CompTIA A+ Core 1

- **A+**
  - CompTIA A+ certified professionals are proven problem solvers. They support today's core technologies from security to networking to virtualization and more. CompTIA A+ is the industry standard for launching IT careers into today's digital world. *(CompTIA.org)*

- **Exam Description**
  - CompTIA A+ 220-1101 covers mobile devices, networking technology, hardware, virtualization, and cloud computing.
- **Five Domains**
  - 15% Mobile Devices
  - 20% Networking
  - 25% Hardware
  - 11% Virtualization and Cloud Computing
  - 29% Hardware and Network Troubleshooting
- **Exam Details**
  - Up to 90 questions in 90 minutes
    - Multiple-choice
    - Drag and drops
    - Performance-based/Simulations
      - Requires a 675 out of 900
      - Recommended Experience:
      - 9 to 12 months hands-on experience in the lab or field
  - Released: April 2022

- **Are You Ready?**
  - Take practice exams
  - Did you score at least 85% or higher?
  - If you need more practice, take additional practice exams to hone your skills before attempting the exam

- **What kind of jobs can I get?**

Shitty!

Learn More...!

Introduction

- OBJ 5.1: Given a scenario, apply the best practice methodology to resolve problems
- **Personal Computers** PC
  - Workstation
    - Computer desk
  - Server
    - Used to host a file and print sharing server
  - Laptop
    - Mobile version of a workstation
  - Tablet
    - Portable computer that consists of a touchscreen and computing hardware
  - Smartphone
    - Smaller version of tablets
  - Smart Device
    - Device that can compute
  - Internet Of Things (IOT) Devices
    - Devices that connect to a network
  - Hardware
    - Parts of the computer that can be picked up, moved around, opened, and closed
  - Storage
    - Saving the data for future use
  - Software
    - Provides the instructions for the hardware
  - Operating System !
    - Provides a method for saving, retrieving, changing, printing, and transmitting information

- Application System
  - Used to create, store, modify, and view information or data
- Driver
  - Used to translate commands from the operating system to hardware
- Firmware
  - Specialized type of software on a chip !

- **Safety Procedures**
  - Personal Safety
    - Trip hazard avoidance
    - Proper lifting techniques
    - Safety gear usage
      - Trip hazard occurs when there is an object where people walk
  - Component Safety
    - Actions taken to prevent damage to components
      - Electrostatic discharge (ESD) occurs when electrons rush from the body to a component
        - Antistatic bag
        - ESD wrist strap
        - ESD mat
  - Electrical Safety
  - Chemical Safety
    - Chemical safety includes proper handling and disposal of hazardous materials and chemicals !

- **Troubleshooting Methodology**
  - Use these six steps to answer the questions on test day
    1. Identify the problem !
    2. Establish a theory of probable cause
    3. Test the theory to determine the cause

- If the theory is not confirmed, re-establish a new theory

4. Establish a plan of action to resolve the problem and implement the solution
5. Verify full system functionality
6. Document the findings, actions, and outcomes

Cable Types

- OBJ 3.1: Explain basic cable types and their connectors, features, and purposes.
- **Cable Types**
  - Common measurements
    - A single "bit" can store one of two values: 1 or 0
    - "Nibble" is 4 bits
    - "Byte" is 8 bits (1B = 8b)
    - 1000 bits
      - 1Kilobit (1Kb)
    - 1Kbps
      - (8bits per byte)
      - 125KB
    - b = bits
    - B = bytes
    - 1,000,000 bits = 1 Megabit (Mb)
    - 1,000,000 bytes = 1 Megabyte (MB) (x 8) bits.
    - 1,000,000,000 bits = 1 Gigabit (Gb)
    - 1,000,000,000 bytes = 1 Gigabyte (GB)
    - 1,000,000,000,000 bits = 1 Terabit (Tb)
    - 1,000,000,000,000 bytes = 1 Terabyte (TB)
  - Types of cables

- Types of video cables

- **Exterior of a PC**
  - CD Drive
    - The ability to read and write information to the system using an optical device
  - Power Button
    - A physical button, that when pushed, sends an electrical signal from a cable directly to the motherboard that tells the computer to turn on
  - Audio Jack
    - Used to connect headphones and microphones to the computer using a 1/8th inch Mini-Jack
  - SuperSpeed USB Connectors
    - Used to connect other peripherals, like a mouse, a keyboard, a webcam, a printer, or other devices to a computer
  - Cooling Fan
    - Blows hot air out of the CPU, the motherboard, and the case which expels the extra heat out of the system to keep the component insides cool
  - HDMI Connector

        - Used to connect a monitor, TV, or another device for a video output display
    - RJ 45 Connector
        - Provides net access to local area networks over a wired connection
    - SPDIF Connector
        - An optical connector that allows high quality audio to a surround sound system
        - USB 2.0 speeds are good for a microphone, a mouse, or a keyboard
    - Kensington Lock
        - Allows the ability to place a metal cable from the desk to the computer tower to ensure the computer tower is not stolen SAFETY!

- **USB Cables**
    - DB 25 Connector
        - A D-shaped sub miniature pin that goes into the back of a computer and has two thumb screws on the side
    - Serial Cable
        - A cable that sends data in ones and zeros in a straight line, but it can only send one bit at a time, which is measured at the speed of cables in bits per second
    - DB9 Connector
        - A slow speed connection for much older mice keyboards and other external modems
        - A USB 1 and a USB 2 run at a much slower speed and should be split across a hub
        - A USB 1.0 has the slowest speed out of a USB with a maximum speed of 1.5 megabits per second

- USB 1.1 humble beginnings!
  - Known as full speed and runs at 12 megabits per second
- USB 2.0
  - Known as high speed and runs at 480 megabits per second
- USB 3.0
  - Known as super speed and is at least 5 gigabits per second
- USB 3.1 Gen One
  - Runs at 5 gigabits per second
- USB 3.1 Gen Two
  - Runs at 10 gigabits per second
- USB 3.2 Gen 2x2
  - Runs at 20 gigabits per second
- USB 4
  - The most modern version of USB and can run at 40 gigabits per second
  - A USB 4 and a USB 3.2 gen 2x2 must have a shorter cable because that is going to give the best performance
  - The longer a cable, the more likelihood that the cable would not work as efficiently, or even at all
    - Type A
    - Type C
    - Type B
    - Type B Mini
    - Type B Micro

- **Video Cables**
  - HDMI
    - Known as high-definition multimedia interface and it is the most widely used video interface in the world

- Lower resolution HDMI can support HD standard, but higher resolution HDMI can support up to 4k
  - Full-Size (Type A Connector)
  - Mini Connector (Type C)
  - Micro Connector (Type D)
- Category 1
  - The standard HDMI that is used for video content
- Category 2
  - The high-speed HDMI that uses higher resolutions

- HDMI Version 2
  - Higher speeds that are specified for data transfer using HDMI
- Display Port Interface
  - Used for digital displays with a high-performance replacement
    - Full-Size Display Port
    - Mini Display Port
  - Display Ports can support high speed data transfer over its cables starting off with 2.7 gigabits per second, but can go up to 20 gigabits per second
- DVI
  - Used to support both analog and digital outputs
    - DVI A
    - DVI D
    - DVI I
  - DVI A only supports analog signals, DVI D only supports digital signals, and DVI I support both signals
- VGA
  - The graphic standard that used a 15-pin standard analog video interface port that would connect to the computer
- Thunderbolt

        - A display interface that is used for data transfer
            - Thunderbolt version 1 and 2 used a physical connector that were backwards compatible
            - All thunderbolt version 3 will support USB-C, but not all USB-C we'll support Thunderbolt 3

- **Storage Cables**
    - Thunderbolt
        - Supports speeds of up to 40 gigabits per second for data transfer over cables
    - Lightning Cable
        - A specific proprietary connector that was created by apple their mobile devices
    - SATA Cable
        - The standard cables that are the main method of connecting a storage device to a motherboard inside of a desktop computer
        - The SATA cable has two cables, one is a seven-pin data cable, which does not supply any power, and the other is a 15-pin SATA power connector to provide the power to the device
        - SATA version 1 can support speeds of up to 1.5 gigabits per second, version 2 can support speeds of up 3 gigabits per second, and version 3 can support speeds of up to 6 gigabits per second
    - External SATA
        - A SATA cable on the outside of the case
    - PATA
        - The old IDE connectors with the exact same cables and connectors and standards but renamed for branding

- Parallel devices have each cable support up to two devices and they both can communicate at the same time

- Molex Power Connector
  - A 4-pin connector that would attach from the power supply directly to a device
- SCIS
  - A legacy parallel bus connector that allows multiple devices to be Daisy chained together
  - A narrow SCIS can support up to 7 devices, but a wide SCIS can support up to 15 devices

Motherboards

- OBJ 3.4: Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards

- **Motherboards**
  - Motherboard
    - Printed circuit board that contains computer components and provides connectors
  - Input
    - Process of accepting data in a form that the computer can use
  - Output
    - Process of displaying the processed data or information
  - Processing
    - Actions performed by the CPU when receiving information
    - Processing is conducted by the CPU or GPU
  - Storage
    - Process of saving or retaining digital data, temporarily or permanently
      - Temporary storage
        - Non-persistent
      - Permanent storage
        - Persistent
    - Data transferred across the motherboard measures the speed of data in MHz or GHz
      - Volatile storage
        - Speed is fast
      - Non-volatile storage
        - Speed decreases rapidly
- **Form Factors**

- Advanced Technology eXtended (ATX)
  - Full-size motherboard and measures 12” x 9.6” in size (305mm x 244 mm)
- Mini-ATX
  - Smaller than ATX but contains the same features (11.2” x 8.2” / 284mm x 208 mm)
- Micro-ATX (mATX)
  - Measures 9.6 inches squared (244mm x 244mm)
  - Micro-ATX is the same as ATX but only has 4 expansion card slots
- Information Technology eXtended (ITX)
  - Designed as a replacement for the ATX but never produced
- Mini-ITX
  - Measures 6.7” x 6.7” with only one expansion slot (170 x 170mm squared)
    - Nano-ITX
    - Pico-ITX
    - Mobile-ITX
- Form Factor
  - Shape, layout, and type of case in a power supply
    - ATX
      - Full-size ATX
      - Mini-ATX
      - Micro-ATX
    - ITX
      - Mini-ITX

- **CPU Architecture**
  - CPU

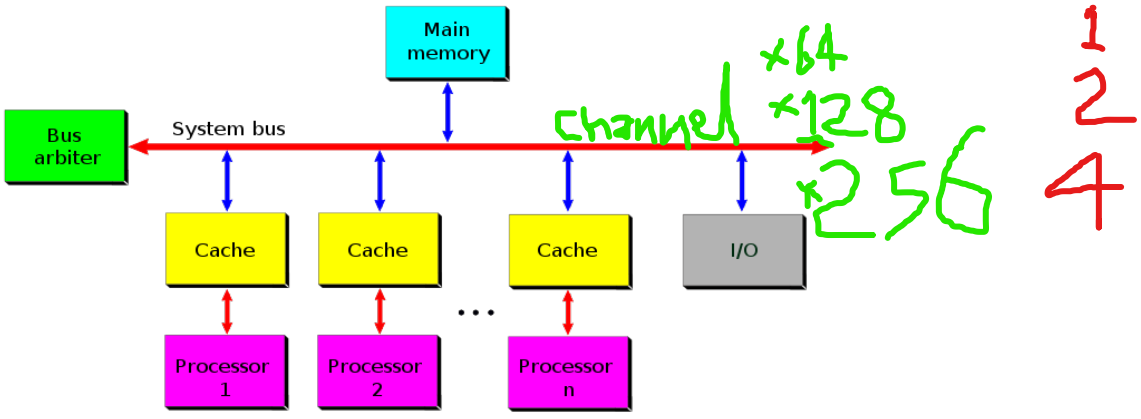
        - The brains of the computer that execute the different programing codes in the software and firmware
        - The CPU is performing the basic operations for every instruction in the computer
        - Once the processor has done the execution of the instruction, it will send that information back to the memory so that it can be stored and used for later use
    - X86
        - Can support a maximum of 4 gigabytes of Ram
    - X64
        - An extension of the X86 instruction set to be able to support 64-bit operations
        - 32-bit systems can only run 32-bit programs, but 64-bit processors can run 64-bit programs and 32-bit programs because they are fully backwards compatible
    - Advanced RISC Machine (ARM)
        - Used for low-power devices (tablets and cell phones)
            - Extended battery life
            - Produces less heat
        - RISC systems use code to do tasks

- **CPU Sockets** DO NOT BREAK!
    - ZIF
        - The ability to insert the CPU without pressing down and applying pressure to it
        - If you bend, snap, or break a pin from a processor, the entire processor is no longer functional
    - LGA Socket !

- A form factor that positions all the pins to be able to connect the CPU processor into the socket

- PGA Form Factor
  - The processor has the pins and the socket have holes which allows the holes to align when installing the processor
- Multi-Socket
  - Multiple CPU's or processors installed on a motherboard
  - You cannot upgrade or change out the processor on a mobile device
  - The two main types of CPU sockets are LGA, which is made by Intel, and we have PGA, which has made by AMD.

- **CPU Features**
  - Simultaneous Multithreading (SMT) / Hyper-threading
    - Single stream of instructions is being sent by a software application to a processor
    - Manufacturers developed a way to allow software to run multiple parallel threads at the same time
  - Symmetric Multiprocessing (SMP)
    - Traditional workstation and servers have multiple processors



  - Multi-core Processors
    - Single CPU with multiple processors inside

        - Multiple processors have multiple cores inside the CPU
    - Dual-core Processor
        - Two CPUs inside a single chip
    - Quad-core Processor
        - Four CPUs inside a single chip
    - Hexa-core Processor
        - Six CPUs inside a single chip
    - Octa-core Processor
        - Eight CPUs inside a single chip
            - Hyper-threading / SMT
            - Symmetric Multiprocessing
            - Multi-core Processors
            - Virtualization
    - VT and AMD-V provide processor extensions to support virtualization
    - Virtualization allows running multiple systems on a single physical host
        - Extended Page Table (EPT)
            - Intel
        - Rapid Virtualization Indexing (RVI)
            - AMD
    - Second Level Address Translation (SLAT)
        - Features of software virtualization are underlying and supported by the hardware processor

- **Installing the Motherboard & CPU**
    1. Review the motherboard's documentation
    2. Place the motherboard aligned at the rear of the case
    3. Insert standoffs that match the hole in the motherboard
    4. Install the processor and memory modules before installing the motherboard

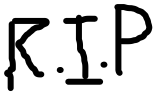
5. Verify the standoffs are properly aligned prior to installing the motherboard
6. Secure the standoffs using the appropriate screw type
7. Install the power supply, disk drives, and add-on cards

- **Expansion Cards**
  - PCI
    - 32-bit expansion card
      - PCI 32-bit cards support only a maximum bus speed of 33 MHz or 133 MBps
  - PCI-X
    - 64-bit expansion card (133 MHz)
  - PCI-X 2.0
    - 266 MHz up to 533 MHz
      - PCI and PCI-X are used for networking cards and audio cards
  - Accelerated Graphics Port (AGP)
    - Used for video graphics cards
      - AGP 1x
      - AGP 2x
      - AGP 4x
      - AGP 8x
  - PCIe (PCI Express) replaces PCI, PCI-X, and AGP
    - PCIe x1
    - PCIe x4
    - PCIe x8
    - PCIe x16
      - PCIe x1 is used for modems, network cards, wireless cards, input/output devices, and audio cards
      - PCIe x16 is used for graphics cards

- Peripheral Component Interconnect Express (PCIe)
  - Connects to the bus to get data to and from the motherboard for external devices
  - PCIe bus is determined by the motherboard and its form factor
    - 16 PCIe lanes
    - 24 PCIe lanes
    - 32 PCIe lanes
  - PCIe x16 and PCIe x1 maximize the number of lanes used on a motherboard
    - PCIe 1.0
    - PCIe 2.0
    - PCIe 3.0
    - PCIe 4.0
    - PCIe 5.0
  - All PCIe slots provide 25 watts of power
  - PCIe x16 card slot provides up to 75 watts of power
    - Up-plugging
      - Putting smaller card in a larger slot
    - Down-plugging
      - Putting larger card in a smaller slot
- Mini PCIe
  - Standard PCIe card with smaller form factor
  - Mini PCIe cards are used inside of laptops, specifically for wireless networking
    - PCIe x1
      - Modems
      - Networking cards
      - Wireless cards

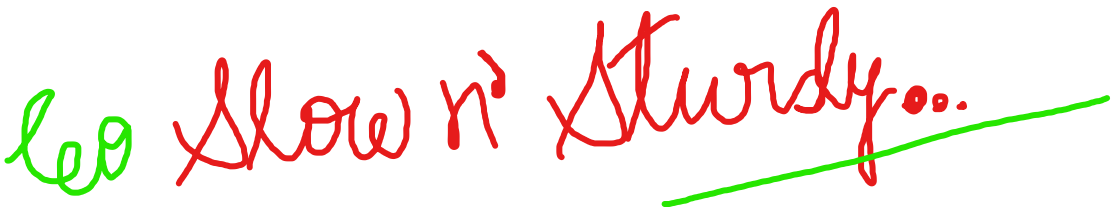
    - Audio cards
- PCIe x16
    - Graphics and video cards (3D)
    - Gaming systems

