dial-up allows the user to connect to a remote computer over a **telephone network**. The remote computer needs to be set up to listen and accept connections.

Wireless

Wireless network connections use **Wi-Fi** technology to connect. Because it is not physically restricted in the area, the network will usually have another layer of security in the form of a password or more complex authentication. Once connected, the functionality is very similar to a wired connection.

Wired

Wired connections usually come in a form of **Ethernet** to the computers. It requires cabling to every computer and may require other network devices like switches and routers.

WWAN (Cellular)

Similar to mobile phones that can access the internet from anywhere, the cellular network can be used to connect to the network. Some tablets and laptops come with built-in cellular hardware.

Proxy Settings

A proxy server is a form of a **gateway**. A common example is a **web proxy** that is set up to filter access to the internet from a local network to improve security.

Remote Desktop Connection

Remote Desktop Connection allows you to connect to a remote Windows computer for full control with a keyboard and mouse, and full graphical interface. The computer needs to be configured to allow access.

Remote Assistance

Remote Assistance allows a **remote desktop connection**, but a request to connect needs to be generated and sent first. It creates a file that can be emailed and used to connect.

Settings for Work Type

When connecting a Windows computer to a new network, it asks you to identify the type of the network: **Home**, **Work**, or **Public**. When selected, the corresponding discovery and firewall settings will be set to align with the security needs.

Firewall Settings

Windows comes with configurable firewall rules to allow or block certain applications or network ports and control the security.

Exceptions

When installing a new application that needs access to the network, Windows may ask if it should be allowed and add an exception to the firewall.

Configuration

The Windows firewall can be manually configured to **allow or deny** applications and network ports.

Enabling/Disabling Windows Firewall

The Windows firewall can be switched off completely for the type of the network. This effectively allows all network traffic and has to be used extremely carefully to avoid exposing the computer to potential network threats and unauthorized access.

Alternative IP Addresses

The IP address of a Windows computer can be dynamically acquired from a DHCP server on the network, or configured manually. This is done within the TCP/IPv4 settings of the network adapter.

IP Addressing

The IP address needs to be in the **same subnet** with other hosts and the gateway, but be unique.

Subnet Mask

A subnet mask determines what hosts are on the same network with the local computer. It needs to match between all the computers and network devices on the local network.

DNS

DNS are servers that **resolve names** (e.g., microsoft.com) to an IP address that the computer can communicate with. More than one DNS server can be configured for reliability.

Gateway

A **default gateway** is a router that can forward the network traffic from the local network to other remote networks. At least one of its interfaces has to be on the same local network as the computer.

Network Card Properties

In addition to IP addresses, other settings can be manually configured on the network card.

Half Duplex/Full Duplex/Auto

- *Duplex* determines if the data can be transferred in both directions at the same time. *Half duplex* operates like a one-way walkie-talkie radio, where only one side can talk, and the other side waits for it to finish before talking.
- In *full duplex* mode, devices on both sides of the network cable can “talk” and “listen” at the same time, making data transfer faster and more reliable.
- The *auto* setting will try to determine if full duplex is available on the cabling or fall back to half duplex.

Speed

Usually, speeds of 10, 100, and 1000 Mbits per second can be seen on networks. This can be set manually or left in auto mode to determine the fastest speed supported by the network.

Wake-on-LAN

Wake-on-LAN is a function of a network card that allows you to power on the computer when a special packet has been received. It may be useful in a scenario with a computer that has resources that need to sometimes be accessed over the network, but power needs to be preserved when it’s not accessed.

QoS

Quality of Service is a set of techniques to prioritize one type of traffic over another. For instance, you may be using a computer for video conferencing while transferring files. The video and audio traffic should take precedence over the file transfer for a better overall experience.

BIOS (On-Board NIC)

A **network interface card** may be separate or part of the motherboard (on-board). In the case of an on-board NIC, some settings may be only available from the BIOS settings.

MacOS and Linux Systems (*scenario*)

MacOS and Linux operating systems come with similar utilities, tools, and commands for configuration and maintenance.

Best Practices

There are some known good practices to maintain the system, data, and performance, and these are the most important ones.

Scheduled Backups

Scheduled backups create a **copy of data and configuration** that can be restored later if needed. The best practice is to frequently create backups of files, and have a copy of important files at a remote location. This remote location may be cloud storage that can be accessed over the internet.

Scheduled Disk Maintenance

There is no scheduled disk maintenance built into MacOS, but the *Automator* allows you to schedule these jobs, and *cron* in Linux can be used to schedule any command. The best practice is to schedule disk maintenance jobs to run **outside of business hours**, or as needed.

System Updates

In **MacOS**, the *System Preferences* for the *App Store* provide the configuration for system updates. You can choose to either manually or automatically download and install the updates.

Linux distros manage updates differently. In **Ubuntu**, the settings are very similar to MacOS and accessed via the *Software & Updates* settings.

The best practice is to install updates as quickly as possible after they're released, but after ensuring there are no compatibility issues.

Patch Management

Patches are smaller updates, usually addressing specific functions and features, security, and bugs. These are managed similarly to *system updates*. The best practice is to allow automatic installation of patches to improve security, if the environment allows this disruption.

Driver/Firmware Updates

Drivers and hardware firmware sometimes get updated too. These are managed similarly to *system updates*. Again, the best practice is to install driver updates as quickly as possible after they're released to improve hardware performance, but after ensuring there are no compatibility issues.

Antivirus/Anti-Malware Updates

Antivirus software may depend on the signatures of viruses and other malicious software that needs to be updated. Make sure that the security software is configured to get frequent updates after installing it.

Tools

To maintain the best practices, MacOS and Linux provide tools for system maintenance. Here are some of them:

Backup/Time Machine

MacOS comes with the *Time Machine* utility to create a backup to an external drive. Linux has many options, a popular one being the *Duplicity* command line utility as well as the *Déjà Dup* GUI interface for that utility. It will copy selected files to a predetermined location on a schedule.

Restore/Snapshot

When files need to be restored from backup, the same *Time Machine* and *Duplicity* tools that were used to create the backups can be used.

Image Recovery

In MacOS, the *Disk Utility* can be used to create and restore *disk images*. The images are files that can be mounted and behave like a disk. Or it can be restored to a physical disk. Linux distros have multiple solutions; *gnome-disk-utility* comes with Ubuntu under the *Disks* name.

Disk Maintenance Utilities

Disk Utility in MacOS and *Disks* in some Linux distros can be used to check the disks for errors.

Shell/Terminal

While MacOS and most Linux distros come with a convenient GUI, they provide a command line interface that may be useful for system commands and tools that are not available in the GUI. Some Linux and MacOS commands are listed in the *Basic Linux Commands* section of this guide.

Screen Sharing

Remote screen sharing and access can be enabled and configured via the *System Preferences* and *Sharing* menu. For Linux GUI, a popular method of screen sharing is using the **VNC protocol** and software.

Force Quit

If an application becomes unresponsive and needs to be closed, you may need to *force quit*. It will terminate the application and you will lose unsaved work. It can be accomplished by selecting the application and pressing the *quit* button in the *Activity Monitor* in MacOS or *Task Manager* in Ubuntu.

Features

MacOS comes with many features that are unique compared to other operating systems. It's important to understand these features so that you can get the most out of using a Mac.

Multiple Desktops/Mission Control—Mission Control is a program that allows you to view everything that is open and also quickly swap between programs. Mission Control also allows you to create multiple desktops (called **Spaces**) that you can use to organize what you are working on.

Keychain—The Keychain feature in Mac operating systems is a tool used for password management. Items that can be stored in Keychain include passwords, private keys, certificates, and secure notes.

Spotlight— Spotlight is a search feature on Mac operating systems. It creates an index of all the items and files on your system so you can look up items quickly.

iCloud—The iCloud program comes default on all Apple products. It is used as a method for storing data in the cloud. This is beneficial as a backup method for Mac users.

Gestures—Apple gestures are small motions that a user can make using the trackpad to complete simple tasks. For example, to move between pages of a document, swipe left or right with two fingers. All of the gestures for Mac devices can be found under system preferences, then by selecting trackpad.

Finder—The Finder is the default file manager for Mac operating systems, similar to the FIle Explorer program in Windows. Finder allows users to search for files, open files, and delete files from one location.

Remote Disc—The remote disc feature allows smaller Mac devices that do not have a disc drive to essentially "borrow" the disc drive of a nearby device. It allows the computer without the disc drive to access the files on a disc that is being used on another device.

Dock—The dock in MacOS is similar to the taskbar in Windows. It is the launching pad for all applications on Mac operating systems.

Boot Camp—Boot Camp is a utility that comes built into Mac devices and lets users switch between MacOS and Windows operating systems.

Basic Linux Commands

To be successful in using Linux operating systems, you will need to be familiar with at least the most basic Linux commands. Being able to navigate the Linux terminal using these basic commands will be very beneficial. It's important to note that Linux commands are case sensitive, so take note of the case you are using when typing them.

`ls`—The ls command is known as the "list" command in Linux. This is because the command will list all of the files or folders in a given directory. In order to use this command, navigate to the folder or directory you're interested in and type "ls". After hitting enter, a list of all the files and folders in that location will be displayed.

`grep`—The grep command stands for global regular expression print. The grep command is a search command. You can use it to search for a string of characters within a file or standard text output. For example, if you are viewing a file in the terminal and type the command grep "unix", the terminal will display all of the instances of the word "unix" in that file.

`cd`—The command cd stands for change directory. This is very similar to the change directory in Windows. You can type `cd ..` (note that there is a space between cd and the two dots) and you will move back one directory from where you are. If you use the command `cd /`, you will go all the way back to the root directory, which is known as /.

`shutdown`—The shutdown command is used to turn the device off. If you use the command shutdown by itself, it will notify all logged in users, log those users off, and then turn off the system. You can also use the shutdown command to restart the computer by using the -r flag on the command. (Example: `shutdown -r`)

`pwd vs. passwd`—While many people see the term pwd and think "password," it actually means something very different in Linux. The command pwd stands for present working directory, and it will display the full path of the current working directory. So, if pwd doesn't change the password, then what command does? The command to change passwords in Linux is the passwd command. This command can be used by typing `passwd` followed by the username that needs its password reset. If no username is specified, it will change the password for the current user.

`mv`—The mv command in Linux is the move command. This command allows a user to move a specified file to another location. Move would be similar to a cut and paste in Windows.

`cp` —The cp command in Linux stands for copy. Its functionality is similar to that of the move file, except that it places a copy in the new location while still leaving the file in the original location.

`rm` —The rm command stands for remove in the Linux operating system. This is similar to a delete functionality, as it removes the file, directory, or other various objects from the location.

`chmod` —To modify Linux file permissions, you must use the chmod command. Before changing Linux file permissions, it's important to first understand how they are represented. Each permission is represented by a letter, as shown here: r: The read permission, w: The write permission, x: The execute permission.

`chown` —While the chmod command changes the permissions, the chown command changes the ownership of a file, directory or other objects.

`iwconfig/ifconfig` —The ifconfig command in Linux is very similar to the ipconfig command in Windows. The ifconfig command is used to display networking information of the Linux device such as IP address, DHCP address, and MAC address. The iwconfig command is similar to ifconfig, but it strictly looks at the wireless interface.

`ps` —The ps command in Linux will display all of the currently running process and their process numbers. The ps command stands for process status.

