2. Data Communication and Networking

2.1 Basic Elements of Communication System

A **communication system** consists of a sender (who sends the message), a receiver (who gets the message), and a medium (the path through which the message travels). For example, in a phone call, the sender is the speaker, the receiver is the listener, and the medium is the telephone network.

Computer Networking: The two or more computing devices linked together to communicate, sharing information(files and software programs) and other hardware resources(printers, hard disk, plotters).

2.2 Concept of Communication System

A communication system is a way to transfer information between people or devices. It could involve speaking, writing, or using electronic systems to share data.

Advantages of Using Computer Networks:

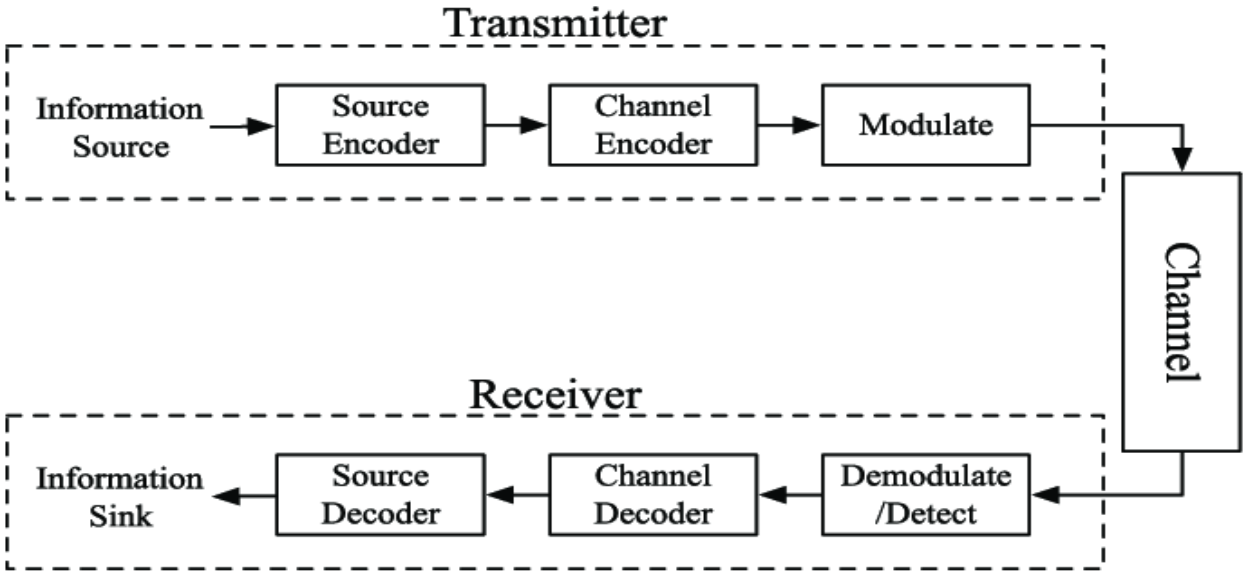
- **Resource Sharing:** Enables sharing of printers, files, and internet connections.
- **Centralized Control & Management:** Simplifies administration and security enforcement.
- **Speedy & Cost-Effective Communication:** Supports instant messaging, emails, and VoIP at low costs.
- **Backup & Recovery:** Ensures data protection with centralized backup solutions.
- **Flexible Access:** Allows remote access to files and applications from anywhere.
- **Workgroup Computing:** Facilitates collaboration and teamwork on shared projects.

Disadvantages of Using Computer Networks:

- **Expensive:** High setup and maintenance costs for hardware and software.
- **Security Problems:** Vulnerable to hacking, viruses, and unauthorized access.
- **Needs Special Technical Knowledge:** Requires skilled professionals for setup and management.
- **Network Failure:** A single failure can disrupt communication and access.
- **Complex:** Managing and troubleshooting networks can be challenging.

2.3 Block Diagram of Communication System / Model

This diagram explains the flow of communication:



1. **Transmitter of information**: Prepares the message for sending.
2. **Channel or medium**: The medium used to send the message.
3. **Receiver of information**: Processes the message so the receiver can understand it.

2.4 Elements of Data Communication/Transmission

Data communication or transmission involves several key elements that ensure the successful transfer of information from a source to a destination. These elements include:

1. Input Signal

The original form of data that needs to be transmitted, such as voice, text, image, or video. It is usually in analog or digital form before being processed for transmission.