- **Expansion Card Types**
    - Video Card/Graphic Adapter
        - Gives quality signal for monitors
    - Graphics Processing Unit (GPU)
        - A specialized processor designed to accelerate graphics rendering
    - High Speed Memory
        - Embeds the memory to give additional capability to offload from the system
    - Graphical Ports
        - Installed outside of the card (Thunderbolt, DisplayPort, and HDMI)
    - Video Capture Card
        - Takes video signals and processes them inside the computer
        - used for recording footage and for security devices
    - TV Capture Card
        - Cables are plugged into a computer to get all cable TV channels



    - Sound/Audio Card
        - Gives better output through audio
            - RJ45 Port
                - 1 Gbps
            - Install NIC into PCIe x1 slot
                - 10 Gbps
            - ST / SC / MT-RJ connector
                - Supports fiber card

- Riser Card
  - Special type of expansion card on a motherboard



Cooling and Power

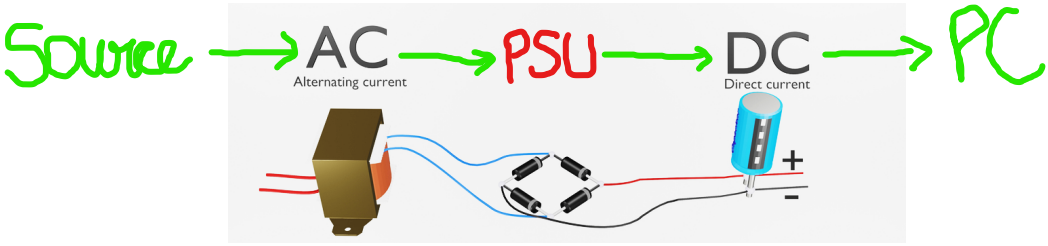
- OBJ 3.4: Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards
- OBJ 3.5: Given a scenario, install or replace the appropriate power supply

- **Cooling the System**
  - Thermal Load
    - Heat from different components inside the computer
  - Passive Cooling
    - Type of cooling that doesn't rely on moving parts or power
  - Heat Sink
    - Finned metal device that radiates heat away from the processor
  - Thermal Paste
    - Compound that ensures heat transfer by eliminating air gaps
      - Passive cooling requires no power to operate and is silent when operating
  - Active Cooling
    - Uses a fan to cool down the heat from the device

- **Liquid Cooling**
  - Closed Loop System
    - Cooling of a single component
  - Open Loop System
    - Liquid cooling-based system of different components
  - Liquid Cooling
    - High performance systems

- **Power Supply Unit (PSU)**

- Alternating current (AC)
  - Cycled between positives and negatives repeatedly
- The main purpose of power supply is to deliver DC to all components inside the PC when receiving an AC power supply



- Modular PSU / Modular Power Supply Unit
  - Allows to unhook the connectors and detach from the unit
  - Modular power supply frees up space inside of the computer

- **Power Supply Connectors**
  - Main Board / Motherboard Adapter
    - Provides power to the motherboard
      - ATX Standard
        - 20-pin connector
      - ATX 12V
        - 24-pin connector
      - 20+4 Pin
        - Two connectors are coupled together before plugging into a 24-pin connector
  - Processor Power/ CPU Power Cooling?
    - Has a four, six, or eight-pin connector
  - Molex Connector
    - Used for IDE and PATA hard disks, CDs, and DVD drives
  - Y Connector
    - One connector that can support multiple devices

- **Input and Output Voltages**
  - 120V AC (Low Line Power)
    - US-based power supply
  - 230V AC (High Line Power)
    - Europe and Asia power supply
  - Most power supplies will support multi-voltage outputs
  - Voltage Sensing / Dual Voltage Power Supplies
    - Detects the outlet and converts it into the voltage of DC
  - Rail
    - Wire that provides current at a particular voltage
      - 12 VDC Rail
        - Cable or wire that provides 12 VDC
        - The 12 VDC rail is the most used voltage in the PC

- **Wattage Rating** GOLD bc its an INEFFICIENT PROCESS! HEAT
  - Wattage Rating
    - Power supply's output capacity or capability
    - The devices inside a computer require power from a power supply
  - Amperage to Wattage
    - A x V
    - I x V

- A/I = Current (Amp.)
- V = Voltage!

Component	Peak Power Usage
RX 6700 XT GPU	230 W
Top-Tier CPU	250 W
Mid-Tier CPU	100-150 W
Motherboard	80 W
Optical Drive	30 W
3.5" Hard Drive	9 W
M.2 or 2.5" SSD	9 W
120 mm Case/CPU Fan	6 W

- The power supply has increments of 50 or 100 Watts
  - Buy a power supply that is bigger than calculated !
- How much power is being drawn out of a wall outlet?
  - A 500-watt power supply that is 70% efficient will draw 714 watts
  - A 500-watt power supply that is 80% efficient will draw 625 watts
- Power supplies are not 100% efficient !

Less heat!
Less Power usage/Bill !

DAMN.

System Memory

- OBJ 3.2: Given a scenario, install the appropriate RAM

- **System Memory**
  - Random Access Memory (RAM)
    - Used to load applications and files into a non-persistent and fast storage area

- **Addressing Memory**
  - Cache
    - High-speed memory
  - Storage
    - Mass storage device that holds more data but is slower than a cache
  - Mass Storage Devices
    - Permanent storage area
  - Random Access Memory (RAM) / System Memory
    - Temporary storage area/non-persistent storage
  - Disk Cache
    - Pulls the files from the disc into memory and replaces the old file
  - Mechanical system
    - Uses an electronic system that can access the RAM with instant speed
  - Addressing Memory
    - Processor reaching the files inside RAM
      - Single Channel Memory Controller
        - 32 or 64 bits
      - x86
        - 32-bit
      - x64

- 64-bit
  - An x86 or 32-bit processor can address a maximum of 4 GB of RAM
  - An x64 or 64-bit processor can access more than 4 GB of RAM (8, 16, 32, or 64 GB)

- **Memory Modules**
  - Single Bank
    - Can put any size of module in any slot
      - Dual Inline Memory Module (DIMM)
        - With 240 or 184-pin connector
  - Dual Data Rate (DDR)
    - Most common type of memory
      - PC133
        - 133 MHz
  - Throughput
    - Calculated based on the bus speed and the width of the data bus
  - Dynamic RAM (DRAM)
    - Oldest type of memory that requires frequent refreshing
      - DRAM storage cell is dynamic
  - Synchronous DRAM (SDRAM)
    - First memory module that operates at the same speed as the motherboard bus (168-pin connector)
      - PC66 (66 MHz bus)
      - PC133 (133 MHz bus)
      - PC266 (266 MHz bus)
  - Double Data Rate Synchronous Dynamic Random-Access Memory (DDR SDRAM)
    - Doubles the transfer speed of an SRAM module (184-pin connector)

- Double Data Rate 2 Synchronous Dynamic Random-Access Memory (DDR2 SDRAM)
  - Higher latency and has faster access to the external bus (240-pin connector)
    - PC2-4200
      - 4200 MB/s or 4.2 GB/s
- Double Data Rate 3 Synchronous Dynamic Random-Access Memory (DDR3 SDRAM)
  - Runs at a lower voltage and at a higher speed than DDR2 (240 keyed pin connector)
    - PC3-10600
      - 10600 MB/s or 10.6 GB/s
  - DDR3 throughput is 6.4 to 17 GB/s with a maximum module size of 8GB per memory module
- Small Outline Dual In-line Memory Module (SODIMM)
  - Classified as DDR3, DDR4, or DDR5

- **Multi-Channel Memory**
  - Multi-Channel Memory
    - Uses two different memory modules to increase the performance and throughput
      - Single-channel Memory
        - 64-bit data bus
      - Dual-channel Memory
        - 128-bit data bus
          - Interleaving
            - Provides increased performance

        - In multi-channel configurations, use the same model, speed, and throughput of memory
    - Single-Channel
        - Uses one memory module on one bus (64-bit data bus)
    - Dual-Channel
        - Requires two memory modules and two memory slots on the motherboard (128-bit data bus)
    - Triple-Channel
        - Uses three memory modules and three memory slots (192-bit data bus)
    - Quad-Channel
        - Uses four memory modules and four memory slots (256-bit data bus)
    - Multiple modules
        - Give faster speeds and add memory for storage

- **ECC Memory**
    - Non-Parity Memory
        - Standard memory that does not check for errors and allows data to be put in or taken out
    - Parity Memory
        - Performs basic error checking and ensures the memory contents are reliable
            - A parity check does basic calculation
                - Every bit has an associated parity bit
                    - Bits can only be a zero or one
    - Error Correcting Code (ECC)
        - Detects and corrects an error

- Buffered / Registered Memory
  - Additional hardware (register) between memory and CPU
    - The system requires buffering or registering the data to reduce the electrical load ?
- Motherboard
  - Supports ECC modules Yeah, no shit.
- DDR5
  - Has an internal error checking for its modules
    - DDR5 modules can still be sold as ECC or non-ECC modules wtf ??

- **Virtual Memory** Fuck yeah!
  - Virtual Memory/Page File
    - Space on a hard drive that is allocated by the OS and pretends to be memory
      - Check the available memory and the free memory
  - Page File or Swap Space
    - A file that is hidden on a storage device and pretend as system memory

Fake it 'till you make it I guess..

lol ;)

BIOS/UEFI

- OBJ 3.4: Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards

- **BIOS and UEFI**
  - Basic Input/Output System (BIOS)
    - Program that a CPU uses to start the computer system
    - BIOS serves as a method of configuring the motherboard using a text-based interface
  - Firmware
    - Software on a chip and contains BIOS program code in the flash memory of a motherboard
  - Unified Extensible Firmware Interface (UEFI)
    - Supports 64-bit processors and provides a GUI

- **Boot Options**
  - Basic Input/Output System (BIOS)
    - Program a computer's microprocessor uses to start and boot after being turned on
    - BIOS is an example of firmware
      - Power-on self-test
      - Hardware configuration
      - Boot order setup
  - Read-Only Memory (ROM)
    - Type of chip embedded in the motherboard and can be upgraded through flashing
  - The new CMOS uses an internal lithium-ion battery that can last up to 10 years
  - Power-On Self-Test (POST)

- Diagnostic testing sequence to check the computer's basic input/output system

- Variable beeps are used to tell what is wrong with the system
  - Keyboard is not detected
    - Two short beeps and one long beep
- The BIOS has a low-level OS which allows to take input and give output to the basic components
  - To configure the settings inside CMOS, enter the BIOS configuration environment

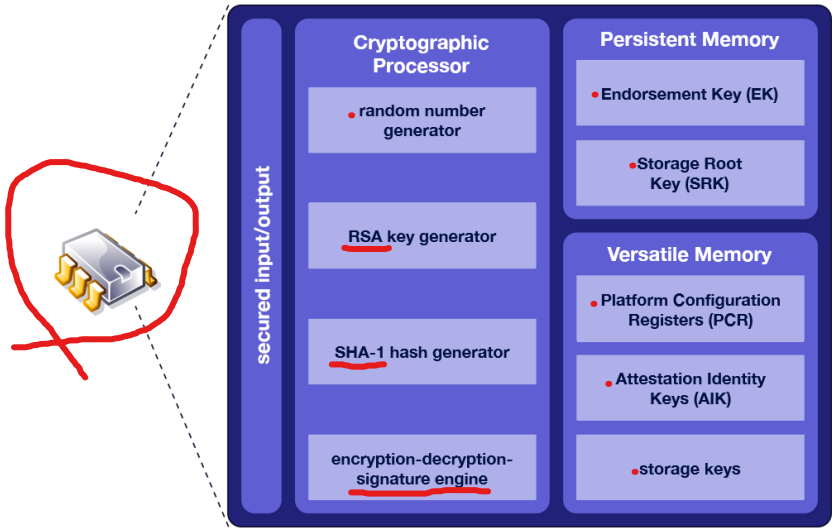
  - BIOS relied on a text-based menu system and a keyboard as its system of input
- Unified Extensible Firmware Interface (UEFI)
  - Updated form of BIOS that allows keyboard and mouse as input and provides a GUI
    - Supports 64-bit systems
    - Supports larger HDDs and SSDs (9.4 zettabytes ~ 9.4 x 10^21 bytes)
    - Supports the new GUID Partition Table (GPT) format
    - Faster boot-up system
    - Uses a larger ROM size
  - Disable booting from an optical drive or USB drive
  - Configure the system to boot from the installed hard drive using the installed OS
  - Boot the OS using PXE as the primary option
- Flashing
  - Performed during upgrades, security fixes, or feature improvements

Secure Boot!

- Back up the configuration and information
- Use a USB flash drive to flash the firmware
- The BIOS or UEFI will copy the firmware to the system and overwrite the old code, Don't off your PC here!

- **BIOS/UEFI Security**
  - BIOS and UEFI are used during loading and booting up the OS
  - Computers that rely on BIOS use MBR to hold the boot information
  - Computers that rely on UEFI use GPT to hold the boot information
  - Supervisor/Administrator/Setup Password
    - Used to protect access to the BIOS or UEFI configuration program and prevents access from unauthorized users
  - User/System Password
    - Used to lock access to the computer
  - Storage/Hard Drive Password
    - Password that locks access to a hard drive connected to the system and requires the end user's password
  - Secure Boot
    - Enabled in the UEFI interface and settings and is not supported by BIOS
  - Root kit
    - a special type of malware
  - Modern systems are configured to enable or disable the USB ports on the motherboard
  - Disable the ability of USB to read and write from mass storage devices
    - Set passwords
    - Enable secure boot
    - Restrict or disable USB ports

- **TPM and HSM**
  - Hardware RoT is the foundation of all secure operations of a computing system
  - Hardware Root of Trust (RoT)
    - Cryptographic module embedded in a computer system that endorses trusted execution and attests to boot settings and metrics
  - A hardware RoT is used to scan the boot metrics in the OS files to verify signatures and then use them to sign the report
  - Trusted Platform Module (TPM)
    - Specification for hardware-based storage of digital certificates, keys, hashed passwords, and other user and platform identification information



    - TPM is a hardware RoT
    - Secured boot-up
    - Provides encryption
    - A TPM can be managed in Windows via tpm.msc console or through group policy

tpm.msc

  - Hardware Security Module (HSM)
    - Appliance for generating and storing cryptographic keys that is less susceptible to tampering and insider threats

- **BIOS/UEFI Cooling Options**
  - BIOS and UEFI can configure fans
    - Quiet mode
      - Reduces the fan speed and allows higher temperatures to occur
    - Balanced mode
      - Normal setting on most computers by default
    - Cool mode
      - Able to run the fans harder and faster to create more air flow
  - Overclocking the processor generates excess heat
  - The motherboard has built-in temperature sensors
    - Temperature is rising
      - Speed up, yeah!
    - Temperature is lower than set point
      - Turn off or slow down, no fuckin' way.

Storage Devices

- OBJ 3.3: Given a scenario, select and install storage devices

- **Hard Disk Drive (HDD)**
  - Hard Disk Drive (HDD)
    - Form of mass storage device
  - Mass Storage Device
    - Non-volatile storage device that holds the data when the system is powered down (GB or TB)
  - Internal Device
    - Device that is placed inside the computer case or tower
  - External Device
    - Device that is placed outside the computer case or tower and connected to an external port
- Solid State Drive (SSD)
  - Solid State Drive
    - Uses flash memory technology to implement mass storage
    - Faster and more durable
  - Main Form Factors
    - 2.5 inch
      - Used when replacing an HDD inside a laptop or a small desktop
    - 1.8 inch
      - Used inside of small laptops
    - M2
      - Like a memory chip, small, sleek, and light
      - Used in a laptops
  - Connections
    - Older SSDs rely on SATA connectors (7+15 pin SATA)

- Used in both 2.5- and 1.8-inch SSDs
- mSATA
  - Allows the SSD to be used as an adapter card that can be plugged into a combined data and power port on the motherboard
  - SSDs are faster than SATA speeds
- NVMe (Non-Volatile Memory Express)
  - A communication protocol used with the M2 form factor to plug directly into the motherboard
- PCIe (Peripheral Component Interconnect Express)
  - Use PCIe slots on the motherboard

Physical Lanes

- A combination of SSDs and HDDs can be advantageous
  - Higher speed from the SSD
  - Larger and cheaper storage from the HDD
- Hybrid Drive
  - Created as a transitional technology
  - Less common today
  - Looks like a hard drive (2.5-inch form factor)
  - Has both an SSD and an HDD in it

R.I.P

- **RAID**
  - Redundant Array of Independent Disks (RAID)
    - Combination of multiple physical hard disks that is recognized by the operating system
      - RAID 0
        - RAID 0 is great for speed but provides no data redundancy
        - RAID 0 has no loss of space on the disks
      - RAID 1
        - RAID 1 provides full redundancy

Mirror!