`su/sudo` —The su command stands for switch user (or substitute user). The su command can be used by adding a username that you wish to switch to after the command (example: `su linuxuser1`) or it can be used by itself, which will by default switch it to the root user. Sudo will switch the user for a single command, while su will switch the user until it's switched back.

`apt-get` — APT stands for advanced packaging tool. The apt-get command is a tool for handling packages in Linux. It is used to retrieve packages from authenticated sources for installation, upgrade, and removal of packages, along with their dependencies.

`vi` —The vi command is short for visual editor. The vi tool is the default text editor that comes with Linux systems.

`dd` —The purpose of the dd command in Linux systems is to copy a file then convert and format it according to the operands. DD stands for data duplicator.

`kill` —In Linux, the built-in command to terminate a process is the kill command. The kill command can be used to terminate a process using the name or PID.

How to Prepare for Questions About Operational Procedures on the CompTIA A+ Core Series 1002 Test

General Information

Operational procedures generally tell you what to do in all sorts of circumstances, guiding you to the best practices for each situation. Below you will find an outline of the basic concepts in this area that occupies roughly one-fourth (23%) of the CompTIA A+ Core Series 1002 test. Nearly half of the questions in this domain are prefaced by a scenario and the headings for those areas are marked below with (*scenario*).

Documentation

It's vital to ensure that you read any required documentation before you begin working on any system. Documentation includes items such as **processes and procedures, network diagrams, knowledge base articles** (also known as **KBs**), and much more. It's also important to **document any fixes** that have been implemented so they can be referenced later. Another example of documentation includes **Safety Data Sheets (SDS)**. The SDS outlines the procedures for disposing of hazardous materials. This should be referenced if there is a question about properly disposing of hazardous material. The SDS is administered by the **Occupational Safety and Health Administration (OSHA)** within the United States.

Network Topology Diagrams

Network topology diagrams are extremely helpful for performing any network **upgrades** or even to **troubleshoot** networking problems. The network topology diagrams will provide a visual representation of how the network is laid out, including both logical and physical information for the devices. **Visio** is a popular tool used when creating network diagrams.

Knowledge Base/Articles

A knowledge base is a repository of **information regarding an application or system**. When working on a system or troubleshooting an issue, individuals should first visit the systems knowledge base to see if a **solution** to their issue already exists.

Incident Documentation

You should adhere to the following order of operations when responding to any incident occurring on your computer network.

First response: The first step is the proper **confirmation** that an incident has happened, or is taking place. You should gather as much **information** as possible on the event, and **report** it through the proper authorized channels at the organization. These items will be outlined in a sound security policy.

Documentation: The next step is to document as much as possible. You can make use of **pictures**, **scratch notes**, or **event logs** to collect and assemble this information.

Chain of custody: Lastly, you want to make sure the **information you have is preserved**, especially in the event that information changes. Maintaining the **integrity of the information** is the most important step from this point forward. Any unaccounted changes could call into question the reliability of the information, making any work done since the first step useless.

Regulatory and Compliance Policy

When dealing with a networking environment, there are several regulations to keep in mind. These include: **electrical codes** for running high/low voltage cabling, **environmental codes** for disposing of chemicals or hardware, **fire prevention codes** requiring the specific use of dry or wet systems, and **building codes** that specify how cabling can be run through a building.

Acceptable Use Policy

An acceptable use policy (**AUP**) is a policy put in place by an organization that states which types of actions are acceptable to perform using their equipment. Many organizations implement acceptable use policies which state how employees are allowed to use their company-owned devices. Whenever accessing a public wi-fi, such as at a coffee shop like Starbucks™, you will have to acknowledge the AUP before getting access to the network.

Password Policy

Password policies state what is required when creating a password. **Weak passwords** can lead to data breaches and identity theft. To ensure that users create **strong passwords**, most password policies will include requirements for **length, complexity, and history**.

Inventory Management

Inventory management is the process of maintaining a database of which devices and systems exist within an organization. Inventory management is often done using a **third-party program** to keep track of devices within larger organizations.

Asset Tags

An asset tag is a method of inventory management. By adding asset tags to devices, it's easier to keep track of devices, including **who has the device** and **where they are located**.

Barcodes

Barcodes are types of asset tags that can be **easily scanned** to keep track of the devices.

Management Change (*scenario*)

Management Change (also called Change Management) is the process of addressing changes within an organization. Whenever a change is going to be made in an organization, **proper procedures** must be followed to ensure that any negative impact on the business or users is minimized.

Documented Business Processes

Any time a change is made within an organization, it's important to ensure that the business processes are documented. If the change is going to affect the current business processes, it should be evaluated and documented.

Purpose of the Change

Before making any changes, the purpose of the change must be documented. Typically, a **cost-benefit analysis** will also be done to see if the purpose of the change is worth the cost to implement and re-train staff on the new procedures.

Scope of the Change

Scope refers to the **extent of the changes** that will be made. While documenting the scope, it should outline exactly which items will be modified and changed through the project.

Risk Analysis

When making any changes within an environment, new risk will likely be introduced. Before making any changes in the environment, a risk analysis must be done. Upon defining the new risks which may arise, the organization must choose to **accept, mitigate, or avoid the risk**.

Plan for Change

Whenever implementing changes, it's also important to plan for changes that may arise throughout that process. **Before implementing** anything, there should be a plan in place for change.

End-User Acceptance

In order for a successful change, **all users must be on board** and prepared for the change. User acceptance testing is a common practice in which real users ensure that the change doesn't negatively affect their ability to perform tasks.

Change Board

A change advisory board (**CAB**) is made up of **individuals from various departments** throughout the organization. The CAB should also include high-level executives and stakeholders. This board will be responsible for **approving the changes** before they can be implemented. They will also be in charge of **overseeing** the project through to completion.

Backout Plan

With any change, there must be a backout plan in case unexpected issues arise. A backout plan would include a way to **revert to a previous version** of the system before the change was applied.

Document Changes

One of the most important aspects of the change management process is to document all changes as they are being made. This includes documenting **any new processes** that must be followed as a result of the change. **All challenges** that arise as a result of the change should also be documented.

Disaster Prevention and Recovery (*scenario*)

All organizations should have a **business continuity and disaster recovery (BCDR) plan** documented and in place. Disaster prevention and recovery refers to the ability to be able to bounce back after any type of disaster, such as a natural disaster or a cyber attack.

Backup and Recovery

Disaster can strike at any time, making it a requirement of information technology teams to have a full set of backups so they can quickly recover after an incident. Organizations should have **full backups** (which includes a backup of everything) and **incremental backups** (which includes only what has changed since the previous backup).

Image Level

An image-level backup creates a **full snapshot of the system** at a given point in time. This creates more of a full picture of the operating system and all the files included. This is a more complete option than file-level backups.

File Level

File-level backups are exactly what they sound like: **individual files and folders are selected** to be backed up.

Critical Applications

Critical applications should always be **a priority** when performing backups. File backups may not cut it when trying to backup critical applications. Microsoft Exchange servers and SQL servers will require additional work to back up above and beyond what file-level backups can offer.

Backup Testing

It's not enough to perform backups; the backups must also be tested. The test serves to **show that the backup files are not corrupt** and that they are backing up everything that would need to be restored in the event of a disaster. Backup tests should be **conducted regularly**.

UPS

If servers are not properly shut down, they can be damaged. This means that if there were to be a power outage, the server operating systems or applications may become corrupt. In order to prevent this type of scenario, systems should be plugged into an **uninterruptible power supply** (UPS). A UPS is an electrical device which provides power to a device in the event that the main power source fails.

Surge Protector

Surges occur when there is a **spike in voltage** or noise along the line. This can cause **damage to equipment** if the surge reaches the equipment. Surge protectors can counter this and send the excess voltage to the ground.

Cloud Storage vs. Local Storage Backups

Organizations will have to choose whether to use local storage backups (such as tape backups) or to back up to cloud storage. Some organizations may **also opt to have both** local and cloud storage as a second layer of disaster recovery. One drawback of cloud storage is that the data owner doesn’t have full control over the data or where it is stored in the cloud.

Account Recovery Options

Account recovery **options will vary** depending on which type of account needs to be recovered. Many online accounts will have a “forgot your password?” option which will allow the user to have a password reset link emailed to them. If local accounts need to be recovered, Windows 10 has built-in features to recover lost passwords.

Common Safety Procedures

When dealing and working with computer components, keep safety **at the forefront** for both your and the device’s sake. The following sections may be delivered as “scenario-based” questions in the exam environment, so you must be very comfortable with these topics.

Equipment Grounding

Equipment grounding is a way to transport any excess electrical discharge away from the component and into the electrical ground wiring. This is a safety mechanism that is included on all outlets, significantly **reducing the risk of electrical shock** should there be a fault within the system.

Proper Component Handling and Storage

You should be fully aware of how to handle and store the various components that can be affected by electrostatic discharge (ESD). The following items are the most common when managing ESD.

Antistatic Bags

These are used to store computer components when removing them from a computer and moving them around. This will ensure **minimal static buildup** and prevent damage.

ESD Straps

These are small wrist straps that can connect to an ESD mat or an ESD jacket for discharge to **reduce your electrostatic presence**.

ESD Mats

An ESD mat can either be a mat **you stand on** (floor mat) or a mat you **place the equipment on**. These ESD mats will reduce ESD risks, and some allow you to snap your ESD wristband into them for better protection.

Self-Grounding

Self-grounding means to remove or minimize the risk of ESD by taking premeditated **actions before working inside a computer**. This can be done by: working on hardwood tables, working on hard floors, wearing cotton clothing, and working in higher humidity environments. By gently running your hand across the bare metal of a computer case prior to reaching inside, you lessen the risk of ESD.

Toxic Waste Handling

You should be familiar with the proper procedures for handling several items that are considered toxic, including these:

Batteries

Newer technology batteries pose greater risks and should be **handled cautiously** when storing, charging, or disposing of. Improper charging can lead to fires and/or explosions that are difficult to extinguish with normal agents due to the chemical makeup of these batteries. Lithium batteries will get warm and might swell or leak if handled incorrectly while charging or transporting. You should wear **protective goggles** when working with these items. They should be taken to **waste facilities** for proper disposal due to chemical properties.

Toner

You should wear **protective goggles** and **air filters** when working with any toner cartridges. Toner appears in the cartridge and the printer as a dark, very fine powdery dust and is difficult to remove from clothing, skin, or other surfaces.

CRT

While not seen as often, cathode ray tube (CRT) monitors were the primary display units up until flat screen displays became mainstream. Some CRT screens contain **mercury**, **lead**, and **other materials** that can be hazardous to you and your surroundings. To power these tubes, they hold **a charge** that can be deadly when discharged. You should wear **protective goggles** when working with these items as well as **electrician gloves** in the event you need to open the case (no serviceable parts are inside). They should be taken to **waste facilities** for proper disposal due to the lead contained in the glass.

Cell Phones

Some states in the U.S. have made it illegal to throw cell phones in the trash, as they consider them hazardous material. This is likely due to the battery inside the smartphones. Instead of throwing the devices in the trash, the better option is to take them to an **electronic recycling facility**.

Tablets

Much like cell phones, tablets **should not be thrown in the trash**. Instead, they should be taken to an organization that recycles these devices.

Personal Safety

Be familiar with the following guidelines related to personal safety when dealing with computer components.

Disconnect Power Before Repairing a PC

All power sources should be disconnected prior to working inside a computer. Power supplies are typically replaced as a whole rather than in smaller individual parts. Normally there are **no serviceable parts inside** and therefore they should not be opened.

