Module 2: Basic Switch and End Device Configuration
Key Concepts:
Operating System (OS) Components:
- Shell: User interface (CLI or GUI).
- Kernel: Bridges hardware and software.
- Hardware: Physical components.

CLI Access Methods:
- Console: Physical port for initial setup (most secure physical access).
- SSH (Secure Shell): Secure remote CLI access over the network (Recommended).
- Telnet: Insecure remote CLI access (sends data in plaintext).

IOS Command Modes:
- User EXEC Mode (>): Limited monitoring commands.
- Privileged EXEC Mode (#): All commands (enable to enter).
- Global Configuration Mode ((config)#): To change device config (configure terminal).
- Subconfiguration Modes: e.g., (config-line)# for lines, (config-if)# for interfaces.

Device Configuration Basics:
- Hostname: hostname
- Passwords:
- Console Password: line console 0 -> password -> login
- Enable Secret: enable secret
- VTY Lines (Telnet/SSH): line vty 0 15 -> password -> login
- Encrypt Passwords: service password-encryption
- Banner MOTD: banner motd # #

Configuration Files:
- running-config: In RAM. Current, active configuration.
- startup-config: In NVRAM. Saved configuration loaded on boot.
- Save Config: copy running-config startup-config
- Erase Config: erase startup-config -> reload

IP Addressing:
- Devices need an IP address, subnet mask, and default gateway to communicate on a network.
- Can be configured manually or automatically via DHCP.
- To remotely manage a switch, configure an IP address on its SVI (Switch Virtual Interface): interface vlan 1 -> ip address -> no shutdown

Verification:
- Test connectivity with the ping command.

Module 3: Protocols and Models
Key Concepts:
Communication Fundamentals: Requires a source, destination, and channel (media).

Network Protocol Requirements:
- Message Encoding
- Message Formatting & Encapsulation
- Message Size

- Message Timing (Flow Control, Timeouts, Access Method)
- Message Delivery Options (Unicast, Multicast, Broadcast, Anycast)

Protocol Suites:
- A group of interrelated protocols (e.g., TCP/IP).
- TCP/IP is the most common suite (open standard).

Standards Organizations:
- ISOC, IAB, IETF, IRTF: Develop and maintain Internet and TCP/IP standards.
- ICANN/IANA: Manage IP addresses and domain names.
- IEEE: Standards for networking (e.g., Ethernet, Wi-Fi), electronics.
- EIA/TIA: Standards for wiring, connectors, racks.
- ITU-T: Standards for video compression, DSL.

Layered Models (TCP/IP vs. OSI):
- Benefits: Assists design, fosters competition, prevents layer changes from affecting others, provides common language.
- TCP/IP Model (4 layers): Application, Transport, Internet, Network Access.
- OSI Model (7 layers): Application, Presentation, Session, Transport, Network, Data Link, Physical.
- Comparison: OSI breaks TCP/IP's Network Access layer into Data Link & Physical, and the Application layer into Application, Presentation, & Session.

Data Encapsulation (PDUs):
- Process: Data -> Segment -> Packet -> Frame -> Bits
- PDU (Protocol Data Unit): The form data takes at each layer.
- Segmenting: Increases speed and efficiency (only lost segments need retransmission).

Data Access (Addressing):
- Layer 3 (Network): Logical IP addressing (Source & Destination IP). Stays the same from source to destination.
- IPv4 Address: Network portion & Host portion.
- Layer 2 (Data Link): Physical MAC addressing (Source & Destination MAC). Changes at every hop (router) along the path.
- Default Gateway (DGW): The router's IP address on a local network. Used when the destination IP is on a remote network. The frame is addressed to the DGW's MAC address.

Module 4: Physical Layer
Key Concepts:
- Purpose: Transports bits across network media. Encodes frames into signals for transmission.
- Physical Layer Standards: Govern Physical Components, Encoding, Signaling.

