CS – 20 NETWORK TECHNOLOGY AND ADMINISTRATION.

Prepared by : Lathiya_Harshal.

- What is a Network?

  A **network** is a system of interconnected devices or nodes (such as computers, servers, printers, and other devices) that can communicate and share data with each other. The devices in a network are connected through communication channels like cables, fiber optics, or wireless signals.

Types of Networks:

LAN (Local Area Network): Covers a small area, like a single building or campus.

WAN (Wide Area Network): Covers large geographical areas, connecting multiple LANs (e.g., the internet).

MAN (Metropolitan Area Network): Spans a city or large campus.

PAN (Personal Area Network): A small network for personal devices (e.g., Bluetooth devices).

- Use of network

A **network** is useful because it lets devices and people **share information** and **resources** easily.

1. **File Sharing**: You can share files (like documents, photos, or videos) between computers, without using USB drives.

2. **Internet Access**: All devices in the network can share a single internet connection, so everyone can browse the web.

3. **Communication**: People can send emails, chat, or do video calls over the network.

4. **Resource Sharing**: You can use shared printers, storage devices (like hard drives), or other tools connected to the network.

5. **Remote Access**: You can access your work computer from home through the network, which makes it easier to work from different places.

In simple terms, a network helps **connect devices and people**, making sharing and communication faster and easier.

- Network model :

1. Peer-to-Peer (P2P) Network Model

In a **Peer-to-Peer (P2P)** network, each device (called a peer) acts as both a client and a server. This means all devices in the network have equal responsibilities and can share resources directly with each other without needing a central server.

Features of P2P:

- **No central server**: Each device can share files, printers, or other resources with other devices directly.
- **Equal roles**: Every device acts both as a provider and a consumer of resources.
- **Simple and cost-effective**: It's easy to set up and doesn't require expensive hardware or dedicated servers.

Examples of P2P Networks:

- Small office or home networks where users share files and printers directly.
- File-sharing systems like BitTorrent, where users download and upload files directly to each other.

Advantages:

- Easy to set up and manage, especially for small networks.
- Less expensive, as no dedicated server hardware is needed.

Disadvantages:

- Not as secure as client-server models since there's no central control.
- Difficult to manage as the network grows larger.

---

2. Client-Server Network Model

In a **Client-Server** network, the devices are divided into two categories:

- **Clients**: These are devices (like computers or smartphones) that request services, such as data or files.
- **Servers**: These are powerful computers that provide services, store data, and manage resources for the clients.

Features of Client-Server:

- **Centralized control**: Servers manage all the resources (files, printers, databases), and clients access these resources through the server.
- **Dedicated roles**: The server provides resources, and clients request and use them.
- **Scalable**: Client-server networks can handle many clients and large-scale operations.

Examples of Client-Server Networks:

- Websites: Your computer (client) requests data from a web server.
- Email systems: The server manages all emails, and users (clients) access their accounts from different devices.

Advantages:

- **Centralized management**: Easier to control security, updates, and resources.
- **Scalability**: Can support large numbers of clients and complex operations.

Disadvantages:

- **Costly**: Requires dedicated server hardware and maintenance.
- **Server dependency**: If the server fails, clients may lose access to resources.

- Network Services

Network Services refer to the various functions provided by a network to help users and devices communicate, share resources, and perform tasks. These services enable computers to **share files, printers, applications**, and other resources over the network, making collaboration and data exchange easier and more efficient.

Types of Network Services

1. File Service

- **Definition**: A **file service** allows users to **store, retrieve, and manage files** on a network. Instead of saving files on their individual computers, users can store them on a central server and access them from any device connected to the network.
- **Example**: A shared folder on a server that can be accessed by employees in an office to collaborate on documents.

2. Print Service

- **Definition**: A **print service** lets users in the network **share printers**. Instead of connecting a printer to every computer, a printer is connected to the network, and multiple users can print to it from their devices.
- **Example**: In an office, multiple employees can send print jobs to a single printer through the network.