Remove Jewelry

All jewelry or anything dangling from your body should be removed. They can create a tangling hazard and/or cause a short circuit when they are near or come in contact with components.

Lifting Techniques

Always lift heavy equipment **using your legs** and not your back, or use multiple people to lift the object.

Weight Limitations

Use a **rolling cart** or something similar for overweight items when possible. Do not attempt to lift overweight items by yourself. **Weight limits are usually posted** on the outside of the boxing material. Observe a **"two-person rule"** when needed.

Electrical Fire Safety

For electrical fires, use specialized dry fire prevention or extinguishing chemicals, such as carbon dioxide. **Wet chemicals or water should never be used** on electrical fires.

Cable Management

Cabling should be **secured together** when run across spaces to prevent tripping, and should be covered if possible. There should never be any loose cabling to pose hazards to personnel or other equipment. Occupational Safety and Health Administration **(OSHA) regulations** should be verified and adhered to when running any cabling.

Safety Goggles

Use goggles when working with chemicals, batteries, or printer toner.

Air Filter Mask

To protect yourself from an environment where dust, smoke, or other air particles exist in the surrounding atmosphere, you should wear a special mask used to filter out these items.

Government Regulations

When dealing with a networking environment, there are several regulations to keep in mind. These include: electrical codes for running high/low voltage cabling, environmental codes for disposing of chemicals or hardware, fire prevention codes requiring the specific use of dry or wet systems, and building codes that specify how cabling can be run through a building.

Environmental Concerns

You should be able to quickly analyze and apply the proper controls for any possible environmental impacts. Some questions in this area will be of the scenario type.

SDS Documentation

The Safety Data Sheet (SDS) outlines the procedures **for disposing of hazardous materials**. This should be referenced if there is a question about properly disposing of hazardous material. The SDS is administered by the Occupational Safety and Health Administration (OSHA) within the United States. Copies are kept locally wherever there might be contact with hazardous materials.

Temperature, Humidity, and Ventilation

The temperature and humidity in the environment where components are stored should reflect the levels outlined in the SDS. For an electronic environment, it is usually best to balance the humidity as efficiently as possible to **avoid extreme condensation or static**

discharge. It is also important to keep a closed-in area **well ventilated** so the room does not become too hot when the equipment is running.

Power Issues

Power issues can occur **anytime and anywhere**. These can range from total outages to flickers or surges, and can be devastating to equipment, data, and clients.

Battery Backup

An uninterruptible power supply (UPS) is used to maintain power to equipment in the event of a power outage or surge when all power can be lost or drop down below a certain threshold. The UPS will **automatically activate and provide power** for the connected equipment via batteries.

Surge Suppressor

A surge suppressor works by **checking for spikes in voltage** along the line. If a spike is detected, the surge protector **moves the excess power** to the ground and only allows the proper amount to be passed along to the connected devices.

Airborne Particles

You should be familiar with these two methods for countering airborne particles:

Enclosures

Your computer can be placed inside a special enclosure if it is in a location where there are a lot of particles in the air, such as smoke or dust. These are typically found in **factory or plant locations**.

Air Filters/Masks

To protect yourself from an environment **where dust, smoke, or other air particles exist** in the surrounding atmosphere, you should wear a special mask used to filter out these items.

Dust and Debris

You should be familiar with these two methods for cleaning dust and debris in a computing environment:

Compressed Air

Compressed air can be used to clean out the inside of computer equipment, as well as printers or other devices. It is better to **use natural compressed air** versus any chemical-based compressed material.

Vacuums

Only specialized anti-static vacuums should be used in electronic environments. These vacuums can help reduce the risk of a static discharge or damage to the component.

Government Regulations

You should be aware of any local regulations regarding the industry in which you operate, such as disposal procedures or safety implications. In addition, the Safety Data Sheet (SDS) outlines how to dispose of hazardous materials. This should be referenced if there is a question about how to properly dispose of any hazardous material or if you simply require more information about the item in question. The SDS is administered by the Occupational Safety and Health Administration (OSHA) within the United States. Environmental concerns are administered nationally by the **U.S. Environmental Protection Agency (EPA)**.

Regulation of Technology Use

Licensing/DRM/EULA

For this exam, you should be very comfortable with the many types of licensing arrangements available today, including **digital rights management (DRM)** and **end user licensing agreements (EULA)** that stipulate how the software can be used.

Open Source vs. Commercial License

An *open source license* means that the software's source code is freely available to the public. This means the software can be modified and recreated if desired by the end user. A *commercial license* is usually closed source, meaning the source code is not available to the general public.

Personal License vs. Enterprise Licenses

A *personal license* is granted only to one end user for recreational purposes. At times, costly commercial software will license its product for non-commercial use to an individual or student, and this is intended for personal use only. *Enterprise licenses* are intended for business use, typically by larger organizations, and are a form of paid commercial software licensed to the company for a certain number of users.

Incident Response

You should adhere to the following order of operations when responding to any incident occurring on your computer network.

First Response

The first step is the proper confirmation that an incident has happened, or is taking place. You should gather as much information as possible on the event and report it through the proper authorized channels at the organization. These items will be outlined in a sound security policy.

Identify— We have tasks to complete every day. While completing these, if something looks different, then you have just *identified* something. By using **checklists** and following these checklists as a daily task, you are more likely to identify an incident long before it possibly affects the system.

Report— Once confirmed, ensure others in your chain of command are notified that an incident has occured. Document the person and title you informed as well as the time they were informed. Having a **standard report form** will assist in this procedure.

Preserve— To obtain a full incident overview, preservation is paramount. Ensuring that the **evidence remains intact** and undisturbed will preserve the incident for investigation.

Documentation

The next step is to document as much as possible and continue documentation as changes are made to the incident. You can make use of pictures, scratch notes, or event logs to collect and assemble this information.

Chain of Custody

Lastly, you want to make sure the information you have is preserved, especially in the event that information changes. Maintaining the integrity of the information is the most important step from this point forward. Any unaccounted changes could call into question the reliability of the information, making any work done since the first step useless.

Tracking of evidence— Evidence of an incident can be vital to proving the who, what, when, and how of the incident. Ensuring this evidence is maintained while the investigation is being completed should be conducted with evidence trackers and chain of custody logs. These can be generic forms or be generated internally, but should be started as soon as the documentation begins.

Documenting progress— During the investigation phase of the incident and all during the process, everything must be documented to maintain the incident. Any slight infraction can lead to “tainted” evidence and the investigation being sidelined.

Regulated Data

Within the scope of information technology is data that must be held to a higher standard than that of other data. In cases of *regulated data*, the federal government has developed standards as to the handling of this data.

PII— **Personally Identifiable Information**: This is information that can be used as a means to identify employees within an organization, such as Social Security numbers and addresses. This information should remain very secure, and there should be clearly defined policies stating who can access it.

PCI— **Payment Card Industry**: Security standards that ensure all companies that accept, process, store, or transmit credit card information maintain the security of such information.

GDPR— **General Data Protection Regulation**: Regulations based on data protection and privacy within the European Union.

PHI— **Protected Health Information**: Information relating to health information of the person stored, transmitted or maintained in electronic or other forms. Subject to state and federal privacy and security rules, including the Health Insurance Portability and Accountability Act (HIPAA).

Policies and Security Best Practices

Most of these policies, including end user policies, were created to best protect the organization's network and should all be followed. Many items that a company may disallow or restrict can pose significant security risks to the computer infrastructure. This makes it **very important that all policies are followed**, and that all employees from entry level to CEO are educated on security best practices.

Communication Techniques and Professionalism (*scenario*)

Those working in IT should be aware of the following concepts in order to use proper communication techniques and professionalism.

Language

You should always **use proper language** when speaking with a customer or client. The majority of end users are not very technology-oriented, so you should **avoid tech slang and acronyms**, breaking down the meaning of all terms used in a constructive manner. We sometimes get caught up in technical language and should always avoid "tech speak" or talking above the client's head.

Attitude

You should display a **great attitude** when dealing with technical issues that may be complex. Use all cases as lessons to acquire more knowledge about technology. Also, **be confident** when discussing technical issues with end users. Be aware that it is more about being able to *find* the right answer than having all the answers memorized. Regardless of the situation, **remain positive** and project confidence in your work. Customers know that you don't know everything, but you should avoid giving the impression that you are unsure of the procedure to find a solution.

Listening

When discussing issues with a customer, **actively listen** and **take notes** when appropriate. Customers should never have to repeat themselves because you did not write down key details. Additionally, **never interrupt** customers while they are giving you information. Let them tell you their story in full and then you can respond with follow-up questions if needed. Remember, always listen to understand what the customer is saying.

Sensitivity

You should always **greet users with respect** and **use their proper professional titles** when addressing them. If someone is a director, don't refer to them as a manager—not in person, in support documentation, or on the phone with one of your colleagues. This is an easy way to offend someone quickly. Remember that some people have different cultural backgrounds than others, so you should always **remain culturally sensitive** to their requests.

Punctuality

Punctuality is extremely important as an IT professional. Often, end users have meetings or their own work to complete and you are seen as the piece that is holding them up. Always arrive on time for pre-scheduled appointments and always **contact clients if there will be any delay** relating to the service. If anything keeps you from arriving at the client's location on time, notify the customer of your situation beforehand and give them an **estimated arrival time**.

Distractions

While working with clients, be sure to avoid all types of distractions. This includes text messages, phone calls, or simply having conversations with other colleagues. You never want to give the impression that the end user does not have 100% of your attention. Their technical problem must appear to be the number one priority when you are in their presence, even though that may not be the case. Listed below are some, but not all, of the distractions that should be avoided at all costs.

- Personal calls
- Texting/social media sites
- Talking to coworkers while with customers
- Personal interruptions

Difficult Situations and Customers

When handling difficult situations or customers, be sure to do the following:

Do not argue— Arguing with customers will not get the result that either of you are hoping to achieve. **Try not to become defensive** when speaking with a client, even if they seem like they are being unreasonable. Letting the customer know that you understand their frustration will help them to feel confident that you can help them solve the problem.

Avoid dismissing customer problems— Try to avoid dismissing the customer's problems or issues. Even though an issue may not seem like a big deal to you, it may be very important to them.

Avoid being judgmental— Avoid being judgemental when working with clients. Something that may seem easy and self-explanatory to you could be quite challenging and difficult to them. It's important to keep in mind that not everyone is tech-savvy.

Clarify customer statements— **Ask questions** to ascertain the root of the problem. When a customer tells you his or her story, restate what you believe the problem to be to confirm an understanding through the verification process.

Maintain privacy— **Never use social media** as an outlet to vent about a particular customer or experience. Things on the Internet typically stay there forever and this could portray you or your company in a bad light.

Meeting Customer Expectations

When working on a client issue, always be prepared to **set initial expectations** with the promise of action to follow. Keep the customer informed of any changes, but make sure all promises are kept in a timely manner.

Options— If possible, always give the customer **multiple options and alternatives**. Even if you prefer one way, remember this is the end user's equipment and they should be given the opportunity to weigh their options.

Documentation— Keep up-to-date documentation and **provide this to the customer when the service is complete**. Customers will feel more at ease if they can review what work was performed on their PC, as they will know exactly how their money was spent on the repair.

Follow up— When the device has been returned to the customer after service, follow up at a later time to **verify satisfaction**. This is one of the most important steps in having repeat customers, as they will feel like you genuinely care about the service.

