**Module 8: Network Access basic routing and advance routing concept , switching concept**

1.Explain Switch ?

🡪 A **switch** in networking refers to a device used to connect multiple devices on a local area network (LAN) and manage data traffic efficiently between them. Switches operate primarily at the **Data Link Layer (Layer 2)** of the OSI model, although some advanced switches also function at the **Network Layer (Layer 3)** for routing purposes.

**Key Functions and Features of a Switch:**

**1. Forwarding Frames:**

* A switch receives data in the form of **frames** from devices connected to its ports.
* It uses **MAC addresses** (Media Access Control addresses) to determine where to forward these frames. Each device connected to the switch has a unique MAC address.
* When a switch receives a frame, it checks the destination MAC address and forwards the frame only to the port where the device with that MAC address is connected. This is known as **frame forwarding**.
* If the switch doesn't know the destination MAC address (for example, if it's the first time receiving a frame from that address), it broadcasts the frame to all ports except the one from which it originated. This is known as **flooding**.

**2. Learning MAC Addresses:**

* A switch **learns** the MAC addresses of devices connected to each of its ports. It maintains a **MAC address table** (also called a **forwarding table**), which maps MAC addresses to specific ports.
* This learning process allows the switch to make more intelligent forwarding decisions and reduces unnecessary broadcasts over the network. Once it has learned the MAC addresses of devices, it can send frames directly to the correct port.

**3. Collision Domain Segmentation:**

* In traditional hub-based networks, all devices shared the same **collision domain**, meaning that if two devices tried to send data at the same time, a **collision** would occur.
* A switch, however, creates a **separate collision domain** for each connected device. This means devices can send and receive data simultaneously without interfering with each other, improving network efficiency.

**4. Full-Duplex Communication:**

* Unlike hubs, which use half-duplex communication (where data can either be sent or received at any given time), switches typically support **full-duplex** communication.
* This allows devices to send and receive data at the same time, improving network performance and speed.

**Types of Switches:**

1. **Layer 2 Switches** (Data Link Layer):
   * These are the most common switches, responsible for learning and forwarding based on MAC addresses.
   * Layer 2 switches operate in the data link layer and are primarily used for internal LAN connectivity.
   * They don't concern themselves with IP addresses (which are Layer 3).
2. **Layer 3 Switches** (Network Layer):
   * Layer 3 switches combine the functionality of a switch (Layer 2) and a router (Layer 3). They can perform routing tasks, such as determining the best path for data based on IP addresses.
   * These switches are capable of forwarding traffic based on IP addresses and can handle inter-VLAN routing (communication between different VLANs) without the need for a separate router.
   * Layer 3 switches are often used in larger, more complex networks.

2. Explain Switch Boot Sequence

🡪 The **switch boot sequence** refers to the process that a network switch follows when it powers up or is reset. During the boot process, the switch loads its software, initializes hardware components, and establishes its configuration, enabling it to perform network functions like forwarding data packets between devices.

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

* When the switch is powered on, it begins by performing a **POST** (Power-on Self-Test). This is a diagnostic test that checks the integrity of the hardware, ensuring that all essential components like the CPU, memory, and ports are functioning correctly.
* If any issues are detected, the switch may display error messages or fail to boot.

**2. Loading Boot Loader**

* After the POST is completed, the switch loads its **boot loader**. The boot loader is a small program that resides in the switch’s **boot ROM (Read-Only Memory)** or **flash memory**. It helps initialize the system, including the CPU and memory, and loads the operating system (OS) or software image into the switch's memory.
* The boot loader may also check for firmware updates, check for specific configuration settings, or even perform recovery operations if necessary.

**3. Loading the Operating System (OS)**

* The switch loads its **network operating system (OS)**, such as **Cisco IOS** (for Cisco switches) or **Juniper Junos** (for Juniper switches). The OS is responsible for managing the switch’s internal operations, network traffic forwarding, security protocols, and device configuration.
* Typically, the OS is stored in **flash memory** on the switch. The boot loader loads the appropriate OS image into **RAM** for execution.

**4. Initial Configuration and System Setup**

* After the OS is loaded, the switch begins its configuration process. If the switch has a **default configuration**, it will start using that.
* If there’s a stored configuration file (often saved in **NVRAM** or flash memory), the switch will attempt to load it during the boot process.
* If no configuration is found, the switch may start in **setup mode** or **factory default settings**, prompting the user to configure the switch manually, either through a command-line interface (CLI) or a web-based interface.

**5. Post-Boot Initialization**

* Once the configuration is loaded or set, the switch proceeds to initialize additional hardware components such as **ports**, **VLANs** (Virtual LANs), and **routing protocols**.
* The switch also initializes any services, such as **Spanning Tree Protocol (STP)** or **Link Aggregation** if configured.

**6. Network Services and Connectivity**

* The switch may start services like **DHCP (Dynamic Host Configuration Protocol)**, **QoS (Quality of Service)**, **ACLs (Access Control Lists)**, **SNMP (Simple Network Management Protocol)**, and others depending on the configuration.
* The switch establishes **network connectivity**, ensuring that all physical ports are active and ready for communication with other devices.

**7. Running Operational Mode**

* Once the boot process completes, the switch enters its **normal operational mode**, where it begins forwarding traffic between connected devices, based on its configured settings.
* During this phase, the switch will monitor the network, handle traffic based on MAC addresses (Layer 2), or potentially IP addresses (Layer 3, if it’s a Layer 3 switch), and implement any security or network management features that are configured.

3. Explain Three Methods to access Switch Command Line Interface

🡪 **1. Console Access (Serial Cable)**

* **Description**: This method uses a **console cable** (also known as a **rollover cable**) to connect the switch's **console port** to a computer's serial port (or USB-to-serial adapter).
* **When to Use**: Console access is often used for initial setup, recovery mode, or when other methods are unavailable. It’s the most basic and direct way to access the switch.

**Telnet Access (Remote Access)**

* **What It Is:** Telnet allows remote access to a switch via the network, using a TCP/IP connection.
* **How It Works:**
  + You connect to the switch's IP address over the network using Telnet client software (e.g., PuTTY or a built-in terminal in Linux or macOS).
  + Telnet sends data in plain text, which means the connection is not encrypted.
  + After establishing the connection, you enter the username and password to access the CLI.
* **When to Use:** Telnet is used when remote access is needed, but it should be avoided in unsecured environments since data (including login credentials) is transmitted unencrypted.

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

* **What It Is:** SSH (Secure Shell) is a secure alternative to Telnet for remote access to a switch's CLI.
* **How It Works:**
  + SSH uses an encrypted connection over the network to secure the transmission of data.
  + Similar to Telnet, you connect to the switch using its IP address, but the connection is encrypted, providing a higher level of security.
  + SSH requires an SSH client (such as PuTTY or OpenSSH) and an SSH-enabled switch (which typically requires the configuration of a username, password, and possibly an encryption key).
* **When to Use:** SSH is recommended for remote access to switches in production environments due to its encryption, which ensures secure communication, especially in public or untrusted networks.

4. Explain and Configuring the Cisco Internet Operating System

🡪

5. Explain Switch Port

3-enable secret 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 neighbor

B. show ipv6 neighbors

C. netsh interface ipv6 show neighbor

D. netsh interface ipv6 show neighbors

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