**ASSIGNMENT 6**

**Module -7: ====&Gt; CCNA - Network Fundamentals**

**1- Which of the following messages in the DHCP process are broadcasted? (Choose two)**

A. Request

1. Offer
2. Discover
3. Acknowledge

**Answer=** A. Request & C. Discover

**2- Which command would you use to ensure that an ACL does not block web-based TCP traffic?**

1. permit any
2. permit tcp any any eq 80
3. permit tcp any eq 80
4. permit any any eq tcp

**Answer=** B permit tcp any any eq 80

**3-Explain Network Topologies?**

**Answer=** **1. Bus Topology**

* **Description:** In this setup, all devices are connected to a single central cable, known as the bus.
* **Pros:** Easy to implement and extend, cost-effective for small networks.
* **Cons:** Limited cable length and number of stations, if the central cable fails, the entire network goes down.

**2. Star Topology**

* **Description:** All devices are connected to a central hub or switch.
* **Pros:** Easy to install and manage, failure of one device does not affect the others.
* **Cons:** Central hub failure leads to network failure, more cabling required compared to bus topology.

**3. Ring Topology**

* **Description:** Each device is connected to two other devices, forming a ring.
* **Pros:** Data packets travel at great speed, no collisions since each device has its own transmission medium.
* **Cons:** A failure in any cable or device can take down the entire network.

**4. Mesh Topology**

* **Description:** Every device is connected to every other device in the network.
* **Pros:** High redundancy, reliable and robust, failure of one link does not affect the network.
* **Cons:** Expensive and complex to install, requires a lot of cabling.

**5. Tree Topology**

* **Description:** A combination of star and bus topologies. Groups of star-configured networks are connected to a linear bus backbone.
* **Pros:** Scalable and easy to manage, supports future expansion.
* **Cons:** If the backbone line fails, the entire network gets disrupted.

**6. Hybrid Topology**

* **Description:** A mixture of two or more different topologies.
* **Pros:** Flexible, scalable, can be designed as per the requirements.
* **Cons:** Complex design and installation, can be expensive.

**4-Explain TCP/IP Networking Model?**

**Answer= 1. Application Layer**

* Description: This layer includes protocols and services that user applications interact with. It is responsible for providing network services directly to applications.
* Protocols: HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), DNS (Domain Name System), etc.
* Functions: Data representation, encoding, and dialog control.

**2. Transport Layer**

* Description: This layer is responsible for end-to-end communication and error recovery. It ensures that data is delivered error-free, in sequence, and without losses or duplications.
* Protocols: TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).
* Functions: Flow control, error checking, and data segmentation.

**3. Internet Layer**

* Description: This layer is responsible for logical addressing and routing. It handles the movement of packets across the network.
* Protocols: IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), and IGMP (Internet Group Management Protocol).
* Functions: Routing, addressing, and packet forwarding.

**4. Link Layer**

* Description: Also known as the Network Interface Layer or Data Link Layer, it is responsible for the physical transmission of data on the network. It provides the means to transfer data between devices on the same network segment.
* Protocols: Ethernet, Wi-Fi, PPP (Point-to-Point Protocol), etc.
* Functions: Framing, physical addressing, and error detection.

**5-Explain LAN and WAN Network?**

**Answer**= **Local Area Network (LAN)**

* Scope: A LAN covers a small geographic area, such as a single building, office, or home. It's typically confined to a single site.
* Ownership: LANs are usually owned, controlled, and managed by a single organization.
* Speed: LANs offer high data transfer rates, typically ranging from 10 Mbps to 10 Gbps.
* Cost: They are relatively inexpensive to set up and maintain due to the limited size and scope.
* Examples: Office networks, home networks, and school networks.
* Technology: Common technologies used in LANs include Ethernet and Wi-Fi.