Bandwidth Terminology:
- Bandwidth: Maximum capacity of a medium (bps).
- Throughput: Actual measured data transfer rate.
- Goodput: Measure of usable data transferred (Throughput minus overhead).
- Latency: Time delay for data to travel.

Copper Cabling:
- Limitations: Attenuation (signal loss over distance), EMI/RFI (interference), Crosstalk.
- UTP (Unshielded Twisted Pair): Most common. Uses RJ-45 connectors. Relies on cancellation and varying twist rates to mitigate interference.

- STP (Shielded Twisted Pair): Better noise protection, more expensive, harder to install.
- Coaxial Cable: Used for cable internet, wireless antenna connections.

Fiber-Optic Cabling:
- Advantages: Long distances, high bandwidth, immune to EMI, less susceptible to attenuation.
- Disadvantage: More expensive.
- Types:
- Single-Mode Fiber (SMF): Small core, uses lasers, long distances.
- Multi-Mode Fiber (MMF): Larger core, uses LEDs, shorter distances (up to 550m), more dispersion.
- Connectors: ST, SC, LC, Duplex LC.
- Jacket Colors: Yellow (Single-Mode), Orange/Aqua (Multi-Mode).

Wireless Media:
- Uses radio or microwave frequencies.
- Limitations: Coverage area, interference, security, shared medium (half-duplex).

Standards:
- Wi-Fi (IEEE 802.11): WLAN
- Bluetooth (IEEE 802.15): WPAN
- WiMAX (IEEE 802.16): Broadband wireless
- Zigbee (IEEE 802.15.4): Low-power IoT

Module 5: Number Systems
Key Concepts:
- Binary: Base 2 system (0, 1). Used by devices.
- Decimal: Base 10 system (0-9). Used by humans.
- Hexadecimal: Base 16 system (0-9, A-F). Compact representation of binary. Used for IPv6 and MAC addresses.
- IPv4 Address: 32 bits, divided into four 8-bit octets. Represented in dotted-decimal notation (e.g., 192.168.1.1).
- IPv6 Address: 128 bits. Every 4 bits is represented by a single hex digit, for a total of 32 hex digits. Grouped into 8 hextets of 4 hex digits each, separated by colons (:).

Conversion:
- Decimal to Binary: Subtract largest power of 2 possible.
- Binary to Decimal: Add the positional values where a 1 is present.
- Decimal/Binary to Hex: Convert to binary, split into groups of 4 bits, convert each group to its hex value.

Module 6: Data Link Layer
Key Concepts:
- Purpose: Prepares data for the physical network. Handles NIC-to-NIC communication.
- Functions: Error detection, frame encapsulation/decapsulation, access control.

IEEE 802 Sublayers:
- Logical Link Control (LLC): Communicates between upper layers and lower hardware.
- Media Access Control (MAC): Handles data encapsulation and media access control.

Topologies:

- Physical Topology: Arrangement of devices and cables.
- Logical Topology: How data travels through the physical topology.
- WAN Topologies: Point-to-Point, Hub-and-Spoke, Mesh.
- LAN Topologies: Star (most common), Extended Star, Bus, Ring.

Duplex Communication:
- Half-Duplex: Communicate in one direction at a time (e.g., legacy hubs, WLANs).
- Full-Duplex: Communicate in both directions simultaneously (e.g., switches).

Media Access Control Methods:
- Contention-Based (CSMA):
- CSMA/CD (Collision Detection): Used in legacy Ethernet. Devices detect and retransmit after a collision.
- CSMA/CA (Collision Avoidance): Used in Wireless (802.11). Devices announce duration to reserve the medium.
- Controlled Access: Deterministic (e.g., Token Ring).

Data Link Frame:
- Structure: Header | Data | Trailer
- Fields: Addressing (MAC), Type, Control, Data, Error Detection (FCS).
- Layer 2 Addressing: MAC Address - physical address, burned-in, used for local delivery on the same network segment. Changes at every router hop.

Common Data Link Protocols: Ethernet, 802.11 (Wi-Fi), PPP, HDLC.