**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**

🡪 Network topologies refer to the physical or logical arrangement of the devices (such as computers, routers, switches, etc.) in a network. These topologies define how different components of a network are connected and how data is transmitted between them.

**Bus Topology**

* In bus topology, all devices (nodes) are connected to a single central cable, known as the **bus**. Data sent by a device travels along the bus, and all devices on the network receive the data, but only the intended recipient processes it.

**Star Topology**

* In star topology, all devices are connected to a central device (usually a **switch** or **hub**). Data is sent from one device to the central hub, which then forwards the data to the appropriate destination.

**Ring Topology**

* In ring topology, each device is connected to two other devices, forming a closed loop or ring. Data travels in one direction (unidirectional) or both directions (bidirectional) around the ring until it reaches the destination.

**Mesh Topology**

* In mesh topology, each device is connected directly to every other device in the network. This creates multiple paths for data to travel between devices.

**Tree Topology**

* Tree topology is a hybrid of star and bus topologies. Devices are organized into a hierarchical tree-like structure, where groups of star-configured networks are connected to a central bus.

**Hybrid Topology**

* Hybrid topology is a combination of two or more different network topologies. For example, a large network may use star topology for smaller segments, with the segments themselves connected in a bus or tree topology.

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

🡪 The TCP/IP networking model is a conceptual framework used to understand and implement network communications on the internet and other networks. It stands for Transmission ControlProtocol/Internet Protocol, which are the two foundational protocols for data transmission across networks. The model consists of four layers that define how data is sent and received between computers in a network.

**1. Application Layer**

The topmost layer of the TCP/IP model, the Application Layer, interacts directly with the end-user applications and provides the interface through which applications can communicate over the network.

Examples of protocols:

* HTTP (Hypertext Transfer Protocol)
* HTTPS (HTTP Secure)
* FTP (File Transfer Protocol)
* SMTP (Simple Mail Transfer Protocol)
* POP3 (Post Office Protocol 3)
* DNS (Domain Name System)

**2. Transport Layer**

The Transport Layer is responsible for end-to-end communication and data integrity. It ensures that data is transferred accurately and in the correct order between systems.

Examples of protocols:

* TCP (Transmission Control Protocol)
* UDP (User Datagram Protocol)

**3. Internet Layer**

The Internet Layer is responsible for addressing, routing, and forwarding data packets across networks, typically via the internet. It defines how data is sent from one host to another, and how it is routed through intermediate devices (like routers) to its destination.

Examples of protocols:

* IP (Internet Protocol)
* ICMP (Internet Control Message Protocol)

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

The Network Access Layer is the lowest layer of the TCP/IP model. It is responsible for the physical transmission of data over the network media (such as Ethernet cables, Wi-Fi, or fiber-optic cables).

Examples of protocols:

* PPP (Point-to-Point Protocol)

**5-Explain LAN and WAN Network**

🡪LAN (Local Area Network):

A Local Area Network (LAN) is a network that connects devices within a limited geographic area, such as a home, office, or campus. It allows for high-speed data transfer between devices and typically uses Ethernet cables or Wi-Fi to link them.

WAN (Wide Area Network):

A Wide Area Network (WAN) spans a much larger geographic area than a LAN, often connecting multiple LANs across cities, countries, or even continents. WANs are used to connect remote locations and facilitate communication between geographically dispersed devices.

**6-Explain Operation of Switch**

🡪

7-Describe the purpose and functions of various network devices

🡪 **1. Router**

* **Purpose**: A router is a device that connects multiple networks together, typically a local area network (LAN) to the internet (WAN). It directs data packets between networks based on their destination IP address.
* **Functions**:
  + **Routing**: Determines the best path for forwarding data between networks by using routing tables and protocols like OSPF, BGP, or RIP.
  + **Network Address Translation (NAT)**: Allows multiple devices in a LAN to share a single public IP address for internet access.
  + **Security**: Often includes a firewall to filter traffic and protect the network from unauthorized access.
  + **DHCP**: Can assign dynamic IP addresses to devices on the network.
  + **Traffic Management**: Manages network traffic to prevent congestion, using techniques like Quality of Service (QoS).

