**Module -7: Network fundamental**

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

1. Request B. Offer C. Discover D. Acknowledge

**ANS=>** A. **Request**  
 C. **Discover**

**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

**Ans = > B. permit tcp any any eq 80**

**3. Explain Network Topologies**

**Ans=>**Network topologies describe the physical or logical arrangement of nodes, connections, and devices in a network. Understanding different topologies helps in designing, implementing, and managing networks effectively. Here’s a breakdown of common network topologies:

1. Bus Topology

* Description: All devices share a single central cable or bus. Each device is connected to this main cable.
* Advantages:
  + Easy to implement and extend.
  + Requires less cable than other topologies.
* Disadvantages:
  + A failure in the central cable can bring down the entire network.
  + Performance issues as more devices are added (due to collisions and traffic).
* Usage: Simple networks with a limited number of devices.

2. Star Topology

* Description: All devices are connected to a central hub or switch. The hub acts as a repeater for data flow.
* Advantages:
  + If one cable fails, only the affected device is impacted.
  + Easy to manage and expand.
* Disadvantages:
  + Requires more cables than bus topology.
  + The central hub represents a single point of failure.
* Usage: Common in home and office networks.

3. Ring Topology

* Description: Devices are connected in a circular fashion. Each device has two connections, one to each neighboring device.
* Advantages:
  + Data packets travel in one direction (or both, if it's a dual-ring) reducing the chance of collision.
  + Easier to manage and troubleshoot.
* Disadvantages:
  + A failure in any single cable or device can disrupt the entire network.
  + More difficult to reconfigure.
* Usage: Used in certain types of LANs and WANs, often in networks requiring high reliability.

4. Mesh Topology

* Description: Each device is connected to every other device in the network. It can be full mesh (every device connected to every other device) or partial mesh (some devices connected to others).
* Advantages:
  + High redundancy and reliability; if one link fails, others can take over.
  + Provides high fault tolerance.
* Disadvantages:
  + Expensive and complex due to the number of connections and cabling required.
  + Difficult to manage and configure.

6. Hybrid Topology

* Description: Combines two or more different topologies. For example, a network that uses both star and ring topologies.
* Advantages:
  + Can be tailored to specific needs, combining the benefits of different topologies.
  + Flexible and scalable.
* Disadvantages:
  + Can be complex to design and manage.
  + More expensive than simpler topologies.
* Usage: Large networks where different parts of the network

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

**Ans=>** The TCP/IP networking model is a framework used to design and understand network communications. It stands for Transmission Control Protocol/Internet Protocol, and it outlines how data should be transmitted and received over a network. The model is divided into four distinct layers, each with specific functions:

1. Link Layer (Network Interface Layer)

* Function: This is the lowest layer and is responsible for the physical transmission of data over network hardware. It handles the communication between devices on the same network.
* Components: Network Interface Cards (NICs), Ethernet, Wi-Fi, and other hardware protocols.
* Responsibilities: Framing data packets, managing access to the physical medium, and error detection.

2. Internet Layer

* Function: This layer is responsible for logical addressing and routing of data across different networks. It ensures that data packets are delivered from the source to the destination even if they have to pass through multiple networks.
* Components: IP (Internet Protocol), including IPv4 and IPv6.
* Responsibilities: Packet forwarding, logical addressing (IP addresses), and routing.

3. Transport Layer

* Function: This layer manages end-to-end communication and ensures reliable data transfer between systems. It handles error recovery, flow control, and data segmentation.
* Components: TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).
  + TCP: Provides a connection-oriented service, ensuring data is delivered accurately and in order.
  + UDP: Provides a connectionless service with lower overhead, suitable for applications where speed is critical and occasional data loss is acceptable.

4. Application Layer

* Function: This is the top layer where network services and applications interact. It provides protocols and interfaces for applications to communicate over the network.
* Components: Protocols like HTTP, FTP, SMTP, DNS, and many others.
* Responsibilities: Defining how data is formatted, transmitted, and received by applications, and ensuring that applications can request and deliver network services.

