**Networking career development program.**

**Assignment: CCNA Module -7: Network fundamental –**

**Section 1. MCQS**

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

* A. request
* C. discover

1. **ACL Command to Allow Web-Based TCP Traffi?**

* B. permit tcp any any eq 80

**Section 2. questions and answers**

1. **Explain Network Topologies**

* There are 6 topologies in networking

Bus topology

Star topology

Ring topology

Mesh topology

Hybrid topology

Tree topology

Explain below

1. 🌐Bus topology : Bus topology connects all devices to a single central cable, called the bus or backbone. Data travels in both directions along the cable, and each device listens for data addressed to it. It's simple and cost-effective but prone to collisions and difficult to troubleshoot.
2. 🔄 **Ring Topology** : In a ring topology, each device connects to exactly two other devices, forming a circular data path. Data travels in one direction around the ring until it reaches its destination. If one device fails, the entire network can be disrupted unless a dual ring is used.
3. ⭐ **Star Topology** : Star topology connects all devices to a central hub or switch. The hub acts as a repeater for data flow. It's easy to manage and expand, and failure of one device doesn’t affect others—but if the central hub fails, the whole network goes down.
4. 🕸️ **Mesh Topology** : Mesh topology provides a point-to-point connection between every device in the network. It offers high redundancy and fault tolerance, as data can take multiple paths to reach its destination. However, it’s expensive and complex to set up.
5. 🌲 **Tree Topology** : Tree topology is a hierarchical structure that combines characteristics of star and bus topologies. Devices are arranged in a parent-child relationship, with branches extending from a central root node. It’s scalable and organized but depends heavily on the root node.
6. 🔧 **Hybrid Topology** : Hybrid topology is a combination of two or more different topologies, such as star-ring or star-bus. It’s flexible and customizable to meet specific network needs, but it can be complex to design and maintain.
7. **Explain TCP/IP Networking Model ?**

* 📡 **What Is the TCP/IP Model?**

The **TCP/IP model** (Transmission Control Protocol/Internet Protocol) is a conceptual framework used to describe how data moves from one computer to another over a network. It was developed in the 1970s by the U.S. Department of Defense to support robust, scalable communication across diverse systems.

Unlike the OSI model which has seven layers, the TCP/IP model has **four layers**, each responsible for specific functions in the communication process

**🧱 Layers of the TCP/IP Model**

**1. Application Layer**

This is the topmost layer where user interaction happens. It includes protocols like HTTP, FTP, SMTP, DNS, and more. These protocols enable services like web browsing, email, and file transfers.

* **Function**: Provides network services directly to applications.
* **Example**: When you open a website, HTTP handles the request and response.

**2. Transport Layer**

This layer ensures reliable data delivery between devices. It uses protocols like TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

* **TCP**: Reliable, connection-oriented (used for web, email).
* **UDP**: Fast, connectionless (used for streaming, gaming).
* **Function**: Manages end-to-end communication, error checking, and data flow control.

**3. Internet Layer**

This layer handles routing and addressing of data packets across networks. The key protocol here is IP (Internet Protocol).

* **Function**: Determines the best path for data to travel across networks.
* **Other** **protocols**: ICMP (used for diagnostics like ping), ARP (resolves IP to MAC addresses).

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

This is the lowest layer, dealing with physical transmission of data over network hardware like Ethernet or Wi-Fi.

* **Function**: Defines how data is physically sent through cables or wireless signals.
* **Includes**: MAC addressing, framing, and hardware interfaces.

**🔄 How It Works Together**

When you send data (like an email or web request), it flows down the layers from Application to Network Access. Each layer adds its own header (encapsulation). At the receiving end, the data flows up the layers, with each layer interpreting and removing its header (decapsulation).

**🧠 Why It Matters**

* **Scalability**: Supports millions of devices across the globe.
* **Interoperability**: Works across different hardware and operating systems.
* **Reliability**: Ensures accurate and complete data delivery.

1. **Explain LAN and WAN Network.**

* LAN (Local Area Network) connects devices within a small area like a home or office, while WAN (Wide Area Network) spans large geographic regions, linking multiple LANs across cities or countries.
* 🏠 **LAN – Local Area Network**

A **LAN** is a network that connects computers and devices within a limited area such as a home, school, or office building. It’s typically owned, managed, and maintained by a single organization or individual.

* **Scope**: Small geographic area (e.g., one building)
* **Speed**: High data transfer rates (often 100 Mbps to 10 Gbps)
* **Ownership**: Privately owned and managed
* **Examples**: Office network, home Wi-Fi, school computer lab
* **Advantages**:
  + Fast communication
  + Easy to set up and manage
  + Low cost
* **Protocols used**: Ethernet, Wi-Fi
* 🌍 **WAN – Wide Area Network**

A **WAN** connects multiple LANs over large distances, such as between cities, states, or countries. It often uses public infrastructure like telephone lines, fiber optics, or satellite links.