Privacy of Records

When working on a customer's issue, use best practices in handling their data. This is the customer's private information, and directly accessing this data is usually not required to complete a repair. It is your duty to keep that information safe and secure for as long as it's in your possession.

Scripting

Scripting can be used to automate IT management processes. It is important to be familiar with all of these concepts.

Script File Types

You should be able to identify the basic types of script files.

.bat— A batch file is a series of commands to be run by the Windows operating system stored in a plain text file.

.ps1— A .ps1 file is used to run scripts in Powershell.

.vbs—A .vbs file contains lines of codes in the Visual Basic programming language which are encoded in plain text format.

.sh— A .sh file is like the batch files of Windows but they can be executed in Linux or Unix.

.py— A .py script is a script written in the Python programming language.

.js—. A .js file is a script written in JavaScript.

Environment Variables

An environment variable is a dynamic-named value that can affect the way running processes act on a computer. **Shell scripts** and **batch files** use environment variables to communicate data and preferences to child processes.

Comment Syntax

Adding comments to your scripts can help both you and individuals who view your script in the future understand what you were trying to accomplish. The syntax used to add comments will vary depending on the programming language, but often a / or // will denote a comment.

Basic Script Constructs

Basic loops— A basic loop structure encloses a sequence of statements in between the loop and end loop statements. With each iteration, the sequence of statements is executed and then control resumes at the top of the loop.

Variables—- A variable is a symbolic name for a piece of memory to which we can assign values, and read and manipulate its contents.

Basic Data Types

You should be aware of the following data types.

Integers— An integer is a whole number (not a fraction) that can be positive, negative, or zero.

Strings—A string is essentially a string of characters used to represent text rather than numbers.

Remote Access Technologies (*scenario*)

Accessing devices remotely is a major part of troubleshooting issues. Let’s look at a few remote access technologies.

RDP

RDP, or **remote desktop protocol**, is a Microsoft proprietary technology for remotely accessing Windows computers. RDP provides a user **with a graphical interface** to connect to another computer over a network connection.

Telnet

Telnet is a protocol which creates a **two-way communication connection** between computers over a network connection (via the Internet or local area network). Telnet has **no graphical user interface** like RDP does; it is strictly **terminal-based**. Telnet typically operates on **port 23**.

SSH

Telnet is not very secure, so SSH has pretty much replaced telnet for communication over the network. SSH is also **a terminal-based program** with **no graphical interface**. SSH operates on **port 22**.

Third-Party Tools

Many third-party tools can provide a quick, reliable, and efficient way to connect to computers.

Screen Share Feature

One common feature that most third-party remote access tools include is screen sharing. A screen sharing feature allows a technician to **view the client's screen** and see exactly what they are seeing.

File Share

File sharing is another feature that comes in handy when working on a remote computer. File sharing allows for **files from one device to be moved** to the other remote device.

Security Considerations

When considering which remote access option to use, it's vital to consider the security ramifications. For example, leaving a telnet port open can create security vulnerabilities. When using third-party tools, it's best to ensure they offer **multi-factor authentication** so that only legitimate users can gain access to the devices remotely.

How to Prepare for Questions about Security on the CompTIA A+ Core Series 1002 Test

General Information

Both the previous and current (2019) versions of the CompTIA A+ Core Series 1002 test devote an entire section of the study outline to this topic. There's a lot to know and study because around one-fourth (**24%**) of the questions are **security-related**. Half of these questions will probably begin with a **scenario.** This is designated by the note (*scenario*) beside the affected headings, below.

Physical Security

When thinking about cybersecurity, it's sometimes easy to forget what an **important role** physical security plays in keeping digital data safe. Physical security is important because no matter how many security measures you put in place on a device itself, physical security is the only thing that will stop a criminal from walking away with the entire device.

Mantrap— A mantrap is exactly what it sounds like. It's a trap used to prevent infiltration methods such as tailgating and piggybacking. A mantrap is a **small area with a set of two locked doors** and it separates the outside world from a secured area. When entering, an individual will enter through the first door, but that door must then be closed behind them before the second door may be opened.

Badge reader— Badge readers can be implemented to help prevent unauthorized access. In this type of environment, employees are given badges such as **proximity cards** or **smart cards**. When the employee scans the badge, he or she is allowed entry to the area.

Smart card— Smart cards are cards that are typically the size of your driver's license or credit card. The **embedded memory and chipset** in these cards can store **identification and authentication** information. A smart card can also be programmed to use as a cash card that is seen in many organizations where employees may use their employee badge to purchase lunch in an onsite cafeteria.

Security guard— Security guards are one of the few security controls that are considered not only preventative controls, but also deterrent controls and detective controls. This is because organizations with **onsite security staff** are less likely to be targeted for attacks than those with no security guards.

Door lock— Door locks should always be utilized whenever possible. Aside from locks preventing unauthorized **entrance to the building**, locks should also be utilized to protect **rooms containing sensitive equipment** (such as the server room or network closet).

Biometric locks— Biometric locks can add an additional layer of protection to an organization's physical security. Smart cards and proximity badges can be lost and possibly wind up in the wrong hands. Biometric locks **use an individual's features**, such as their retina or fingerprints, to authenticate them.

Hardware tokens— A hardware token is a physical device that **stores authentication information**. One example of a hardware token is an **RSA key fob**. These hardware tokens randomly generate numbers that can be paired with usernames and passwords for added security.

Cable locks— Cable locks can be used to help prevent a thief from walking off with laptops. A cable lock is used by looping the cable around a heavy (preferably immovable) object and then securing the lock to a small security hole on the side of the laptop.

Server locks— Due to their important role within organizations, servers should never be left vulnerable to a physical attack. Not only should the **server room** be locked when not in use, but the **rack in which the servers are located** should also be locked.

USB locks— Many attacks can be delivered via an unsecured USB port on a server, laptop, or desktop. USB locks are small locks that plug directly into open USB ports and **prevent unauthorized access**.

Privacy screen— Privacy screens are screen covers that go on your phone, tablet, monitor, or laptop screen. These screens make it very hard to see what is happening on the screen unless you are sitting directly in front of it. This **prevents shoulder-surfing**, which is the act of spying on another person's screen to collect information.

Key fobs— Key fobs are small security devices that **store authentication information**.

Entry control roster— An entry control roster is a document kept by a security guard that has a **record of all the individuals who have entered and left the building**. This is often used in conjunction with mantraps.

Logical Security Measures

Unlike physical security controls that you can see and touch, logical security controls are items such as **security policies** and **software safeguards** that are used to protect our systems. You should be able to explain these.

Active Directory

Active Directory (AD) is the **Microsoft® directory** used to manage users, applications, computers, and much more. AD can be used to **help implement security measures** across your organization.

Login Script

A login script can be thought of as a series of **instructions given for a device to perform** upon login. Login scripts can be set on the profile tab of a user in AD. Login scripts can be used to map network drives, log computer access, gather information from a computer, and much more.

Domain

Ensuring that **all computers in an environment** are in your domain helps to ensure that they will be given the proper security policies. When a computer is in your domain, you'll be able to see it and manage it within AD.

Group Policy/Updates

Group policies can be extremely useful in **securing an organization**. Group policies can be used to set password policies, block unwanted applications, and even block access to the Internet entirely in some cases. They can also be used to push out security updates, which are important to keep an organization safe.

Organizational Units

Organization units (often referred to as OUs) are **subdivisions of your domain** within active directory. For example, if the organization ACME Corp had three separate locations, they may choose to have three organizational units within their domain.

Home Folder

A home folder can be set for each user in AD. If the home folder doesn't exist when it's added in AD, then AD will create the folder and set the permissions for you. By default, this folder can be **accessed only by the user and the domain administrators**. Home folders should be used by folders to store their files on the server. Because computers can be lost or stolen, it's best for users to store their documents on the server in this way rather than store them locally on their own machines.

Folder Redirection

Folder redirection allows administrators (and in some cases users) to redirect the path of a specific folder to a **new location**. One popular implementation of this is to redirect a user's Documents folder (that is stored locally on his or her machine) to a network location, such as the Home folder.

Other Methods

There are other methods to ensure security. Here are some of them.

Software Tokens

Software tokens are **similar to hardware tokens**, except they come in the form of either a piece of software on your laptop or an app on your mobile device.

MDM Policies

Mobile device management (MDM) policies are used to **enforce security measures on mobile devices** such as cell phones and tablets. Many organizations require that their users access email or other business related apps on their phone, but this can present security risks to the organization. MDM policies can help offset some of the risk. An example of an MDM policy would be an organization requiring anyone accessing business email or business apps to have a lock screen on their phone with a PIN.

Port Security

To **prevent unauthorized devices from forwarding traffic**, port security should be used. There are a number of different options when implementing port security. For example, you can define the maximum number of MAC addresses that can be used on the port.

MAC Address Filtering

MAC address filtering, or simply MAC filtering, is a method in which **only devices with specific MAC addresses are able to send data** on the network. If a device tries to connect to a network and it doesn't have one of the agreed up on MAC addresses, it will not be permitted to join the network.

Certificates

Digital certificates help users **know when they are accessing a trusted website**. Digital certificates are signed by a trusted certificate authority (CA). The CA can ensure that the public key you are getting from a website is actually from the web server and not an attacker.

Antivirus/Anti-malware

Users should never be allowed to browse the Internet without an antivirus/anti-malware program. While it's important to note that antivirus and anti-malware programs are not able to prevent all malware, they do **prevent a large number of attacks**.

Firewalls

Firewalls should be used by organizations as a first layer of defense for their networks. Firewalls come in many different types including packet filtering firewalls, proxy firewalls, and stateful inspection firewalls. At the most basic level, firewalls allow for the creation of rules, known as **access control lists**, which specify the types of packets that are allowed and disallowed. Firewalls come as both **hardware** and **software** devices. They can be standalone or part of another network device such as a router or a switch.

User Authentication

User authentication is the cornerstone of any organization's security. Physical security and firewalls won't help you if a user's password is Password123. Security policies that enforce users to choose **strong passwords** should be created. Many organizations now require users to choose passwords that are at least 12 characters and contain both symbols, numbers, and multi-case letters.

Multifactor Authentication

Even the strongest passwords can be compromised. This is where multi-factor authentication comes in. Multi-factor authentication (commonly referred to simply as MFA) requires two or more *different* authentication types. Authentication types are typically broken down into categories such as **something you know** (password, PIN, security question), **something you have** (authenticator, token), and **something you are** (biometrics). Because MFA requires two or more different *types* of authentication, a user would not be able to use just a PIN and a password, since they both fall into the category of something you know. Rather, the user would need a combination such as a password and a token.

Directory Permissions

Not all users within an organization should be given access to all data that the organization has stored. For example, a customer service representative will most likely not require the same level of access as the Chief Information Security Office (CISO). In order to restrict users from accessing data they should not see, directory permissions should be used. Directory permissions **allow administrators to control what level of access a user should be given** on a per directory level. Some of the permission types include full control, modify, and read.

VPN

Virtual private networks (VPNs) are extremely useful for organizations that allow users to work **remotely** and also **multi-location organization**. For organizations where employees work remotely, it can be set up so that a user is able to connect securely to the organization's network via a client VPN. For organizations that have multiple locations, site-to-site VPN tunnels can be configured to expand the network across all of these locations.