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

**Ans =>** LAN (Local Area Network) and WAN (Wide Area Network) are two fundamental types of networks that differ primarily in their geographic scope, scale, and purpose. Here’s a detailed comparison:

Local Area Network (LAN)

Definition: A LAN is a network that connects computers and other devices within a limited geographic area, such as a single building or a campus.

Characteristics:

* Geographic Scope: Typically confined to a small area like an office, school, or home.
* Speed: Generally offers high-speed data transfer rates, often ranging from 100 Mbps to 10 Gbps or higher, depending on the technology used (e.g., Ethernet, Wi-Fi).
* Ownership: Usually owned, managed, and maintained by a single organization or individual.
* Setup: Involves network hardware like switches, routers, access points, and cabling, or wireless connections.
* Security: Generally easier to secure compared to WANs because of its limited scope and the control one has over the hardware and network traffic.

Common Uses:

* Connecting computers, printers, and other devices within a home or office.
* Sharing resources such as files, applications, and internet connections within a local area.

Examples:

* A home network connecting a few devices like computers, smartphones, and smart TVs.
* An office network connecting workstations, printers, and servers within a corporate building.

Wide Area Network (WAN)

Definition: A WAN is a network that covers a broad geographic area, often spanning cities, countries, or even continents. It connects multiple LANs and other types of networks.

Characteristics:

* Geographic Scope: Can cover extensive areas, from intercity connections to global networks.
* Speed: Typically has lower speeds compared to LANs due to the longer distances and various transmission mediums involved. Speeds can vary widely based on the technology and infrastructure used (e.g., fiber optics, satellite).
* Ownership: Often involves multiple stakeholders, including telecom providers and service providers. It can be owned by a single organization (private WAN) or a network of providers and users (public WAN).
* Setup: Involves complex infrastructure such as leased lines, fiber optic cables, satellite links, and VPNs. WANs require routing and switching equipment to manage data transmission across large distances.
* Security: More challenging to secure due to its vast and distributed nature, often requiring advanced encryption, firewalls, and security protocols.

Common Uses:

* Connecting remote offices of a company that are spread across different cities or countries.
* Providing internet access and enabling communication between geographically dispersed users and systems.
* Supporting global communications and data exchange for large organizations and service providers.

Examples:

* The internet itself is a massive WAN connecting millions of LANs around the world.
* A corporate network that links various branch offices located in different cities or countries.

Comparison:

* Scope: LAN is for small, localized areas; WAN spans larger, often global distances.
* Speed: LAN generally provides higher speeds compared to WAN.
* Complexity: WANs are more complex due to the need for advanced infrastructure and management of long-distance communications.
* Cost: Setting up and maintaining WANs can be more expensive compared to LANs, particularly due to the costs associated with long-distance communication and infrastructure.

**6. Explain Operation of Switch**

**Ans=>** A network switch is a crucial component in modern networking, serving as a central device that connects multiple devices within a Local Area Network (LAN). It operates primarily at Layer 2 (Data Link Layer) of the OSI model, but some advanced switches can also operate at Layer 3 (Network Layer) for routing capabilities. Here’s a detailed explanation of how a switch operates:

Basic Operation of a Switch

1. Frame Reception
   * Data Packet: Devices on a network communicate by sending data packets, which are encapsulated in frames.
   * Incoming Frames: When a device sends a frame to the switch, the switch receives this frame on one of its ports.
2. MAC Address Learning
   * Source MAC Address: As the switch receives a frame, it reads the source MAC (Media Access Control) address from the frame header.
   * MAC Address Table: The switch then updates its MAC address table (or forwarding table) with this source MAC address and the port on which the frame was received. This table keeps track of which MAC addresses are associated with which ports.
3. Frame Forwarding
   * Destination MAC Address: The switch examines the destination MAC address in the frame header.
   * Table Lookup: It looks up this destination MAC address in its MAC address table to determine which port the frame should be forwarded to.
   * Forwarding Decision: If the destination MAC address is found in the table, the switch forwards the frame out of the corresponding port. If it’s not found, the switch may flood the frame out of all ports except the port it came in on (known as broadcasting) to ensure it reaches the intended device.
4. Frame Filtering
   * Unicast: If the destination MAC address is known and corresponds to a specific port, the switch sends the frame only to that port.
   * Broadcast: If the MAC address is not in the table, the switch sends the frame to all ports (except the port it came from) to reach any device with that MAC address.
   * Multicast: For multicast addresses, the switch may use special techniques to efficiently distribute frames to multiple ports.
5. Learning and Aging
   * Learning: As new frames arrive, the switch continues to learn new MAC addresses and update its MAC address table accordingly.
   * Aging: To maintain the accuracy of the MAC address table, entries are periodically aged out. If a MAC address hasn’t been seen for a certain period, its entry is removed from the table.