2. Input Transducer

A device that converts the input signal into an electrical or optical signal.

Examples: Microphone (converts sound to electrical signals), Camera (converts light into electronic signals).

3. Transmitter

The device that processes and sends the signal into the transmission medium. It performs functions like encoding, modulation, and amplification to make the signal suitable for transmission.

Examples: Modem, Router, Radio Transmitter.

4. Transmission Medium

The physical or wireless path through which data travels from sender to receiver. Can be wired (cables like fiber optics, twisted pair, coaxial) or wireless (radio waves, infrared, microwaves).

5. Noise

Unwanted disturbances that can interfere with the transmitted signal, causing errors. Sources include electromagnetic interference, crosstalk, and environmental factors. Noise can distort the original data and affect communication quality.

6. Receiver

The device that receives the transmitted signal and processes it for interpretation. It may include demodulators, amplifiers, and error detection mechanisms to retrieve the original data.

Examples: Computer, Radio Receiver, Mobile Phone.

7. Output Transducer

Converts the received electrical or optical signal back into a readable format.

Examples: Speaker (converts electrical signals to sound), Monitor (displays visual data), Printer (outputs text/images on paper).

Each of these elements plays a crucial role in ensuring that data is transmitted accurately and efficiently from the sender to the receiver.

2.5 Communication Modes

- **Simplex**: Data flows in one direction only (e.g., TV broadcast).
- **Half-Duplex**: Data flows in both directions, but one at a time (e.g., walkie-talkie).
- **Full-Duplex**: Data flows in both directions at the same time (e.g., phone call).

Simplex Communication

Simplex Communication is a one-way communication mode where data flows in only one direction from the sender to the receiver. The sender transmits the information, and the receiver only listens or reads the data, without any feedback or interaction. A common example of simplex communication is a television broadcast, where the station sends signals, and viewers only receive them without any sending back of information.

Half-Duplex Communication

Half-Duplex Communication allows data to flow in both directions, but not at the same time. In this mode, each device can either send or receive data, but not simultaneously. Walkie-talkies are a classic example, where one person speaks while the other listens, and then they switch roles. While more flexible than simplex, half-duplex communication still limits simultaneous interactions.

Full-Duplex Communication

Full-Duplex Communication enables data to flow in both directions simultaneously, allowing both parties to send and receive information at the same time. This mode offers the most efficient and interactive communication. Examples include phone calls, where both speakers can talk and listen simultaneously, and modern internet connections, where data flows back and forth without delay.

2.6 Concept of LAN and WAN

In computer networking, networks are categorized based on their geographical coverage. The three primary types are:

1. **LAN (Local Area Network)**
2. **MAN (Metropolitan Area Network)**
3. **WAN (Wide Area Network)**

1. LAN (Local Area Network)

A LAN is a network that connects computers and devices within a small geographical area, such as a home, office, school, or campus.

Advantages:

- High Speed: Faster data transfer rates (typically 100 Mbps to 10 Gbps).
- Low Cost: Requires fewer networking devices, making it cost-effective.
- Easy Maintenance: Simple to install, configure, and manage.
- Secure: Restricted access due to limited coverage area.
- Reliable: Minimal signal interference and data loss.

Disadvantages:

- Limited Range: Covers only a small area (a few hundred meters).
- High Setup Cost (Initially): Requires switches, routers, and cables for setup.
- Security Risks: Internal threats and unauthorized access if not properly secured.

Examples:

1. Office or school computer networks
2. Home Wi-Fi networks
3. College campus networks

2. MAN (Metropolitan Area Network)

A MAN is a network that spans a city or a large geographical area (up to 50 km). It is larger than a LAN but smaller than a WAN.

Advantages:

- Covers a Larger Area: Connects multiple LANs within a city or town.
- High-Speed Data Transfer: Faster than WAN but slower than LAN.
- Efficient Resource Sharing: Organizations can share data across different locations.

Disadvantages:

- Expensive Infrastructure: Requires fiber-optic cables, routers, and leased lines.
- Complex Management: Needs dedicated network administrators.
- Security Issues: Data may be intercepted if not encrypted properly.