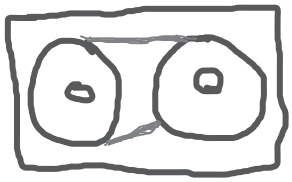
- RAID 5
  - Striping with parity
  - One disk can be lost without losing any data
- RAID 6
  - Double striping with parity
  - Two disks can be lost without losing any data
- RAID 10
  - Redundancy and performance

- Failure Resistant
  - Protection against the loss of erased data (RAID 1/RAID 5)
- Fault Tolerant
  - Raid can function even when a component fails (RAID 1/RAID 5/RAID 6)
- Disaster Tolerant
  - RAID with two independent zones with full data access (RAID 10)
  - RAIDs provide redundancy and high availability

- **Removable Storage**
  - Hot-Swappable
    - Capable of being removed or replaced without disruption or powering off the device
    - Hot-swappable drives are safe to remove without losing the data
      - This feature gives the ability to add/remove additional storage
  - Advanced Host Controller Interface (AHCI)
    - Technical standard developed by Intel that allows hot-swappable capability with SATA devices
  - SATA was developed as a replacement for PATA as an internal connector RIP
  - The newest versions of USB have speeds of 10, 20, or 40 Gbps
  - Drive Enclosure

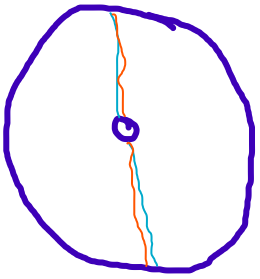
- Takes an internal hard drive and puts it in an enclosure

- Memory Stick
  - Proprietary protocol that is used on Sony devices
- The original secure digital (SD) cards had a maximum capacity of 2 GB
  - Original (Up to 25 MB/s)
  - UHS-1 (Up to 108 MB/s)
  - UHS-2 (Up to 312 MB/s)
  - UHS-3 (Up to 624 MB/s)
- A tape drive uses a magnetic tape and is placed into a reader
  - Standard Tape
    - 140 GB data
  - LTO Ultrium Tape
    - 3 TB data



- A removable mass storage device is any device that can store data and can be carried
- An external hard drive or SSD is the same type of device that is used inside a system

- **Optical Drives**
  - CD (Compact Disc)
    - Oldest form of optical drive that stores 74 to 80 minutes of music (650-700 MB)
  - DVD (Digital Versatile Disc)
    - Stores 4.7 GB or 8.4 GB (DL)
  - BD (Blu-ray Disc)
    - Stores 25 GB or 50 GB (DL)
  - Categories of Optical Drives



- Read-only (ROM)
- Write-once (R)
- Write-many/Erasable (RW/RAM/RE)
- The CD-ROM, DVD-ROM, or BD-ROM is a read-only disc !
  - Write-once (R)
    - Writing that cannot be erased (CD-R, DVD-R, DVD+R, and BD-R)
  - CD-RW allows to write and erase the file to create a new one
    - DVD-RW versions are like the CD-RW versions
    - The DVD-RAM discs are like DVD-RW but have a different type of form factor !
    - Blu-ray Disc (BD-RE)
      - Has write-many type of disc called erasable disc
      - BD-RE is like CD-RW or DVD-RW

- The optical drive speeds are measured using the X-rating !
  - CD (1X = 150 KB/s)
    - 1X = Music
    - 2X/44X/16X/24X =Data
    - 52X drive is 150 KB/s multiplied by 52 (7800 KB/s or 7.6 MB/s)
  - DVD (1X = 1.385 MB/s)
  - Blu-ray (1X = 4.5 MB/s)

{ i used to handout CDs before they were buying, lets do it, lets do it... }

Let this...

Virtualization Concepts

- OBJ 4.2: Given a scenario, select and install storage devices

- **Virtualization** – VirtualBox, VMware Player/ESX-I, PROXMOX
  - Virtualization
    - Host computer installed with a hypervisor that can be used to install and manage multiple guest operating systems or virtual machines (VMs)
      - Type I Hypervisor (Bare Metal)
        - Runs directly on the host hardware and functions as the operating system
      - Type II Hypervisor
        - Runs within the normal operating system !
    - Ensure that each virtual machine runs its own copy of an operating system !
      - Server-based (Terminal services)
        - Server-based solution that runs the application on servers in a centralized location
      - Client-based (Application streaming)
        - Client-based solution that allows an application to be packaged up and streamed directly to a user's PC ! (VDI)

- **Containerization** – Docker
  - Containerization
    - Type of virtualization applied by a host operating system to provision an isolated execution environment for an application !
      - Docker
      - Parallels Virtuozzo
      - OpenVZ

1. When a physical server crashes, all the organizations hosted on that same server are affected
2. An organization's failure to secure the virtual environments hosted on a shared server poses a security risk for the other organizations
    - Set up virtual servers in the cloud with proper failover, redundancy, and elasticity
    - Hosting all VMs on the same type of hypervisor can also be exploited
        - Proper configurations
        - Patched and up-to-date hypervisor
        - Tight access control

- **Purposes of VMs**
    - Hypervisor
        - Manages the distribution of the physical resources of a server to the VMs
            - Type I
                - Bare metal
            - Type II
                - Hosted
    - Container-Based Virtualization (Containerization)
        - Each container relies on a common host OS as the base for each container
        - Container-based virtualization has less resources because it doesn't require its own copy of the OS for individual container
    - Hyperconverged Infrastructure
        - Allows for the full integration of the storage, network, and servers without hardware changes
    - Application Virtualization

        - Encapsulates computer programs from the underlying OS on which they are executed
    - Virtual Desktop Infrastructure (VDI)
        - Hosts desktop OSs within a virtualized environment hosted by a centralized server or server farm
    - Sandbox
        - An isolated environment for analyzing pieces of malware
    - Cross-Platform Virtualization
        - Allows for the testing and running of software applications for different operating systems
            - Emulation
                - System imitation
            - Virtualization
                - New "physical" machine

really is a flattery, it just annoy me...

- **Resource Requirements**
    - Second Level Address Translation (SLAT)
        - Improves the performance of virtual memory when running multiple virtual machines on a single physical host
            - Intel
                - Extended Page Table (EPT)
            - AMD
                - Rapid Virtualization Indexing (RVI)
        - x86
            - 32-bit processor
            - 32-bit operating system can only access 4GB of RAM
        - x64
            - 16 exabytes of RAM

R.I.P

        - 32-bit processor cannot run a 64-bit application
    - ARM
        - Reduced instruction set and computer architecture in a computer processor
    - System Memory
        - Amount of physical memory installed on a physical server
        - Barebones Windows installation takes 20-50 gigabytes of space
        - Linux installation takes 4-8 gigabytes of space
        - Mac environment takes 20-40 gigabytes of space
    - NIC teaming configuration allows multiple cards for higher speeds
        - CPU, processor, and capabilities
        - System memory
        - Networking
        - Storage

- **Security Requirements**
    - VM Escape
        - Threat attempts to get out of an isolated VM and send commands to the underlying hypervisor
        - VM escape is easier to perform on a Type II hypervisor than a Type I hypervisor
            - Patched
            - Up to date
    - VM Hopping
        - Threat attempts to move from one VM to another on the same host
            - VM Hopping
                - VM to VM
            - VM Escape

- VM to hypervisor or host OS - VM Escape
  - Up to date
  - Patched
  - Securely configured
- Sandbox
  - Separates running processes and programs to mitigate system failures or software vulnerabilities
- Sandbox Escape
  - Occurs when an attacker circumvents sandbox protections to gain access to the protected OS or other privileged processes
    - Patched
    - Up to date
    - Strong endpoint software protection
    - Limited extensions or add-ons
- Live Migration
  - Migrates the virtual machine from one host to another while it is running
  - Ensure that live migration only occurs on a trusted network or utilizes encryption
- Data Remnants
  - Leftover pieces of data that may exist in the hard drive which are no longer needed
    - Encrypt virtual machine storage location
    - Destroy encryption key
- VM Sprawl
  - Uncontrolled deployment of virtual machines

Cloud Computing

- OBJ 4.1: Summarize cloud-computing concepts
- OBJ 2.2: Compare and contrast common networking hardware

- **Cloud Computing**
  - Cloud Computing
    - The practice of using a network of remote servers hosted on the Internet

Just someone else's computer!

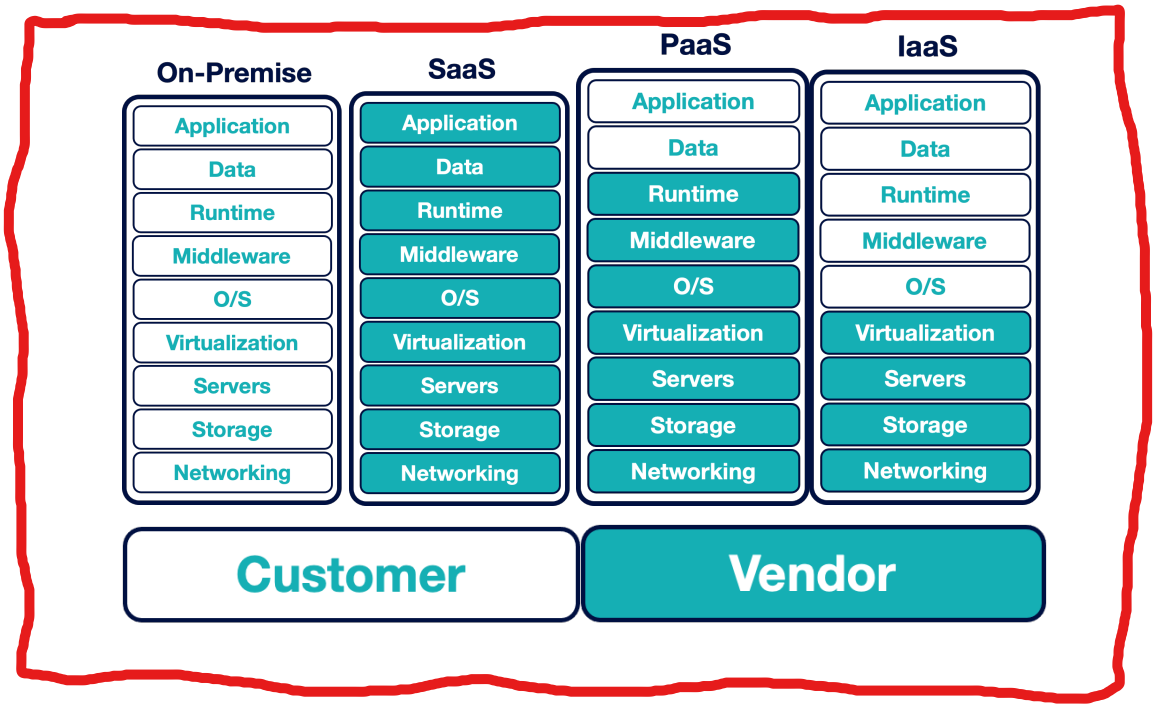
- **Characteristics of the Cloud**
  - High Availability
    - Services experience very little downtime when using the cloud
    - Availability is the percentage of uptime versus downtime
  - Scalability
    - Ability to increase the number of items in a system at a linear rate or less than a linear rate
  - Vertical Scaling (Scaling Up)
    - Increasing the power of the existing resources in the working environment
  - Horizontal Scaling (Scaling Out)
    - Adding additional resources to help handle the extra load being experienced
  - Rapid Elasticity
    - The ability to quickly scale up or down
      - Elasticity is the system's ability to handle changes to demand in real time
  - Metered Utilization
    - Being charged for a service on a pay per use basis

        - The benefit of using the cloud is that most things are done on a metered basis
    - Measured Services
        - Charging is based upon the actual usage of the service being consumed
        - Measured services are charged based on the actual usage of the service being consumed
    - Shared Resources
        - The ability to minimize the costs by putting VMs on other servers
        - Shared resources is pooling together all the hardware to make a cloud provider
    - File Synchronization
        - The ability to store data that can spread to other places depending on the configuration

- **Cloud Deployment Models**
    - Public Cloud
        - Systems and users interact with devices on public networks, such as the Internet and other clouds
    - Private Cloud
        - Systems and users that only have access with other devices inside the same private cloud or system
    - Hybrid Cloud
        - Combination of private and public clouds
    - Community Cloud
        - Collaborative effort where infrastructure is shared between several organizations from a specific community with common concerns
    - Multitenancy

        - The ability for customers to share computing resources in a public or private cloud
    - Single-Tenancy
        - Assigns a particular resource to a single organization

- **Cloud Service Models**
    - On-Premise Solution
        - The need to procure hardware, software, and personnel necessary to run the organization's cloud
        - On-premise solution allows the ability to control all the physical and logical access to servers
    - Hosted Solution
        - Third-party service provider that provides all the hardware and facilities needed to maintain a cloud solution



- **Virtual Desktop Infrastructure (VDI)**
    - Virtual Desktop Infrastructure (VDI)

        - Hosts desktop OSs within a virtualized environment hosted by a centralized server or server farm (VDI)
    - Server: POWERFUL PCs
        - Performs all the application processing and data storage
    - Centralized Model
        - Hosts all the desktop instances on a single server or server farm
    - Hosted Model/ Desktop as a Service (DAAS)
        - Maintained by a service provider and provided to the end user as a service ?
    - Remote Virtual Desktop Model
        - Copies the desktop image to a local machine prior to being used by the end user ?

- **Cloud Storage Services**
    - Cloud Storage Application
        - Amount of space on a cloud-based server as file storage
    - File Synchronization
        - The ability to synchronize from different devices using a single account !
    - Content Delivery Network (CDN)
        - Network of servers that locates the nearest server to minimize delay or download time

- **Software Defined Network (SDN)**
    - Software-Defined Networking (SDN)
        - Enables the network to be intelligently and centrally controlled, or programmed, using software applications
            - Can be changed automatically by the network itself using automation and orchestration

- Application Layer
  - Focuses on the communication resource requests or information about the network as a whole
- Control Layer
  - Uses the information from the applications and decides how to route a data packet on the network
- Infrastructure Layer
  - Contains the network devices that receive information about where to move the data
- Management Plane
  - Used to monitor traffic conditions and the status of the network
    - Provides a layer of abstraction between the devices and the control and data flow that happen on the network

Networking Basics

- OBJ 2.2: Compare and contrast common networking hardware
- OBJ 2.4: Summarize services provided by networked hosts
- OBJ 2.7: Compare and contrast Internet connection types, network types, and their features
- OBJ 2.8: Given a scenario, use networking tools
- OBJ 3.1: Explain basic cable types and their connectors, features, and purposes

- **Networking Hardware**
  - Network Interface Card (NIC)
    - Provides an ethernet connection to the network
  - Hub
    - Has several different ports between 4 and 48 ports
  - Switches
    - Smart hubs that remember the ports that are connected to them
      - Switches can have multiple people talking at one time
  - Unmanaged Switch
    - Performs its functions without requiring a configuration
  - Managed Switch
    - Performs its functions with configuration
  - Wireless Access Point
    - Device that allows wireless devices to connect to a wired network
  - Router
    - Used to connect different networks together
  - Firewall
    - Scans and blocks traffic that enters or leaves a network
      - Unified threat management (UTM) contains firewall features
  - Patch Panel

        - Device that allows cable network jacks from a wall into a central area
    - Power Over Ethernet (PoE)
        - Supplies electrical power from a switch port over an ordinary data cable to a power device
    - Power Injector
        - Plugs into a wall outlet to get power
    - Cable Modem
        - Device that translates coaxial cable signals into radio frequency waves
    - Digital Subscriber Line (DSL modem)
        - Device that translates coaxial cable signals into phone lines
    - Optical Network Terminal (ONT)
        - Terminates fiber connection
    - Software Defined Networking (SDN)
        - Way of virtualizing the network hardware

- **Network Types**
    - Personal Area Network (PAN)
        - Smallest type of wired or wireless network and covers the least amount of area
    - Local Area Network (LAN)
        - Connects components within a limited distance
            - Up to a few hundred feet
    - Campus Area Network (CAN)
        - Connects LANs that are building-centric across a university, industrial park, or business park
            - Up to a few miles
    - Metropolitan Area Network (MAN)
        - Connects scattered locations across a city or metro area

        - Up to about 25 miles
    - Wide Area Network (WAN)
        - Connects geographically disparate internal networks and consists of leased lines or VPNs
            - Worldwide coverage
    - Wireless Local Area Network (WLAN)
        - A wireless distribution method for two or more devices that creates a local area network using wireless frequencies
    - Storage Area Network (SAN)
        - Provisions access to configurable pools of storage devices that can be used by application servers
    - Small Office, Home Office (SoHo) LAN
        - Uses a centralized server or simply provides clients access to local devices like printers, file storage, or the Internet

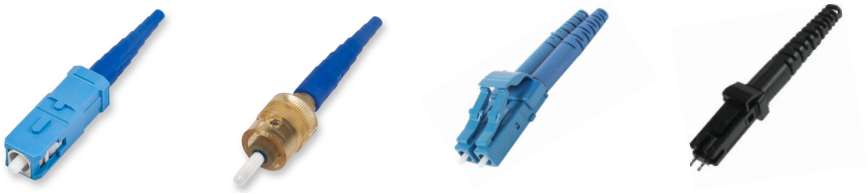
- **Internet of Things**
    - Internet of Things
        - A global network of appliances and personal devices that have been equipped with sensors, software, and network connectivity to report state and configuration
            - Segregation of IoT devices is critically important for the business network's security
- **Twisted Pair Cables**
    - STP and UTP operate about the same
    - Keep cable runs under 70 meters from the IDF to the office
    - Registered Jack (RJ)
        - Carries voice or data which specifies the standards a device needs to meet to connect to the phone or data network

- Bandwidth
  - The theoretical measure of how much data could be transferred from a source to its destination
- Throughput
  - The actual measure of how much data is successfully transferred from a source to its destination
- Ethernet Standard
  - A designation given to a particular category that provides the ability to understand the bandwidth and the cable type to be used
- Straight-Through Cable (Patch Cable)
  - Contains the exact same pinouts on both ends of the cable
- 568b
  - The standard that's preferred when wiring jacks inside of buildings
- Crossover Cable
  - The ability to take send and receive pins from one cable and swap those on the other end
- MDIX
  - A medium dependent interface crossover (MDIX) is an automated way to electronically simulate using a crossover cable
- Direct Burial
  - A cable rating that specifies that a cable has a stronger sheathing and jacket that can withstand more extreme weather conditions
    - A plenum rated cable is more fire resistant and it minimizes the amount of dangerous fumes that are released