Types of Switches

1. Unmanaged Switch
   * Description: Simple plug-and-play devices with no configuration options. They work automatically based on their default settings.
   * Use Case: Small networks or home environments where advanced features are not required.
2. Managed Switch
   * Description: Offers advanced features such as VLAN support, traffic management, network monitoring, and security options. Managed switches can be configured via a web interface, command line, or network management software.
   * Use Case: Larger networks requiring sophisticated control, monitoring, and optimization.
3. Layer 3 Switch
   * Description: Combines the functionalities of a Layer 2 switch with Layer 3 routing capabilities. It can perform routing functions and make decisions based on IP addresses in addition to MAC addresses.
   * Use Case: Networks requiring routing between VLANs or different IP subnets.

Benefits of Using a Switch

1. Improved Network Efficiency
   * Collision Domains: Each port on a switch creates its own collision domain, reducing collisions and improving overall network performance compared to hubs.
   * Dedicated Bandwidth: Switches provide dedicated bandwidth to each connected device, enhancing network efficiency and speed.
2. Enhanced Security
   * Traffic Segmentation: Switches can segment network traffic, reducing the chance of unauthorized access and improving security.
3. Scalability
   * Expandability: Switches allow for easy expansion of the network by adding more devices without significant reconfiguration.

**7.Describe the purpose and functions of various network devices**

**Ans=>**

Network devices play essential roles in the design, management, and operation of networks. Here’s an overview of various network devices, their purposes, and their functions:

**1. Router**

**Purpose**: Connects multiple networks and directs data packets between them.

**Functions**:

* **Routing**: Determines the best path for data to travel from source to destination across different networks (e.g., between a home network and the internet).
* **Packet Forwarding**: Directs packets based on IP addresses, using routing tables to decide the most efficient route.
* **NAT (Network Address Translation)**: Translates private IP addresses used within a local network to a public IP address for internet access.
* **Firewall**: Can provide basic security features to filter incoming and outgoing traffic based on predefined rules.

**2. Switch**

**Purpose**: Connects devices within the same network and manages data traffic efficiently.

**Functions**:

* **MAC Address Learning**: Builds and maintains a MAC address table to keep track of which devices are connected to which ports.
* **Frame Forwarding**: Directs data frames to the appropriate port based on MAC addresses, reducing unnecessary traffic.
* **Collision Domain Separation**: Each port creates a separate collision domain, improving network performance and reducing collisions.

**3. Hub**

**Purpose**: Connects multiple devices in a network, but without the intelligence of a switch.

**Functions**:

* **Broadcasting**: Sends incoming data packets to all connected devices, regardless of their intended destination.
* **Basic Connectivity**: Provides a simple way to connect multiple devices, though it is less efficient and secure compared to switches.

**4. Access Point (AP)**

**Purpose**: Provides wireless connectivity to devices within a network.

**Functions**:

* **Wireless Communication**: Allows wireless devices (e.g., laptops, smartphones) to connect to the wired network.
* **Signal Amplification**: Extends the range of a network by broadcasting a wireless signal.
* **SSID Broadcasting**: Advertises the network name (SSID) to allow devices to find and connect to the network.

**5. Modem**

**Purpose**: Converts digital data from a computer into an analog signal for transmission over telephone lines or other communication mediums, and vice versa.