3. Communication Service (Comm. Service)

- **Definition**: A **communication service** facilitates **communication between users** on the network, such as sending messages, making voice or video calls, or chatting in real-time.
- **Example**: Email servers (like Microsoft Exchange) and messaging apps (like WhatsApp or Microsoft Teams) that allow users to send messages or make video calls.

4. Database Service

- **Definition**: A **database service** provides users with access to **centralized databases**. This service allows multiple users to **store, retrieve, and manipulate data** in databases over the network.
- **Example**: A company's customer database that can be accessed and updated by different departments (like sales, support) through the network.

5. Security Service

- **Definition**: A **security service** helps protect the network and its resources from unauthorized access, viruses, and cyberattacks. It includes mechanisms like **firewalls, encryption, and user authentication** to keep the network secure.
- **Example**: A firewall that controls which data can enter or leave a company's network or a login system that ensures only authorized users can access certain files.

6. Application Service

- **Definition**: An **application service** refers to the **centralized hosting of software applications** on a network. Instead of installing software on every device, users can access the application from the server.
- **Example**: Cloud-based applications like Google Docs or Microsoft Office 365, where the software is hosted on a remote server, and users can access and work on it over the internet.

- Network Access Methods

Network Access Methods are rules or protocols that determine how devices in a network can **access the communication channel (the shared medium)** to send data. In a network, multiple devices share the same communication medium (such as a cable or wireless channel), and access methods prevent collisions or conflicts when multiple devices try to send data at the same time.

These methods ensure that devices can efficiently and fairly send and receive data without interference or data loss.

Types of Network Access Methods

1. CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

- **Definition**: CSMA/CD is an access method used mainly in **wired networks** (like Ethernet). Before a device sends data, it first listens to check if the communication medium (cable) is **free**. If it's clear, the device sends the data. However, if two devices send data at the same time, a **collision** occurs. In CSMA/CD, the devices can **detect** this collision, stop sending, wait for a random time, and then try again.

- **How it works**:

    1. The device checks if the line is free (carrier sensing).
    2. If free, it sends the data.
    3. If a collision occurs, devices stop sending and wait before retrying.
- **Example**: Used in **Ethernet networks** (older wired LANs).

---

2. CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

- **Definition**: CSMA/CA is used in **wireless networks** (like Wi-Fi). Similar to CSMA/CD, it listens to the channel before sending data. However, instead of dealing with collisions after they happen (like in CSMA/CD), CSMA/CA tries to **prevent** collisions by waiting for a random period and sending a **warning signal** to other devices before transmitting data.

- **How it works**:

    1. The device checks if the channel is free (carrier sensing).
    2. It sends a warning to other devices, letting them know it is about to send data.
    3. After the warning, it sends the data, avoiding a collision.
- **Example**: Used in **Wi-Fi networks** to avoid collisions in wireless communication.

---

3. Token Passing

- **Definition**: In **Token Passing**, a special data packet called a "token" is passed around the network. Only the device that holds the token can send data. Once the device finishes sending data, it passes the token to the next device. This ensures that **only one device** can transmit at a time, preventing collisions.

- **How it works**:

    1. A token circulates around the network.
    2. A device must wait until it receives the token before it can send data.
    3. After sending, the token is passed to the next device.
- **Example**: Used in **Token Ring** networks (an older network technology).

---

4. Polling

- **Definition**: In **Polling**, a central device (like a server or a master device) controls which device can transmit data by "polling" or **asking each device** in turn if it has data to send. If a device has data, it sends it when polled. This method ensures organized access to the network medium.