- **Optical Cabling**
  - Fiber Optic Cable

        - Uses light from an LED or laser to transmit information through a thin glass fiber
            - Greater usable range
            - Greater data capacity
    - Switches, routers, and end-user devices can become a limitation
    - Single Mode Fiber (SMF)
        - Used for longer distances and has smaller core size which allows for only a single mode of travel for the light signal
            - SMF's core size is 8.3-10µ in diameter
    - Multimode Fiber (MMF)
        - Used for shorter distances and has larger core size which allows for multiple modes of travel for the light signal
            - MMF's core size is 50-100µ in diameter
            - Up to 2 kilometers or less

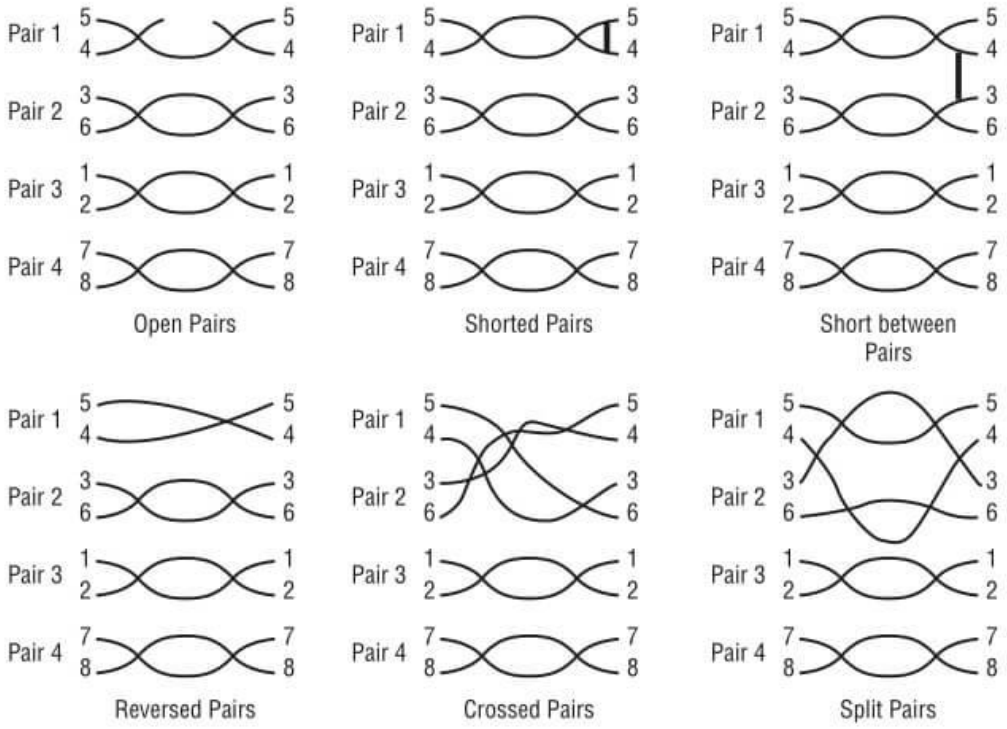
MMF	SMF
Larger core size	Smaller core size
Covers shorter distances	Covers longer distance
Less expensive	More expensive



- Coaxial Cabling
    - Coaxial Cable (Coax)
        - One of the oldest categories of copper media that is still used in networking today

- Twinaxial Cable
  - Like coaxial cable but uses two inner conductors to carry the data instead of just one

- **Networking Tools**
  - Snip/Cutter
    - Used to cut a piece of cable off a larger spool or run of cable
  - Cable Stripper
    - Used to strip off the end of the cable and prepare it for attachment to a connector
  - Cable Crimper
    - Used to attach the connector to the end of the cable
  - Wire Mapping Tool
    - Works like a cable tester, but specifically for twisted pair ethernet cables



- Cable Certifier
  - Used to determine a cable's category or data throughput
- Punch-Down Block
  - Terminates the wires and strips off excess installation and extra wires that are no longer needed
- Tone Generator/Toner Probe
  - Used to generate a tone on one end of the connection and use the probe to audibly detect the wire connected on the other side
- Loopback Adapter/Device
  - Facilitates the testing of simple networking issues
- Tap
  - Connects directly to the cable infrastructure and splits or copies those packets for analysis, security, or general network management
- Wireless Analyzer

- Ensures proper coverage and prevents overlap between wireless access point coverage zones and channels

Wireless Networks

- OBJ 2.3: Compare and contrast protocols for wireless networking

- **Wireless Frequencies**
  - Direct-Sequence Spread Spectrum (DSSS)
    - Modulates data over an entire range of frequencies using a series of signals known as chips
  - Frequency-Hopping Spread Spectrum (FHSS)
    - Allows devices to hop between predetermined frequencies
  - Orthogonal Frequency Division Multiplexing (OFDM)
    - Uses a slow modulation rate with simultaneous transmissions over 52 different data streams
  - Each band has specific frequencies/channels to avoid overlapping with other signals
  - Channel
    - A virtual medium through which wireless networks can send and receive data
      - For the 2.4 GHz spectrum, there can be 11 or 14 channels
      - Channels 1, 6, and 11 avoid overlapping frequencies in the 2.4 GHz band
      - We can use 5.725-5.875 GHz to run our wireless networks in the 5 GHz band
      - There are 24 non-overlapping channels in the 5 GHz band
  - Channel Bonding
    - Allows for the creation of a wider channel by merging neighboring channels into one
      - The standard channel size for both 2.4 GHz and 5 GHz networks is 20 MHz

- **Wireless Standards**

Standard	Band	Bandwidth
802.11a	5 GHz	54 Mbps
802.11b	2.4 GHz	11 Mbps
802.11g	2.4 GHz	54 Mbps
802.11n (Wi-Fi 4)	2.4 and 5 GHz	150 Mbps/600 Mbps (MIMO)
802.11ac (Wi-Fi 5)	5 GHz	6.9 Gbps (MU-MIMO)
802.11ax (Wi-Fi 6)	2.4, 5, and 6 GHz	9.6 Gbps (MU-MIMO)

    - Multiple-Input and Multiple-Output (MIMO)
        - Uses multiple antennas to send and receive data than it could with a single antenna
    - Multiple User Multiple Input Multiple Output (MU-MIMO)
        - Allows multiple users to access the wireless network and access point at the same time
    - Radio Frequency Interference (RFI)
        - Occurs when there are similar frequencies to wireless networks in the area
    - As signal decreases in strength or interference increases, the signal-to-noise ratio worsens

- **Wireless Security**
    - Pre-Shared Key
        - Both the access point and the client use the same encryption key
        - It's not a good idea to use pre-shared keys in large environments
    - Wired Equivalent Privacy (WEP)

- Original 802.11 wireless security standard which is an insecure security protocol
- WEP uses 24-bit Initialization Vector (IV) sent in clear text

- Wi-Fi Protected Access (WPA)
  - Replaced WEP and follows the Temporal Key Integrity Protocol (TKIP)
  - WPA uses 48-bit Initialization Vector (IV) instead of 24-bit
    - Rivest Cipher 4 (RC4)
      - For encryption
    - Message Integrity Check (MIC)
      - To confirm data was not modified in transit
    - Enterprise Mode
      - To authenticate users before exchanging keys
- Wi-Fi Protected Access 2 (WPA2)
  - Created as part of IEEE 802.11i standard and requires stronger encryption and integrity checking through CCMP
    - Advanced Encryption Standard (AES)
      - To provide additional security by using a 128-bit key or higher
    - Personal Mode
      - Pre-shared key
    - Enterprise Mode
      - Centralized authentication

If asked about…	Look for…
Open	No security or protection
WEP	IV
WPA	TKIP and RC4
WPA2	CCMP and AES

- MAC Address Filtering

        - Configures an access point with a listing of permitted MAC addresses (like an ACL)
    - Disabling SSID Broadcast
        - Configures an access point not to broadcast the name of the wireless LAN

- **Fixed Wireless**
    - Wi-Fi (802.11)
        - Creates point to point connections from one building to another over a relatively short distance
    - Cellular
        - Uses a larger antenna and a larger hotspot powered by a power outlet within an office or home
    - Microwave
        - Creates point to point connection between two or more buildings that have longer distances
        - A traditional microwave link can cover about 40 miles of distance
    - Satellite
        - A long range and fixed wireless solution that can go for miles
            - Low Earth Orbit
                - Requires more satellites to cover the entire planet but gives lower latency speeds
            - Geosynchronous Orbit
                - One satellite can cover a large portion of the Earth
                - Geosynchronous orbit gives higher latency and lower quality

- **NFC, RFID, IR, and Bluetooth**
    - Near Field Communication (NFC)

        - Uses radio frequency to send electromagnetic charge containing the transaction data over a short distance
    - Radio Frequency dentification (RFID)
        - A form of radio frequency transmission modified for use in authentication systems
    - Infrared Data (IrDA)
        - Allows two devices to communicate using line of sight communication in the infrared spectrum
    - Bluetooth
        - Creates a personal area network over 2.4 GHz to allow for wireless connectivity
            - Bluejacking
                - Sending unsolicited messages to a Bluetooth device
            - Bluesnarfing
                - Making unauthorized access to a device via Bluetooth connection
            - BlueBorne
                - Allows the attacker to gain complete control over a device without even being connected to the target device
    - Tethering
        - Sharing cellular data Internet connection from a smartphone to multiple other devices
        - Only connect to trusted wireless networks

Internet Connections

- OBJ 2.7: Compare and contrast Internet connection types, network types, and their features

- **Internet Connections**
  - Internet Service Provider (ISP)
    - Establishes high speed links between their network and clients

- **Dial-up and DSL**
  - Plain Old Telephone Service (POTS)
    - Runs as a dial-up connection and is used on the public switched telephone network (PSTN)
    - Analog connections can be voice or data converted from ones and zeros
    - Dial-up modems have a maximum bandwidth of 53.3 kb/s
  - Legacy System
    - Old system that is still used in some critical functions
  - Integrated Services Digital Network (ISDN)
    - Supports multiple 64 Kbps channels
    - ISDN is an older technology designed to carry voice, video, or data over B (bearer) channels
  - Asymmetric DSL (ADSL)
    - Has different speeds of download and upload
      - Maximum Download Speed
        - 8 Mbps
      - Maximum Upload Speed
        - 1.544 Mbps
    - ADSL maximizes the download and minimizes the uploads
  - Symmetric DSL (SDSL)

        - Has equal speeds of download and upload
    - Very High Bit-Rate DSL (VDSL)
        - Has high speeds of download and upload
            - Download Speed
                - 50 Mbps or more
            - Upload Speed
                - 10 Mbps or more
        - ADSL Maximum Distance to DSLAM
            - 18,000 ft.
        - VDSL Maximum Distance to DSLAM
            - 4,000 ft.

- **Cable Connections**
    - Cable Modems
        - Uses a cable TV network that is made up of a hybrid fiber-coaxial (HFC) distribution network
    - Data-Over-Cable Service Interface Specifications (DOCSIS)
        - Specific frequency ranges used for upstream and downstream transmissions
            - Upstream
                - 5 MHz to 42 MHz
            - Downstream
                - 50 MHz to 860 MHz
    - Cable modems transmit and receive over cable television infrastructure

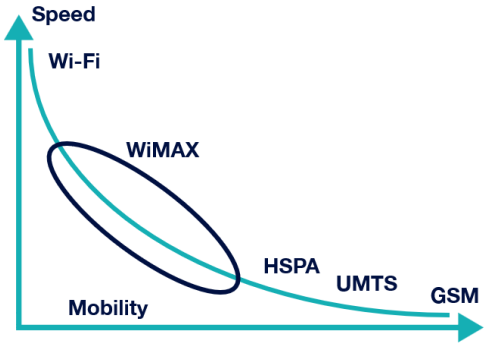
- **Fiber Connections**
    - Fiber To The Curb (FTTC)
        - Runs a fiber optic cable from an internet provider access point to a curb

- Fiber To The Premises (FTTP)
  - Fiber optic that connects directly to a building and connects to an optical network terminal (ONT)
- Optical Network Terminal (ONT)
  - Physical devices that convert optical signals to electrical signals

- **Cellular Connections**
  - The G refers to the generation of cellular technology being used
    - SMS and text messaging
    - International roaming
    - Conference calling
    - Use of internet
    - Introduction to EDGE
  - Wideband Code Division Multiple Access (WCDMA)
    - Used by the UMTS standard and could reach data speeds of up to 2 Mbps
  - High Speed Packet Access (HSPA)
    - Reaches speeds of up to 14.4 Mbps and is sometimes referred to as 3.5G
  - High Speed Packet Access Evolution (HSPA+)
    - Reaches speeds of up to 50 Mbps and is sometimes referred to as 3.75G
  - 4G Long-term Evolution (4G LTE)
    - 100 Mbps
  - LTE Advanced (LTE-A)
    - 1 Gbps
  - Frequencies are operated in the millimeter wave band
  - The higher the G, the newer standard, it has increased in speeds

Technology		Frequency	Speed
1G		30 KHz	2 Kbps
2G		1800 MHz	14.4-64 Kbps
3G		1.6-2 GHz	144 Kbps to 2 Mbps
4G		2-8 GHz	100 Mbps to 1 Gbps
5G	Low-band	600-850 MHz	30-250 Mbps
	Mid-band	2.5-3.7 GHz	100-900 Mbps
	High-band	25-39 GHz	Extremely high speed (in Gbps)

- **WISP Connections**
  - Microwave
    - Uses a beam of radio waves in the microwave frequency range to transmit information between two fixed locations
      - Ultra-high frequency (UHF)
      - Super high frequency (SHF)
      - Extremely high frequency (EHF)
    - Both antennas must maintain a line of sight



- **Satellite Connections**
  - Satellite
    - A method of using communication satellites located in space to connect a user to the Internet

- Slow
- Expensive
- High latency

Network Configurations

- OBJ 2.1: Compare and contrast Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports, protocols, and their purposes
- OBJ 2.5: Given a scenario, install and configure basic wired/wireless small office/home office (SOHO) networks
- OBJ 2.6: Compare and contrast common network configuration concepts

- **Network Configurations**
    - Link/Network Interface Layer
        - Responsible for putting frames in the physical network's transmission media
        - In the link/network interface layer, the data can only travel through the local area network
    - Internet Layer
        - Used to address packets and route them across the network
    - Transport Layer
        - Shows how to send the packets
            - TCP
                - Transmission Control Protocol
            - UDP
                - User Datagram Protocol
    - Application Layer
        - Contains all the protocols that perform higher-level functions

- IPv4

10	1	2	3
172	21	243	67

	1st Octet	2nd Octet	3rd Octet	4th Octet
Dotted-decimal	192	168	1	4
Binary digits	11000000	10101000	00000001	00000100
Subnet mask	255	255	255	0
Subnet mask	11111111	11111111	11111111	00000000
	Network bits			*Host bits*

Class	1st Octet Value	Default Subnet Mask				Possible Hosts
A	1-127	255	0	0	0	16.7 million (256 x 256 x 256)
		N	H	H	H	
B	128-191	255	255	0	0	65,536 (256 x 256)
		N	N	H	H	
C	192-223	255	255	255	0	256
		N	N	N	H	
D	224-239	-				-
E	240-255	-				268 million (reserved)

  - Multicast Address
    - A logical identifier for a group of hosts in a computer network
  - Classful Mask
    - Default subnet mask for a given class of IP addresses

- Classless Inter-Domain Routing (CIDR)
  - Allows for borrowing some of the host bits and reassigning them to the network portion

Class	1st Octet Value	Default Subnet Mask				CIDR Notation
A	1-127	255	0	0	0	/8
		N	H	H	H	
B	128-191	255	255	0	0	/16
		N	N	H	H	
C	192-223	255	255	255	0	/24
		N	N	N	H	

- Public (Routable)
  - Can be accessed over the Internet and is assigned to the network by an Internet service provider
- Private (Non-Routable)
  - Can be used by anyone any time, but only within their own local area network
  - Private IP ranges include those that start with either 10, 172, or 192
- Network Address Translation (NAT) allows for routing of private IPs through a public IP

Class	Starting Value	IP Range	Possible Hosts
A	10	10.0.0.0- 10.255.255.255	16.7 million (256 x 256 x 256)
B	172.16-172.31	172.16.0.0- 172.31.255.255	1.05 million (16 x 256 x 256)
C	192.168	192.168.0.0- 192.168.255.255	65,536 (256 x 256)

- Loopback Address (127.0.0.1)
  - Creates a loopback to the host and is often used in troubleshooting and testing network protocols on a system
- Automatic Private IP Addresses (APIPA)

- Used when a device does not have a static IP address or cannot reach a DHCP server
    - 169.254.0.0 to 169.254.255.255

D iscover

O ffer

R equest

A cknowledge

- **Assigning IPv4 Addresses**
    - Static Assignment
        - Manually type the IP address for the host, its subnet mask, default gateway, and DNS server
        - Static assignment of IP addresses is impractical on large enterprise networks
    - Dynamic Assignment
        - Dynamic allocation of IP addresses
    - Domain Name System (DNS)
        - Converts the domain names used by a website to the IP address of its server
        - DNS is the internet version of a phone book
    - Windows Internet Name Service (WINS)
        - Identifies NetBIOS systems on a TCP/IP network and converts those NetBIOS names to IP addresses
    - Bootstrap Protocol (BOOTP)
        - Dynamically assigns IP addresses and allows a workstation to load a copy of boot image to the network
    - Dynamic Host Control Protocol (DHCP)