**Functions**:

* **Signal Modulation and Demodulation**: Converts digital signals from the computer to analog signals for transmission and then converts incoming analog signals back to digital form.
* **Connection to ISP**: Provides the interface between a home or office network and the Internet Service Provider (ISP).

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

**Purpose**: Provides a hardware interface for a device to connect to a network.

**Functions**:

* **Data Link Layer Processing**: Handles the data link layer functions for communication over the network, including error checking and frame creation.
* **Physical Connection**: Connects to the network via Ethernet cables (wired NIC) or Wi-Fi (wireless NIC).

**8. Repeater**

**Purpose**: Extends the range of a network by amplifying or regenerating signals.

**Functions**:

* **Signal Amplification**: Boosts the strength of weak signals to cover longer distances.
* **Signal Regeneration**: Reconstructs distorted signals to maintain data integrity over longer distances.

**9. Bridge**

**Purpose**: Connects and filters traffic between two network segments to make them act as a single network.

**Functions**:

* **Traffic Filtering**: Operates at the data link layer to filter traffic based on MAC addresses, reducing collisions and improving performance.
* **Network Segmentation**: Divides a large network into smaller segments to reduce congestion and improve efficiency.

**10. Gateway**

**Purpose**: Connects different types of networks, often with different protocols or architectures.

**Functions**:

* **Protocol Conversion**: Translates between different network protocols or formats.
* **Data Integration**: Facilitates communication between systems that use different data formats or communication methods.

**7.Make list of the appropriate media, cables, ports, and connectors**

**Ans=>**

**Media**

1. **Physical Media**
   * **DVDs/Blu-rays**: For movies, software, and data.
   * **USB Flash Drives**: For transferring and storing data.
   * **External Hard Drives/SSDs**: For large-scale data storage and backup.
   * **Memory Cards (SD, microSD)**: For cameras, smartphones, and other devices.
2. **Digital Media**
   * **Streaming Services**: For movies, TV shows, and music (e.g., Netflix, Spotify).
   * **Online Storage**: Cloud services (e.g., Google Drive, Dropbox).

**Cables**

1. **Power Cables**
   * **AC Power Cables**: For connecting devices to power outlets.
   * **DC Power Cables**: For powering specific devices like laptops or adapters.
2. **Data Cables**
   * **USB Cables**: For data transfer and power (USB-A, USB-C, USB-B).
   * **HDMI Cables**: For high-definition video and audio.
   * **DisplayPort Cables**: For video output, especially in professional settings.
   * **VGA Cables**: Older standard for video output.
   * **Ethernet Cables (Cat5e, Cat6, Cat7)**: For network connections.
3. **Audio Cables**
   * **3.5mm Audio Cables**: For headphones and speakers.
   * **RCA Cables**: For audio and video connections (red, white, yellow).
   * **Optical Cables**: For digital audio connections.

**Ports**

1. **USB Ports**
   * **USB-A**: Standard port for many peripherals.
   * **USB-C**: Newer, reversible port for data and power.
   * **USB-B**: Common in printers and some external devices.
2. **Video Ports**
   * **HDMI**: For connecting monitors, TVs, and projectors.
   * **DisplayPort**: For high-resolution displays and multiple monitors.
   * **VGA**: Legacy port for older monitors and projectors.
3. **Audio Ports**
   * **3.5mm Jack**: For headphones, microphones, and speakers.
   * **Optical Audio**: For high-quality audio connections.
4. **Network Ports**
   * **Ethernet Port**: For wired internet connections.
5. **Specialized Ports**
   * **Thunderbolt**: High-speed data and power transfer, often used for external drives and docking stations.
   * **Docking Station Ports**: Various ports found on docking stations for connecting multiple peripherals.