- **How it works**:

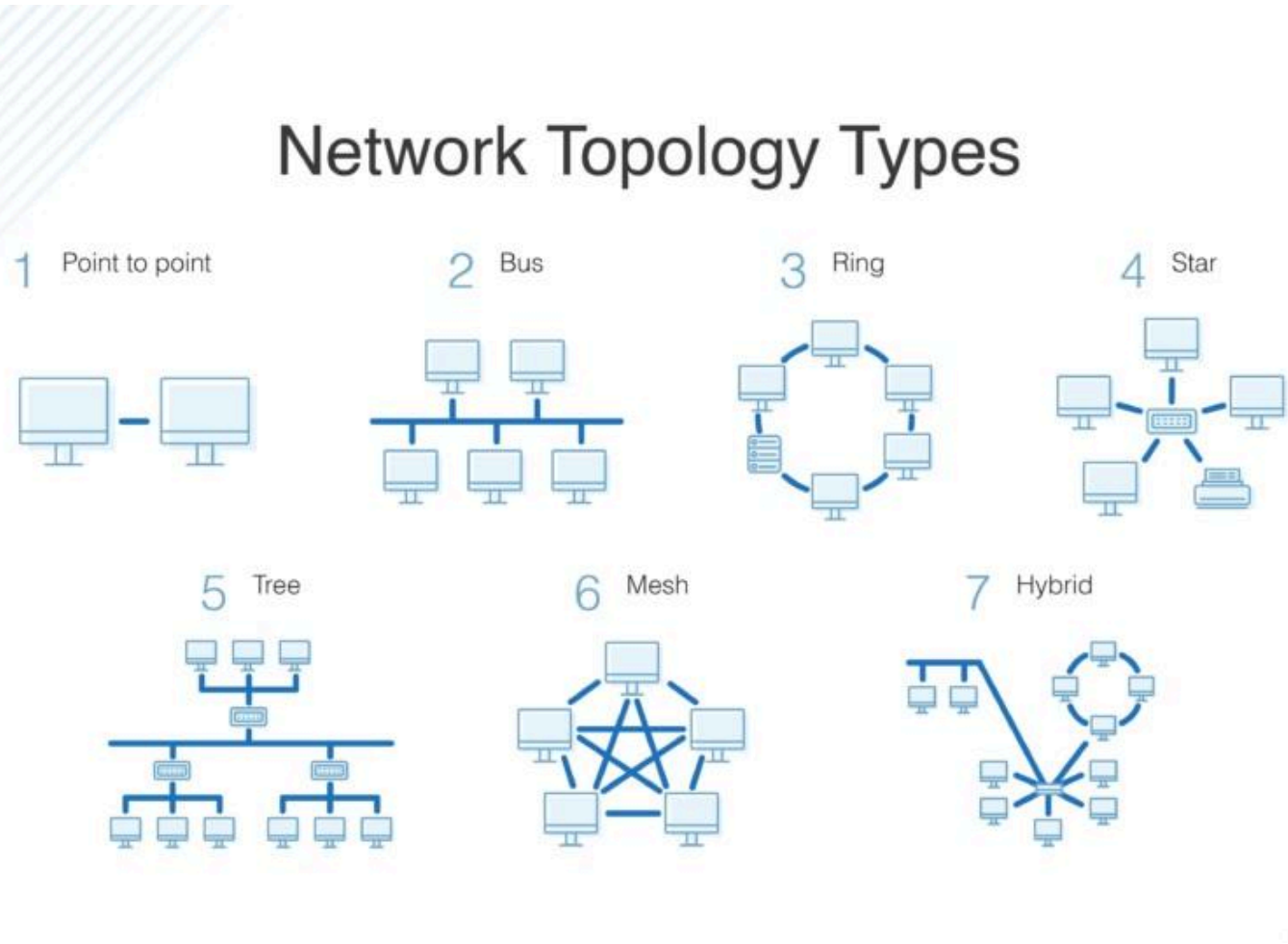
    1. A central controller asks each device one by one if it has data to send.
    2. Devices only send data when they are polled.
    3. This process continues in a round-robin fashion.
- **Example**: Used in some **serial communication** systems and older network protocols.

Summary:

- **CSMA/CD**: Devices detect collisions after they occur and retry later (used in wired Ethernet networks).
- **CSMA/CA**: Devices avoid collisions by sending a warning before transmitting (used in Wi-Fi).
- **Token Passing**: Devices must wait for a token to send data, ensuring only one device transmits at a time.
- **Polling**: A central device controls access, polling each device to see if it has data to send.