* **Scope**: Large geographic area (e.g., across continents)
* **Speed**: Slower than LAN due to long-distance transmission
* **Ownership**: Often managed by telecom providers or ISPs
* **Examples**: The Internet, corporate networks linking global offices
* **Advantages**:
  + Enables global communication
  + Connects remote offices and users
* **Technologies used**: MPLS, leased lines, VPNs, satellite links

**🔁 Key Differences**

- **LAN** is localized, fast, and inexpensive to maintain.

- **WAN** is distributed, slower, and more complex to manage.

- **LANs** are ideal for internal communication;

- **WANs** are essential for connecting across regions.

1. **Explain Operation of Switch**

* A network switch operates at the Data Link Layer (Layer 2) of the OSI model and is responsible for forwarding data frames between devices based on their MAC addresses. It ensures efficient and secure communication within a LAN

⚙️ **How a Network Switch Works**

A **network switch** is a device that connects multiple devices (like computers, printers, and servers) within a local area network (LAN). Unlike a hub, which broadcasts data to all ports, a switch intelligently forwards data only to the intended recipient.

Here’s a step-by-step breakdown of its operation:

1. **MAC Address Learning**

When a device sends data through the switch, the switch reads the **source MAC address** from the incoming frame and stores it in its **MAC address table** along with the port it came from. This helps the switch know which device is connected to which port.

**2. Frame Forwarding**

When the switch receives a frame, it checks the destination MAC address:

- If the address is in its MAC table, it forwards the frame to the correct port.

- If the address is unknown, it broadcasts the frame to all ports except the one it came from.

3. **Filtering**

Switches **filter traffic** by ensuring that frames are only sent to the device that needs them. This reduces unnecessary traffic and improves network efficiency

4. **Full Duplex Communication**

Modern switches support **full duplex**, allowing devices to send and receive data simultaneously, doubling the effective bandwidth

5. **Error Checking**

Switches perform basic **error checking** using techniques like **CRC (Cyclic Redundancy Check)** to ensure data integrity before forwarding frames.

6. **Support for VLANs**

Advanced switches can segment networks into **Virtual LANs (VLANs)**, isolating traffic for security and performance.

🔄 **Types of Communication Supported**

* **Unicast**: One-to-one communication
* **Multicast**: One-to-many (specific group)
* **Broadcast**: One-to-all (within the LAN)

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

* Network devices are essential components that enable communication, data transfer, and connectivity across computer networks. Each device plays a specific role in managing traffic, ensuring security, and maintaining efficient data flow

🔌 1. Hub

A hub is a basic networking device that connects multiple computers in a LAN. It broadcasts incoming data to all connected devices, regardless of the destination.

- Purpose: Simple data distribution

- Function: Operates at Layer 1 (Physical Layer); no filtering or routin

🔁 **2. Switch**

A **switch** connects devices in a LAN and forwards data only to the device that needs it, using MAC addresses.

* **Purpose**: Efficient data forwarding within a LAN
* **Function**: Operates at Layer 2 (Data Link Layer); builds MAC address table for intelligent switching

🌐 **3. Router**

A **router** connects different networks and directs data packets between them using IP addresses.

* **Purpose**: Inter-network communication
* **Function**: Operates at Layer 3 (Network Layer); performs routing, NAT, and traffic management

🔄 **4. Repeater**

A **repeater** regenerates and amplifies signals to extend the range of a network.

* **Purpose**: Signal boosting over long distances
* **Function**: Operates at Layer 1; used in wired and wireless networks

🌉 **5. Bridge**

A **bridge** connects two LAN segments and filters traffic based on MAC addresses.

* **Purpose**: Network segmentation and traffic control
* **Function**: Operates at Layer 2; reduces collisions and improves performance

🚪 **6. Gateway**

A **gateway** acts as a translator between different network protocols or architectures.

* **Purpose**: Protocol conversion and external network access
* **Function**: Operates across multiple layers; used to connect enterprise networks to the Internet

📶 **7. Access Point (AP)**

An **access point** allows wireless devices to connect to a wired network.

* **Purpose**: Wireless connectivity
* **Function**: Operates at Layer 2; supports Wi-Fi standards and manages wireless clients

**🔐 8. Firewall**

A firewall monitors and controls incoming and outgoing network traffic based on security rules.

- **Purpose**: Network security

- **Function**: Operates at Layer 3 and above; filters packets, blocks threats, and enforces policies

📡 **9. Modem**

A **modem** modulates and demodulates signals for data transmission over telephone lines or cable.