DLP

Data loss prevention (DLP) is the practice of preventing unauthorized data from leaving an organization. Sensitive data can be leaked either intentionally or unintentionally. Regardless of the cause, the ramifications can be severe. DLP methods can't prevent data loss entirely, but they are used to **reduce the chances of data leakage** wherever possible. .

Access Control Lists

Access control lists are used to specify which traffic should be allowed through a firewall and which traffic should be blocked. Using access control lists, **traffic can be blocked or allowed** based upon a number of items including source or destination port as well as source or destination IP address.

Smart Card

Smart cards are typically the size of your driver's license or credit card. The embedded memory and chipset in these cards can store identification and authentication information. Smart cards can also be programmed to use as a cash card that is seen in many organizations where employees may use their employee badge to purchase lunch in an onsite cafeteria.

Email Filtering

Spam is a common way to spread malware. Even when spam doesn't contain malicious links and attachments, it still clutters up user inboxes, making them less productive. Organizations can **reduce the amount of spam** received by implementing an email filter. Email filters can **review messages** both inbound and outbound. In some cases, email filtering can also check outgoing email messages for **sensitive data**, therefore helping with DLP.

Trusted and Untrusted Software Sources

Because end users may not be as well-versed in what programs are legitimate and which are not, software installations should always be reviewed by an administrator. A user may believe they are downloading a trusted program, but it could turn out to be malware. By disallowing user installations and **requiring administrator approval**, this scenario is less likely to occur.

Principle of Least Privilege

Permissions should only be given to a user if they absolutely need them to complete their job. This idea is known as the principle of least privilege. The **fewer users who have access** to sensitive files, the less likelihood that something will happen to those files.

Wireless Protocols and Authentication

Wireless networks are inherently less secure than wired networks. However, there are **several methods** that can be used to secure wireless networks.

Protocols and Encryption

WEP— Wired Equivalent Privacy (WEP) was one of the first attempts at securing wireless networks. WEP **should not be used today** because it contains a flaw that makes it very vulnerable to attackers.

WPA—Wi-Fi Protected Access (WPA) is a **more secure** option than WEP, as it used TKIP.

WPA2— Wi-Fi Protected Access 2 (WPA) improved upon WPA by using the Advanced Encryption Standard (AES). WPA2 is **the standard that should be used today** for securing wireless networks.

TKIP— The Temporal Key Integrity Protocol (TKIP) provides a new encryption key for every sent packet. TKIP helped improve WPA and make it more secure than WEP, but it was found that TKIP **also has its own vulnerabilities**.

AES— AES, which stands for Advanced Encryption Standard, is a **secure encryption method that is still used today**. WPA2 uses AES in order to secure wireless networks.

Authentication

Wireless networks should never be left open, and they should always require some form of authentication. Let’s look at a few wireless authentication methods.

Single-factor— Single-authentication requires that the user only provide **one form** of authentication. It’s common to see wireless networks that only require a pre-shared key to join the network. This is an example of single-factor authentication, and it is considered to be a **weak** authentication method.

Multi-factor— Multi-factor authentication requires a user to provide **more than one authentication type** as discussed earlier in this study guide. A common implementation of multi-factor relating to wireless authentication is the **Extensible Authentication Protocol-Transport Layer Security** (EAP-TLS), which requires the user to not only have a password but also a certificate installed on the computer.

RADIUS— **Remote Authentication Dial-In User Service** (RADIUS) is an authentication method used to allow for centralized authentication and accounting. Although it gets its name from the days of dial-up Internet, RADIUS is now the **common method used** to authenticate over VPNs and wireless networks.

TACACS— TACACS and TACACS+ were originally developed by Cisco®, but were released as an open standard. These protocols are used for the authentication of users on network devices such as **routers** and **switches**.

Malware (*scenario*)

To succeed on questions about malware, you should be able to **evaluate** a given scenario, **find** malware, and **remove** it with effective tools and procedures. You should also know how to **prevent** malware in the future.

What Is Malware?

The term malware is used to describe any malicious software that includes (but is not limited to) **trojans, spyware, viruses**, and **worms**. Let's take a deeper look at some of the different types of malware that exist today.

Ransomware

Ransomware was given its name because it essentially holds your files and data ransom until you pay the attacker. As the popularity of **cryptocurrency** (such as **bitcoin**) has grown, so has ransomware. This is because now attackers can request bitcoin as their method of payment to release the data after a ransomware attack making the attackers more difficult to track down.

Trojan

Trojans are **malicious programs** that **disguise themselves as valuable programs**. Imagine a scenario where a user downloads a program that they believe will allow them to listen to music or watch a movie for free. They download the program because they believe it to be a valuable and legitimate program. However, when they go to run the program, they have actually installed malware on their device. This is an example of a trojan.

Keylogger

Some attacks will try to install keyloggers onto a user's computer in order to steal private data, passwords, or credit card numbers. Keyloggers come in both hardware and software forms. A keylogger will **track all of the keystrokes** made on the computer running the keylogger. This information can then be transmitted over to the attack for them to parse looking for useful stolen information.

Rootkit

Rootkits are malicious programs with the goal of gaining privileged access to a computer. Rootkits hide themselves by **taking advantage of operating system functions**, and they can attack operating systems, hypervisors, and firmware.

Virus

A virus is defined as any malicious program that **replicates itself and attempts to infect** other computers. Viruses, unlike worms, need human interaction to spread. They are only able to replicate to other drives on the same computer and not across the network. Viruses could have many different goals from corrupting data to stealing information.

Botnet

When an **attacker gains full control of a system** and they plan to use that system to carry out other attacks (such as a DDOS attack), that computer becomes a **bot**. The infected computer is essentially a zombie, as it's no longer under the control of its owner, but rather it is under the control of the attacker. A **botnet** is a large group of these bot computers that can be used to carry out various attacks such as sending **spam** or performing a **denial-of-service attack**.

Worm

A worm is similar to a virus. The feature that separates a worm from a virus is that a worm can **replicate itself without any user intervention**.

Spyware

Spyware is a type of malware that covertly **collects data on a user** after it is installed on their computer.

Tools and Methods

Antivirus

Many threats described above can be mitigated simply by having an antivirus program installed. Antivirus is made up of **two main components**, the antivirus **engine** and the antivirus **database**. The antivirus engine is responsible for real-time scanning. The antivirus definitions database is a repository of signatures used to detect known malware.

Anti-Malware

Anti-malware software is extremely similar to antivirus, but it takes the detection a step farther. Anti-malware software can usually **check files outside of the windows file systems** such as those on malicious websites and those coming in via email.

Recovery Console

Windows offers a **suite of built in recovery tools** known as the Windows® Recovery Console. This console can be especially helpful if a computer has been infected by malware. Some of the tools in the recovery console will allow you to reset the operating system back to default or simply restore the computer to an earlier time (such as before the computer become infected.)

Backup/Restore

Sometimes, an attack occurs and the only way to resolve the issue and remove the risk is to completely **wipe the computer and start fresh**. When this happens, users may lose all of their data on the hard drive. Losing data can be a huge burden for an organization. This is where backup/restore comes in. Important files should always be backed up. In cases of ransomware, files may be encrypted and deemed unusable. Rather than pay the attacker to restore your data, you could simply reformat those devices and restore the data that you have backed up.

End User Education

While there are plenty of wonderful tools out there to help protect against attacks, end user education is one of the most important. This is because antivirus software and spam filters are not perfect. It is **important for users to understand** what types of items they should download and not download, what types of websites they should not visit, and how to identify a phishing scam.

Software Firewalls

When referring to software firewalls in this section, we are referring to firewalls that come as **part of the operating system**. Windows® computers come with a built-in software firewall called Windows® Defender Firewall. This firewall can help prevent against worms and malicious inbound connections.

DNS Configuration

One way to **prevent users from navigating to malicious URLs** is to implement a **filtered DNS** service. When filtered DNS is configured and a user tries to access a malicious URL they will receive a page stating that the content is not reachable due to a policy that was put in place.

Social Engineering, Threats, and Vulnerabilities

You should be able to compare and contrast different types of threats, social engineering, and vulnerabilities when taking this test. Following are details about these issues.

Social Engineering

Social engineering is the fraudulent act of manipulating individuals into giving you unauthorized access to a building or room, or giving you private information.

Phishing— Phishing is the most common type of social engineering. In a phishing attack, the attacker sends a **fraudulent email** pretending to be from a legitimate source such as a colleague, vendor, or even a user's bank. The goal of a phishing attempt is to get the unsuspecting user to **give up their private information**.

Spear Phishing— A spear phishing attack is a **targeted phishing attack**. In most phishing attacks, the phishing email will be sent out in bulk hoping to get users to bite. In a spear phishing attack, the attacker has done research on the target and has crafted a phishing email specifically for them.

Impersonation— One common social engineering tactic is impersonation. Social engineers will often pretend to be someone else **to gain access** to what they are looking for. One example of this would be an attacker pretending to be from your Internet provider asking for access to your network closet.

Shoulder Surfing— Shoulder surfing is the act of stealing a person's data by **looking over their shoulder as they type** in private information on a computer or a code into a door or ATM.

Tailgating— Social engineers will sometimes "tailgate" or **follow another person into a building**. This means sneaking into a locked door right behind a person who has permission to enter. Sometimes, the social engineer may carry boxes so that an individual, who is just trying to be polite, will unlock and hold the door open for them.

Dumpster Diving— Businesses and individuals throw away a lot of valuable information that can be used by an attacker. When an attacker **digs through the trash** hoping to find private information that wasn't shredded, this is known as dumpster diving.

Other Concepts and Considerations

DDoS

A distributed denial of service (DDOS) is a denial of service attack in which multiple **computers** (often a botnet) are used to **send an abundance of traffic** in an attempt to bring down a network's resources.

DoS

This refers to a denial of service attack in which a large amount of **meaningless traffic is sent** in an attempt to overburden and bring down a device or network.

Zero-Day

A zero-day attack is one that **targets a vulnerability** for which developers have not had time to release a patch for or fix yet.

Man-in-the-Middle

A man-in-the-middle (MiTM) attack is an **eavesdropping** attack. The attacker will try to plant himself/herself between two systems and intercept the traffic.

Brute Force

In a brute force attack, the attacker will **attempt to guess** as many of the possible values as they can. Brute force is generally used as a method of password cracking, but can be used in some other scenarios as well.

Dictionary

One form of a brute force attack is known as a dictionary attack. Rather than the attacker trying to come up with passwords to guess themselves, they can **use a list of all leaked passwords** online (known as a dictionary) and try them instead.

Rainbow Table

A rainbow table is a **database of a plaintext passwords** and their corresponding hash values. This can be used in a brute force attack.

Spoofing

Spoofing is a form of an **impersonation** attack. Some commonly spoofed items include source IP address, source MAC address, source email address, and usernames.

Non-Compliant Systems

Non-compliant software or systems can pose a threat to an organization's network. It's important to fix non-compliant devices as soon as you notice them.

Zombie

A zombie is another word for a **bot**. This is a computer that has been taken over by an attacker and can be used for malicious activities.

Microsoft Windows® OS Security

Microsoft Windows® provides useful settings that can be used to enhance security. It is important that you know their names and how they are used.

Users and Groups

As mentioned previously, users will not all require the same level of access control. **Windows® permissions** is a critical part of access control.

Administrator— Administrator accounts should be reserved for those who absolutely require them. The more administrators that exist on a network, the more room for error. An administrator will have **access to everything**.

Power user— A power user account is one step down from an administrator account. It is the **second most powerful** account type within the Windows® operating system.