- Assigns an IP based on an assignable scope or addresses and provides the ability to configure other options
- 192.168.1.100 through 192.168.1.200
  - Each IP is leased for a period of time and returns to the pool when the lease expires

- IP Address Management
  - Manages the IPs being assigned and returned over time
- DHCP is the modern implementation of BOOTP
- Automatic Private IP Addressing (APIPA)
  - Used when a device does not have a static IP address or cannot reach a DHCP server
  - Allows for the quick configuration of a LAN without the need for a DHCP server
  - APIPA-assigned devices cannot communicate outside the LAN or with non-APIPA devices
- Zero Configuration (ZeroConf)
  - New technology that provides the same features as APIPA
  - Assign an IPv4 link-local address to a client
  - Resolve computer names to IP addresses without the need for DNS by using mDNS (multicast domain name service)
  - Perform service discovery on a network
    - Windows
      - Link-Local Multicast Name Resolution (LLMNR)
    - Linux
      - SystemD

- **DHCP**
  - Dynamic Host Configuration Protocol (DHCP)
    - Provides an IP address to every machine on the network and eliminates configuration errors
  - Scope
    - List of valid IP addresses available for assignment or lease to a client computer or endpoint device on a given subnet
    - 254 available Ips
  - DHCP Reservation
    - Excludes some IP addresses from being handed to devices unless they meet a certain condition

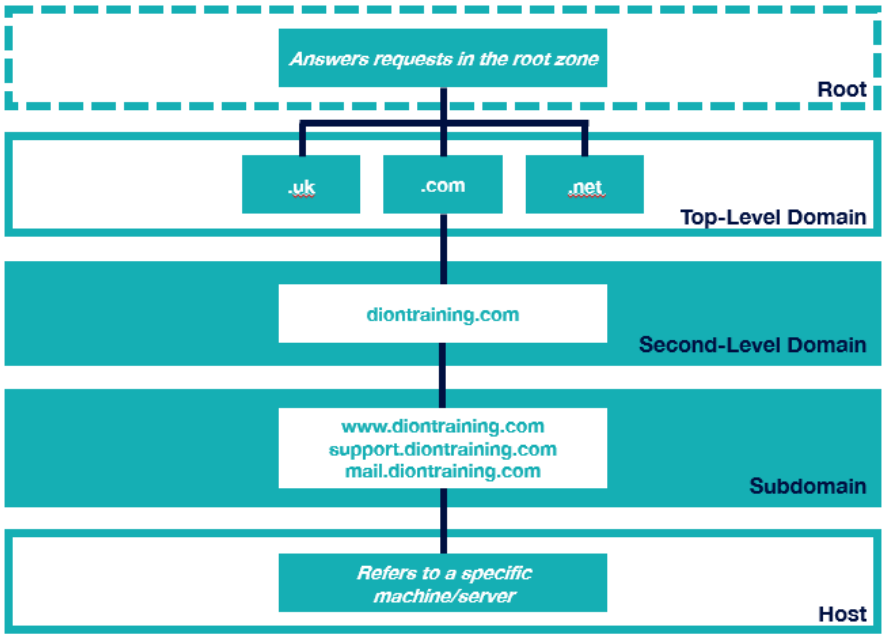
      Discover

      Offer

      Request

      Acknowledge
  - IP addresses can also be statically assigned

- **DNS**
  - Domain Name System (DNS)
    - Helps network clients find a website using human-readable hostnames instead of numeric IP addresses
  - Fully Qualified Domain Name (FQDN)
    - Domain name under a top-level provider



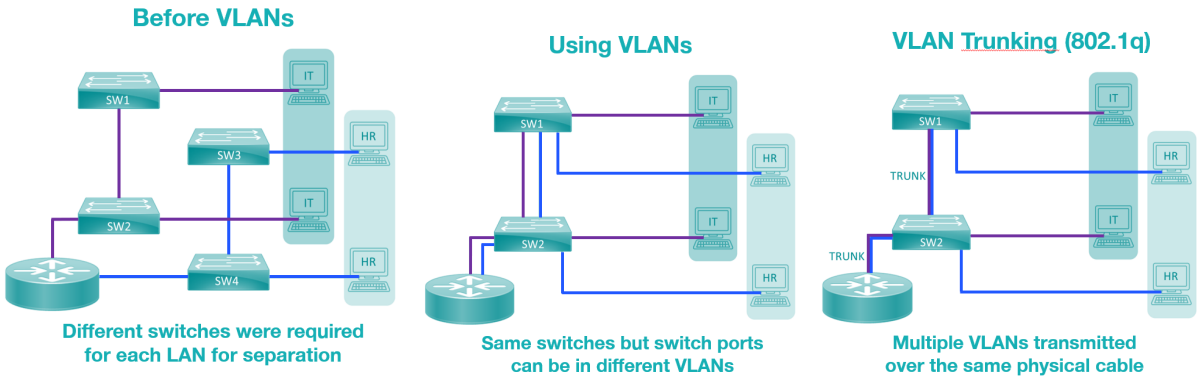
- Uniform Resource Locator (URL)
  - Contains the FQDN with the method of accessing information

DNS Record	Description	Function
A	Address	Links a hostname to an IPv4 address
AAAA	Address	Links a hostname to an IPv6 address
CNAME	Canonical Name	Points a domain to another domain or subdomain
MX	Mail Exchange	Directs emails to a mail server
TXT	Text	Adds text into the DNS
NS	Nameserver	Indicates which DNS nameserver has the authority

- CNAME records can only be used to point to another domain or subdomain, not to an IP address
- Sender Policy Framework (SPF)
  - DNS record that identifies the host authorized to send mail for the domain
- DomainKeys Identified Mail (DKIM)
  - provides the cryptographic authentication mechanism for mail using a public key published as a DNS record

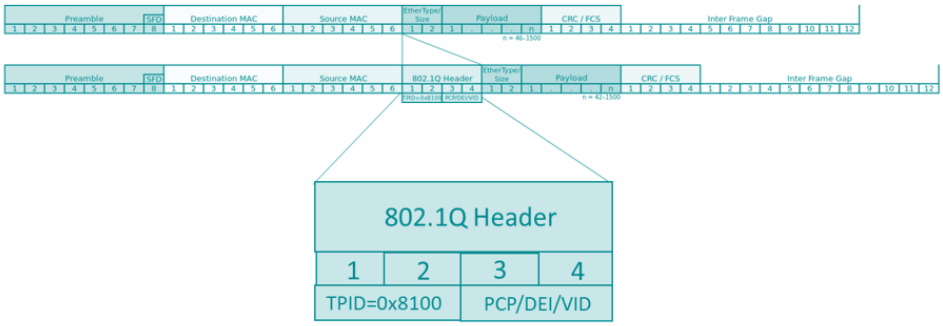
- Domain-based Message Authentication, Reporting & Conformance (DMARC)
  - Framework that is used for proper application of SPF and DKIM, utilizing a policy that's published as a DNS record
- Nameserver
  - Type of DNS server that stores all the DNS records for a given domain
- Internal DNS
  - Allows cloud instances on the same network access each other using internal DNS names
- External DNS
  - Records created around the domain names from a central authority and used on the public Internet
- Time to Live (TTL)
  - Tells the DNS resolver how long to cache a query before requesting a new one
- DNS Resolver/DNS Cache
  - Makes a local copy of every DNS entry it resolves as connected to websites
- Recursive Lookup
  - DNA server communicates with several other DNS servers to hunt down the IP address and return to the client
- Iterative Lookup
  - Each DNS server responds directly to the client with an address for another DNS server that may have the correct IP address

- **VLAN**
  - Virtual Local Area Network (VLAN)
    - Allows different logical networks to share the same physical hardware and provides added security and efficiency

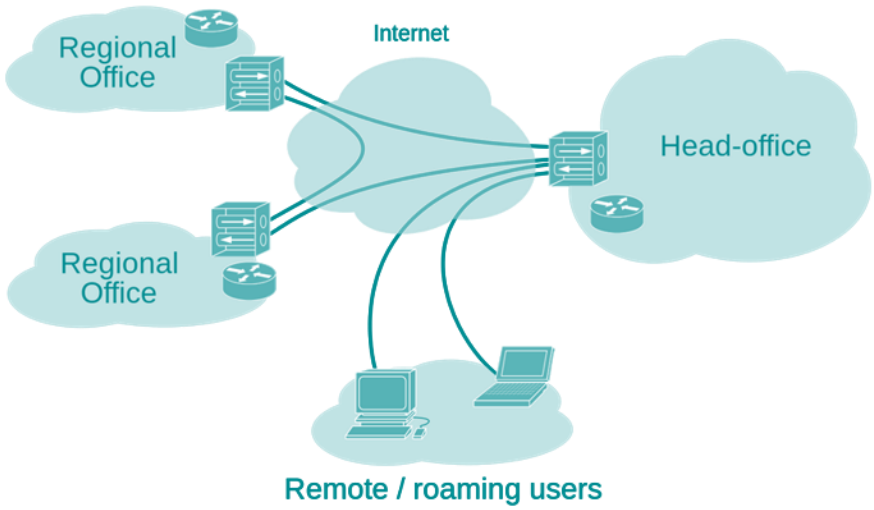


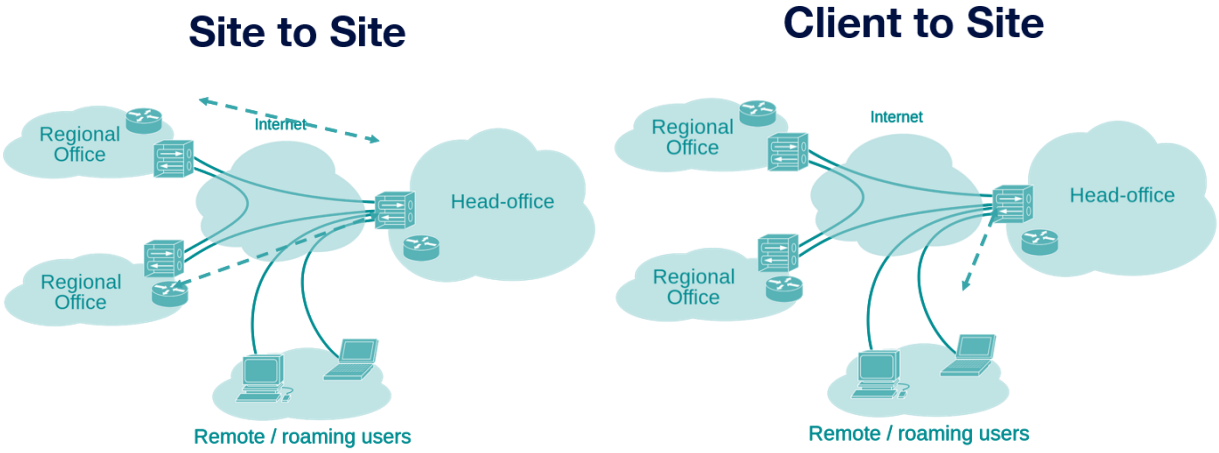
  - 4-byte Identifier
    - Tag Protocol Identifier (TPI)
    - Tag Control Identifier (TCI)

One VLAN is left untagged (called the Native VLAN)



- **VPN**
  - Virtual Private Network (VPN)
    - Extends a private network across a public network and enables sending and receiving data across shared or public networks





  - Full Tunnel VPN
    - Routes and encrypts all network requests through the VPN connection back to the headquarters
  - Split Tunnel VPN

        - Routes and encrypts only the traffic bound for the headquarters over the VPN, and sends the rest of the traffic to the regular Internet
    - Clientless VPN
        - Creates a secure remote-access VPN tunnel using a web browser without requiring a software or hardware client
    - Secure Socket Layer (SSL)
        - Provides cryptography and reliability using the upper layers of the OSI model (Layers 5, 6, and 7)
    - Transport Layer Security (TLS)
        - Provides secure web browsing over HTTPS

- **IPv6**
    - IPv4 = 2^{32}
        - 4.2 billion addresses
    - Address Exhaustion
        - Running out of network addresses in IPv4
            - IPv4 = 2^{32}
                - 4.2 billion addresses
            - IPv6 = 2^{128}
                - 340 undecillion addresses
    - IPv5 was an experimental protocol but some of its concepts have been incorporated into IPv6
            - Larger address space
            - No broadcasts
            - No fragmentation
            - Can coexist with IPv4
            - Simplified header
    - Dual Stack

- Simultaneously runs both the IPv4 and IPv6 protocols on the same network devices

- Tunneling
  - Allows an existing IPv4 router to carry IPv6 traffic

IPv4 Header			
Ver. 4	HL	TOS	Datagram Length
Datagram-ID		Flags	Flag Offset
TTL	Protocol		Header Checksum
Source IP Address			
Destination IP Address			
IP Options (with padding, if necessary)			

IPv6 Header			
Ver. 6	Traffic Class	Flow Label	
Payload Length		Next Header	Hop Limit
Source IP Address			
Destination IP Address			

- An IPv6 address uses hexadecimal digits and allows the use of shorthand notation
- Unicast Address
  - Used to identify a single interface
    - Globally Routed
      - Like IPv4's unicast class A, B, and C addresses and begins with 2000-3999
    - Link-Local/Local Use
      - Used like a private IP in IPv4 that can only be used on the local area network and begins with FE80
- Stateless Address Autoconfiguration (SLAAC)

        - Eliminates the need to obtain addresses or other configuration information from a central server
    - Multicast Address
        - Used to identify a set of interfaces and begins with FF
    - Anycast Address
        - Used to identify a set of interfaces so that a packet can be sent to any member of a set
    - Extended Unique Identifier (EUI)
        - Allows a host to assign itself a unique 64-bit IPv6 interface identifier called EUI-64
    - DHCPv6 Protocol
        - Allows DHCP to automatically assign addresses from a DHCPv6 server
    - Neighbor Discovery Protocol (NDP)
        - Used to determine the Layer 2 addresses that are on a given network

- **Ports and Protocols**
    - Port
        - Logical communication endpoint that exists on a computer or server
    - Inbound Port
        - Logical communication opening on a server that is listening for a connection from a client
    - Outbound Port
        - Logical communication opening created on a client to call out to a server that is listening for a connection
    - Ports can be any number between 0 and 65,535
    - Well-Known Ports
        - Ports 0 to 1023 are considered well-known and are assigned by the Internet Assigned Numbers Authority (IANA)

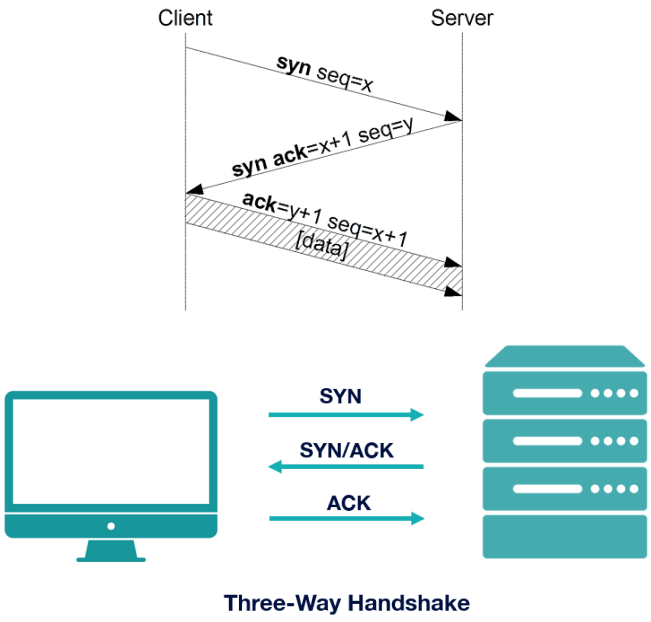
- Registered Ports
  - Ports 1024 to 49151 are considered registered and are usually assigned to proprietary protocols
- Dynamic or Private Ports
  - Ports 49152 to 65535 can be used by any application without being registered with IANA
  - Dynamic or Private Ports are commonly used for gaming, instant messaging, and chat
    - File Transfer Protocol (FTP)
      - Ports 20, 21
      - Provides insecure file transfers
    - Secure Shell (SSH)
      - Port 22
      - Provides secure remote control of another machine using a text-based environment
    - Secure File Transfer Protocol (SFTP)
      - Port 22
      - Provides secure file transfers
    - Telnet
      - Port 23
      - Provides insecure remote control of another machine using a text-based environment
    - Simple Mail Transfer Protocol (SMTP)
      - Port 25
      - Provides the ability to send emails over the network
    - Domain Name Service (DNS)
      - Port 53

    - Converts domain names to IP addresses, and IP address to domain names
- Dynamic Host Control Protocol (DHCP)
    - Ports 67, 68
    - Automatically provides network parameters such as assigned IP address, subnet mask, default gateway, and the DNS server
- Hypertext Transfer Protocol (HTTP)
    - Port 80
    - Used for insecure web browsing
- Post Office Protocol Version Three (POP3)
    - Port 110
    - Used for receiving incoming emails
- Network Basic Input/Output System (NetBIOS)
    - Ports 137, 139
    - Used for file or printer sharing in a Windows network
- Internet Mail Application Protocol (IMAP)
    - Port 143
    - A newer method of retrieving incoming emails which improves upon the older POP3
- Simple Network Management Protocol (SNMP)
    - Ports 161, 162
    - Used to collect data about network devices and monitor their status
- Lightweight Directory Access Protocol (LDAP)
    - Port 389
    - Used to provide directory services to your network
- Hypertext Transfer Protocol – Secure (HTTPS)