- Network Topologies

Network Topology refers to the **arrangement or layout** of devices (nodes) in a network, and how they are connected to each other. It describes the **physical or logical structure** in which devices communicate. Different topologies offer various advantages and disadvantages in terms of performance, cost, and reliability.



Types of Network Topologies

1. Bus Topology

- **Definition**: In a **Bus Topology**, all devices are connected to a single central cable, known as the **backbone** or **bus**. Data sent by any device travels along this bus, and all devices receive the signal, but only the intended recipient processes it.

- **Features**:
- Simple and cost-effective for small networks.
- Data travels in one direction at a time.
- **Example**: Older LAN networks (though it is now less commonly used).

---

2. Ring Topology

- **Definition**: In a **Ring Topology**, devices are connected in a circular fashion, forming a **closed loop**. Data travels in one direction (or both directions in a dual ring) around the ring, and each device has two neighbors.

- **Features**:
- Data passes through each device until it reaches its destination.
- Can be efficient in managing traffic.
- **Example**: Token Ring networks, older LAN setups.

---

3. Star Topology

- **Definition**: In a **Star Topology**, all devices are connected to a central device like a **switch** or **hub**. Each device has a dedicated connection to the central hub, which manages data transmission.

- **Features**:
- If one connection fails, it doesn't affect the rest of the network.
- Easy to manage and troubleshoot.
- **Example**: Common in **Ethernet** LANs and home networks.

---

4. Mesh Topology

- **Definition**: In a **Mesh Topology**, each device is connected to **every other device** in the network. This creates multiple paths for data to travel, ensuring high **redundancy** and reliability.

- **Features**:
- Highly reliable as there are multiple paths for data to travel.
- Fault-tolerant: If one connection fails,data can take an alternate path.
- **Example**: Used in **military** or **mission-critical systems** for high reliability.

---

5. Tree Topology

- **Definition**: **Tree Topology** is a hierarchical topology that combines **multiple star topologies** together. Devices are grouped into star networks, and these groups are then connected to a central backbone, forming a tree-like structure.

- **Features**:
- Easy to scale by adding more devices.
- Central backbone connects all star networks.
- **Example**: Large organizations with distributed departments or branches.

---

6. Hybrid Topology

- **Definition**: A **Hybrid Topology** is a combination of two or more different topologies. For example, a network might use a **star topology** for one part of the network and a **bus topology** for another. This allows networks to combine the strengths of different topologies.

- **Features**:
- Flexible and scalable, as it can adapt to different network requirements.
- Can combine the advantages of different topologies.
- **Example**: Large enterprise networks, which may use a hybrid of **star and mesh** or **tree** topologies for various departments.

Summary:

- **Bus Topology**: All devices share a single central cable; simple but not scalable.
- **Ring Topology**: Devices are connected in a circle; efficient but can fail if one device disconnects.
- **Star Topology**: Devices are connected to a central hub; reliable but dependent on the central device.
- **Mesh Topology**: Every device is connected to every other device; highly reliable but costly.
- **Tree Topology**: A hierarchical structure combining star topologies; scalable but backbone-dependent.
- **Hybrid Topology**: A mix of two or more topologies, offering flexibility but complexity.

- Advanced Network Topologies: Ethernet, CDDI, and FDDI

These advanced network topologies are used in specific network environments to offer high-speed data transmission and reliable performance

1. Ethernet Topology

- **Definition**: **Ethernet** is a widely-used **local area network (LAN)** technology that defines the standards for **wired communication** between devices. While Ethernet itself is not a topology, it primarily uses the **Star Topology** for modern networks (with a central switch or hub) and previously used the **Bus Topology** in older networks.

  Modern Ethernet networks can offer speeds ranging from **10 Mbps to 100 Gbps**.