Guest— The guest account on Windows is an account that exists on every Windows® machine. It's a very low-privilege account that can be used for individuals who only need occasional access to the device.

Standard user— Most users will fall into the standard user category. A standard user will have varying permissions based upon roles and groups set by the administrator.

NTFS vs. Share Permissions

NTFS should be used whenever possible as it will provide the most control over data resources. NTFS is the New Technology File System. The advantage of using NTFS permissions over share permissions is that they are applied to both local users and network users and that they are based on the permissions granted to an individual user at the Windows® logon. Share permissions are not applied to users who log in locally to the machine.

Allow vs. Deny

It's possible to allow and deny access to individual resources. Generally, **deny permissions will take precedence over allow permissions**. Also, permissions that have been added directly to an object will override **inherited permissions**.

Moving vs. Copying Folders and Files

When a file is moved or copied, **permissions propagation** is the process that Windows goes through to decide which permissions should be applied to files that were moved or copied. It is important to remember that just because a folder has been moved or copied to a new location, it will not always inherit the new location's NTFS permissions.

File Attributes

It's possible to encrypt individual files and folders on a computer using the **Encrypted File System (EFS)** that is built into professional versions of Windows. This can be done from the Advanced Attributes dialog box for the files and folders.

Shared Files and Folders

Sharing files and folders can be an easy way to collaborate with others. However, it's important to be aware of the security concerns that come along with it.

Administrative Shares vs. Local Shares

Windows has some shares that are built in by default. These shares are known as administrative shares. These shares, such as **C$**, are built in to allow administrators access to these resources despite how they are accessing them (locally or remotely). On the other hand, any share that is created manually is known as a *local share*.

Permission Propagation

When files or folders are copied or moved, Windows has to go through the process of determining which permissions should be assigned to them in their new location. This process is known as permissions propagation. There are many factors that influence this process, such as whether the file is being copied or moved and whether this is happening within one NTFS-based volume or between two NTFS-based volumes.

Inheritance

Rather than needing to specify permissions on each and every file and folder, administrators can configure inheritance. Inheritance allows files and folders within another folder to inherit the permissions of the top level folder.

Other Topics

System Files and Folders

A system file or folder is an object which Windows or some other program has deemed **crucial** to the overall function of the operating system. These files will have the system attribute toggled on.

User Authentication

Users may authenticate in a number of different ways to access a company's resources. **Single sign-on** is one method of authentication in which the user only needs to authenticate once to have access to all of the resources.

Run as Administrator vs. Standard User

When a user wants to run a program that requires an administrator to run, they'll receive a UAC (user access control) pop-up. This pop-up will **request an administrator password** before the program will run. UAC can be beneficial as it forces an administrator to approve a program before it is run or installed. This can come in handy when users who are not particularly tech savvy try to download or run programs that might end up being malicious.

BitLocker®

BitLocker® is a program that offers full **drive encryption**. It is available on Windows Ultimate® and Enterprise® versions as well as Windows 8/8.1 Pro®. Unlike EFS, which encrypts individual files, BitLocker® encrypts the entire drive. BitLocker® relies on the computer having a **Trusted Platform Module** (TPM) chip to function.

BitLocker To Go®

BitLocker To Go® is an encryption method like BitLocker® that allows you to encrypt **removable/portable drives** such as external hard drives and USB drives. Unlike the full version BitLocker® , BitLocker To Go® does not require a TPM chip.

EFS

The **Encrypting File System** (EFS) is a feature that is available in professional versions of Windows. EFS makes it possible to encrypt individual files and folders with just the click of a button. EFS can be configured in the Advanced Attributes dialog box of a file or folder.

Workstation Best Practices (*scenario*)

During the test, you will need to be able to take a given scenario about a workstation and develop appropriate security measures on a “best practice” level to optimally secure that workstation. Here is some information concerning this.

Password Best Practices

Passwords are one of the **first lines of defense** against an attacker. It’s important to set **strong** and **memorable** passwords.

Setting Strong Passwords

There are many different opinions on what constitutes a strong password. The definition will most likely change depending on who you ask. The standard rule, however, is **at least eight characters, containing letters, numbers, and symbols**.

Password Expiration

Users should be **required to change their password** at regular intervals. This is enforced using a password expiration policy. Common intervals are every 30, 60, or 90 days.

Screensaver Required Password

For individuals who use screensavers, it’s a good idea to set a screensaver password. This will require a password to reenter your computer after the screensaver has come up. The screensaver then becomes similar to locking the computer.

BIOS/UEFI Passwords

BIOS/UEFI passwords can be set to prevent individuals from gaining unauthorized access to the BIOS configuration.

Requiring Passwords

Passwords should **always** be required. The user should never be able to access his or her computer without using a password. The requirement of passwords, as well as the password expiration and password complexity, should be specified in a **password policy**.

Account Management

Administrators are in charge of ensuring the security of workstations using various policies.

Restricting User Permissions

Organizations should always use the **Principle of Least Privilege**. This means that users should only be given access to the resources that they need in order to complete their jobs and nothing more. Having strong permissions helps to prevent unauthorized access whether intentional or accidental.

Logon Time Restrictions

If your organization only has users working **between certain hours of the day** (for example: between 9 a.m. and 5 p.m.), one good security restriction to put in place is logon time restrictions. It's possible to put policies in place that restrict users from logging into a computer outside of their normal working hours.

Disabling Guest Account

The Guest account on Windows® machines is a **low-privilege account** for guest users. If this account will not be used, it's best to **immediately disable** it. Even though it is a low-privilege account, **attackers have ways to escalate privilege** if they are given access to a machine.

Failed Attempts Lockout

A common **way to combat brute force password attacks** is to implement a lock out policy. After so many failed attempts at logging in, the account will become locked out and an administrator will have to unlock it.

Timeout/Screen Lock

Leaving a computer unlocked while you are away is dangerous. Any person can come up and begin working on your computer without your knowledge. For this reason, organizations should implement screen lock or screen timeout policy. This policy would **force the computer to lock after a few minutes of inactivity**.

Change Default Admin User Account/Password

Default passwords should never be used in any circumstances. It's best to **immediately change** default passwords or **disable default accounts** all together and create new accounts.

Basic Active Directory Functions

Active Directory Users and Computers (ADUC) is a great place to **manage user accounts**. Let's look at some basic functions of ADUC.

Account creation— When creating an account in ADUC, you can configure the account with many different options. You will have to create the password. You can choose to force the password to be changed upon the first login.

Account deletion— Organizations should have a policy to delete **old accounts** when they are no longer needed.

Password reset/unlock account— When a user believes that a password has been compromised (or has been forgotten), the password may be reset from Active Directory. You can also unlock an account that has been locked out from Active Directory.

Disable account— Sometimes it is a better choice to disable an account, rather than delete it. For example, if an organization has seasonal employees, they may choose to disable the seasonal employee's credentials while they are off season rather than delete the entire account.

Disable Autorun

Certain programs or discs will run immediately when put into the computer. It is best practice to disable the autorun and autoplay features on the operating system. This is because it gives you **time to evaluate** the item before allowing it to run on the PC.

Data Encryption

Data encryption, whether through BitLocker®, EFS, or another method, is a great way to protect your data. Data encryption ensures that your **data is protected** in the event of a lost or stolen computer.

Patch/Update Management

Operating systems and other software push out updates or patches whenever vulnerabilities that need to be fixed are found. It's **crucial to a computer's well-being** that these patches are installed. Organizations will typically use some third-party program for patch and update management.

Mobile Device Security (*scenario*)

Mobile devices have become an important part of business as we know it. Employees are expected to be available at all times via their phone. But with the new wave of mobile devices in business, organizations must consider the risks.

Screen Locks

When a user has access to business resources via a mobile device, it's necessary to ensure that the mobile device is **just as secure as a workstation** would be. This means having a lock on the screen so that if the phone is lost or stolen, attackers don't have access to the business resources.

Fingerprint lock— One method of screen locking is a fingerprint lock. Fingerprint locks use biometrics. In order to access the phone, the user must scan his or her fingerprint.

Face lock— A face lock is another form of biometrics. Essentially, the screen is able to recognize the user's features and only unlock if his or her face is visible.

Swipe lock—Swipe locks use a pattern created by the user to lock the screen. The individual must know the pattern to unlock the device.

Passcode lock— Finally, one of the most common screen lock options on a mobile device is the passcode lock. The passcode is usually 4 to 6 numbers. The individual must know the code to unlock the device.

Remote Actions

Often, a user must consent to give the organization remote administration over their mobile device if they want to be able to access the organization's resources from their mobile device.

Remote Wipes

Organizations are able to remotely wipe devices after they were given remote administration control. This is useful if a user reports that their phone has been lost or stolen.

Remote Backup Applications

Some organizations may choose to remotely backup the mobile devices that store data. Because mobile devices are typically used during travel, they are more likely to be lost or stolen.

Locator Applications

Locator applications can help individuals find their devices if they have been lost or stolen. These applications use GPS technology. The location services on the device must be turned on for these applications to work.

Authentication

Authentication is just as important on mobile devices as it is on standard computers and laptops. Let's look at some of the types of authentication.

Biometric Authentication

Biometric authentication is a common method for securing mobile devices. Biometrics include items such as face scans, fingerprint locks, and retina scanners.

Multi-factor Authentication

Multi-factor authentication (MFA) can be used to access applications on mobile devices in the same way that it's used to protect data on computers. MFA requires at least two different types of authentication. For example, when MFA is in use, an individual may be required to use a password and an authenticator app.

Authenticator Applications

Early in this guide we discussed hardware authenticators. Usually, hardware authenticators come in the form of tokens that are only used for authentication. However, mobile devices can also be used as an authenticator. They are **more convenient** because then users are not required to carry multiple devices for authentication.

Other Methods

Failed Login Attempts Restrictions

In the same way that you can lock a user's account on a computer, you can lock an account on a mobile device. Mobile devices should lock the ability to log in after so many failed attempts.

Antivirus/Anti-Malware

In the same way that you would protect your computer from viruses and malware using antivirus and antimalware software, you can download mobile antivirus and antimalware applications. There are not as many providers for mobile antivirus and antimalware as there are for computers but the market is growing.

Patching/OS Updates

Whenever an update is available for a mobile device, it should be installed. Applications on the phone should also be kept up to date. When vulnerabilities are found, developers will put out updates to fix the vulnerabilities. This is why devices must be kept up to date.

Full Device Encryption

Mobile devices can also be encrypted to protect the data that is stored on the device. This adds another layer of protection in the case that the device is lost or stolen.

Trusted Sources vs. Untrusted Sources

Software and applications can come from trusted sources or untrusted sources. Users should never download applications from untrusted sources. An application of this sort may be a malicious program disguised as a useful one.

Firewalls

A mobile firewall acts as a screen between mobile devices and an organization's network. It will monitor all inbound network traffic before it is allowed to access the network system.

Policies and Procedures

Policies should be put in place by an organization so that users understand exactly how to use mobile devices on the organization's network.

BYOD vs. corporate-owned— Corporate-owned devices are completely under the control of an organization. In this scenario, the organization can specify policies about which applications can be installed as well as what the device can be used for. However, many organizations are moving to a Bring Your Own Device (BYOD) environment. BYOD environments are most complicated to manage because while policies can be put in place for accessing corporate resources, ultimately the device is owned by the end user.

Profile security requirements— When accessing an organization's resources, users must meet all profile security requirements set forth by the organization.