Examples:

1. City-wide Wi-Fi networks
2. Cable TV networks
3. University networks across multiple campuses

3. WAN (Wide Area Network)

A WAN is a network that spans large geographical areas (countries, continents, or globally). The internet is the largest example of a WAN.

Advantages:

- Global Connectivity: Connects users worldwide.
- Scalability: Can expand to accommodate new locations.
- Efficient Communication: Enables remote access and cloud computing.

Disadvantages:

- Slow Speed: Data transfer is slower compared to LAN or MAN.
- High Cost: Requires satellite links, leased lines, and multiple ISPs.
- Security Risks: Vulnerable to hacking, cyber-attacks, and data breaches.

Examples:

1. The Internet
2. Banking Networks (connecting ATMs worldwide)
3. Corporate Networks with offices across different countries

2.7 Transmission Medium: Guided and Unguided

- **Guided**: Physical cables like fiber optics and coaxial cables.
- **Unguided**: Wireless methods like radio waves or microwaves.

Feature	LAN	WAN
Coverage area	Small (up to a few km, e.g., office, school)	Large (across cities, countries, or globally)
Speed	High (100 Mbps to 10 Gbps)	Lower (1 Mbps to 100 Mbps)
Latency	Low	High due to long-distance communication
Ownership	Owned by a single organization	Shared among multiple organizations or ISPs
Cost	Low setup and maintenance cost	High setup and operational cost
Security	More secure due to limited access	Less secure, requires encryption and security protocols
Reliability	More reliable, fewer failures	Less reliable due to external factors like weather and ISP issues
Infrastrcture	Uses switches, routers, and Ethernet cables	Uses routers, fiber-optic cables, satellites, and leased lines
Data transmission	Faster and stable	Slower, with possible interruptions
examples	Office network, School network, Home Wi-Fi	Internet, Banking Networks, Corporate Networks

Guided Transmission Medium

Transmission media refers to the physical path or channel through which data is transmitted from one device to another in a network. It is classified into two main categories:

1. **Guided Media (Wired Transmission Media)** – Data travels through a physical medium like cables.
2. **Unguided Media (Wireless Transmission Media)** – Data is transmitted through the air using electromagnetic waves.

Guided Media (Wired Transmission Media)

1. Twisted Pair Cable

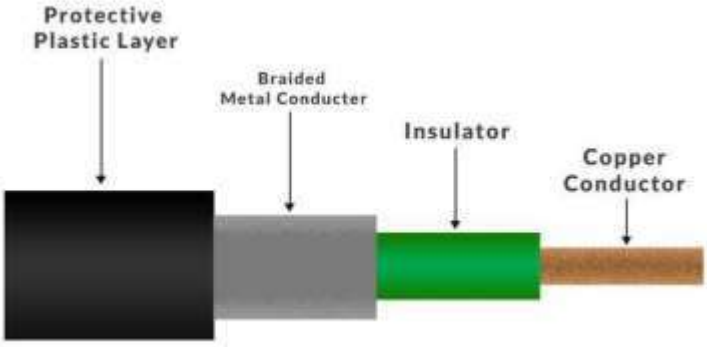
- **Definition:** A type of cable consisting of two insulated copper wires twisted together to reduce electromagnetic interference.
- **Types:**
  - **Unshielded Twisted Pair (UTP):** Commonly used in LANs and Ethernet networks.
  - **Shielded Twisted Pair (STP):** Has an extra shield to protect against interference.
- **Advantages:**
  ✓ Low cost
  ✓ Easy to install and maintain
  ✓ Supports high-speed data transmission (up to 10 Gbps in Cat6a cables)

- **Disadvantages:**
  ✕ Limited distance (up to 100 meters for Ethernet)
  ✕ Susceptible to interference and noise

