**Name: ramani Harshil sureshbhai**

**Module : 8 Network access basic rounting and advance rounting concept, switching concept**

**• Beginner Question**

**1. Explain Switch**

**Ans = > A switch is a networking device that connects devices within a local area network (LAN) and facilitates data communication between them. It operates at the data link layer (Layer 2) of the OSI model, meaning it uses MAC (Media Access Control) addresses to identify devices on the network. Here’s a breakdown of what it does and how it works:**

**1. Primary Functions of a Switch**

* **Forwarding and Filtering: Switches determine the destination of each data packet and forward it only to the specific device it’s intended for, rather than broadcasting to all devices. This improves network efficiency.**
* **Learning: Switches learn the MAC addresses of devices connected to their ports. When a device communicates for the first time, the switch records its MAC address and the port it’s connected to. Over time, the switch builds a MAC address table to improve packet forwarding.**
* **Loop Avoidance: Managed switches support protocols like Spanning Tree Protocol (STP), which helps prevent loops in the network that could cause broadcast storms and degrade network performance.**

**2. Switch Types**

* **Unmanaged Switch: Basic plug-and-play device with no configuration options. Ideal for simple, small networks.**
* **Managed Switch: Can be configured to provide better control over data traffic, security, and performance. Suitable for larger, more complex networks.**

**3. How a Switch Works**

**When a device sends data, the switch reads the MAC address in the frame and checks its MAC address table:**

* **If the address is in the table, it forwards the data directly to the port associated with that MAC.**
* **If not, it floods the data to all ports except the source port, and then learns the destination’s MAC and port when it responds.**

**Advantages of Using a Switch**

* **Improves Network Performance: By reducing unnecessary traffic, only forwarding packets to the correct destination.**
* **Increases Security: With managed switches, you can control which devices have access to specific parts of the network.**
* **Scalability: Switches can support large numbers of devices, making it easy to expand networks.**

**Switches are foundational to modern LANs, offering an efficient way to manage data flows and network resources.**

**2.**  **Explain Switch Boot Sequence**

**Ans = >The switch boot sequence is the process a network switch goes through when it starts up or reboots. This sequence involves several stages that ensure the switch’s hardware and software are ready for operation. Here’s a step-by-step breakdown of the boot sequence in a typical managed network switch (like Cisco):**

**1. Power-On Self-Test (POST)**

* **The switch powers up and immediately performs a POST to check the functionality of essential hardware components (CPU, memory, interfaces, etc.).**
* **If any hardware issues are detected, the switch will typically signal this with error codes or LED indicators.**

**2. Loading the Bootstrap (Bootloader)**

* **The switch loads a small piece of software called the bootstrap or bootloader. The bootstrap is responsible for locating the switch’s operating system (usually an image stored in flash memory).**
* **The bootstrap is stored in ROM (read-only memory) and initializes the hardware, helping the switch load the operating system.**

**3. Loading the IOS Image (Operating System)**

* **The switch loads its IOS (Internetwork Operating System) image or equivalent OS from flash memory.**
* **If there’s a problem loading the IOS, the switch may enter ROM Monitor (ROMmon) mode to allow manual recovery or troubleshooting.**

**4. Initialization of Hardware and Interfaces**

* **Once the IOS is loaded, the switch initializes its hardware interfaces (Ethernet ports, etc.) and brings them online.**
* **This step involves configuring default interface settings and activating hardware resources needed for network connectivity.**

**5. Execution of Startup Configuration**

* **The switch checks NVRAM (Non-Volatile RAM) for a startup configuration file (commonly named *startup-config*).**
* **If a startup-config file is found, the switch loads it and applies all pre-configured settings, such as VLAN configurations, IP addressing, port security, and other operational parameters.**
* **If no startup configuration file is found, the switch may enter setup mode (often called "initial configuration dialog") to guide the user in creating a basic configuration.**

**6. Post-Boot Configuration**

* **After the startup configuration is applied, the switch is operational and ready to forward packets.**
* **The switch may also run additional protocols (such as Spanning Tree Protocol for loop prevention) and establish trunk or access links as configured.**

**Summary of Key Stages in Switch Boot Sequence**

1. **Power-On Self-Test (POST) – Basic hardware check.**
2. **Bootstrap Loading – Load bootloader from ROM.**
3. **IOS Image Loading – Load operating system from flash memory.**
4. **Hardware and Interface Initialization – Prepare ports and interfaces.**
5. **Load Startup Configuration – Apply configuration settings from NVRAM.**
6. **Operational State – The switch becomes fully functional.**