**2. Switch**

* **Purpose**: A switch is a device used to connect devices within a single network, allowing them to communicate by forwarding data packets to the correct destination device based on MAC addresses.
* **Functions**:
  + **Forwarding Data**: Uses MAC address tables to forward frames only to the correct device, reducing unnecessary network traffic.
  + **Learning**: Learns and stores the MAC addresses of devices connected to each port.
  + **Segmentation**: Creates separate collision domains for each port, reducing network collisions and improving efficiency.
  + **VLAN Support**: Can segment networks into Virtual LANs (VLANs) for improved security and performance.
  + **Bandwidth Management**: Can allocate bandwidth more effectively by reducing the chances of collisions.

**3. Hub**

* **Purpose**: A hub is an older, simple network device that connects multiple devices within a LAN, allowing them to communicate. Unlike a switch, a hub broadcasts data to all connected devices.
* **Functions**:
  + **Data Broadcasting**: Sends incoming data to all connected devices, regardless of the destination, resulting in more network traffic and potential collisions.
  + **Basic Connectivity**: Provides basic physical connectivity between devices but does not manage traffic or reduce collisions.
* **Limitations**: Hubs are less efficient and more prone to network congestion compared to switches, making them largely obsolete in modern networks.

**4. Access Point (AP)**

* **Purpose**: An Access Point is a device that provides wireless connectivity to a wired network, allowing Wi-Fi-enabled devices (such as smartphones, laptops, and tablets) to connect to the network.
* **Functions**:
  + **Wireless Communication**: Transmits and receives radio signals to enable wireless devices to access the network.
  + **Network Extension**: Can extend the coverage of a wired LAN by providing wireless access to areas not covered by wired connections.
  + **Security**: Implements wireless security protocols like WPA3, WPA2, or WEP to protect data and restrict unauthorized access to the network.
  + **SSID (Service Set Identifier)**: Manages network names (SSIDs) to distinguish between different wireless networks.

**5. Firewall**

* **Purpose**: A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It can be hardware or software-based.
* **Functions**:
  + **Traffic Filtering**: Inspects data packets to determine whether to allow or block them based on security policies.
  + **Network Protection**: Protects internal networks from unauthorized access and potential threats from external networks, such as the internet.
  + **Access Control**: Enforces access control policies to limit which devices or services can communicate across the network.
  + **Intrusion Detection and Prevention**: Detects and prevents attacks or unauthorized access attempts.

**6. Modem**

* **Purpose**: A modem (short for modulator-demodulator) is a device that converts digital data from a computer into analog signals suitable for transmission over telephone lines (in the case of DSL or dial-up) or cable systems (in the case of cable modems).
* **Functions**:
  + **Signal Conversion**: Modulates digital data into analog signals for transmission and demodulates incoming analog signals back into digital form for the receiving device.
  + **Internet Connectivity**: Provides a connection to the internet by converting the data into a form that can be transmitted over telephone lines, cable, or fiber-optic connections.
  + **Interface with ISP**: Communicates with the Internet Service Provider (ISP) to provide network access.

**7. Bridge**

* **Purpose**: A bridge is a device used to connect two or more network segments, allowing them to communicate as if they were part of the same network. It operates at the Data Link Layer (Layer 2) of the OSI model.
* **Functions**:
  + **Segmentation**: Reduces traffic by dividing a large network into smaller, manageable segments, helping to reduce collisions and improve performance.
  + **Frame Forwarding**: Forwards data based on MAC addresses. A bridge learns the MAC addresses of devices in each segment and decides whether to forward the frame to the other segment.
  + **Filtering**: Can filter traffic by preventing unnecessary traffic from passing between segments.

**8. Gateway**

* **Purpose**: A gateway is a network device that acts as an entry or exit point between two different networks, often with different communication protocols. It operates at multiple layers (usually Layer 3 and above) of the OSI model.
* **Functions**:
  + **Protocol Translation**: Converts communication between different protocol formats, enabling different types of networks (e.g., between IPv4 and IPv6, or between two different network architectures).
  + **Network Bridging**: Links networks with different technologies, such as connecting a local network to the internet or between different subnets.
  + **Security**: Can also act as a firewall, filtering traffic between networks.