---

2. Coaxial Cable

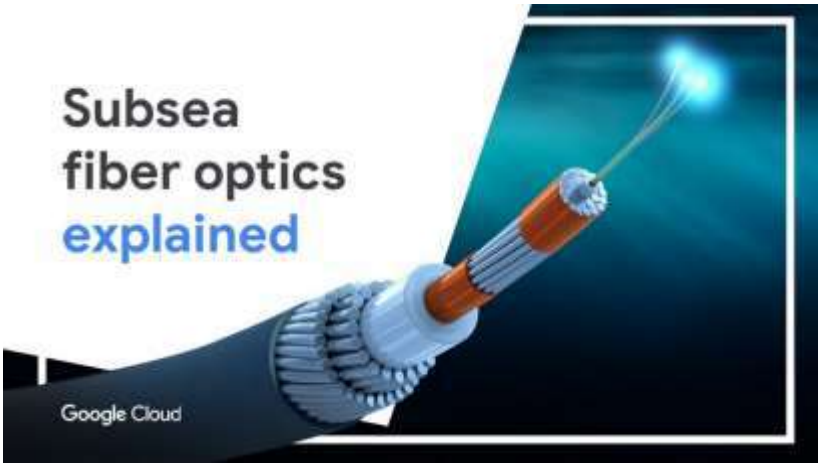
- **Definition:** A cable with a central copper conductor, surrounded by an insulating layer, metallic shield, and outer plastic cover.
- **Uses:** Used in cable TV, broadband internet, and CCTV networks.
- **Advantages:**
  ✓ Better shielding than twisted pair cables
  ✓ Can carry signals over longer distances
  ✓ Less signal interference
- **Disadvantages:**
  ✕ Bulkier and harder to install
  ✕ More expensive than twisted pair cables



---

3. Fiber Optics Cable

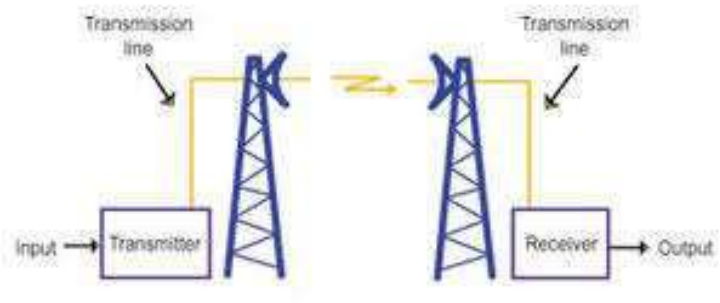
- **Definition:** Uses light signals to transmit data through glass or plastic fibers, providing ultra-fast and long-distance communication.
- **Types:**
  - **Single-Mode Fiber (SMF):** Used for long distances (up to 100 km)
  - **Multi-Mode Fiber (MMF):** Used for short distances (up to 2 km)
- **Advantages:**
  ✓ Extremely high data transfer speed
  ✓ Immune to electromagnetic interference
  ✓ Can transmit data over long distances without signal loss
- **Disadvantages:**
  ✗ Expensive installation and maintenance
  ✗ Fragile and difficult to splice



Unguided Media (Wireless Transmission Media)

1. Microwave System

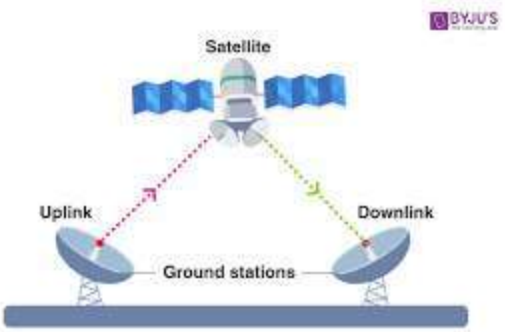
- **Definition:** Uses high-frequency radio waves (1 GHz – 300 GHz) for point-to-point communication.
- **Types:**
  - **Terrestrial Microwave:** Requires line-of-sight communication between two ground stations.
  - **Satellite Microwave:** Uses satellites to relay signals.
- **Advantages:**
  ✓ High bandwidth and data transmission speed
  ✓ Used in mobile communication and broadcasting
- **Disadvantages:**
  ✗ Affected by weather conditions (rain, storms)
  ✗ Requires line-of-sight between antennas



---

2. Satellite Communication

- **Definition:** Uses artificial satellites to relay signals across long distances (e.g., TV broadcasting, GPS, internet services).
- **Types:**
  - **Geostationary Satellites (GEO):** Fixed position, covers large areas (e.g., weather monitoring).
  - **Low Earth Orbit Satellites (LEO):** Closer to Earth, used in internet services (e.g., Starlink).
- **Advantages:**
  ✓ Provides global coverage
  ✓ Useful in remote areas where wired networks are unavailable
- **Disadvantages:**
  ✗ Expensive to deploy and maintain
  ✗ Signal delay due to long distance



---

3. Infrared Technology

- **Definition:** Uses infrared light waves (IR) for short-range wireless communication.
- **Uses:** Remote controls, wireless keyboards, and short-range data transfer.