- **Types of Ethernet**:
  - **Fast Ethernet**: 100 Mbps.
  - **Gigabit Ethernet**: 1 Gbps.
  - **10 Gigabit Ethernet**: 10 Gbps, typically used in data centers.

---

2. CDDI (Copper Distributed Data Interface)

- **Definition**: **CDDI** is a high-speed, **fiber-optic-based** LAN technology that is a version of **FDDI** designed to operate over **copper wiring** (instead of fiber). It was primarily used in the 1990s in high-speed network environments.

  CDDI can offer speeds of up to **100 Mbps**.

---

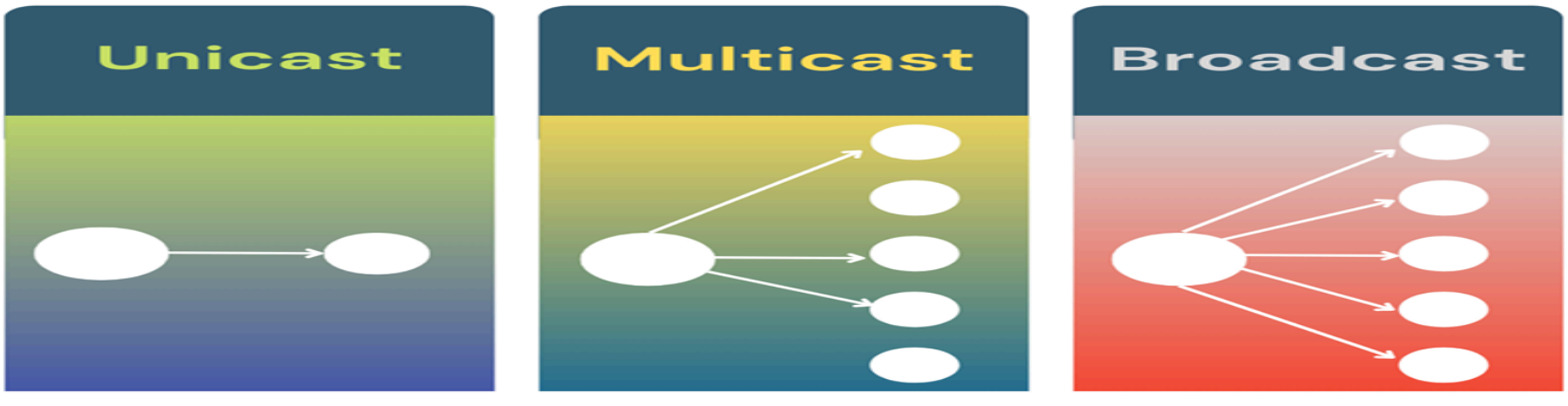
3. FDDI (Fiber Distributed Data Interface)

- **Definition**: **FDDI** is a **high-speed network standard** that uses **fiber-optic cables** to transmit data in a **Ring Topology**. FDDI is designed to provide high-performance networking over long distances with built-in redundancy for fault tolerance.

FDDI supports speeds up to **100 Mbps**.

- Communication Methods

Communication Methods in networking refer to the techniques used for sending data from one device to another across a network. The method determines how data is transmitted, how many receivers will receive it, and how it is addressed in the network. The three primary communication methods are **unicasting**, **multicasting**, and **broadcasting**, each of which serves different purposes and use cases.



1. Unicasting

- **Definition**: **Unicasting** is the transmission of data from one **single sender** to one **single receiver**. This is the most common form of communication in networking, where a message is intended for a specific device or destination.

- **How it works**:
    - The sender identifies a specific receiver's device through an **IP address** or **MAC address**.
    - The data is sent directly to that device, and only that device processes the data.
    - Unicasting is a **one-to-one** communication method.
- **Example**:
- **Web browsing**: When you visit a website, your browser sends a request (unicast) to the server, which responds only to you.
- **Emails**: An email sent from one person to another is an example of unicast communication.

---

2. Multicasting

- **Definition**: **Multicasting** is the transmission of data from one sender to **multiple specific receivers** who have requested or are interested in receiving the data. Unlike broadcasting, multicast sends data only to the devices that need it, making it more efficient.

