Module 8: CCNA - Network Access, Basic routing and Advance routing concept, switching concept

**• Beginner Question**

1. Explain Switch

ANS.

A **switch** is a network device that connects multiple devices within a local area network (LAN) and facilitates communication between them. Here’s how it works and its key features:

**Functions of a Switch**

1. **Data Forwarding:**
   * Switches receive data packets from one device and forward them only to the intended recipient. This reduces unnecessary traffic and increases efficiency.
2. **MAC Address Learning:**
   * Switches maintain a MAC address table that maps devices' MAC addresses to their corresponding ports. When a packet arrives, the switch checks the table to determine where to send it.
3. **Collision Domain Isolation:**
   * Each port on a switch creates a separate collision domain, meaning that devices connected to different ports can transmit data simultaneously without collisions.
4. **Broadcasting:**
   * If the destination MAC address is unknown, the switch will broadcast the packet to all ports except the one it originated from, ensuring the intended device receives it.

**Types of Switches**

1. **Unmanaged Switches:**
   * Simple plug-and-play devices with no configuration options. Suitable for small networks.
2. **Managed Switches:**
   * Offer advanced features such as VLAN support, port mirroring, and traffic monitoring, allowing for better control over the network.
3. **Layer 2 and Layer 3 Switches:**
   * **Layer 2 Switches:** Operate at the data link layer and forward frames based on MAC addresses.
   * **Layer 3 Switches:** Include routing capabilities, allowing them to forward packets based on IP addresses.

**Benefits of Using Switches**

* **Efficiency:** By reducing network collisions and managing data traffic, switches improve overall network performance.
* **Scalability:** They allow for easy expansion of the network by simply adding more devices.
* **Segmentation:** Managed switches can create virtual LANs (VLANs) to segment traffic for better security and performance.

2. Explain Switch Boot Sequence

ANS.

The **switch boot sequence** refers to the process a network switch undergoes from power-up to being fully operational and ready to forward traffic. Here’s a breakdown of the typical boot sequence for a managed switch:

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

* **Initial Check:** When the switch is powered on, it performs a POST to check the hardware components, such as the CPU, memory, and interfaces, ensuring they are functioning correctly.
* **Error Reporting:** If any issues are detected during this test, the switch may display error messages or indicate failure through LED indicators.

**2. Load Bootstrap Program**

* **Bootstrap Program:** After POST, the switch loads a small bootstrap program stored in ROM (Read-Only Memory). This program initializes the system hardware and prepares it to load the operating system.

**3. Load Operating System**

* **Operating System (OS):** The bootstrap program locates and loads the switch's OS, typically stored in Flash memory. This OS is responsible for managing switch functions and features.
* **Configuration File:** The OS looks for a configuration file, often called startup-config, which contains the switch’s settings (such as VLANs, IP addresses, and security settings).

**4. Apply Configuration**

* **Configuration Initialization:** The switch applies the settings found in the configuration file. If no configuration file is found, it may load a default configuration.
* **Dynamic Learning:** During this phase, the switch starts learning MAC addresses from the incoming traffic, building its MAC address table.

**5. Initialize Interfaces**

* **Interface Startup:** The switch initializes its network interfaces, making them ready to connect to devices.
* **Link Status:** It checks the status of each port (e.g., whether devices are connected) and may perform additional tasks like auto-negotiation for speed and duplex settings.

**6. Running State**

* **Operational State:** Once the OS is loaded, the configuration is applied, and interfaces are initialized, the switch enters the running state. It is now ready to forward frames between connected devices.
* **Monitoring and Management:** The switch begins to monitor traffic, manage network performance, and accept management commands via protocols like SNMP (Simple Network Management Protocol) or a web interface.

**7. Continuous Operation**

* **Normal Operation:** The switch continues to operate, forwarding packets based on its MAC address table and handling any management tasks as needed.
* **Runtime Changes:** Administrators can make changes to configurations dynamically, which can be saved for the next reboot.

3. Explain Three Methods to access Switch Command Line Interface

ANS.

Accessing the Command Line Interface (CLI) of a network switch is essential for configuration and management. Here are three common methods to access the CLI of a switch:

**1. Console Access**

* **Description:** This method involves using a physical console cable (often a rollover cable) to connect directly from a computer's serial port to the switch's console port.
* **How to Access:**
  1. Connect the console cable to the switch's console port and the other end to a serial port on your computer (or USB-to-serial adapter).
  2. Use terminal emulation software (e.g., PuTTY, Tera Term, or HyperTerminal) to establish a connection.
  3. Configure the terminal settings (typically 9600 baud rate, 8 data bits, no parity, 1 stop bit, no flow control).
  4. Once connected, press Enter to access the switch CLI.
* **Use Cases:** Console access is typically used for initial configuration, troubleshooting, and when network connectivity is unavailable.

**2. SSH (Secure Shell)**

* **Description:** SSH provides a secure, encrypted way to access the switch remotely over the network. It’s commonly used in modern networks for secure management.
* **How to Access:**
  1. Ensure that SSH is enabled on the switch and that an IP address is configured on one of its interfaces.
  2. Open an SSH client (like PuTTY or OpenSSH).
  3. Enter the switch's IP address and select the SSH protocol.
  4. Log in with the appropriate credentials (username and password).
* **Use Cases:** SSH is preferred for remote management due to its security features, especially when accessing devices over the internet or untrusted networks.

**3. Telnet**

* **Description:** Telnet allows remote access to the switch over a network, but it does not encrypt the session, making it less secure than SSH.
* **How to Access:**
  1. Ensure Telnet is enabled on the switch and that an IP address is assigned.
  2. Use a Telnet client (like PuTTY or the command line on various OS).
  3. Enter the switch's IP address and select the Telnet protocol.
  4. Log in with the appropriate credentials.
* **Use Cases:** Telnet can be used in trusted environments where security is less of a concern. However, it's generally recommended to use SSH instead due to the security risks associated with Telnet.

4. Explain and Configuring the Cisco Internet Operating System

5. Explain Switch Port

**Multiple Choice**

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 neighbour 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.) (Choose two)

**A. R1**

**B. R2**

C. R3

D. R4

E. None of the routers will exchange routing information.

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

**A. MD5**

B. AH

C. PSK

D. ESP

E. WPA2

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.

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

A. show ipv6 neighbour

B. show ipv6 neighbour

**C. netsh interface ipv6 show neighbour**

D. netsh interface ipv6 show neighbours

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

**A. List**

B. Dictionary

C. Simple

D. Unsigned integers

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

A. Host component

**B. Time to Live**

**C. Source address**

**D. Destination address**