- Port 443
- Used as a secure and encrypted version of web browsing
  - SSL (Secure Socket Layer)
  - TLS (Transport Layer Security)

- Server Message Block (SMB)
  - Port 445
  - Used for Windows file and printer sharing services
- Remote Desktop Protocol (RDP)
  - Port 3389
  - Provides graphical remote control of another client or server
  - RDP provides a full graphical user interface

- **TCP Versus UDP**
  - Transmission Control Protocol (TCP)
    - Connection-oriented protocol, which means it's a reliable way to transport segments across the network



Three-Way Handshake

- User Datagram Protocol (UDP)
  - Unreliable and it transmits segments called data grams

TCP	UDP
Reliable (three-way handshake)	Not reliable
Connection-oriented	Connectionless
Segment retransmission and flow control (windowing)	No retransmission and no windowing
With segmentation of sequencing	Without sequencing
With acknowledgment	Without acknowledgment

- TCP (Connection-Oriented)
  - SSH, HTTP or HTTPS
- UDP (Connectionless)
  - Audio, video streaming, DHCP, and TFTP
    - Dynamic Host Control Protocol (DHCP)
      - Ports 67, 68
      - Automatically provides network parameters such as assigned IP address, subnet mask, default gateway, and the DNS server
    - Trivial File Transfer Protocol (TFTP)
      - Ports 69
      - a connectionless protocol that uses UDP as its transport

Network Services

Objective 2.4

- OBJ 2.4: Summarize services provided by networked hosts

- **File and Print Servers**
    - Server
        - Can be configured to allow the clients on the network to access the network and be able to read and write to its disk (file share)
    - Print Server
        - Another server that could be a physical workstation or network infrastructure that provides printing functionality
    - Windows-based file and print server
        - Relies on the NetBIOS protocol or SMB
            - Network Basic Input/Output System (NetBIOS)
                - Ports 137, 139
                - Used for file or printer sharing in a Windows network
            - Server Message Block (SMB)
                - Port 445
                - Used for Windows file and printer sharing services
    - Samba
        - Provides the ability for a Linux or Unix server to be able to host files or printers that can then be used by Windows clients running the SMB protocol
    - Linux or Unix-based file and print server
        - Supports windows machines known as Samba
            - File Transfer Protocol (FTP)
                - Ports 20, 21
                    - Provides insecure file transfers

- IP-based File and Print Server / Cloud Printing
  - Allows for printing anywhere in the world

- **Web Servers**
  - Web Servers
    - Any server that provides access to a website
      - HTTP
        - Port 80
      - HTTPS
        - Port 443
  - Internet Information Services (IIS)
    - Extensible web server software, created by Microsoft (HTTP, HTTP/2, and HTTPS)
  - Apache
    - Most popular way to run a web server these days
  - NGINX
    - Reverse proxy, load balancer, mail proxy, and HTTP cache
  - Uniform Resource Locator (URL)
    - Combines the fully qualified domain name with a protocol at the beginning
  - When a web browser connects to a server, it will be able to see a digital certificate to create a random code

- **Email Servers**
  - Email Server
    - Servers that are set up to compose a message and send it to another user
      - Simple Mail Transfer Protocol (SMTP)

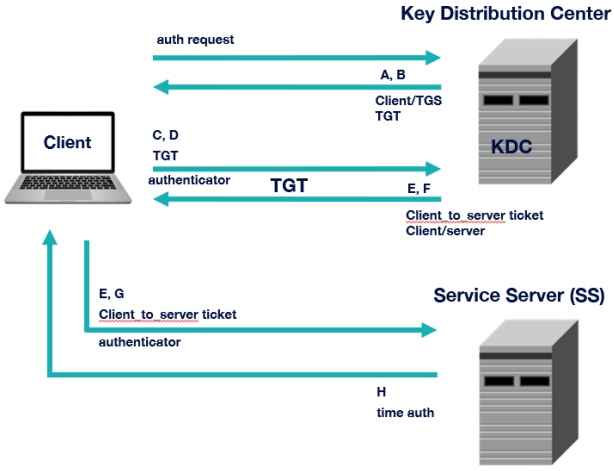
    - Specifies how emails should be delivered from one mail domain to another
    - Send mail transfer protocol
    - SMTP operates over port 25
  - Post Office Protocol 3 (POP3)
    - Older email protocol which operates over port 110
  - Internet Message Access Protocol (IMAP)
    - Mail retrieval protocol
    - IMAP operates over port 143 and can connect to a server and receive and read messages
  - Microsoft Exchange
    - Mailbox server environment designed for Windows-based domain environments
    - Microsoft Exchange Server is widely used in many corporate environments

- **AAA Servers**
  - 802.1x
    - Standardized framework used for port-based authentication on wired and wireless networks
  - Authentication
    - Occurs when a person's identity is established with proof and is confirmed by the system
      - Something you know
      - Something you are
      - Something you have
      - Something you do
      - Somewhere you are

- Lightweight Directory Access Protocol (LDAP)
  - A database used to centralize information about clients and objects on the network
- Active Directory (AD)
  - Used to organize and manage the network, including clients, servers, devices, users, and groups
- Remote Authentication Dial-In User Service (RADIUS)
  - Provides centralized administration of dial-up, VPN, and wireless authentication services for 802.1x and the EAP
    - RADIUS operates at the application layer
    - RADIUS utilizes UDP for making connections
- Terminal Access Controller Access-Control System Plus (TACACS+)
  - Proprietary version of RADIUS that can perform the role of an authenticator in 802.1x networks

TACACS+	RADIUS
Relies on TCP	Relies on UDP
Separates authentication, authorization, and accounting processes	Combines authentication and authorization
Supports all network protocols	Does not support all network protocols
Exclusive to Cisco devices	Has cross-platform capability

- Authorization
  - Occurs when a user is given access to a certain piece of data or certain areas of a building
- Kerberos
  - Authentication protocol used by Windows to provide for two-way (mutual) authentication using a system of tickets



- A domain controller can be a single point of failure for Kerberos

- Accounting
  - Ensures the tracking of data, computer usage, and network resources is maintained
- Non-repudiation
  - Occurs when you have proof that someone has taken an action

- **Remote Access Servers**
  - Telnet Port 23
    - Sends text-based commands to remote devices and is a very old networking protocol
    - Telnet should never be used to connect to secure devices
  - Secure Shell (SSH) Port 22
    - Encrypts everything that is being sent and received between the client and the server
  - Remote Desktop Protocol (RDP) Port 3389
    - Provides graphical interface to connect to another computer over a network connection
    - Remote desktop gateway (RDG) creates a secure connection to tunnel into the RDP

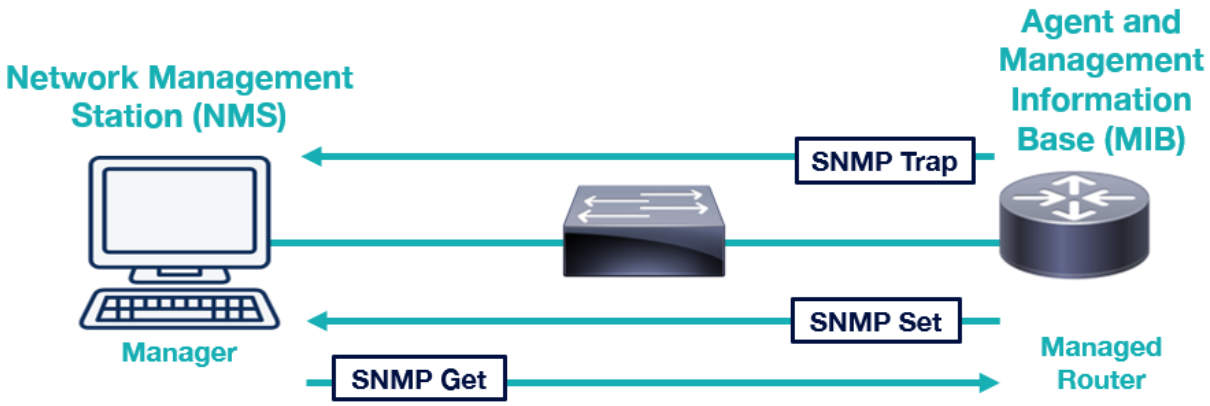
- Virtual Network Computing (VNC) Port 5900
  - Designed for thin client architectures
- Terminal Emulator (TTY)
  - Any kind of software that replicates the TTY I/O functionality to remotely connect to a device
  - TTY is the terminal or end point of the communication between the computer and the end-user

- **Network Monitoring Servers**
  - Syslog
    - Enables different appliances and software applications to transmit logs to a centralized server
    - Syslog is the de facto standard for logging events
      - PRI code (Priority code)
      - Header
      - Message

New Syslog
Uses TCP
Uses TLS
Uses MD5 and SHA1

  - Simple Network Management Protocol (SNMP)
    - TCP/IP protocol that aids in monitoring network-attached devices and computers
  - Managed Devices
    - Computers and other network-attached devices monitored using agents by a network management system
  - Agents

        - Software that is loaded on a managed device to redirect information to the network management system
    - Network Management System (NMS)
        - Software running on one or more servers to control the monitoring of network-attached devices and computers



    - Management should be conducted on an out-of-band network to increase security

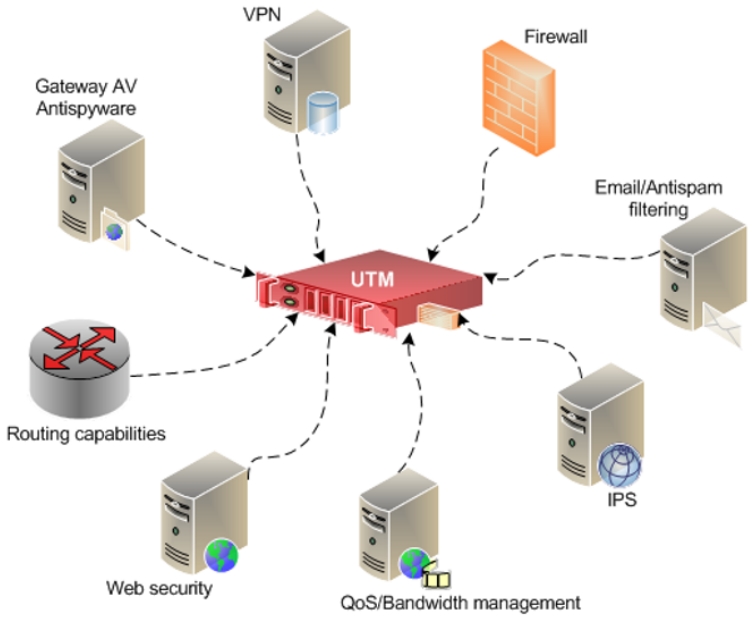
- **Proxy Servers**
    - Proxy Server
        - Devices that create a network connection between an end user's client machine and a remote resource (web server)
            - Increased network speed and efficiency
            - Increased security
            - Additional auditing capabilities
- **Load Balancers**
    - Load Balancer/ Content Switch
        - Distributes incoming requests across several servers inside a server farm or a cloud infrastructure
        - A load balancer is one of the key things to help defend against a DoS attack or a DDoS attack

- Denial of Service (DoS)
    - Involves a continual flooding of victim systems with requests for services, causing the system to crash (single attacker)
- Distributed Denial of Service (DDoS)
    - Multiple machines simultaneously launch attacks on the server to force it offline (multiple attackers)
- Blackholing/Sinkholing
    - Identifies any attacking IP addresses and routes their traffic through a Knoll interface
- Intrusion Prevention System (IPS)
    - Works for small-scale attacks against DoS
- Elastic Cloud
    - Allows to scale up the demand as needed

- **Unified Threat Management**
    - Access Control List (ACL)
        - Rule sets placed on the firewalls, routers, and other network devices that permit or allow traffic through a particular interface
        - The actions are performed top-down inside of an ACL
            - Top
                - Specific rules
            - Bottom
                - Generic rules
    - Firewall
        - Inspects and controls the traffic that is trying to enter or leave a network's boundary
            - Packet-filtering

- Stateful
- Proxy
- Dynamic packet-filtering
- Kernel proxy

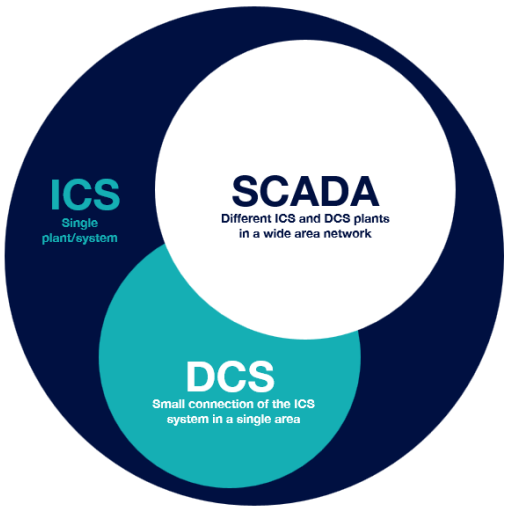
- Unified Threat Management (UTM)
  - Provides the ability to conduct security functions within a single device or network appliance



Advantages	Disadvantages
Reduced number of devices to learn, operate, and maintain	Single point of failure
Lower upfront costs, maintenance, and power consumption	Lacks detail provided by a specialized tool
Easier to install and configure	Performance is not as efficient as single function devices

- **ICS/SCADA**
  - Information Technology (IT)
    - Includes computers, servers, networks, and cloud platforms

- Operational Technology (OT)
  - Communications network designed to implement an ICS
  - Technology that interacts with the real world
- Industrial Control System (ICS)
  - Provides the mechanisms for workflow and process automation by controlling machinery using embedded devices
  - Multiple ICSs can create a distributed control system (DCS)
- Fieldbus
  - Digital serial data communication protocol used in OT networks to link different PLCs
- Programmable Logic Controller (PLC)
  - Type of digital computer used in industrial settings that enables automation and assembly lines, autonomous field operations, robotics, and other applications
- Human-Machine Interface (HMI)
  - Can be a local control panel or software that runs on a computer
- Supervisory Control and Data Acquisition (SCADA)
  - Type of ICS used to manage large scale multi-site devices and equipment in a geographic region from a host computer



- Cellular
- Microwave
- Satellite
- Fiber
- VPN-based LAN

- **Embedded Systems**
  - Embedded Systems
    - Computer system that is designed to perform specific and dedicated functions
    - These systems are considered static environments, where frequent changes are not allowed
  - Programmable Logic Controller (PLC)
    - Type of digital computer used in industrial or outdoor settings
    - The PLC patch is every six months or two years
  - Real-time Operating System (RTOS)
    - Type of OS that prioritizes deterministic execution of operations that ensure consistent response for time-critical tasks
    - Embedded systems in critical applications
  - System-on-a-Chip
    - Processor integrates the platform functionality of multiple logical controllers onto a single chip
      - Processor
      - Memory
      - Storage
      - Graphics processor
      - Peripherals
- **Legacy Systems**

- Legacy System
  - Computer system that is no longer supported by its vendor and no longer provided with security updates and patches
  - Identify legacy systems and put mitigations in place to keep operating such systems
- Proprietary System
  - System that is owned by its developer or vendor

Mobile Devices

- OBJ 1.2: Compare and contrast the display components of mobile devices
- OBJ 1.3: Given a scenario, set up and configure accessories and ports of mobile device
- OBJ 1.4: Given a scenario, configure basic mobile-device network connectivity and application support

- **Mobile Devices**
  - Mobile Device
    - Any device that makes it portable and easy to use

- **Mobile Display Types**
  - Capacitive Touch Screen
    - Any touchscreen that works by seeing the distortion in an electrostatic field
    - A single tactile input is one touch at a time
  - Multi-Touch Screen
    - Can process two or more contact points simultaneously
  - Liquid-Crystal Display (LCD)
    - Uses liquid crystal where the properties can change with the application of voltage
  - Pixel (Picture Element)
    - Individual point on a screen inside of a display
    - A thin-film transistor (TFT) is referred to as an LCD panel
  - Twisted Nematic (TN)
    - Contains crystals that twist or untwist in response to the voltage being applied or removed
    - TN supports fast response time in comparison to other TFT technologies and displays

- In-Plane Switching (IPS)
  - Uses crystals that rotate to be able to deliver color
  - IPS panels can support 178° horizontal and vertical viewing angles
- Vertical Alignment (VA)
  - Crystals are tilted to be able to deliver color
  - A VA display has a contrast ratio of two to three times better than a standard IPS display
- Cold Cathode Fluorescent Lamp (CCFL)
  - Lamp that sits behind the display and lights up the liquid crystal display to show the colors and images properly on the screen
  - CCFL requires AC voltage
- Light-Emitting Diode (LED)
  - Newer form of light that uses direct current (DC)
  - The use of LEDs uses less power, leading to longer battery life and better performance
- Organic LED (OLED)
  - Each pixel has its own separate LED that provides the light
  - OLEDs can be made from plastic
  - OLEDs can be folded, rolled up, or manipulated to create different shapes and sizes of displays

- **Mobile Device Components**
  - Digitizer
    - Layer sandwiched between a layer of protective glass and the display panel inside of a touchscreen display
    - Haptic feedback provides a form of touch responsiveness from the display back to the end-user
  - Accelerometer

        - Combination device that uses hardware and software to measure the velocity, rotation, and shaking of a mobile device
        - The accelerometer works when dealing with the X (horizontal) and Y (vertical) axis
    - Gyroscope
        - An improved version of the basic accelerometer
            - Detects pitch (Y), roll (X), and yaw (Z)
            - Performs actions
            - Stabilizes images