- **How it works**:
    - The sender sends a single copy of the data to a **multicast group address**, which is then received by all devices that have subscribed to that group.
    - Devices that are not part of the multicast group do not receive the data.
- **Example**:
    - **Streaming video**: A live broadcast of a sporting event where only devices that are subscribed to the stream (via multicast group address) receive the data.

---

3. Broadcasting

- **Definition**: **Broadcasting** is the transmission of data from one sender to **all devices** on the network. Every device on the network (within the broadcast domain) receives the data, regardless of whether they need or want it.

- **How it works**:

    - The sender sends data to a special **broadcast address** (like **255.255.255.255** in IPv4).
    - All devices within the same network or broadcast domain receive and process the broadcasted data.

• OSI reference model

TRICK TO REMEMBER SEVEN LAYERS OF OSI

The **OSI (Open Systems Interconnection)** model is a conceptual framework used to understand how different networking protocols interact and function in a network. It was developed by the **(ISO)** to standardize and simplify network communication between various systems. The OSI model divides network communication into **7 layers**, each responsible for specific tasks related to data transmission, starting from the physical hardware up to the application used by the end-user.

---

1. Physical Layer (Layer 1)

- The **Physical Layer** is the lowest layer in the OSI model and is responsible for the **physical transmission of data** over the network. It deals with the hardware aspects of communication, such as cables, switches, and electrical signals.

---

2. Data Link Layer (Layer 2)

- The **Data Link Layer** is responsible for providing **error-free transfer of data frames** between two devices over the physical layer. It ensures the reliable transmission of data by detecting and possibly correcting errors in the physical layer.

---

3. Network Layer (Layer 3)

- The **Network Layer** is responsible for the **routing** and **forwarding** of data packets across the network. It determines the best path for data to travel from the source to the destination, even if they are on different networks.

---

4. Transport Layer (Layer 4)

- The **Transport Layer** ensures **end-to-end communication** and data integrity. It is responsible for breaking data into smaller units (called segments) and reassembling them at the destination.

---

5. Session Layer (Layer 5)

- The **Session Layer** manages **sessions** or connections between two devices, ensuring that communication can be established, maintained, and terminated gracefully.