* **Purpose**: Internet access via ISP
* **Function**: Converts digital data to analog and vice versa

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

* Here’s a detailed list of **appropriate media, cables, ports, and connectors** for the **8 common network devices** we discussed earlier. This will help you understand what physical components are typically used with each device:

**1. Hub**

* Media: Twisted Pair (UTP/STP)
* Cables: Ethernet cables (Cat5e, Cat6)
* Ports: RJ-45 ports (usually 4 to 24)
* Connectors: RJ-45 connectors

**2. Switch**

* Media: Twisted Pair, Fiber Optic
* Cables:
  + Ethernet cables (Cat5e, Cat6, Cat6a)
  + Fiber optic cables (for uplinks or backbone)
* Ports:
  + RJ-45 ports (for copper Ethernet)
  + SFP/SFP+ ports (for fiber modules)
  + Connectors:
* RJ-45
* LC, SC (for fiber

**3. Router**

* Media: Twisted Pair, Fiber Optic, Coaxial
* Cables:
  + Ethernet cables (Cat5e, Cat6)
  + Fiber optic cables (for high-speed WAN links)
  + Coaxial (for cable internet)
* Ports:
  + RJ-45 (LAN/WAN)
  + SFP/SFP+ (fiber)
  + Coaxial (for cable modems)
* Connectors:
* RJ-45
* LC/SC (fiber)
* F-type (coaxial)

**4. Repeater**

* Media: Twisted Pair, Fiber Optic
* Cables:
  + Ethernet cables
  + Fiber optic cables
* Ports:
  + RJ-45
  + Fiber ports
* Connectors:
* RJ-45
* LC/SC

**5. Bridge**

* Media: Twisted Pair
* Cables: Ethernet cables
* Ports: RJ-45
* Connectors: RJ-45

**6. Gateway**

* Media: Twisted Pair, Fiber Optic, Coaxial
* Cables:
  + Ethernet cables
  + Fiber optic cables
  + Coaxial cables
* Ports:
  + RJ-45
  + SFP
  + Serial ports (for legacy systems)
* Connectors:
* RJ-45
* LC/SC
* DB-9/DB-25 (serial)

**7. Access Point (AP)**

* Media: Wireless (Radio Frequency), Twisted Pair
* Cables: Ethernet (for PoE or uplink)
* Ports: RJ-45 (PoE or LAN)
* Connectors:
* RJ-45
* Antenna connectors (RP-SMA for external antennas)

**8. Modem**

* Media: Coaxial, Twisted Pair, Fiber Optic
* Cables:
  + Coaxial (cable modem)
  + DSL cable (RJ-11)
  + Fiber optic (ONT modems)
* Ports:
  + RJ-11 (DSL)
  + RJ-45 (Ethernet)
  + Coaxial (Cable)
* Connectors:
* RJ-11
* RJ-45
* F-type (coaxial)
* LC/SC (fiber)

1. **connect switches to other**

* 🧩 Step-by-Step: Connecting Switches to Other Devices

1. **Connect Switch to Router**

Use a **crossover cable** (older convention) or **straight-through cable** (modern switches with auto-MDIX).

Plug one end into the **GigabitEthernet or FastEthernet port** on the switch.

Plug the other end into the **Ethernet port** on the router.

**2. Connect Switch to PC or Laptop**

Use a **straight-through cable**.

Connect from the switch’s **FastEthernet port** to the PC’s **Ethernet NIC**.

**3. Connect Switch to Another Switch**

Use a **straight-through cable** (modern switches) or **crossover cable** (older switches).

 Connect from one switch’s **GigabitEthernet port** to the other switch’s **GigabitEthernet port**.

* Optionally, configure **trunking** on these ports if VLANs are involved:

Switch(config)# interface GigabitEthernet0/1

Switch(config-if)# switchport mode trunk

4. **Verify Connections**

* Use the **“Show” commands**:

Switch# show ip interface brief

Switch# show cdp neighbors

1. **Define Network devices and hosts**

* Network devices are hardware components that manage and facilitate communication within a computer network, while hosts are end-user devices that send or receive data across the network.
* **🧠 What Are Network Devices?**

Network devices are specialized hardware used to connect, manage, and route data between computers and other devices in a network. They operate across different layers of the OSI and TCP/IP models and perform tasks like signal regeneration, packet switching, routing, and access control.

**🔧 Common Types of Network Devices:**

* **Router**: Directs data packets between different networks and assigns IP addresses.
* **Switch**: Connects devices within the same network and forwards data based on MAC addresses.
* **Hub**: Broadcasts data to all connected devices (less efficient than switches).
* **Bridge**: Connects two LANs and filters traffic based on MAC addresses.
* **Repeater**: Regenerates signals to extend the range of a network.
* **Gateway**: Translates data between different network protocols.
* **Access** **Point**: Provides wireless connectivity to wired networks.

These devices help ensure *efficient, secure, and reliable communication* across networks.

* **🖥️ What Are Hosts?**

A **network host** is any device connected to a network that can send or receive data. Hosts typically include:

**Computers**

**Servers**

**Smartphones**

**Printers**

**IoT devices**

Each host is assigned at least one **IP address**, allowing it to communicate with other hosts. Hosts can act as:

**Clients**: Requesting services or data (e.g., web browsers).

**Servers**: Providing services or data (e.g., web servers, file servers).

Hosts are the endpoints of communication and are essential for user interaction with the network.