- **Mobile Device Accessories**
    - Track Pad
        - Device that can be used to manipulate the cursor on the screen
    - Drawing Pad
        - Large format touch device attached as a peripheral to a laptop, smartphone, or tablet
        - A drawing pad uses a touch pen
    - Microphone
        - Any device used to record audio or capture voice when making a phone call
    - Speaker
        - Allows to hear things that are coming out from devices, such as music or videos
    - Headset
        - Combines both the microphone and speaker into one device
    - Digital Camera
        - Provides the ability to capture a live image in a still format

- **Mobile Device Wireless Connectivity**
  - Wi-Fi (Wireless Network)
    - Comes in different types of Wi-Fi, including wireless a, b, g, n, ac, and ax
    - Wireless connectivity on smaller devices is slower than it is on larger devices
    - Larger antennas pick up signals with more strength and faster speeds
  - Cellular
    - Network that allows to connect to the Internet using cellular radio inside the handset and connect to a network service provider
  - Global System for Mobile Communication (GSM)
    - Cellular technology that takes the voice during a call and converts it into a digital format
  - Code-Division Multiple Access (CDMA)
    - Cellular technology that uses code division to split up the channel
    - CDMA is a more powerful and flexible technology than GSM
      - W-CDMA
        - Wideband CDMA
      - UMTS
        - Universal Mobile Telecommunications System
    - An electronic SIM is a cheaper way of getting a data service when overseas
  - Preferred Roaming List (PRL)
    - Contains all the information about different cellular towers
    - Restrictions vary from model to model and depends on the device's country of origin
  - Bluetooth
    - Used as a short-range point-to-point network connection between a mobile device and an accessory

- Near-Field Communication (NFC)
  - Allows a device to receive and send information in the NFC format
  - The pairing process can be done automatically by using NFC connection

- **Mobile Device Wired Connectivity**
  - Lightning Cable
    - Proprietary cable that is only used by Apple devices
  - USB-C
    - Modern version of USB that operates at USB 3.0 speeds and can provide data
  - DB9 Cable
    - D-shaped connector with 9 pins that is used to connect external serial devices like modems
  - Universal Asynchronous Receiver-Transmitter (UART)
    - Device that allows to connect to a device and get information from it

- **Port Replicators & Docking Stations**
  - Port Replicator
    - Uses the exact same features as a laptop
    - Port replicator makes life easier by providing easier access to all the ports
  - Docking Station
    - Advanced type of port replicator that provides all the capabilities and features of a laptop
      - Port Replicator
        - Port mirror
      - Docking Station
        - Additional ports

Mobile Applications

- OBJ 1.4: Given a scenario, configure basic mobile-device network connectivity and application support

- **Mobile Applications**
  - Mobile Applications
    - Used to provide different features and functionality to a mobile device

- **Mobile Device Synchronization**
  - Android
    - Offers an open-source code base
  - iOS
    - Developed by Apple for use on iPhones and iPads
    - iOS relies on closed-source code
  - Open-Source
    - The software and the original source code are available to download, modify, and redistribute
    - Android OS has a lower cost of services by using an open-source platform as a code base
  - Closed-Source Software
    - Proprietary software that is licensed under the exclusive legal rights of the copyright holder
      - Open-Source Software
        - Creativity and change
      - Closed-Source Software
        - Change is not allowed
  - App Store

        - Application on an iOS device to access a store to purchase and download applications
            - iOS Application
                - Swift and Xcode
            - Android Application
                - Java and Android Studio
    - Microsoft 365
        - Provides the ability to have office productivity software and a large amount of storage space in the cloud (OneDrive)

- **Data for Synchronization**
    - Mobile Device Synchronization/Sync
        - Act of copying data back and forth between different devices
    - Contact
        - Record inside of an address book that contains fields of names, addresses, emails, phone numbers, notes, etc.
    - vCard
        - Standard format and is widely supported by most address books and software applications
    - Calendar Information
        - Any record with fields for appointments or tasks with their corresponding subject, date, location, and attendees
        - Cloud-based service is easier and more synchronized
    - POP3
        - Oldest format and does not support the synchronization across devices
    - IMAP and Exchange can manage the state of an email
    - When buying an application, consider what apps are supported on which devices

- Third-party password managers provide the ability to generate strong, random passwords when signing up for a new account

- **Synchronization Methods**
  - Synchronization to the Cloud
    - Provides the access to the cloud from all devices and becomes the central repository of all data
    - Encrypted data that is stored in the cloud is relatively safe
    - Synchronization to the cloud requires a large amount of data
  - Synchronization to the Computer
    - Synchronizes directly to the desktop or laptop using a USB or Bluetooth connection
    - Install the iTunes app on the Windows PC to transfer the data from the iPhone
  - Synchronization with the automobile

- **MDM and MAM**
  - Enterprise Mobility Management (EMM)
    - Class of software designed to apply security policies for use on mobile devices
  - Mobile Device Management (MDM)
    - Sets device-level policies for authentication, feature use, and conductivity
    - MDM is a type of software that allows to control the device
  - Mobile Application Management (MAM)
    - Sets forth policies for apps that can process corporate data and prevent data transfer to personal apps
  - Sandbox Solution

        - Configures an enterprise-managed container or workspace where the company's data is stored
    - Data Loss Prevention (DLP)
        - Detects when data is being taken from a device, ensuring it's only being used in the proper way
    - Apple Business Manager (ABM)
        - MAM suite that allows applications from a private repository to devices that are part of the corporate network
    - Managed Google Play
        - Managed version of the Google Play store that contains apps that are distributed to employees' devices

- **Multifactor Authentication (MFA)**
    - Knowledge Factor
        - Simplest form of authentication and refers to something you know
    - Possession Factor
        - Refers to something you have
    - Inherence Factor
        - Refers to something you are
    - Behavior Factor
        - Refers as something you do
        - Voice recognition systems are not looking at what is said, but at how it is said
    - Location Factor
        - Refers to somewhere you are
    - Authenticator
        - Application that serves as a possession factor inside of a mobile device
    - Multi-factor authentication has two or more factors

- **Location Services**
  - Course Positioning
    - Oldest method of positioning using mobile phones
  - Global Positioning System (GPS)
    - Space-based radio navigation system, consisting of satellites and networks of ground stations
  - Indoor Positioning System (IPS)
    - Allows a device to be used indoors to figure out the location
  - Change the location service as a privacy aspect
  - Geo-Tracking
    - Tracking of a location for a given amount of time
    - Disable GPS and IPS to block geo-tracking
    - Geotagging is the GPS coordinates inside photos

- **Corporate Email Configuration**
  - Configure SSL or TLS when connecting to the email servers

POP3	Port 995
IMAP	Port 993
SMTP	Port 465

  - POP3/IMAP
    - Receiving email/Inbound mail
  - STMP
    - Sending/Outbound mail
    - Major providers like Gmail, Outlook, or Yahoo use auto configuration
    - Small or medium-sized businesses use their own institutional email server
  - Transport Layer Security (TLS)
    - New and advanced secure version of encryption

Configuration	Unencrypted	Encrypted
IMAP	Port 143	Port 993
POP3	Port 110	Port 995
SMTP	Port 25	Port 465

Laptop Hardware

- OBJ 1.1: Given a scenario, install and configure laptop hardware and components

- **Security Components**
  - Biometric Sensor
    - Allows users to create a template of a feature of the laptop's body (fingerprint, facial scan, or voice recognition)
  - Near-Field Communication Scanner (NFC scanner)
    - Used to pair peripheral devices to a smartphone or tablet
  - Kensington Lock (K-Slot/ Kensington Security Slot)
    - Small port on the side of a laptop that able to connect a metal braided cable to lock

- **Replacing the Keyboard**
  - Entire keyboard
  - Particular key
  - Touch pad
  - When replacing the keyboard or touch pad, use one from the manufacturer

Printers and MFDs

- OBJ 3.6: Given a scenario, deploy and configure multifunction devices/printers and settings

- **Unboxing and Setup**
  - Check the manufacturer's instructions before starting the process
  - During the unboxing, look for extra pieces, cables, documentation, or driver disks
    - Printhead
      - Inkjet printer
    - Drum and toner cartridges
      - Laser printer
  - The hot temperature causes condensation and moisture inside the printer
  - The location of the printer should be well-ventilated
  - The location of the printer should be convenient
    - Print queuing system
    - Print authentication system

- **Printer Connectivity**
  - USB Connection
    - Found in a home environment
    - Windows has the ability to detect a printer using plug and play
  - Ethernet Connection
    - Network cable that uses an RJ45 port
    - A printer with Ethernet capability supports DHCP
  - Wireless Connection
    - Comes with either Wi-Fi or Bluetooth
      - Infrastructure Mode
        - Printer is connected to the access point

- Wi-Fi Direct Mode
    - Allows the printer to act as an access point
- Bluetooth
    - Uses a wireless point-to-point connection from the printer to the computer

- **Printer Drivers**
    - Printer
        - Program that controls physical printers
    - Printer Driver
        - Integrated into a printer
        - You must have administrative rights to install print drivers
    - Windows 11
        - Start > Settings > Bluetooth & devices > Printers & scanners
    - Windows 10
        - Start > Settings > Devices > Printers & scanners
    - MacOS
        - Settings > Printers & scanners
    - Page Description Language (PDL)
        - Used to create a raster file from the print commands that are sent by a software application
    - Scalable Font
        - Capable of being resized to any size
    - Vector Graphic
        - Size can be changed before printing
            - Bitmap
                - Distorted
            - Vector

        - Clear
    - Additive
        - Display
    - Subtractive
        - Printer
- Printer Control Language (PCL)
    - Developed by HP and is closely tied to the features of different printer models
- Postscript
    - Created by Adobe and is designed to be a device-independent PDL
- XML Paper Specification (XPS)
    - Microsoft's page description language (PDL)
- Portable Document Format (PDF)
    - Created by Adobe which keeps a file's original look when viewed or printed on different systems
    - PDF is larger in size than XPS format files

1. When installing a printer, also install the appropriate driver
2. Two generic formats: PCL and Postscript
3. Virtual printers: XPS and PDF

- **Sharing Print Devices**
    - Print Server
        - Software application or hardware device that manages print requests and printer queue status information
        - Centralized print server allows to control, to configure, and to troubleshoot the devices remotely from a network
        - Print servers are suitable for small and home offices with up to fifty servers

        - Embedded print servers support one printer
    - Microsoft Management Console (MMC)
        - Allows to share network printers and centralize the print server from the centralized window server
    - Printer Share
        - Allows to connect a printer using Bluetooth or USB
    - Print Spooler
        - Service built into the Windows OS and exists to help print jobs

- **Securing Print Devices**
    - User Authentication
        - Sets permissions for the printer that require a log in with a username or password
    - Audit Log
        - Record of jobs that have been sent and printed on a particular device
    - Secured Print
        - Device held on the printer until the user's authentication
- **Scanning Services**
    - Scanning
        - Allows the printer to be used as a copy machine or a scanner
    - Scanner
        - Digital imaging device
    - Optical Character Recognition (OCR)
        - Convert scanned text into digital documents that can be manipulated using a word processing program

Printer Types

- OBJ 3.7: Given a scenario, install and replace printer consumables

- **Laser Printers**
  - Laser Printer
    - Creates an entire page at one time during the printing process
  - Image Drum
    - Main component that creates the image to be applied to the paper
  - Fuser Assembly
    - Heats up and melts the toner onto the page to adhere properly to the page
  - Transfer Belt/Roller
    - Used to transfer the image from the image drum and become fused
  - Pickup Roller
    - Used to pick up the paper from the feed tray and feed it through the system
  - Paper Separation Pad
    - Helps the pickup rollers to ensure they only pick up a single piece of paper at a time
  - Duplexing Assembly
    - Moves the paper from the front to the back
  - A toner cartridge is a plastic housing that contains toner powder
  - The drums last longer than the toner
  - Processing
    - The OS uses a print driver to translate what's on the screen to print
  - Most laser printers support memory upgrading using a SODIMM module
  - Charging
    - The imaging drum is conditioned with the primary charge roller

- Exposing
  - The surface coding of the photosensitive imaging drum is losing its charge when exposed to light
- Developing
  - The laser printer takes the toner and applies it to a developer roller
- Transferring
  - Moving the toner from the imaging drum into the print media
- Fusing
  - The fuser squeezes the paper between a hot roller and a pressure roller
- Cleaning
  - The photosensitive drum needed to be cleaned and get all the remaining toner particles cleaned off
- Charging voltage is -600 VDC (negative 600 volts DC)
- Most laser printers have a duplexing assembly installed

- **Laser Printer Maintenance**
  - Turn off the laser printer and allow it to cool down
  - Loading paper
    - Buy laser paper that is rated for the type of printer
    - Store the paper in a nice dry area that does not have high humidity or excessive dust
  - Toner cartridges replacement
    - Standard toner cartridge has 2500 pages
    - High-yield cartridge has 6000 pages
  - Use of maintenance kit
    - Feed rollers pull up one sheet at a time and feed it through the system
    - Transfer rollers are used to take the toner off the imaging drum and apply it to the paper

        - Fuser unit is responsible for heating up the toner and making it bond to the page
        - Page count indicates when to change the feed roller, transfer roller, or the fuse unit
    - Calibration
        - Process by which the printer determines the print density or color balance to use
    - Cleaning the printer
        - If toner gets on the skin, wash it with cold water
        - Do not use compressed air
        - Some printers with filters must be kept free from dust and dirt

- **Inkjet Printers**
    - Inkjet printer creates an image on the paper through a nozzle or jet on a print head onto the paper
    - High-end inkjet printers have seven different cartridges
    - Printhead
        - Device that takes the droplets of ink and directs into the paper
    - Piezoelectric/Charge Method
        - Uses a nozzle that reacts to changes in voltage
    - Thermal Method
        - Used by HP, Canon, and Lexmark printers, and relies on heating up the ink in the nozzle of the printhead
    - Thermal method replaces the printhead when replacing the ink cartridge
    - Piezoelectric method does not require to replace the printhead when replacing the ink cartridge
    - Roller

        - Responsible for advancing the paper through the inkjet printer
    - Feeder
        - Allows multiple pieces of paper in a tray to be selected one piece of paper at a time and passes it to the roller
    - Duplexing Assembly
        - Allows an inkjet printer to print on both sides of a piece of paper
    - Carriage Belt/Carriage System
        - Allows the printhead to move back and forth across the page
    - Unidirectional Printing
        - Printhead will only apply ink from left to right
    - Bi-directional Printing/Two-Directional Printing
        - Apply ink from left to right and from right to left

- **Thermal Printers**
    - Thermal Printer
        - Type of printer that uses a heating element to create an image
    - Thermal paper works in high-speed environments
    - Thermal ribbon has a mixture of colors (CMYK) and is used to create the heat transfer
    - The number of pins on the thermal printhead determines the quality of the printout
        - Laser Printer
            - 300 - 600 dpi
        - Thermal Printer
            - 100 - 300 dpi
    - Color Thermal Printer
        - Uses thermal ribbon to create images
    - Replacing the paper

        - Open the printer case
        - Insert the role (shiny part facing outward)
        - Place the end of the paper by the printhead and close again
    - Cleaning the heating element
        - Use isopropyl alcohol with cotton swab to clean the printhead
    - Removing debris
        - Unplug the thermal printer
        - Take out the paper role
        - Clean the feed mechanism

- **Impact Printers**
    - Impact printers are measured based on the quality of the dots
    - Impact printer has the highest resolution of 240 dpi
    - Tracks
        - Series of holes going down the side of the paper with a perforation between the regular paper and tracks
    - Printhead
        - Device that has a series of pins that make up the dot matrix that forms the image
    - Ribbon
        - Fabric or material held within a plastic housing in front of the printhead
    - Tractor Feed
        - Exists on both sides of the printer and pulls the paper through the printer using tractor fed paper
    - Power off the printer and let it cool down for 30 to 60 minutes

- **3-D Printers**
    - 3D Printer

        - Type of printer that creates images in three dimensions (height, width, and depth)
    - A slice is one layer of the overall 3D model
    - Print bed/Build plate
        - Flat plate where the material will be extruded and built
    - Bed/Build Surface
        - Sheet placed on top of the base plate that hold the object into position while printing
    - Extruder
        - Printhead for 3D printers
    - Fan
        - Helps to cool down the melted filament to retain the consistency
    - Filament
        - Ink for 3D printers (1.75 mm or 3 mm)

Troubleshooting Methodology

- OBJ 5.1: Given a scenario, apply the best practice methodology to resolve problems

- **Troubleshooting Methodology**
    1. Identify the problem
    2. Establish a theory of probable cause
    3. Test the theory to determine the cause
    4. Establish a plan of action to resolve the problem and implement the solution
    5. Verify full system functionality
    6. Document the findings, actions, and outcome

- **Identify the Problem**
    - What happened?
    - What was the status before?
    - What is the status after that?
    - Are there any changes in the system?