- **Advantages:**
  ✅ Secure as signals do not pass through walls
  ✅ No interference from radio signals
- **Disadvantages:**
  ❌ Short-range (a few meters only)
  ❌ Requires a clear line-of-sight between sender and receiver

Feature	Twisted Pair	Coaxial Cable	Fiber Optics	Microwave	Satellite	Infrared
Type	Wired	Wired	Wired	Wireless	Wireless	Wireless
Speed	Medium	Medium	Very High	High	Medium	Low
Cost	Low	Medium	High	High	Very High	Low
Interference	High	Low	None	Affected by weather	Affected by weather	None
Distance	Short	Medium	Very Long	Medium to Long	Very Long	Very Short
Example Uses	Ethernet, Telephones	Cable TV, CCTV	Internet, Data Centers	Cellular Networks	GPS, TV, Internet	Remote controls

2.8 Transmission Impairments/distortion/weakening Terminology

Transmission impairments refer to factors that degrade the quality of a signal as it travels through a transmission medium. These impairments can lead to errors, delays, and poor communication quality. Below are some key terminologies related to transmission impairments:

Jitter

Jitter is the variation in packet arrival times, causing delays in real-time applications like VoIP and video streaming. It leads to choppy or delayed audio and video, impacting communication quality.

Attenuation

Attenuation is the loss of signal strength over distance due to resistance in the medium. It results in weaker signals, which may cause data loss or errors.

Distortion

Distortion occurs when a signal's shape is altered during transmission, affecting its integrity. This leads to unclear or misaligned audio and video signals.

Noise

Noise refers to unwanted signals that interfere with the transmitted data, causing errors or degradation. It can include thermal noise, intermodulation, or impulse noise.

Echo

Echo is the reflection of a transmitted signal back to the sender, causing a delayed version of the signal. This results in confusing voice feedback in communication systems.

Singing

Singing is a sustained, high-pitched feedback loop caused by a signal being continuously amplified and fed back into the system. It typically occurs in audio systems with microphones and speakers.

Crosstalk

Crosstalk is interference between adjacent channels or wires, leading to signal leakage and data corruption. It is common in unshielded cables, causing overlapping signals.

Bandwidth

Bandwidth is the maximum data transfer rate of a communication channel, determining its capacity. A higher bandwidth enables faster data transfer and supports more simultaneous users.

Number of Receivers

The number of receivers affects signal strength, as more devices can lead to signal attenuation or interference. Proper design ensures the system handles multiple receivers without degradation.

2.9 Basic Concept of Network Architecture: Client-Server and Peer-to-Peer

- **Client-Server**: One computer (server) provides services, and others (clients) use them.
- **Peer-to-Peer**: All computers have equal roles in sharing resources.

Client-Server Architecture

In a **Client-Server Architecture**, the network is structured with dedicated servers providing resources or services and clients accessing them. The server acts as a central hub that stores data,

processes requests, and manages resources like files, databases, or web services. Clients (e.g., personal computers or smartphones) request these services, and the server responds. This model is efficient for managing large networks, as it centralizes data and allows better control. However, it depends heavily on the server; if the server fails, the entire network may be disrupted.

Peer-to-Peer Architecture

In a **Peer-to-Peer (P2P) Architecture**, all devices (peers) in the network are equal and share resources directly with each other without requiring a central server. Each peer can act as both a client and a server, sharing files, processing power, or bandwidth. This model is decentralized, making it more resilient to failures, as there is no single point of dependency. However, it can be harder to manage in large-scale networks and may lack the centralized security features of a client-server setup.

Feature	Peer-to-Peer (P2P) Network	Client-Server Network
Definition	A decentralized network where all computers (peers) share resources and communicate directly.	A centralized network where clients request services from a dedicated server.
Structure	Each device acts as both a client and a server.	Clients depend on a central server for data and services.
Data Storage	Data is distributed across all peers.	Data is stored on a central server.
Performance	Slower for large networks, as each device handles both requests and responses.	More efficient with a dedicated server managing requests.
Security	Less secure, as each device is independent and vulnerable.	More secure due to centralized control and authentication.
Example	File-sharing networks like BitTorrent.	Web applications, email servers, and database servers.