---

6. Presentation Layer (Layer 6)

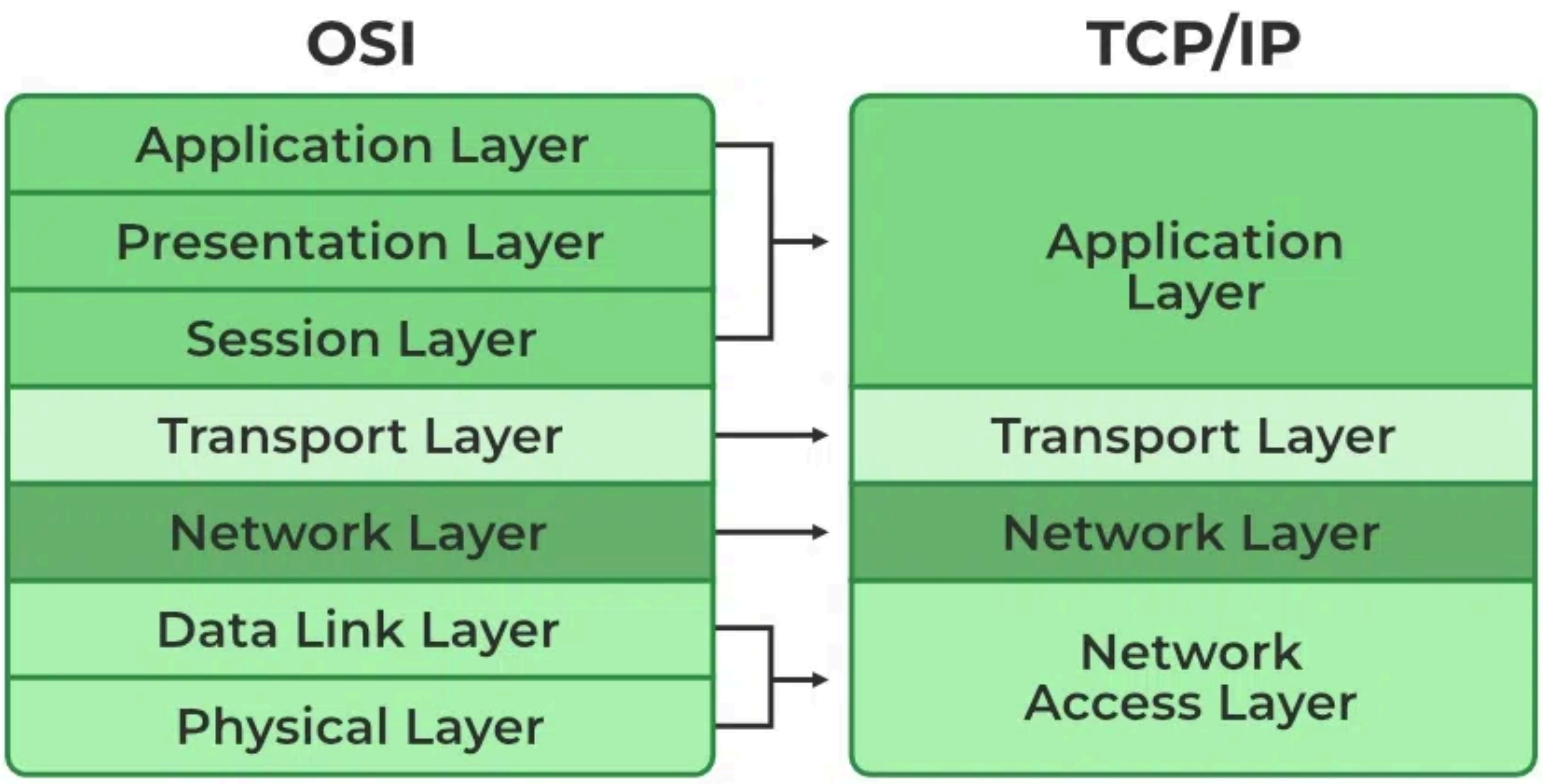
- The **Presentation Layer** is responsible for **data translation** and **data encryption**. It ensures that the data sent by the application layer of one system can be understood by the application layer of another system.

---

7. Application Layer (Layer 7)

- The **Application Layer** is the **topmost layer** and is closest to the end-user. It provides services and interfaces for applications to communicate over the network, ensuring that the data sent and received is meaningful to the user.

TCP/IP Network Model (4 Layers).



The **TCP/IP (Transmission Control Protocol/Internet Protocol)** model is a set of protocols used for communication over the internet and other networks. It is often referred to as the **Internet Protocol Suite** because it is the foundational model that governs the structure of most modern networks, including the internet. Unlike the **OSI model**, which has 7 layers, the TCP/IP model consists of **4 layers**, with each layer corresponding to different functionalities in network communication.

---

1. Application Layer

- **Definition**: The **Application Layer** is the topmost layer of the TCP/IP model. It deals with **high-level protocols** and applications that users directly interact with. This layer enables end-user applications to communicate over a network.

---

2. Transport Layer

- **Definition**: The **Transport Layer** is responsible for **end-to-end communication** and data integrity. It ensures reliable data transmission between the sender and the receiver, using protocols like **TCP** and **UDP**.

---

3. Internet Layer

- **Definition**: The **Internet Layer** is responsible for routing and addressing data across different networks. This layer defines how data packets are transmitted between different networks and ensures they reach their destination.

---

4. Network Interface Layer (or Link Layer)

- **Definition**: The **Network Interface Layer** (also called the **Link Layer**) is responsible for the physical transmission of data over the hardware and media (such as Ethernet, Wi-Fi). It deals with the **data link** and **physical layers** of network communication in the OSI model.