Module -7: Network fundamental

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

**A. Request**

B. Offer

**C. Discover**

D. Acknowledge

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

A. permit any

**B. permit tcp any any eq 80**

C. permit tcp any eq 80

D. permit any any eq tcp

3-Explain Network Topologies

**ANS**.

Network topologies refer to the arrangement or layout of different elements (nodes, links, etc.) in a computer network. Understanding network topologies is crucial for designing, implementing, and managing networks effectively. Here’s an overview of the most common types of network topologies:

**1. Bus Topology**

* **Description**: All devices are connected to a single central cable (the bus). Data travels in both directions along the bus.
* **Advantages**: Easy to implement and cost-effective for small networks.
* **Disadvantages**: If the central bus fails, the entire network goes down. Performance degrades as more devices are added.

**2. Star Topology**

* **Description**: All devices are connected to a central hub or switch. Each device communicates with the hub, which manages data traffic.
* **Advantages**: If one connection fails, it doesn’t affect the entire network. Easy to add or remove devices.
* **Disadvantages**: If the central hub fails, the whole network is affected. Requires more cable than bus topology.

**3. Ring Topology**

* **Description**: Each device is connected to two other devices, forming a circular pathway for data. Data travels in one direction (or both in some variations).
* **Advantages**: Data packets travel at high speeds; no collisions occur.
* **Disadvantages**: If one device fails, it can disrupt the entire network. Troubleshooting can be complex.

**4. Mesh Topology**

* **Description**: Each device is interconnected with multiple other devices. Can be either full mesh (every device connected to every other device) or partial mesh.
* **Advantages**: High redundancy and reliability; if one connection fails, data can take alternative paths.
* **Disadvantages**: Expensive to implement due to the amount of cabling and complexity.

**5. Tree Topology**

* **Description**: A combination of star and bus topologies. Groups of star-configured networks are connected to a linear bus backbone.
* **Advantages**: Scalable and hierarchical, allowing for easy expansion.
* **Disadvantages**: If the backbone fails, segments of the network can become isolated.

**6. Hybrid Topology**

* **Description**: A combination of two or more different topologies. For example, a star-bus network combines elements of both star and bus topologies.
* **Advantages**: Flexible and can be designed to meet specific needs.
* **Disadvantages**: Complexity in design and maintenance.

4-Explain TCP/IP Networking Model

**ANS**.

The TCP/IP networking model, also known as the Internet Protocol Suite, consists of four layers, each responsible for different aspects of network communication:

**1. Application Layer**

* **Function**: Provides network services to end-user applications.
* **Protocols**: HTTP, FTP, SMTP, DNS.
* **Role**: Formats data for applications like web browsing and email.

**2. Transport Layer**

* **Function**: Ensures reliable data transfer and error recovery.
* **Protocols**: TCP (connection-oriented) and UDP (connectionless).
* **Role**: Manages segmentation and delivery of data packets.

**3. Internet Layer**

* **Function**: Routes data packets across networks.
* **Protocols**: IP (IPv4 and IPv6), ICMP, ARP.
* **Role**: Addresses and packages data for routing.

**4. Network Interface Layer (Link Layer)**

* **Function**: Handles the physical connection and transmission over the medium.
* **Protocols**: Ethernet, Wi-Fi, PPP.
* **Role**: Manages hardware addressing and frame encapsulation.

5-Explain LAN and WAN Network

**ANS**.

**LAN (Local Area Network)**

**Definition**: A Local Area Network (LAN) is a network that connects computers and devices within a limited geographic area, such as a home, office, or school.

**Characteristics**:

* **Geographic Range**: Typically spans a small area, like a single building or a campus.
* **Speed**: Generally offers high data transfer rates, often ranging from 100 Mbps to several Gbps.
* **Ownership**: Usually owned and managed by a single organization or individual.
* **Examples**: Home networks, office networks, and school networks.

**Advantages**:

* **Cost-Effective**: Lower setup and maintenance costs compared to larger networks.
* **High Speed**: Faster data transmission due to shorter distances and fewer devices.
* **Ease of Setup**: Relatively simple to install and manage.

**WAN (Wide Area Network)**

**Definition**: A Wide Area Network (WAN) connects computers and devices over a large geographic area, often spanning cities, countries, or even continents.

**Characteristics**:

* **Geographic Range**: Covers a broad area, potentially thousands of miles.
* **Speed**: Typically slower than LANs, with data transfer rates that can vary widely.
* **Ownership**: Often involves multiple organizations or service providers; may include leased lines or satellite links.
* **Examples**: The Internet, corporate networks connecting multiple offices in different locations, and telecommunications networks.