**Wide Area Network (WAN)**

* Scope: A WAN covers a large geographic area, often spanning cities, states, countries, or even continents. It connects multiple LANs together.
* Ownership: WANs are typically operated by multiple organizations or service providers.
* Speed: WANs have lower data transfer rates compared to LANs, usually ranging from 56 Kbps to several Mbps.
* Cost: They are more expensive to set up and maintain due to the extensive infrastructure and long-distance connections.
* Examples: The Internet, corporate networks connecting multiple offices, and telecommunications networks.
* Technology: Common technologies used in WANs include MPLS (Multiprotocol Label Switching), Frame Relay, ATM (Asynchronous Transfer Mode), and leased lines.

**6-Explain Operation of Switch?**

**Answer= 1. Learning Mode**

* When a switch is first powered on, it operates in learning mode. It listens to the network traffic on all of its ports and builds a MAC address table (also known as a forwarding table).
* The MAC address table maps each device's MAC address to the port on which the device is connected.
* Example: If a device with MAC address AA:BB:CC:DD:EE:FF sends a frame through port 1, the switch records this information in its MAC address table.

**2. Forwarding Mode**

* After learning the MAC addresses, the switch operates in forwarding mode.
* When a frame is received on a switch port, the switch examines the destination MAC address of the frame and looks it up in the MAC address table.
* If the destination MAC address is found in the table, the switch forwards the frame to the corresponding port.
* If the destination MAC address is not found in the table, the switch broadcasts the frame to all ports except the one it was received on (this is known as flooding).

**3. Filtering**

* The switch filters out frames that are destined for the same network segment on which they originated. This helps to reduce network traffic and prevent loops.
* This is achieved through the MAC address table and ensuring that frames are only sent to the appropriate destination ports.

**4. Loop Prevention**

* Switches use protocols like Spanning Tree Protocol (STP) to prevent network loops.
* STP creates a loop-free logical topology by blocking redundant paths and allowing only one active path between two network devices.
* This ensures that frames do not circulate indefinitely, which can cause network congestion.

**5. VLANs (Virtual Local Area Networks)**

* Switches can create VLANs to segment the network into smaller, isolated sub-networks.
* Each VLAN acts as a separate logical network, even though the devices may be physically connected to the same switch.
* VLANs improve network performance and security by limiting broadcast domains and isolating sensitive data.

**Summary of Key Functions**

* MAC Address Table: Maintains a mapping of MAC addresses to switch ports.
* Forwarding and Filtering: Directs traffic to the appropriate destination ports and filters out unnecessary traffic.
* Loop Prevention: Uses protocols like STP to prevent network loops.
* VLAN Support: Creates and manages virtual sub-networks for improved performance and security.

**7-Describe the purpose and functions of various network devices?**

**Answer= 1. Router**

* Purpose: Connects multiple networks, including LANs and the Internet.
* Functions: Routing data, NAT, firewall.

**2. Switch**

* Purpose: Connects devices within a LAN.
* Functions: Frame switching, MAC address table, VLAN support.

**3. Access Point (AP)**

* Purpose: Provides wireless connectivity.
* Functions: Wireless communication, roaming, security.

**4. Modem**

* Purpose: Connects a network to the Internet via telephone lines or cable systems.
* Functions: Modulation, demodulation, bridge.

**5. Firewall**

* Purpose: Protects the network by filtering traffic.
* Functions: Packet filtering, stateful inspection, proxy service.

**6. Repeater**

* Purpose: Extends the range of a network.
* Functions: Signal boosting, regeneration.

**7. Bridge**

* Purpose: Connects and filters traffic between network segments.
* Functions: Traffic filtering, collision domain reduction.

**8. Gateway**

* Purpose: Connects networks with different architectures and protocols.
* Functions: Protocol conversion, traffic management, security.