**3.** **Explain Three Methods to access Switch Command Line Interface**

**Ans = >There are three common methods to access the Command Line Interface (CLI) of a network switch, each suitable for different networking scenarios and user preferences. Here’s a breakdown of each method:**

**1. Console Access**

* **Description: Console access is a direct, local connection to the switch using a physical console cable (usually a serial cable or RJ-45 to serial adapter).**
* **How It Works:**
  + **Connect the console cable from the switch’s console port to a computer or terminal.**
  + **Open a terminal emulation program on the computer (e.g., PuTTY, Tera Term, or HyperTerminal) and configure it with the correct serial settings (typically, 9600 baud rate, 8 data bits, no parity, 1 stop bit, no flow control).**
* **When to Use: Ideal for initial configuration or troubleshooting when there is no network configuration on the switch, or remote access is unavailable.**
* **Advantages: Doesn’t rely on the network; as long as you’re physically near the switch, you can access it directly.**

**2. Telnet Access**

* **Description: Telnet is a remote access protocol that allows you to connect to the switch over an IP network.**
* **How It Works:**
  + **The switch must have an IP address configured on one of its interfaces (e.g., management VLAN).**
  + **Use a Telnet client (such as PuTTY or Tera Term) to initiate a connection by entering the switch’s IP address.**
* **When to Use: Suitable for remote access if the switch is configured with an IP address and is reachable on the network.**
* **Advantages: Provides remote access, allowing configuration and management from anywhere on the network.**
* **Security Considerations: Telnet sends data, including login credentials, in plaintext, so it’s insecure for use on public or unsecured networks. It’s generally recommended only for internal, secure networks.**

**3. SSH (Secure Shell) Access**

* **Description: SSH is a secure remote access protocol that provides encrypted connections to the switch over an IP network.**
* **How It Works:**
  + **Similar to Telnet, SSH requires that the switch has an IP address configured.**
  + **Use an SSH client (such as PuTTY or OpenSSH) to connect to the switch’s IP address.**
  + **SSH encrypts all data, including login credentials, making it much safer than Telnet.**
* **When to Use: Recommended for remote access in any production environment, especially on public or sensitive networks.**
* **Advantages: Provides secure, encrypted remote access, which protects login credentials and data during transmission.**

**Summary of Access Methods**

1. **Console Access: Local, physical connection for initial setup or troubleshooting.**
2. **Telnet Access: Remote access over an IP network but insecure due to lack of encryption.**
3. **SSH Access: Secure remote access over an IP network with encrypted connections for improved security.**

**For production environments, SSH is the preferred method due to its security features, while console access is valuable for initial setups and troubleshooting.**

1. **Explain and Configuring the Cisco Internet Operating System**

**Ans = >The Cisco Internetwork Operating System (IOS) is a network operating system used on Cisco routers and switches. It provides the CLI for configuring and managing network devices. Cisco IOS offers commands to configure network protocols, security, interfaces, and much more.**

**Here's a detailed overview of Cisco IOS and a basic guide to configuring it.**

**Cisco IOS Overview**

**Cisco IOS operates at the core of Cisco devices, allowing network administrators to control and monitor the device’s functionality. Key features include:**

* **Configuration Management: Allows users to set up IP addresses, routing protocols, VLANs, security settings, etc.**
* **Device Management: Provides options to monitor device performance, resource utilization, and troubleshoot network issues.**
* **Security: Enables security configurations, including access control lists (ACLs), secure remote access, and encryption protocols.**

**Basic Modes of Cisco IOS**

**Cisco IOS has several command modes, each with specific functions:**

1. **User EXEC Mode (>)**
   * **The most basic mode, where you can run simple commands like ping, show, etc.**
   * **Prompt: Switch>**
2. **Privileged EXEC Mode (#)**
   * **Provides access to more advanced commands, including the ability to enter global configuration mode.**
   * **Entered by typing enable from User EXEC mode.**
   * **Prompt: Switch#**
3. **Global Configuration Mode ((config)#)**
   * **Allows you to configure global settings that affect the entire device, such as network protocols and security settings.**
   * **Entered by typing configure terminal from Privileged EXEC mode.**
   * **Prompt: Switch(config)#**
4. **Interface Configuration Mode ((config-if)#)**
   * **Used to configure specific interfaces, like Ethernet or VLAN interfaces.**
   * **Entered by typing interface**
5. **Explain Switch Port**