- **Establish a Theory**
    - Probable Cause
        - Different possible causes that may have happened
    - Burning smell
        - Damaged processor or motherboard components
    - Clicking or grinding sound
        - Hard drive
    - No spinning fan
        - Power issue or broken fan

Question the obvious	External research (internet)	Internal research (system)

- **Test the Theory**
  - Theory is confirmed
  - Theory is not confirmed
  - Lack skills or authority
  - Unable to solve
  - Escalate when there is an issue

- **Establish a Plan of Action**
  - Repair
  - Replace
  - Workaround
  - How many are the resources
  - How much time does it take
  - How much is the cost
  - Impact on the users and system
  - A change of plan needs to get the authorization again

- **Verify System Functionality**
  - Identify the problem
  - Establish a theory
  - Test the theory
  - Establish a plan of action
  - Verify system functionality
  - Check that the problem has been solved

- Inspect the other components to ensure nothing else is damaged, broken, or disconnected
- Check the logs and diagnostic tools to confirm everything is working the way they should
- Verify system functionality
- Implement preventative measures

- **Documentation**
  - Documentation
    - Document the findings, actions, and outcomes
  - The trouble ticketing system allows to do the trend analysis
  - The trouble ticketing system can document the amount of work

Troubleshooting Hardware Issues

- OBJ 5.2: Given a scenario, troubleshoot problems related to motherboards, RAM, CPU, and power

- **Power Issues**
  - Power button is not connected properly to the motherboard
  - Wall outlet is faulty
    - Use a multimeter or voltmeter to test the power outlet
      - 110-120V/60Hz

        US or Canada
      - 220-240V/50Hz

        Europe or Asia
  - Power cable to the computer is faulty
    - Positive pin
    - Negative pin
    - Grounding pin
  - Power supply is faulty
    - 12V DC
    - 5V DC
    - 3.3V DC
    - A power supply tester has a small variation or tolerance
      - Bottom

        Largest connector
      - Top

        4,6,8 Pin connectors/SATA/Molex
  - Power cables from power supply to components are faulty
    - When testing detachable cables, check each pin on each side of the cable to verify full continuity

- Incorrect voltage setting on power supply unit

- **POST Issues**
  - Power-On Self-Test (POST)
    - Diagnostic program inside the system firmware

Code	Meaning
1 Short beep	Normal POST - system is OK
2 Short beeps	POST error - error code shown on screen
No beep	Power supply issue, motherboard problem, or faulty onboard speaker
Continuous beep	Problem with system memory modules or memory controller
Repeating short beeps	Power supply fault or motherboard problem
1 Long, 1 short beep	Motherboard problem
1 Long beep, 2 or 3 beeps	Video adapter error
3 Long beeps	Keyboard issue (check that a key is not depressed)

    - POST beep codes are specific to the motherboard's manufacturer
    - POST-test expansion card identifies which component on the motherboard is faulty and needs to be replaced

- **Crash Screens**
  - Crash Screen
    - Displays an error whenever the operating system has issue
      - Windows
        - Blue Screen of Death (BSOD)
          - Indicates that there is a problem with the underlying hardware that Windows cannot solve
            - CRITICAL_PROCESS_DIED
            - SYSTEM_THREAD_EXCEPTION_NOT_HANDLED
            - IRQL_NOT_LESS_OR_EQUAL
            - VIDEO_TDR_TIMEOUT_DETECTED

- PAGE_FAULT_IN_NONPAGED_AREA
- SYSTEM_SERVICE_EXCEPTION
- DPC_WATCHDOG_VIOLATION

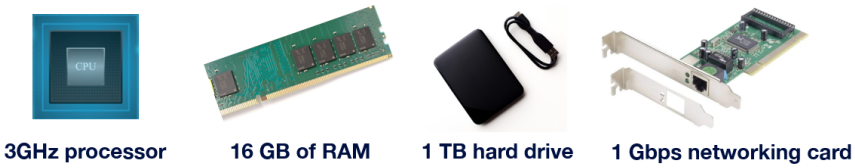
- MAC
  - Pinwheel of Death
    - macOS (OS X)
      - Made by Apple and it runs on Apple hardware (desktops and laptops)
- Linux
  - Kernel Panic
    - In kernel panic, the system display gives an exit code

- **Cooling Issues**
  - When the system is operating, all the components are generating heat that builds up a thermal load
  - When it comes to cooling, make sure that all cooling components are working
    1. Shut down the system
    2. Boot into the UEFI or BIOS
  - In UEFI or BIOS, look at the temperature sensors inside of the system
  - A thermal issue causes intermittent shutdowns or continual rebooting

- **Physical Component Damage**
  - Excessive exposure to thermal loads can cause permanent damage
  - Plugging or unplugging cables can cause wearing out, and pins getting bent or damaged
  - The rancid smell comes from a blown or burst capacitor

- When a capacitor starts emitting internal chemicals, it loses the ability to regulate electricity

- **Performance Issues**



  - Modern systems can protect against overheating
  - Overheating systems could reboot or shut down
  - Increasing the page size in Windows or the swap space in Linux

- **Inaccurate System Date/Time**
  - Motherboards have a battery to keep the real-time clock (RTC) in sync
  - Most modern operating systems set the date and time automatically
    - Complementary Metal–Oxide–Semiconductor (CMOS)
      - Non-volatile type of memory that stores the BIOS settings and is built into the motherboard
    - Non-Volatile RAM (NVRAM)
      - Stores data without being constantly refreshed
        - CMOS
        - Real-time clock

Troubleshooting Storage Devices

- OBJ 5.3: Given a scenario, troubleshoot and diagnose problems with storage drives and RAID arrays

- **Boot Issues**
  - SSD/Hard drive
  - Removable media
  - Network
  - Master Boot Record (MBR)
    - Legacy method of providing the boot information
    - A partition on a storage device is the logical part of an entire drive
      - Windows

        Single partition
      - Linux

        Multiple partitions
      - Boot Configuration Data (BCD)

        Windows
      - GRUB/LILO

        Linux
  - GUID Partition Table (GPT)
    - Specialized boot scheme with modern advantages
    - Inability to find a bootable device indicates a problem with MBR or GPT
      - Bootable device not found
      - Operating system not found
      - Invalid drive specification
    - The UEFI and BIOS set prioritized boot order based on their configurations

        - Check if the internal storage device is working properly by looking, listening, and feeling

- **Storage Device Issues**
    - Hard Disk Drive (HDD)
        - Older storage devices that spin and move the read/write head across the platter
        - Low-cost, slower speed
    - Solid-State Device
        - Non-volatile memory that stores data and can access data from the device
        - High cost, less storage, faster speed
        - Solid-state devices have a limit on the amount of time to read and write data
    - Clicking sounds or grinding noises are signs of a hard disk drive mechanical problem
    - The light is not blinking during read or write from the device
        - The LED activity light is constantly blinking
    - Adding physical memory will stop the disk from being used as a swap file or page file
    - Use disk management tools to see if the device is detected
    - Sector
        - Allows to read and write on the hard drive by identifying the sector
        - Use disk utility to identify which sectors are bad and try to recover them
            - Sectors

              Windows/Linux
            - Blocks

              Solid-state device

- It is always a best practice to have a good backup drive

- **Drive Performance Issues**
  - Self-Monitoring, Analysis, and Reporting Technology (SMART)
    - Self-diagnostic program that alerts the OS if there is a failure
    - SMART monitors the hard drive and understands the health status of the drive
      - Read Error Rate
      - Spin-Up Time
      - Reallocated Sector Count
      - Seek Error Rate
      - Power-On Hours
      - Temperature
    - SMART utility is monitoring input/output operations per second (IOPS)
      - A hard disk drive has a lower IOPS than a solid-state device
      - Cloud can measure performance by using IOPS
      - Low IOPS can be an issue with the hardware or the software
    - The defragmentation tool can put files back together and reduce read and write times
      - Deleting and rewriting causes fragmentation

- **Issues with RAIDs**
  - RAID protects data against the risk of data loss
  - Single disk failure
    - If a RAID loses a disk, it will continue to operate as normal but at a slower speed
    - RAID rebuild is the utility used to rebuild the RAID
  - Full Raid Failure

- Entire array or volume stops working
- When the RAID fails, restore from backup, reconfigure, and rebuild using new disks

Troubleshooting Video Issues

- OBJ 5.4: Given a scenario, troubleshoot video, projector, and display issues

- **Physical Cabling and Source Selection**
  - Physical Cables That Carry Digital Signals
    - HDMI
    - DisplayPort
    - Thunderbolt
    - DVI-D
    - DVI-I
  - Broken cable
  - Cables are not properly inserted
    - Check both ends of the cable are properly connected
  - Cheap cable
    - Use high-speed rated HDMI cable that supports higher bandwidth
    - HDMI, DisplayPort, and Thunderbolt carry audio
    - VGA or DVI cables do not carry sound
  - Incorrect data source selected
  - HDMI device issue
  - High-Bandwidth Digital Content Protection (HDCP)
    - Protects the audio and video signals between the systems over HDMI and DisplayPort
    - Upgrade the quality of the HDMI cable

- **Projector Issues**
  - Dim images
  - No images
  - Shut down or restart
  - Burned-out bulb is when the projector bulb has no light and cannot send an image
  - Projector bulb has a lifespan of about 500-2000 hours
  - Use gloves to protect the life of the bulb
  - Cool down the projector for 15 to 30 minutes before removing the bulb
  - The projector without the source input will shut down

- **Video Quality Issues**
  - Dim images
    - Dim image occurs when there is no brightness or color contrast control set for displays
  - Fuzzy images
    - Fuzzy image occurs when the output resolution from the computer is lower
  - Flashing screens
    - Flashing screen means the cable is not properly connected
  - Dead pixels
    - There is no fix for a dead pixel
  - Burn-in
    - Burn-in occurs when the same static picture is displayed on a screen for a long time
    - Animated screensaver
    - Turn on inactivity
  - Color Bit

- Actual number of colors displayed
  - 8-bit color palette
    - (256 color variations)
  - 16-bit color palette
    - (32,768 color variations)
  - 24-bit color palette
    - (True color display)
    - (16,777,216 color variations)
  - 32-bit color palette
    - (Deep color display)
    - (1B color variations)
  - Adobe RGB
  - sRGB IEC
  - Display P3

Troubleshooting Networks

- OBJ 5.7: Given a scenario, troubleshoot problems with wired and wireless networks

- **Wired Connectivity Issues**
  - Physical connection
  - Cable length
  - Interference
  - Port flapping
  - The link light shows a valid link
  - The activity light blinks when sending or receiving data
    - 10 Mbps (Off)
    - 100 Mbps (Orange)
    - 1000 Mbps (Green)
  - A repeater is used to increase the connectivity signal
  - Interference with wired connections is coming from an external interference source
    - Power lines
    - Fluorescent lighting
    - Motors
    - Generators
  - The network cables near power lines use fiber optic connections
  - Port Flapping
    - Caused by an intermittent connectivity issue between the client and the network switch
    - Port flapping status is from upstate to downstate

- **Network Performance Issues**
  - Network Performance Issues

        - Manifesting the slowdown of network
    - Half Duplex
        - Network that sends or receives information
        - Half duplex is the standard in hubs and network
    - Full Duplex
        - Network that sends or receives information at the same time
        - Network interface cards are set to auto negotiation
    - Data exfiltration is sending data in the background without the user seeing it

1. Mismatch in the duplex setting
2. Mismatch in the speed setting
3. Network adapter drivers are out of date
4. Malware infection

- **Wireless Connectivity Issues**
    - Intermittent wireless connectivity
    - Signal interference
    - Low signal strength
    - Standards mismatch
        - Intermittent Wireless Connectivity

          Connected or disconnected network
        - Intermittent Wired Connectivity

          Upstate to a downstate of switch port
    - Signal interference is causing signal issues
    - Channels 1, 6, and 11 spread out the network and avoid interference
    - Wireless a, n, ac, and ax are less prone to signal interference
    - Received Signal Strength Indicator (RSSI)
        - Used to measure the signal strength based on an index level and gives a value in decibels (dB)

- RSSI is displayed in negative decibels
    - Increase the power of transmission
    - Increase the antenna size
    - Move closer to the source
    - Wireless a, n, ac, and ax

      5 GHz
    - Wireless b, g, or n

      2.4 GHz
- What frequency is being used?
- What is the maximum speed of that frequency?
- Which versions of wireless networking are being used?
- Configure the wireless access points to support the modern versions of the protocols

- **VoIP Issues**
    - Voice Over Internet Protocol (VoIP)
        - Set of protocols that are used to send streaming voice and video in real time
    - Latency
        - Time it takes for a signal to reach the intended client
        - Keep latency under 50 to 100 milliseconds
    - Jitter
        - Measurement of the variation in delay over time
        - When latency increases by up to 30-50 milliseconds, it starts to have jitter
        - Increase network performance
        - Implement quality of service
    - The set settings for quality of service only affect things inside the network
    - Setting the quality of service (QoS) allows prioritization of voice traffic

- **Limited Connectivity Issues**
    - Limited Connectivity
        - Specialized message to receive within the operating system
    1. Affects one network client
    2. VLAN is properly configured
    - Limited connectivity issue is having a DHCP issue
        - IP address
        - Subnet
        - Default gateway
        - DNS server IPs

Troubleshooting Mobile Devices

- OBJ 5.5: Given a scenario, troubleshoot common issues with mobile devices

- **Mobile Power Issues**
  - Poor battery health
  - Charging issues
  - Swollen batteries
  - As batteries age, the maximum charge they can hold decreases
  - Swollen batteries are caused by overcharging

- **Mobile Hardware Issues**
  - Overheating damage
    - Any device that's unable to properly cool itself down
  - Liquid damage
    - Dry off excess liquid
    - Power off the device
    - Disassemble the device
    - Clean the circuit boards and contacts
    - Replace the battery
  - Physical port damage
    - To fix the damaged port is to remove the port and replace it

- **Mobile Display Issues**
  - Broken screens
    - Glass
    - Digitizer
    - Screen
    - Backlight

- Dim images
  - Backlight
  - Inverter
- Digitizer issues
  - Digitizer
    - Device underneath the glass that responds to the input of the user
  - The digitizers fail because of shock damage from dropping or liquid damage
- Calibration issues
  - When troubleshooting a cursor issue, check the touch pad sensitivity and observe the user

- **Mobile Connectivity Issues**
  - Physical issues
    - Connected to the right SSID
    - Connected using the right password
    - Move closer to the wireless access point
    - Put the higher gain antenna on
    - Operate 30 to 50 meters away from the wireless access point to maintain a good connection
  - Software configuration issues
    - Bluetooth enabled
    - Properly paired
    - Adequate battery
    - Right range
    - Bluetooth is a personal area network and used at up to 10 meters

    - The wireless NIC is properly connected to the antennas

- **Mobile Malware Infections**
    - Antivirus or anti-malware solution
    - Excessive power drain
    - Significant data transmission
    - Camera and microphone
    - Asking for additional permissions
    - Back up the data
    - Format the device and re-install the base operating system

Troubleshooting Print Devices

- OBJ 5.6: Given a scenario, troubleshoot and resolve printer issues

- **Printer Connectivity Issues**
  - Locally connected printer
  - Printer not found
  - Printer has an online or offline status
  - Assign the printer a valid IP address, subnet mask, gateway, and DNS server
  - Use the right SSID and password to ensure the printer joins the correct network
  - To bring the printer back online, turn off the printer, wait ten seconds, and power it on again
  - Power Cycling
    - Printer is turned on and off to release printing memory
      - Local connections
      - Wired connections
      - Wireless connections

- **Print Feed Issues**
  - Paper jam
  - Grinding noise
  - Check the printer for debris and paper tracks
  - Inkjet and dot matrix printers are easier to detect a jam
  - Paper feed issue is when the printer selects more than one piece of paper through the printer
    - Thin Paper - Low weight
    - Thick Paper - High weight
  - The pickup rollers are designed to pick up one piece of paper at a time

- Carriage mechanism brings the printhead across the page in an inkjet or impact printer
  - Toner cartridge
  - Fuser
  - Gears and rollers

- **Print Quality Issues**
  - Faded printout
    - Draft output mode uses less ink and toner
    - Faded printout is caused by the running out of ink inside of a printer ink cartridge or toner
  - Blank pages
    - Blank page is caused by a software issue
  - White stripes
    - White stripes in laser printers are caused by an issue with the toner cartridge or the drum
    - The uniform white stripe on the page indicates a problem with the drum
  - Black stripes
    - Indicates the primary charge roller is dirty or damaged, or the high voltage power supply to the developer unit is malfunctioning
    - To fix the black stripes issue, troubleshoot the corona wire or replace the drum and the toner cartridge
  - Speckling output
    - Clean the printer using an approved toner vacuum
  - Vertical or horizontal lines
    - The vertical or horizontal line is caused by dirty feed rollers
    - Dirty photosensitive drum can create vertical or horizontal lines
  - Toner does not fuse

        - Check the voltage of the fuser and get the proper input voltage
    - Double or echo image
        - A double/echo/ghost/shadow image indicates a drum issue
    - Incorrect chroma display
        - Software or printer driver issue could be causing the incorrect color
    - Missing color
        - Use rubbing alcohol to clean the contacts between the printer and the cartridge
        - Consistent white line indicates a blocked or clogged inkjet nozzle
        - Replace the printhead and this will replace the dots inside of it
        - Platen adjusts the gap between the paper and the printhead to different paper sizes

- **Print Finishing Issues**
    - Incorrect page sizes
    - Incorrect page orientations
    - Issues with stapling
    - Issues with hole punching
    - Use the right paper size to print
    - Word processor sets portrait as the default
    - Slide presentation sets landscape as the default
    - To solve staple jams, remove the staple cartridge and replace it

- **Print Job Issues**
    - Print monitor
        - Software program used to transmit the print job and provide status information

        - Print monitors look at toner and ink cartridge levels and notify when they get low
    - Print queue
        - Software that collects all the print jobs and manages them
    - Print spooler
        - Manages the paper printing jobs sent from a computer or a printer server
            - Print Queue

              Pending
            - Print Spooler

              Active
    - Print driver
        - Garbled Print Job
            - Any output that is scrambled or encrypted
            - Garbled printouts are a driver issue
            - A font can cause a garbled printout