**8-Make list of the appropriate media, cables, ports, and connectors to 8-**

**Answer**= **1. Router**

* Media: Ethernet, Fiber Optic
* Cables: Cat5e, Cat6, Cat6a, Fiber Optic cables
* Ports: RJ45, SFP, SFP+
* Connectors: RJ45 connectors, SFP modules

**2. Switch**

* Media: Ethernet, Fiber Optic
* Cables: Cat5e, Cat6, Cat6a, Fiber Optic cables
* Ports: RJ45, SFP, SFP+
* Connectors: RJ45 connectors, SFP modules

**3. Access Point (AP)**

* Media: Wireless, Ethernet
* Cables: Cat5e, Cat6, Cat6a
* Ports: RJ45
* Connectors: RJ45 connectors, antenna connectors

**4. Modem**

* Media: Coaxial, Telephone, Ethernet
* Cables: Coaxial cables, RJ11, Cat5e, Cat6
* Ports: Coaxial port, RJ11 port, RJ45 port
* Connectors: Coaxial connectors, RJ11 connectors, RJ45 connectors

**5. Firewall**

* Media: Ethernet, Fiber Optic
* Cables: Cat5e, Cat6, Cat6a, Fiber Optic cables
* Ports: RJ45, SFP, SFP+
* Connectors: RJ45 connectors, SFP modules

**6. Repeater**

* Media: Ethernet, Wireless, Fiber Optic
* Cables: Cat5e, Cat6, Cat6a, Fiber Optic cables
* Ports: RJ45, SFP
* Connectors: RJ45 connectors, SFP modules

**7. Bridge**

* Media: Ethernet, Fiber Optic
* Cables: Cat5e, Cat6, Cat6a, Fiber Optic cables
* Ports: RJ45, SFP
* Connectors: RJ45 connectors, SFP modules

**8. Gateway**

* Media: Ethernet, Fiber Optic, DSL, Coaxial
* Cables: Cat5e, Cat6, Cat6a, Fiber Optic cables, Coaxial cables, RJ11
* Ports: RJ45, SFP, Coaxial port, RJ11 port
* Connectors: RJ45 connectors, SFP modules, Coaxial connectors, RJ11 connectors

**9-connect switches to other?**

**Answer= Using Ethernet Cables**

1. Identify Uplink Ports: Look for dedicated uplink ports on the switches, often labeled as "Uplink" or "SFP".
2. Choose the Cable: Use appropriate Ethernet cables (Cat5e, Cat6, Cat6a) for the connection.
3. Connect the Switches: Plug one end of the Ethernet cable into the uplink port of the first switch and the other end into an available port (or another uplink port) on the second switch.

**Using Fiber Optic Cables**

1. Identify SFP Ports: If the switches have SFP ports, you can use fiber optic cables for higher speed and longer distance connections.
2. Install SFP Modules: Insert compatible SFP modules into the SFP ports on both switches.
3. Connect the Switches: Use a fiber optic cable to connect the SFP modules in both switches.

**Configuring the Switches**

1. Enable Spanning Tree Protocol (STP): Ensure STP is enabled on both switches to prevent network loops.
2. Configure VLANs: If using VLANs, configure the VLAN settings consistently across both switches.
3. Assign IP Addresses: Assign unique IP addresses to the management interfaces of each switch for easy administration.

**10-Define Network devices and hosts?**

**Answer= Network Devices**

Network devices are hardware components used to connect and manage computer networks. They facilitate communication, data transfer, and network management. Common network devices include:

* Router: Connects multiple networks and directs data traffic between them.
* Switch: Connects devices within a LAN and uses packet switching to forward data to its destination.
* Access Point (AP): Provides wireless connectivity for devices in a network.
* Modem: Modulates and demodulates digital data for transmission over analog communication lines.
* Firewall: Monitors and controls incoming and outgoing network traffic based on security rules.
* Repeater: Extends the range of a network by amplifying and retransmitting signals.
* Bridge: Connects and filters traffic between two or more network segments.
* Gateway: Connects networks with different architectures and protocols.

Hosts

Hosts are devices or systems connected to a network that use network resources and services. They can send, receive, and process data. Common examples of hosts include:

* Computers: Desktops, laptops, and servers.
* Smartphones and Tablets: Mobile devices connected to the network.
* Printers: Networked printers that can receive print jobs from other devices.
* IoT Devices: Smart home devices, such as smart thermostats, lights, and security cameras.
* Network Storage Devices: NAS (Network-Attached Storage) devices that provide shared storage to network users.