**Ans = > A switch port is a physical interface on a network switch that connects devices to the network. Each port allows data to flow between the switch and connected devices, such as computers, printers, and other network devices. Switch ports are key components for managing data flow within a Local Area Network (LAN).**

**Key Aspects of Switch Ports**

1. **Types of Switch Ports**
   * **Access Ports: Designed to connect end devices, like computers and printers, to the network. An access port belongs to only one VLAN (Virtual Local Area Network) and typically handles untagged traffic associated with that VLAN.**
   * **Trunk Ports: Used to connect switches to each other, allowing multiple VLANs to pass traffic across a single link. Trunk ports tag frames to indicate the VLAN they belong to, usually using IEEE 802.1Q tagging.**
   * **Hybrid Ports: Found on some switches, these ports can function as either access or trunk ports, depending on the configuration. Hybrid ports are often seen in more complex network setups where port flexibility is needed.**
2. **Port Speed and Duplex Settings**
   * **Switch ports can operate at various speeds (10 Mbps, 100 Mbps, 1 Gbps, or 10 Gbps) depending on the device’s capabilities.**
   * **Duplex Mode: Ports can operate in half-duplex (data flows in one direction at a time) or full-duplex (data flows in both directions simultaneously). Full-duplex is commonly used for modern networks to improve performance.**
3. **Power over Ethernet (PoE) Ports**
   * **Some switch ports support Power over Ethernet (PoE), which allows them to provide both data and electrical power to connected devices, like IP phones, cameras, and wireless access points. PoE eliminates the need for separate power cables, simplifying device installations.**
4. **Switch Port Security**
   * **Switch ports can be configured with security features to control which devices can connect to them. Port security allows only specific MAC addresses to access a port, which helps prevent unauthorized access and network attacks.**
5. **Switch Port Configuration Modes**
   * **Each port on a managed switch can be configured to suit network needs. For example:**
     + **VLAN Assignment: You can assign each port to a specific VLAN to segment network traffic.**
     + **Port Mirroring: Some ports can be configured to mirror traffic from another port for monitoring or troubleshooting purposes.**
     + **Spanning Tree Protocol (STP): Switch ports can run STP to prevent network loops, ensuring that there’s only one active path between network devices.**

**4-R1, R2, R3, and R4 have their Fast Ethernet 0/0 interfaces attached to the same VLAN. A network engineer has typed a configuration for each router by using a word processor. He will later copy and paste the configuration into the routers. Examine the following exhibit, which lists configuration for the four routers, as typed by the network engineer. Assuming that all four routers can ping each other’s LAN IP addresses after the configuration has been applied, choose the routers that will be able to form a neighbor relationship with the other routers on the LAN. (You can assume that, if not shown in the exhibit, all other related parameters are still set to their defaults.)**

**Ans = > R2 and R3**

**3-enable secret [password] is hashed using the algorithm.**

**A. MD5**

**B. AH**

**C. PSK**

**D. ESP**

**E. WPA2**

**Ans = > a. md5**

**4- An engineer connects to Router R1 and issues a show ip ospf neighbor command. The status of neighbor 2.2.2.2 lists FULL/BDR. What does the BDR mean?**

**A. R1 is an Area Border Router.**

**B. R1 is a backup designated router.**

**C. Router 2.2.2.2 is an Area Border Router.**

**D. Router 2.2.2.2 is a backup designated router.**

**Ans = > B. R1 is a backup designated router.**

**5-Which command is used to view the neighbor discovery table on a PC?**

**A. show ipv6 neighbor**

**B. show ipv6 neighbors**

**C. netsh interface ipv6 show neighbor**

**D. netsh interface ipv6 show neighbors**

**Ans = > C. netsh interface ipv6 show neighbor**

**6-What type of variable is being shown? Routers = [R1,R2,R3]**

**A. List**

**B. Dictionary**

**C. Simple**

**D. Unsigned integers**

**Ans = > A. List**

**7- Identify the fields in an IPv4 header. (Choose three)**

**A. Host component**

**B. Time to Live**

**C. Source address**

**D. Destination address**

**Ans = > B. Time to Live**