**Advantages**:

* **Connectivity**: Enables communication and resource sharing across vast distances.
* **Scalability**: Can connect multiple LANs and support a large number of users and devices.
* **Flexibility**: Supports various communication technologies and infrastructures.

6-Explain Operation of Switch

**ANS**.

A switch is a critical networking device that operates primarily at Layer 2 (Data Link Layer) of the OSI model. Its main function is to connect devices within a local area network (LAN) and facilitate communication between them. Here’s how a switch operates:

**1. Learning MAC Addresses**

* When a switch is powered on, it starts by learning the Media Access Control (MAC) addresses of the devices connected to its ports.
* Each time a device sends data (a frame) to the switch, the switch reads the source MAC address and records it in its MAC address table along with the corresponding port.

**2. Forwarding Frames**

* When a device sends data to another device, it encapsulates the data in a frame that includes the destination MAC address.
* The switch checks its MAC address table to determine which port the destination MAC address is associated with.
  + **If the address is found**: The switch forwards the frame only to the port associated with the destination MAC address, minimizing unnecessary traffic on other ports.
  + **If the address is not found**: The switch broadcasts the frame to all ports (except the originating port) to discover the correct destination.

**3. Filtering Frames**

* Switches can filter frames based on MAC addresses, ensuring that data is only sent to the appropriate devices. This enhances network efficiency and security by reducing unnecessary traffic.

**4. Segmenting Traffic**

* By using switching, devices connected to the same switch can communicate with minimal collisions, as each port can operate in full-duplex mode (simultaneous send and receive).
* This segmentation leads to better overall performance in the network.

**5. Maintaining the MAC Address Table**

* The switch continuously updates its MAC address table. If a device moves to a different port, or if its MAC address changes, the switch learns and adapts to these changes to maintain accurate forwarding.

**6. VLAN Support**

* Many switches support Virtual Local Area Networks (VLANs), allowing network administrators to segment networks logically. This improves security and traffic management.

7-Describe the purpose and functions of various network devices 7-Make list of the appropriate media, cables, ports, and connectors.

**ANS**.

**Purpose and Functions of Various Network Devices**

1. **Router**
   * **Purpose**: Connects different networks and routes data.
   * **Functions**: Chooses optimal paths for data packets, provides NAT, and may include firewall features.
2. **Switch**
   * **Purpose**: Connects devices within a local network (LAN).
   * **Functions**: Learns MAC addresses to efficiently forward data and reduces collisions.
3. **Access Point (AP)**
   * **Purpose**: Provides wireless connectivity to a wired network.
   * **Functions**: Bridges wired and wireless networks.
4. **Modem**
   * **Purpose**: Connects to the internet via telephone or cable.
   * **Functions**: Converts digital signals for transmission and vice versa.
5. **Firewall**
   * **Purpose**: Protects networks by controlling traffic.
   * **Functions**: Monitors and filters traffic to prevent unauthorized access.
6. **Network Interface Card (NIC)**
   * **Purpose**: Enables devices to connect to a network.
   * **Functions**: Converts data for transmission and includes a MAC address.
7. **Repeater**
   * **Purpose**: Extends network range.
   * **Functions**: Amplifies and retransmits signals.

**Media, Cables, Ports, and Connectors**

**Media Types**

* **Twisted Pair Cable**: Used for Ethernet (e.g., Cat5e, Cat6).
* **Coaxial Cable**: For cable internet and TV.
* **Fiber Optic Cable**: For high-speed data transmission.

**Cables and Connectors**

* **Ethernet Cable (RJ-45)**: Connects devices in a wired LAN.
* **Coaxial Cable (F-type)**: For internet and TV connections.
* **Fiber Optic Cable (SC, LC connectors)**: For fiber connections.
* **USB Cable**: Connects devices to computers.

**Ports**

* **Ethernet Port (RJ-45)**: Common for network connections.
* **Coaxial Port**: For modems and cable boxes.
* **USB Ports**: For peripherals and devices.

8-Define Network devices and host

**ANS**.

**Network Devices** are hardware components that facilitate communication and data exchange between computers and other devices in a network. Common examples include:

* **Routers:** Direct data packets between different networks and manage traffic.
* **Switches:** Connect devices within a single network, forwarding data only to the intended recipient.
* **Access Points:** Allow wireless devices to connect to a wired network.
* **Modems:** Convert digital data from a computer to an analog signal for transmission over telephone lines (or vice versa).
* **Firewalls:** Monitor and control incoming and outgoing network traffic based on security rules.

**Hosts** refer to any devices connected to a network that can send or receive data. This includes:

* **Computers:** Desktops, laptops, and servers that participate in network communication.
* **Mobile Devices:** Smartphones and tablets that access network services.
* **IoT Devices:** Smart appliances and sensors that connect to the internet.