Data Destruction and Disposal (*scenario*)

As discussed earlier in this guide, dumpster diving is a method of obtaining private information or data from the trash. Let's look at how to properly dispose of computer equipment.

Physical Destruction

One of the only ways to ensure that data is no longer accessible is to completely destroy it.

Shredder— To prevent dumpster divers from stealing private information, organizations should have a shredding policy in place to shred **all documents** before throwing them in the trash.

Drill/hammer— **Destroying a hard drive** with a drill or hammer is one of the only ways to ensure that an attacker is unable to retrieve data from the device.

Electomagnetic (deguassing)— Using an electromagnet is one way to wipe a hard drive. However, it's often still possible for individuals to pull data off of a hard drive even though it's been wiped. One wipe using a magnet is not enough. This process **must be done over and over** again.

Incineration— Some organizations may choose to completely incinerate their devices to ensure that data can not be pulled off of the devices.

Certificate of destruction— When an organization uses a **third party vendor** to dispose and destroy their devices, they may receive a certificate of destruction stating that the items have been recycled and all data storage components have been wiped or destroyed pursuant to all applicable laws including environmental and waste management regulations.

Recycling or Repurposing

Rather than destroy the devices, many organizations will take the route of recycling or repurposing the devices.

Low-Level Format vs. Standard Format

A standard format simply removes all of the data from the device. This should **not be used in the event that the device contained extremely sensitive data** as it may be possible to retrieve the old data with the right equipment.

Overwrite

An overwrite would simply be completely reformatting the device with a **new operating system**.

Drive Wipe

There are many different tools that can be used to wipe a drive such as software and magnets. It's important to always wipe a drive **multiple times** to ensure that the data is not easily retrieved.

Wireless and Wired SOHO Security (*scenario*)

It will also be important for you to be able to consider a scenario about a Small Office/Home Office (SOHO) and devise best practice security measures for that environment, whether it is wired or wireless.

Wireless-Specific

There are some security measures specific to wireless networks. Let's take a look at some of these items.

Changing Default SSID

Keeping the default SSID can provide a potential attacker with information they need to target you. For example, the default SSID may show exactly what type of wireless device you are using. It's best to change the SSID before you begin using the wireless network.

Setting Encryption

Setting wireless encryption secures your wireless network with an authentication protocol. Wireless encryption will **require both a password and an encrypted key** when you connect. The encryption key can generally be located in the setup page of a wireless router.

Disabling SSID Broadcast

Disabling the SSID is one way to prevent attackers from finding your wireless network. It adds a **few extra steps** for getting yourself and other users connected to the network, but it does add that **additional layer of protection**. Experienced hackers will still be able to locate hidden networks, but generally attackers go after the low hanging fruit.

Antenna and Access Point Placement

Ideally, when setting up a wireless network, you want the network to span your entire building or workspace, without leaking outside of your organization. It's a difficult task to do perfectly, but this can be achieved by doing wireless network surveys and ensuring that your antennas and access points are placed in the right locations.

Radio Power Levels

By lowering the radio power levels, you can ensure that the wireless device isn't broadcasting the signal well outside of the necessary range for you organization.

WPS

WPS , which stands for Wi-Fi Protected Setup, was created to make setting up wireless networks easier for the average user. However, it has a built-in flaw that makes it extremely **vulnerable to attacks**. It is best practice that, if you purchase a wireless router with WPS, you should immediately ensure that it is turned off.

Additional Actions

Change Default Usernames and Passwords

It is very easy to do an online search and find the default usernames and passwords of wireless devices. When setting up a wireless network, ensure that the default passwords are not being used.

Enable MAC Filtering

MAC Filtering is the concept of only allowing specific MAC addresses to connect to the wireless network. By only allowing specific MAC addresses to connect, you are able to prevent unauthorized devices from connecting as well. While this can reduce the likelihood of an attack, it is possible for attackers to spoof a MAC address so it's **not a perfect solution**.

Assign Static IP Addresses

It is generally a good idea to set a static IP address on your wireless router so that, in the event of an Internet outage or power outage, the IP address will not change when the device is back online.

Firewall Settings

Many wireless routers today have built-in firewalls. These settings can be configured in the management console of the device.

Port Forwarding/Mapping

Port forwarding/mapping can be configured on a wireless device in the same way that it can on a wired network.

Disabling Ports

Disabling **ports that are not in use on the wireless router** can prevent unauthorized parties from plugging in and gaining access to the entire network.

Content Filtering/Parental Controls

Some wireless routers will come with built-in content filtering and parental controls. These can be used to block users from navigating to sites that could contain malware.

Update Firmware

Just like any other device that we've talked about, the firmware on a wireless device should be kept up to date. Whenever the latest updates are not installed on a device, that device is susceptible to attacks.

Physical Security

Physical security of wireless devices is just as important as the physical security of wired devices. While it may not be feasible to lock all of the wireless access points in the server room, the devices should be **locked down** so that an unauthorized individual can't access them.

How to Prepare for Questions about Software Troubleshooting on the CompTIA A+ Core Series 1002 Test

General Information

When a software program doesn't perform correctly or adequately, the user will turn to the tech person—that's you. You'll need to know how to determine what is wrong and devise an action plan to get things back up and running. Approximately one-fourth (26%) of the questions on the CompTIA A+ Core Series 1002 test address software troubleshooting, so you'll need to be familiar with all of the concepts in this study guide. *All* software troubleshooting questions will begin with a scenario.

Problems with Microsoft Windows OS (*scenario*)

Many organizations utilize Microsoft Windows as their operating system of choice. This means that, as a tech, you should be able to **troubleshoot** issues with the Windows OS and quickly identify common problems.

Common Symptoms

It's important to be able to recognize common symptoms in the Windows OS and quickly determine **how to best resolve** the issue. Let's look at several common symptoms that we see when there is an issue with the Windows OS

Slow performance— One of the most common reports that techs hear from end users is that their computer is running "slow." Unfortunately, this can mean different things for each user. When users tell you that their computer is running slower than normal, it's important that you **ask for specifics**.

Limited Connectivity— Limited connectivity is a type of **network issue**. Essentially, the computer is able to see the network, and even partially connect to it, but there is an issue with that connection. For example, if a computer connects to a network but doesn't receive IP address information from a DHCP server, it will show the limited connectivity message.

Failure to boot— A failure to boot occurs when the computer is **unable to load the operating system**. One type of failure to boot is "No OS found."

No OS found— No OS found is a specific **type of failure to boot**. No OS found occurs when the computer is **unable to locate OS files**. This can be either because the storage devices do not contain any OS files, or the **boot configuration** loader is pointing to the wrong partition.

Application crashes— It is not uncommon for applications to crash on a computer and there are many different causes for these crashes. When an application crashes, the user may see the application **close unexpectedly** or simply "**freeze**." If the application freezes rather than closes when it crashes, it may be necessary to **end the task** in Task Manager.

Blue screens— A blue screen, or more commonly known as **BSOD (blue screen of death)**, is a **proprietary crash screen** on Windows OS. A BSOD that occurs during the initial boot sequence could be caused by bad hardware, drivers and/or bad applications. Since a BSOD can be caused by many different things, technicians will need to do research on the **specific error message** given during a BSOD.

*Black screens— Black screens are similar to blue screens, but they are usually caused by an **error at POST**. When a black screen occurs, the best course of action is typically to attempt to **reboot** into Safe Mode or last known good configuration.

Printing issues— Printers are a great resource for users, but they don't come without their own set of problems. Printing issues can range from **not being able to print at all** to **printing only gibberish**. Printing problems can be caused by **driver** issues, **network** issues, and even physical **hardware** issues.

Services fail to start— Services are the backbone of our computer. Sometimes, necessary services do not start when the computer loads. Services can be stopped, started, and restarted in the **services menu** and can be also be viewed from **Task Manager**. When a service associated with a specific application won't start, it might be time to consider **reinstalling** the application.

Slow boot-up— If a system is taking longer than normal to boot, this could be caused by a myriad of circumstances. The hard drive may be experiencing **errors**. In this case, running a **defrag** could be beneficial. Slow boot-ups can also be a symptom of faulty or outdated **hardware**.

Slow profile load— A profile that takes a long time to load can be a result of having **too many applications** load at startup. It could also be a result of **insufficient hard drive space** or memory.

Common Solutions

In the above section, we have discussed some of the common symptoms of computer issues. Below, let's look at some common solutions to these problems.

Defragment the hard drive— Disks can become fragmented as files are created, deleted, and modified over time. Defrag **realigns all the file fragments into contiguous files** on the drive. This not only speeds up disk access, but also eliminates wear on the drive. Keep in mind that **solid-state drives should never be defragmented**.

Reboot— The phrase "Have you tried rebooting it?" is a common joke among IT folks because this is typically the first question that must be asked when a problem arises. However, rebooting should be taken seriously because **many issues can be solved** with a simple reboot. Before diving into any more complicated troubleshooting, a reboot should always be **one of the first steps** in troubleshooting.

Kill tasks— If an application freezes or will not close, ending the task from Task Manager is often a quick way to resolve these issues. To end a task, launch **Task Manager** and locate the application in question. When the application is located, click "End Task".

Restart services— Services are related to both system functions and specific applications. If an application or program isn't running as it should, the service should be restarted to see if that helps. To restart a service, open **Services.msc**. In the services menu, search for the service in question. In the left panel, there should be an option to restart the service.

Update network settings— Network issues can arise when a device is given the same IP addresses as another device by accident, or when something in the network has changed (such as the gateway) and the devices haven't been updated. When a device is having network **connectivity issues**, technicians must check the network settings and update as needed.

Reimage/reload OS— In some extreme cases, it may be easier to simply **uninstall and reload** the operating system. Windows has options so that files can be saved even when a refresh of the OS is needed.

Roll back updates— Although updates are meant to improve computers, sometimes they can corrupt files and cause issues. In these cases, it's necessary to roll back the updates and take your computer **to a previous state** before the updates were installed.

Roll back device drivers— In the same way that updates must sometimes be rolled back, device drivers may require this also. If the computer isn't behaving as it should after a driver has been updated or installed, it is best to roll the device driver back.

Apply updates— When a device is not acting as it should, it's important to check to see if the latest updates have been installed. Updates are often put out to **resolve security or performance issues**.

Repair application— Applications can be repaired from the **Add or Remove Programs** menu. Locate the program in question, and instead of selecting **Uninstall**, select **Modify**. This will usually give you the option to repair the program. This can be especially useful with regard to Microsoft Office products.

Update boot order— At times, it is necessary to boot to a different location than the default. The boot order can be changed in the **BIOS** of the device.

Disable Windows services/applications— If a windows service or application seems to be causing issues on the device, it's best to disable it while troubleshooting further. To disable a service, navigate to the **Services.msc** program, locate the service in question and double-click on it. In the menu for that service, you can choose the disable option.

Disable application startup— If an application is causing the startup to be slower than normal, it can be disabled from the startup programs. In Windows 10, open **Task Manager**, and the **Startup** tab is displayed. This shows all of the startup programs and allows a user to disable a program from startup.

Safe boot— Booting a Windows computer into **Safe Mode** or **Safe Mode with Networking** will boot the computer with only the necessary configuration. Safe Mode boots the system with **only drivers absolutely necessary** to do so. If you suspect problems with drivers, or need to modify system settings that are otherwise unavailable due to booting issues, Safe Mode can help. To enter Safe Mode, repeatedly press **F8** during initial boot.

