* Network Access Basic Routing and Advance Routing Concept Switching Concept.

1. **Explain switch**

Ans:

**What is a Switch?**

A switch is a networking device that connects multiple devices within a network, allowing them to communicate with each other. It operates at the Data Link layer (Layer 2) of the OSI model.

**How Does a Switch Work?**

Here's a step-by-step explanation of how a switch works:

1. Receiving Data Packets: A switch receives data packets from devices connected to its ports.

2. Examining Destination MAC Address: The switch examines the destination MAC address of the incoming data packet.

3. Checking MAC Address Table: The switch checks its MAC address table to determine which port the destination device is connected to.

4. Forwarding Data Packet: If the destination MAC address is found in the MAC address table, the switch forwards the data packet to the corresponding port.

5. Flooding: If the destination MAC address is not found in the MAC address table, the switch floods the data packet to all ports except the one it received the packet on.

**Type of switches**

1. Unmanaged Switch: A basic switch that simply forwards data packets without any configuration options.

2. Managed Switch: A switch that can be configured and managed to provide advanced features such as VLANs, QoS, and security.

3. Smart Switch: A switch that provides a balance between unmanaged and managed switches, offering some configuration options but not as many as a fully managed switch.

**Switching Methods**

1. Store-and-Forward Switching: The switch stores the incoming data packet in its buffer and then forwards it to the destination port.

2. Cut-Through Switching: The switch forwards the incoming data packet to the destination port as soon as it receives the destination MAC address.

3. Fragment-Free Switching: The switch stores the incoming data packet in its buffer and then forwards it to the destination port, but only if the packet is fragment-free.

**Advantages of Switches**

1. Improved Network Performance: Switches improve network performance by reducing collisions and increasing bandwidth.

2. Increased Security: Switches provide security features such as VLANs and access control lists to restrict network access.

3. Easy Installation: Switches are easy to install and require minimal configuration.

1. **Explain Switch Boot Sequence**

Ans.

**Step 1: Power-On Self-Test (POST)**

1. The switch performs a POST to verify its hardware components, such as the CPU, memory, and interfaces.

2. The POST checks for any hardware failures or issues.

**Step 2: Bootloader Execution**

1. If the POST is successful, the switch executes its bootloader.

2. The bootloader is responsible for loading the switch's operating system.

**Step 3: Operating System Loading**

1. The bootloader loads the switch's operating system, which is typically stored in flash memory.

2. The operating system is responsible for managing the switch's hardware and software resources.

**Step 4: Configuration Loading**

1. Once the operating system is loaded, the switch loads its configuration file.

2. The configuration file contains settings such as VLANs, port assignments, and security configurations.

**Step 5: System Initialization**

1. After loading the configuration file, the switch initializes its system components, such as interfaces, routing protocols, and security features.

2. The switch is now ready to forward traffic and provide network services.

**Step 6: Running Configuration**

1. The switch loads its running configuration, which is a combination of the startup configuration and any changes made to the configuration since the last reboot.

2. The running configuration is stored in RAM and is used by the switch to operate.

**Types of Boot Sequences**

There are two types of boot sequences:

**1. Cold Boot**

A cold boot occurs when the switch is powered on or restarted. This type of boot sequence involves loading the operating system and configuration from scratch.

**2. Warm Boot**

A warm boot occurs when the switch is restarted without powering off. This type of boot sequence involves reloading the operating system and configuration without losing any existing connections or settings.

1. Regularly Back Up Configurations

Regularly back up your switch configurations to prevent loss of settings in case of a failure.

2. Use Redundant Power Supplies

Use redundant power supplies to ensure that the switch remains operational in case of a power supply failure.

3. Monitor Switch Performance

Regularly monitor switch performance to detect any issues that may affect the boot sequence.

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

Ans.

**Method 1: Console Connection**

1. Connect a console cable (usually a USB-to-serial or RJ-45-to-serial cable) to the switch's console port.

2. Connect the other end of the console cable to a computer or laptop.

3. Open a terminal emulation program (such as HyperTerminal, PuTTY, or SecureCRT) on the computer or laptop.

4. Configure the terminal emulation program to connect to the switch's console port (usually using a baud rate of 9600, 8 data bits, 1 stop bit, and no parity).