**Connectors**

1. **USB Connectors**
   * **USB-A**: Rectangular, used for many peripherals.
   * **USB-C**: Reversible, compact, supports high-speed data and power.
   * **USB-B**: Square, used for printers and some external devices.
2. **Video Connectors**
   * **HDMI**: Rectangular with 19 pins, used for video and audio.
   * **DisplayPort**: Rectangular with 20 pins, supports high-resolution displays.
   * **VGA**: D-shaped with 15 pins, older standard for video.
3. **Audio Connectors**
   * **3.5mm TRS/TRRS**: For audio input/output, with variations for stereo or mic.
   * **RCA**: Color-coded (red, white, yellow) for audio and video.
   * **Optical Audio**: Square with a small hole, for digital audio.

**8.connect switches to other**

**Connecting Network Switches**

1. **Identify Ports**:
   * **Ethernet Ports**: Usually, Ethernet ports on switches are labeled as 1, 2, 3, etc. and are used for connecting devices.
   * **Uplink Port**: Some switches have a dedicated uplink port or a higher-speed port (like Gigabit Ethernet) for connecting to other switches or routers. If available, this should be used for connecting to other switches.
2. **Choose the Right Cable**:
   * **Ethernet Cable (Cat5e, Cat6, Cat6a, Cat7)**: Use an Ethernet cable to connect the switches. The category of the cable should match or exceed the speed capability of your switches (e.g., Cat6 for Gigabit Ethernet).
3. **Connect the Switches**:
   * **Direct Connection**: Connect one end of the Ethernet cable to an available port on the first switch and the other end to an available port on the second switch. If both switches are capable of Gigabit Ethernet, use a Cat6 or higher cable for optimal performance.
   * **Uplink Port (if available)**: If the switches have dedicated uplink ports, connect one end of the Ethernet cable to the uplink port of the first switch and the other end to the uplink port of the second switch. This setup can help in simplifying and optimizing network traffic management.
4. **Verify the Connection**:
   * **Link Lights**: Check the LED indicators on the ports where you connected the cable. These lights typically indicate the status of the connection (e.g., solid or blinking lights suggest an active connection).
   * **Network Configuration**: Ensure that both switches are configured correctly if they have managed features. For unmanaged switches, no configuration is needed.

9. Define Network devices and hosts

ANS=>

**Network Devices**

**Network devices** are hardware components that manage, direct, and facilitate the flow of data across a network. They play crucial roles in network communication, performance, and security. Common types of network devices include:

1. **Router**:
   * **Function**: Routes data packets between different networks, such as between a local network and the internet. It determines the best path for data to travel.
   * **Example**: Home router that connects your home network to your ISP.
2. **Switch**:
   * **Function**: Connects devices within the same network (e.g., LAN) and uses MAC addresses to forward data only to the devices that need it.
   * **Example**: Network switch in an office that connects computers, printers, and other devices.
3. **Hub**:
   * **Function**: Connects multiple devices in a network, but unlike switches, it broadcasts data to all connected devices, which can lead to network inefficiencies.
   * **Example**: Basic network hub used in older networks.
4. **Modem**:
   * **Function**: Modulates and demodulates signals for communication between digital data (from a computer) and analog signals (over phone lines or cable).
   * **Example**: Cable modem provided by an ISP for internet access.
5. **Access Point (AP)**:
   * **Function**: Allows wireless devices to connect to a wired network using Wi-Fi. It extends the coverage of a wireless network.
   * **Example**: Wi-Fi access point in a public library.
6. **Firewall**:
   * **Function**: Monitors and controls incoming and outgoing network traffic based on predetermined security rules to protect the network from unauthorized access.
   * **Example**: Hardware firewall used in a corporate network.
7. **Network Interface Card (NIC)**:
   * **Function**: Provides the hardware interface between a computer and the network. It can be wired (Ethernet NIC) or wireless (Wi-Fi NIC).
   * **Example**: Built-in Ethernet card in a desktop computer.
8. **Repeater**:
   * **Function**: Amplifies or regenerates signals to extend the distance over which data can travel on a network.
   * **Example**: Signal repeater used to boost Wi-Fi coverage in a large building.
9. **Bridge**:
   * **Function**: Connects and filters traffic between two or more network segments, helping to reduce network collisions and manage traffic.
   * **Example**: Network bridge used to connect two network segments in a large office.