**Assignment Module-8**

**Section 1: Short Answer**

1. Explain Switch

Answer: A switch is a device that can connect or disconnect conducting paths in an electrical circuit, acting like a gate to control the flow of electricity. It's also a networking component that connects multiple devices within a local area network (LAN), enabling them to communicate with each other by forwarding data packets. Essentially, a switch can be used to turn electrical circuits on or off, or to change the path of an electrical signal.

* Purpose: Network switches are essential components in local area networks (LANs).
* Function: They receive data packets, determine the destination based on MAC addresses, and forward the packets only to the intended recipient(s), unlike hubs which broadcast to all connected devices.
* Efficiency: By directing traffic efficiently, switches reduce network congestion and improve overall network performance.
* Types: Switches can be managed or unmanaged, with varying port counts and features depending on network needs.
* Example: Imagine a busy office with multiple computers, printers, and servers. A switch would connect all these devices and manage the flow of data between them, such as sending a document from a computer to a printer or allowing multiple computers to access a shared file server.

1. Explain Switch Boot Sequence

Answer: The switch boot sequence is a series of steps a network switch performs to initialize itself and load its operating system, the Cisco IOS. It begins with a power-on self-test (POST), followed by loading the boot loader, which initializes the CPU and flash file system. Finally, the boot loader locates and loads the IOS image, transferring control of the switch to the operating system.

* Power-On Self-Test (POST): The switch begins by executing a POST program stored in ROM. This program performs hardware checks, testing the CPU, DRAM (memory), and the flash file system.
* Boot Loader Initialization: After successful POST, the boot loader, also stored in ROM, takes over. It initializes low-level CPU components, including registers that control memory mapping and speed.
* Flash File System Initialization: The boot loader initializes the flash file system on the switch's system board, preparing it for the operating system.
* Cisco IOS Image Loading: Finally, the boot loader locates and loads the Cisco IOS (the operating system) into memory. It typically uses the BOOT environment variable to find the image. If this variable is not set, it performs a recursive search of the flash file system to find the image. Once loaded, the IOS takes control of the switch, and the switch is ready to operate.

1. Explain Three Methods to access Switch Command Line Interface

Answer: Three primary methods exist for accessing a network switch's Command Line Interface (CLI):

* Console Connection: This method involves a direct physical connection between a computer and the switch's dedicated console port using a console cable (often a rollover cable). A terminal emulation program (e.g., PuTTY, Tera Term, Secure CRT) is run on the computer, configured with specific serial port settings (e.g., 9600 baud, 8 data bits, no parity, 1 stop bit, no flow control) to establish communication with the switch. This method is crucial for initial setup, password recovery, or when network access is unavailable.
* Telnet: Telnet is a network protocol that allows remote access to the switch's CLI over an IP network. A Telnet client on a computer connects to the switch's IP address or hostname. While convenient for remote access, Telnet transmits all data, including usernames and passwords, in clear text, making it insecure for sensitive environments.
* Secure Shell (SSH):SSH provides a secure, encrypted alternative to Telnet for remote CLI access. Similar to Telnet, SSH clients connect to the switch's IP address or hostname over the network. However, SSH encrypts all communication, protecting credentials and data from eavesdropping. SSH is the recommended method for remote CLI access in production environments due to its security features.

1. Explain and Configuring the Cisco Internet Operating System

Answer: Cisco IOS (Internetwork Operating System) is the operating system software that runs on Cisco networking devices like routers, switches, and firewalls. It's a command-line interface (CLI) software that provides a wide array of services for routing, switching, security, wireless management, and network management.

Configuring the Cisco Internet Operating System:

Configuring a Cisco Internetwork Operating System (IOS) involves setting up basic device information, access control, and network connectivity. Key steps include setting a hostname, configuring passwords for secure access, and assigning IP addresses to interfaces. Additionally, you might configure routing protocols, DHCP, and access control lists for a more robust network setup.

The basic configuration process:

1. Access and Initial Setup:
   * + **Console Access:** Connect to the router or switch using a console cable and terminal emulator (like PuTTY).
     + **Login:** Enter the enable mode using the enable command (and potentially a password).

* + - **Global Configuration Mode:** Enter configure terminal to access global configuration mode.

1. Basic Device Configuration:

* **Hostname:** Assign a unique hostname to the device using the hostname command (e.g., hostname Router A).
  + - **Enable Secret:** Set a strong, encrypted enable secret password to protect privileged mode access using the enable secret command.

* + - **IP Addressing:** Assign IP addresses to interfaces using the interface command (e.g., interface GigabitEthernet0/0) and the IP address command (e.g., IP address 192.168.1.1 255.255.255.0).

* + - **Interface Status:** Enable interfaces using the no shutdown command.

* + - **Default Gateway:** Configure a default gateway for the device using the IP default-gateway command.

1. Explain Switch Port

Answer: A switch port is a physical interface on a network switch where devices connect to transmit and receive data. These ports allow devices to communicate with each other within a local area network (LAN) and, through the switch, to access the internet. Switch ports can be configured for different purposes, such as connecting to specific VLANs or handling multiple VLANs, depending on the network architecture and requirements.

Key aspects of switch ports:

* Physical Connection: Switch ports are the physical openings where network cables (like Ethernet cables) are plugged in to connect devices to the switch.
* Data Transmission: They facilitate the transmission of data packets between devices connected to the switch.
* VLAN Support: Switch ports can be configured to handle different VLANs (Virtual LANs), allowing for network segmentation and improved security.
* Access Ports: These ports are typically used to connect end-user devices like computers, printers, or IP phones to a specific VLAN.
* Trunk Ports: Trunk ports are used to connect switches and carry traffic from multiple VLANs, often used in larger networks.
* Hybrid Ports: These ports can be configured to handle both tagged and untagged traffic, offering flexibility in network configuration.
* Combo Ports: Some switches offer combo ports, which are physical ports that share the same switch fabric. They can be used interchangeably, often offering options for both copper and fiber connections.
* Layer 2 Functionality: Switch ports operate at Layer 2 of the OSI model, using MAC addresses to forward data packets.
* Collision Domains: Each switch port acts as a separate collision domain, meaning that devices connected to different ports don't interfere with each other's transmissions.

**Section 2: Multiple Choice:**

1. 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.) (Choose two)

Answer: B.) R2 & D.) R4

1. enable secret [password] is hashed using the algorithm.

Answer: A.) MD5

1. 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?

Answer: D.) Router 2.2.2.2 is a backup designated router.

1. Which command is used to view the neighbor discovery table on a PC?

Answer: C.) netsh interface ipv6 show neighbor

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

Answer: A.) List

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

Answer: B.) Time to Live

C.) Source address

D.) Destination address