5. Press Enter to access the switch's CLI.

**Method 2: Telnet Connection**

6. Ensure that the switch is configured to allow Telnet connections.

7. Open a Telnet client program (such as PuTTY or SecureCRT) on a computer or laptop.

8. Enter the switch's IP address and Telnet port number (usually 23) in the Telnet client program.

9. Press Enter to connect to the switch's CLI.

10. Log in to the switch using a valid username and password.

**Method 3: SSH (Secure Shell) Connection**

11. Ensure that the switch is configured to allow SSH connections.

12. Open an SSH client program (such as PuTTY or SecureCRT) on a computer or laptop.

13. Enter the switch's IP address and SSH port number (usually 22) in the SSH client program.

14. Press Enter to connect to the switch's CLI.

15. Log in to the switch using a valid username and password.

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

Ans.

**What is Cisco IOS?**

Cisco IOS is a software used to manage and control Cisco network devices such as routers, switches, and firewalls. It provides a command-line interface (CLI) for configuring and monitoring network devices.

**Cisco IOS Modes**

There are several modes in Cisco IOS, each with different levels of access and functionality:

1. User EXEC Mode: This is the basic mode that allows users to execute basic commands.

2. Privileged EXEC Mode: This mode provides access to more advanced commands and configuration options.

3. Global Configuration Mode: This mode allows users to configure global settings for the device.

4. Interface Configuration Mode: This mode allows users to configure settings for specific interfaces.

Configuring Cisco IOS

**Here are the basic steps to configure Cisco IOS:**

1. Connect to the device: Connect to the device using a console cable or remotely using Telnet or SSH.

2. Enter privileged EXEC mode: Enter the command "enable" to enter privileged EXEC mode.

3. Enter global configuration mode: Enter the command "configure terminal" to enter global configuration mode.

4. Configure settings: Configure settings such as IP addresses, subnet masks, and routing protocols.

5. Save changes: Enter the command "copy running-config startup-config" to save changes to the startup configuration.

Basic Configuration Commands

**Here are some basic configuration commands:**

1. Hostname: Set the hostname of the device using the command "hostname <name>".

2. IP address: Set the IP address of an interface using the command "Ip address <address> <mask>".

3. Subnet mask: Set the subnet mask of an interface using the command "Ip subnet-mask <mask>".

4. Routing protocol: Configure a routing protocol such as RIP or OSPF using the command "router <protocol>".

5. Interface: Configure an interface using the command "interface <interface>".

Verifying Configuration

**Here are some commands to verify configuration:**

1. Show running-config: Displays the current running configuration.

2. Show startup-config: Displays the startup configuration.

3. Show Ip interface brief: Displays a brief summary of IP interfaces.

4. Show Ip route: Displays the IP routing table.

Common Cisco IOS Commands

**Here are some common Cisco IOS commands:**

1. Show: Displays information about the device or configuration.

2. Config: Enters global configuration mode.

3. Interface: Configures an interface.

4. Router: Configures a routing protocol.

5. Copy: Copies the running configuration to the startup configuration.

6. Write: Writes the running configuration to the startup configuration.

7. Reload: Reloads the device.

8. Shutdown: Shuts down an interface.

9. No shutdown: Enables an interface.

1. **Explain Switch Port**

**Ans.**

What is a Switch Port?

A switch port is a physical or virtual interface on a network switch that connects devices to the network. It is the point of entry and exit for data packets transmitted between devices on the network.