Rebuild Windows profiles— If there is only an issue with a specific Windows profile, it may not be necessary to rebuild the entire computer operating system; instead, rebuilding that user's profile could do the trick. This is because **profiles can become corrupted**.

PC Security Issues (*scenario*)

Some computer issues have to do with security. To address them, you should spot the signs of particular problems and know what tools are available to render a solution.

Pop-ups

Pop-ups occur from a variety of reasons. While in a browser, a pop-up may expose you to **malware** if you choose to click on the pop-up. Pop-ups that occur randomly should be addressed with one of the available malware cleaners.

Browser Redirection

If you find your browser has been changed, or that the results of a search come from a third-party site, it is likely that your browser has been redirected by **malware**. An anti-malware cleaner may or may not address the issue. You may want to **restore your system** from a known good backup.

Security Alerts

While browsing on the Internet, you may receive a security alert. This may tell you that the site is not secure or the site certificate is not trusted. Your browser will give you an indication of the problem and you need to determine the best course of action.

Slow Performance

While slow system performance could be the cause of faulty hardware or an operating system problem, it could also be caused by a security issue. If a system is infected with **malware**, system performance may be slowed considerably.

Internet Connectivity Issues

Internet connectivity issues are not always the result of networking. **Malware-infected** systems may prevent you from browsing to certain sites or you may be redirected somewhere else altogether.

PC/OS Lockup

Malware can attack the operating system in a number of ways, even to the point where the system will no longer boot. A malware cleaner may address the issue or you may have to restore to a known good backup. You may be able to find the root cause by accessing the **Event Viewer**.

Application Crash

Application crashes can be a sign that the computer has been infected with **malware**. Malware may cause applications to crash or you may get a message that says the program is no longer working.

OS Update Failures

If an operating system won't install updates, this could be a symptom of a **virus**. Malware can interfere with normal operating system updates.

Rogue Antivirus

Antivirus should only be installed from **trusted antivirus websites and vendors**. Attackers can create their malware to look like antivirus and when the user installs it, they are actually infecting the machine with a virus.

Spam

Spam is unsolicited email messages, usually advertising a product, but may actually be a **phishing attack**. A good **spam filter** is one way to control this.

Renamed System Files

Malware can attack an operating system by simply renaming a system file, **rendering it useless**.

Disappearing Files

Malware can cause files to disappear by **deleting** the file or simply **renaming** it.

File Permission Changes

File permissions and ownership can be modified by **malware**.

Hijacked Email

One of the results of spam is to make a user the author of yet more spam. The unknown user is now being hacked to send out spam to others.

Responses from users regarding email— If a user is receiving numerous responses from other users regarding email he supposedly sent, but doesn't recognize, this is a sign that the account has been **hijacked**. The hijacker will probably have deleted anything from the Sent folder as well to cover their tracks.

Automated replies from unknown sent email— Another sign of a hijacked email is receiving a lot of **automated replies** to an email that the user doesn't recognize sending. Because spam is often sent out in a large bulk quantity, it's likely that there will be automated replies sent back.

Access Denied

Malware can change the permissions of files, preventing access to the rightful user.

Invalid Certificate (Trusted Root CA)

If you are browsing the Internet and receive a security alert that the site has an invalid certificate, it could indicate the **site should be avoided** or possibly that there is something as **simple** as an **incorrect PC clock setting** because the site certificate date is too far from your PC's date.

System/Application Log Errors

The System and Application logs in the Event Viewer can show a user what has been occurring on their device. If there are a lot of unknown errors or log in attempts, this could be due to an **unauthorized user** or attacker attempting to gain access to the system.

Malware Removal (*scenario*)

Malware can spread rapidly and cause severe damage. Discovering malware is just the first step. It's vital that you are able to remove the malware **quickly without causing further damage**. Be sure to follow these steps *in order*.

1. Identify and research malware symptoms.

Malware is not often as obvious as strange error messages and odd security warnings. It may be as subtle as a **slight slowdown** of the system or **unexplained files** appearing. There are plenty of sites that are dedicated to describing malware symptoms so thorough research should be done.

2. Quarantine the infected systems.

Any system suspected of being infected by malware should immediately be quarantined. This is so that the malware doesn't spread across the network to other devices. The easiest way to quarantine a device is to simply **pull out the network cord** or **disconnect it from Wi-Fi**. Maintain all the files on the machine and don't attempt to move them to another system.

3. Disable System Restore (in Windows).

The next step after quarantine would be to disable system restore in Windows. You do not want the virus to infect your restore points.

4. Remediate the infected systems.

When you have identified that type of malware and ensured that it can't spread to other devices, remediation can begin.

a. *Update the anti-malware software.* — The first step would be to ensure you have an updated **anti-virus application** with a new engine and signature files.

b. *Scan and use removal techniques (Safe Mode, pre-installation environment).* — Restart the system in **Safe Mode**, pre-installation environment, and run a virus scan. While some viruses are more complicated and may require further remediation techniques, this will be able to remove most basic malware infections.

5. Schedule scans and run updates.

When a virus is removed, set the anti-virus to automatically update the signature files and schedule scans to run in order to **prevent future infections**.

6. Enable System Restore and create a restore point (in Windows).

The next step is to re-enable system restore and create Windows restore points.

7. Educate the end user.

Users are the last line of defense when it comes to computer security. This is because there is **no antivirus or spam filter program that is 100% accurate**. Even with these items in place, the user should be educated on **proper email and Internet usage** to avoid getting a malware infection on his or her device.

Mobile Application Problems (*scenario*)

Portable devices are becoming more common in the workplace, so you will need to become familiar with the following items related to support of these devices.

Dim Display

For mobile devices with dim displays, try to adjust the screen brightness, assuming you can see the screen in a darkened room. For **Android devices**, go to **Settings** > **Display** > **Brightness Level**. For **Apple IOS**, go to **Settings** > **Displays and Brightness**. If that doesn't work, the entire display must be replaced.

Intermittent Wireless

Determine the distance to the wireless access point and determine if that can be modified. Verify Wi-Fi connections on the device. If a mobile device can connect to all other Wi-Fi networks except a specific one, the issue may lie with the **Wi-Fi access point** rather than the device itself.

No Wireless Connectivity

Verify the Wi-Fi settings are correct. Perform a **hard reset** on the specific device, if necessary.

No Bluetooth Connectivity

Check bluetooth configuration parameters: **unpair and pair** the device. Perform a **hard reset** on the specific device, if necessary.

Cannot Broadcast to External Monitor

Devices vary, so check the setup for the remote device. Verify network functionality: Are they on the same subnet?

Touchscreen Non-Responsive

If the device is completely blank, you may be able to get the power option to appear on an Apple device by holding down the Power button, then power off. Hold the Power button and the Home button simultaneously for 10 seconds to perform a hard reset of the device.

For *most* Android devices, hold the Volume Up button and press and hold the Power button until the screen becomes black. However, note that, depending on the make and model of the hardware, you may also be able to either simply either hold the Power button, or hold the Power button and the Volume Down button. After 1 minute or so, power the device back on using the Power button.

Apps Not Loading

Reboot the device and retry the application. Also, try to perform a **hard reset**.

If it is just one app that will not load, try to **reinstall that app**.

Slow Performance

You may have to administratively stop the application in question, then restart. On an iPhone, double-tap home and slide the application out of memory. On an **iPhone 10 or later** (which no longer has a home button from the Home screen), swipe up from the bottom of the screen and pause slightly in the middle of the screen. Next swipe right or left to see the apps that you want to close. Swipe up on the preview of the app in question to close.

For **Android**, go to **Settings** > **Apps**, and then select the app and tap Force Stop.

Unable to Decrypt Email

To decrypt email, **mobile keys** are necessary. You may have to contact the sender and exchange keys.

Extremely Short Battery Life

The most likely causes of short battery life are that the battery needs to be replaced and that there are too many applications running consecutively.

Overheating

If a cell phone appears to be running too hot, check to see which application is using the most **CPU**. This and **recharging** a battery are common causes for the heat generated in a cell phone.

Frozen System

To bring a mobile device out of a frozen state, you should run a **hard reset** of the device. On **IOS**, press and hold the Home and Power buttons simultaneously for 10 seconds.

On **newer iPhones** that no longer have the home button (10 and above) , press and release the Volume Up button, then do the same for the Volume Down button. Next press and hold the Side button, and hold until the display suddenly shuts off, which should take about 10 seconds.

For an **Android**, press and hold the Power, Volume, and Home buttons simultaneously for 10 seconds.

No Sound from Speakers

Verify that the **volume control** is set to the proper level. Test the internal speaker by plugging in an **earphone**. Perform a **factory reset** on the device.

Inaccurate Touch Screen Response

Perform a **hard reset** of the device. If that fails, replace the **digitizer**.

System Lockout

On an Apple iOS device, **ten failed login attempts** will cause the device to erase everything internally. This feature is the default setting, but **can be disabled**. On an Android, use the Google account associated with the device to unlock the device.

App Log Errors

Although users of mobile devices do not usually see it, the mobile devices keep event logs just like computers do. The logs can show what is happening at a given time. To be able to view these logs in **iOS**, you would need the **Xcode** application. And for **Android**, you could use **Logcat**.

Mobile Application Security Problems (*scenario*)

The following are concerns and symptoms you need to be familiar with when dealing with mobile devices.

Signal Drop/Weak Signal

Weak signal can be caused by various factors such as interference and being too far from a cell tower.

Power Drain

Portable devices have a finite amount of available power. If you find the battery is constantly running low, you may want to see what other **applications are currently running** and eliminate them if not vital. Also, many portable devices have **batteries** that are getting old and may need to be replaced.

Slow Data Speeds

The available amount of **bandwidth** (speed) from a cell tower diminishes as distance is increased. To verify the theoretical maximum throughput, you may want to utilize a third-party application that will verify the amount of bandwidth available.

Unintended Wi-Fi Connection

If you feel there are unauthorized connections to your WiFi, you may want to investigate using a **network analyzer** to see how traffic is being handled.

Unintended Bluetooth Pairing

It is possible your Bluetooth is paired with an **unintended user**. Check your mobile device to see what is actually paired with you and consider disabling Bluetooth when you're not using it.

Leaked Personal Files/Data

Mobile devices are susceptible to unauthorized access through **malicious software**. When infected, personal files and data can be leaked to unauthorized users. Consider an **anti-malware scan** for mobile devices, much the same as for PCs and laptops. If applications that were not installed appear, consider a **factory reset** and **clean installation**.

Data Transmission Over Limit

Depending on your carrier, the amount of data you use is limited by your contract. When you near the limited amount, the carrier usually notifies you. If you are unaware of this and go over your data limit, your carrier may disable data usage.

Unauthorized Account Access

Be certain you are connecting through a trusted Wi-Fi network so you know exactly what is being sent.

Unauthorized Location Tracking

To prevent unauthorized GPS tracking on a mobile phone, the user needs to **disable** the tracking (location) feature of the phone.

Unauthorized Camera/Microphone Activation

Cameras and microphones on mobile devices are susceptible to hacking, allowing access to these devices. To prevent this, as with most cases of mobile hacking, users need to be vigilant when it comes to acquiring applications. **Only download applications from a trusted site.**

High Resource Utilization

The cause of shortened battery life could be having too many applications running at any one time or an excessive amount of network utilization. Higher than normal resource utilization could also be caused by malicious software running on the device.

Skillcertpro – skillcertpro.com

All the very best!