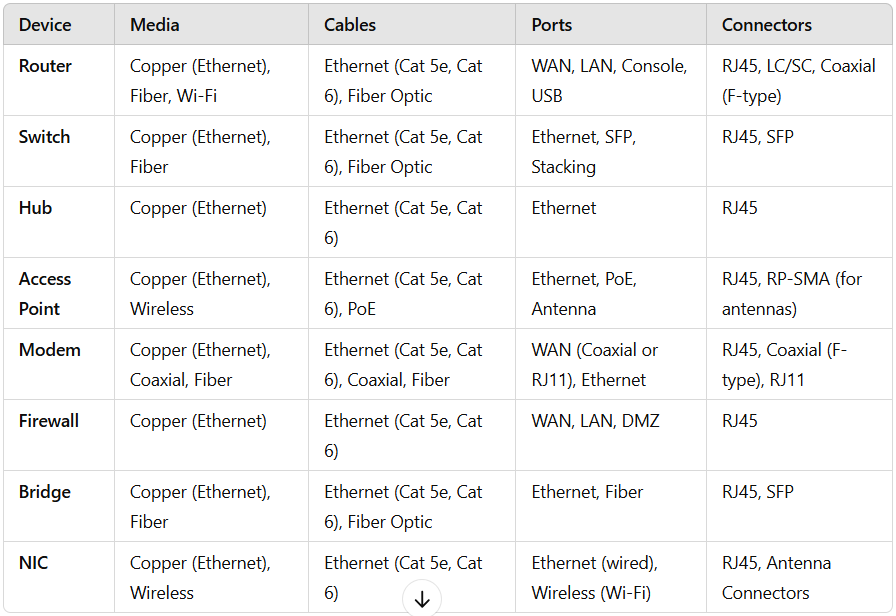
**9. Network Interface Card (NIC)**

* **Purpose**: A Network Interface Card (NIC) is a hardware component that allows a device (such as a computer, server, or printer) to connect to a network. It can be wired (Ethernet) or wireless (Wi-Fi).
* **Functions**:
  + **Physical Connection**: Provides the physical interface between the device and the network medium (e.g., Ethernet cable or Wi-Fi).
  + **Data Link Layer Communication**: Operates at the Data Link Layer (Layer 2) of the OSI model, managing the sending and receiving of data frames.
  + **MAC Address Assignment**: Each NIC has a unique MAC address for device identification on the network.

**10. Repeater**

* **Purpose**: A repeater is a device used to extend the range of a network by amplifying or regenerating the signal to overcome distance limitations.
* **Functions**:
  + **Signal Amplification**: Boosts the strength of a network signal that may degrade over long distances, allowing it to travel further.
  + **Network Extension**: Helps extend the reach of a network beyond the normal transmission distance, typically used in wireless networks to improve coverage.

8-Make list of the appropriate media, cables, ports, and connectors to connect switches to other

🡪 

**9-Define Network devices and hosts**

🡪 **Network Devices:**

Network devices are physical or virtual devices that facilitate the communication and management of data across a network. These devices are responsible for routing, switching, and connecting various devices within the network. Below are some common types of network devices:

1. Router: A router is a device that forwards data packets between different networks (e.g., between your local network and the internet). It determines the best path for data to travel.
2. Switch: A switch connects multiple devices within a local area network (LAN) and directs data to the correct device based on its MAC address. Unlike a hub, a switch can intelligently send data only to the device it is intended for.
3. Hub: A hub is a basic network device that connects multiple devices in a network. It broadcasts data to all devices, which is less efficient than a switch.
4. Access Point (AP**)**: An access point is a device that allows wireless devices to connect to a wired network. It acts as a bridge between wireless clients (like smartphones and laptops) and the wired LAN.
5. Modem: A modem (short for modulator-demodulator) converts digital data from a computer into analog signals that can travel over telephone lines or other communication media, and vice versa.
6. Firewall: A firewall is a security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules, protecting the network from unauthorized access or attacks.
7. Gateway: A gateway connects two different networks, often operating at the boundary between an internal network and an external network (like the internet). It acts as a translator between different communication protocols.

**Network Hosts:**

A network host refers to any device that is connected to a network and is capable of sending, receiving, or forwarding data. Hosts typically include devices such as computers, smartphones, servers, printers, or any other device that can interact over a network. Hosts usually have IP addresses, which uniquely identify them on the network. Key points about hosts:

1. Computers/Servers: These are devices that provide services or run applications within the network. A server might offer web hosting, file sharing, email, or other services.
2. Workstations: These are typically desktop or laptop computers that end users use to access network resources.
3. Printers/IoT Devices: Devices such as printers, smart devices, and other peripherals can be hosts on a network, allowing them to be managed or accessed remotely.
4. IP Address: Each host is assigned a unique IP address that identifies it within the network. It allows other devices to send data to and communicate with it.
5. End Devices: Hosts are often referred to as "end devices" because they are the endpoints where users interact with the network (e.g., users accessing the internet, databases, or applications).