**Types of Switch Ports**

1. Access Port: A port that connects a device to the network, such as a computer or printer.

2. Trunk Port: A port that carries traffic from multiple VLANs (Virtual Local Area Networks) between switches.

3. Hybrid Port: A port that can function as both an access port and a trunk port.

4. Management Port: A port used for managing the switch, such as a console port or a management Ethernet port.

**Switch ports have several characteristics:**

1. Port Number: A unique number assigned to each port on the switch.

2. Port Speed: The speed at which data is transmitted over the port, such as 10 Mbps, 100 Mbps, or 1 Gbps.

3. Port Duplex: The duplex mode of the port, which can be half-duplex or full-duplex.

4. VLAN Assignment: The VLAN (Virtual Local Area Network) assigned to the port.

5. Port Status: The current status of the port, such as up, down, or disabled.

**Configuring Switch Ports:**

1. Interface Configuration: Configure port settings, such as speed, duplex, and VLAN assignment.

2. Port Security: Configure port security settings, such as MAC address filtering and port locking.

3. VLAN Configuration: Configure VLAN settings, such as VLAN creation and port assignment.

4. Port Mirroring: Configure port mirroring, which allows traffic to be copied from one port to another.

**Best Practices for Switch Port Configuration**

1. Use VLANs: Use VLANs to segment the network and improve security.

2. Configure Port Security: Configure port security settings to prevent unauthorized access.

3. Use Port Mirroring: Use port mirroring to monitor traffic and improve network troubleshooting.

4. Document Configuration: Document switch port configuration to ensure easy troubleshooting and maintenance.

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)

Ans. (A) R1 and (C) R3

**R1 and R3**

- R1 and R3 have the same subnet mask (/24) and are configured with the OSPF routing protocol.

- R1 and R3 also have the same network statement (network 10.1.1.0 0.0.0.255 area 0) which allows them to form a neighbor relationship.

- R2 and R4 are not using OSPF, so they will not be able to form a neighbor relationship with R1 and R3.

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

Ans. A. MD5

The "enable secret [password]" command in Cisco IOS is hashed using the MD5 (Message-Digest Algorithm 5) algorithm.

- B. AH (Authentication Header) is a protocol used for authentication and integrity, but it's not an algorithm used for hashing passwords.

- C. PSK (Pre-Shared Key) is a type of authentication that uses a shared secret key, but it's not an algorithm used for hashing passwords.

- D. ESP (Encapsulating Security Payload) is a protocol used for encrypting and authenticating IP packets, but it's not an algorithm used for hashing passwords.

- E. WPA2 (Wi-Fi Protected Access 2) is a wireless security protocol, but it's not an algorithm used for hashing passwords in Cisco IOS.

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?

Ans. B. R1 is a backup designated router.

The output "FULL/BDR" from the "show Ip ospf neighbor" command indicates that the neighbor (2.2.2.2) is in the FULL state, and the local router (R1) is the Backup Designated Router (BDR).

- In OSPF, a Designated Router (DR) is elected on each multi-access network (such as Ethernet or FDDI) to act as a central point for exchanging routing information.

- The BDR is a backup to the DR and takes over if the DR fails or becomes unavailable.

- The BDR is also responsible for monitoring the DR and taking over if necessary.

So, in this case, R1 is the BDR, which means it is the backup to the DR (which is likely another router on the same network).

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

Ans. D. "netsh" interface ipv6 show neighbors

- The "netsh" command is used to configure and manage various aspects of Windows networking, including IPv6.

- The "interface ipv6" option specifies that you want to work with IPv6 settings.

- The "show neighbors" option displays the neighbor discovery table, which contains information about neighboring devices on the network, including their IPv6 addresses and link-layer addresses.

**The other options are not correct because:**

- A and B are Cisco IOS commands, not Windows commands.

- C is close, but the correct option is "show neighbors", not "show neighbor".

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

Ans. A. List

- In the given example, Routers = [R1, R2, R3], the variable Routers is assigned a value that is enclosed in square brackets [].

- In programming, square brackets [] are used to define a list, which is a collection of values that can be of any data type, including strings, integers, and other lists.

- In this case, the list Routers contains three values: R1, R2, and R3, which are likely string values representing the names of routers.

**The other options are not correct because:**

- B. Dictionary: A dictionary is a collection of key-value pairs, and is typically defined using curly brackets {}.

- C. Simple: This is not a valid data type.

- D. Unsigned integers: The values in the list Routers are not integers, but rather string values representing router names.

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

Ans.

B. Time to Live

C. Source address

D. Destination address

- B. Time to Live (TTL): This field specifies the maximum number of hops that the packet can take before it is discarded. It is an 8-bit field that is decremented by 1 each time the packet is forwarded by a router.

- C. Source address: This field specifies the IPv4 address of the device that sent the packet. It is a 32-bit field that identifies the source of the packet.

- D. Destination address: This field specifies the IPv4 address of the device that the packet is intended for. It is a 32-bit field that identifies the destination of the packet.

**The other options are not correct because:**

- A. Host component: This is not a field in the IPv4 header.

- E. Network address: While the network address is part of the IPv4 address, it is not a separate field in the IPv4 header.