2.10 Basic Terms and Tools in Networking

- **IP Address**: A unique number for each device on a network.
- **Subnet Mask**: Divides IP addresses into parts.
- **Gateway**: Connects local networks to the internet.
- **MAC Address**: A hardware address for network devices.
- **Internet/Intranet/Extranet**: **Internet** => Global network,**Intranet** => private network, **Extranet** => extended private network to access by outside user over internet using dedicated and secure channel.

2.11 Network Tools

- **Packet Tracer**: A simulator for practicing networking setups.
- **Remote Login**: Accessing a computer from another location.

Packet Tracer is a powerful network simulation tool used to design, configure, and test network setups in a virtual environment. Developed by Cisco, it allows users to practice creating and managing networks without the need for physical hardware. Packet Tracer is commonly used by students and professionals to understand networking concepts, troubleshoot configurations, and simulate real-world scenarios. Its user-friendly interface and extensive features make it an essential learning tool in networking education.

Remote Login

Remote Login is a technique that allows users to access and control a computer or server from a remote location. Using tools like SSH (Secure Shell) or RDP (Remote Desktop Protocol), users can perform tasks on a distant machine as if they were physically present. It is widely used for troubleshooting, managing servers, and accessing files securely. Remote login provides convenience and efficiency, but it requires robust security measures to prevent unauthorized access.

2.12 Network Connecting Devices

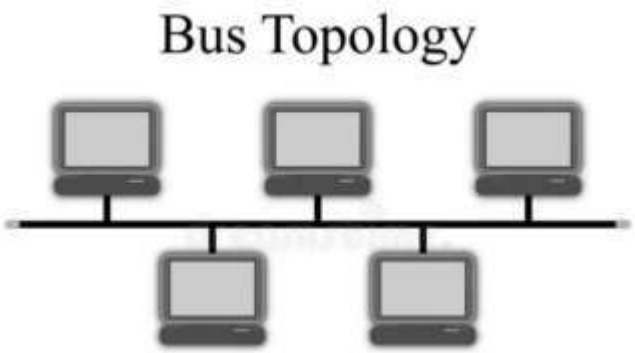
- **NIC (Network Interface Card)** – A hardware component in a computer that connects it to a network using cables or Wi-Fi.
- **Modem (Modulator-Demodulator)** – Converts digital signals from a computer into analog signals for the internet and vice versa. It helps connect to the internet via telephone lines, fiber, or cable.
- **Hub** – A basic device that connects multiple computers in a network and sends data to **all** devices, even if it's not needed. (Not very efficient)
- **Switch** – Smarter than a hub; it sends data **only** to the specific device it is meant for, improving speed and efficiency.
- **Bridge** – Connects two different networks of the same type, like two LANs (Local Area Networks), to work as one.
- **Router** – Directs data between **different networks** (e.g., home Wi-Fi and the internet). It decides the best path for data to travel.
- **Brouter (Bridge + Router)** – Works as both a **bridge** (connecting similar networks) and a **router** (directing data between different networks).
- **Repeater** – Boosts and extends network signals over long distances, preventing signal loss.
- **Gateway** – Connects two completely different networks (e.g., a LAN and the internet) by converting data formats, protocols, or addresses.

- **Bluetooth** – A wireless technology for short-distance communication between devices (like phones, speakers, and smartwatches).
  - **Wi-Fi** – A wireless networking technology that connects devices to the internet without cables.
  - **Workstation** – A high-performance computer used for professional tasks like designing, programming, or video editing in a network.

2.13 Network Topologies

1. Bus Topology

📌 **Definition**: All devices are connected to a single central cable (bus). Data travels in both directions.



✅ **Advantages:**

- Easy and cheap to set up
- Requires less cable
- Works well for small networks
- Simple to expand

❌ **Disadvantages:**

- If the main cable fails, the whole network stops
- Slower when traffic increases
- Data collisions can occur
- Difficult to troubleshoot

---

2. Ring Topology

📌 **Definition**: Devices are connected in a circular loop, where data moves in one direction (or both in dual ring).

✅ **Advantages:**

- No data collisions
- Performs well with a high volume of traffic
- Easy to install and maintain
- Uses fewer cables than mesh

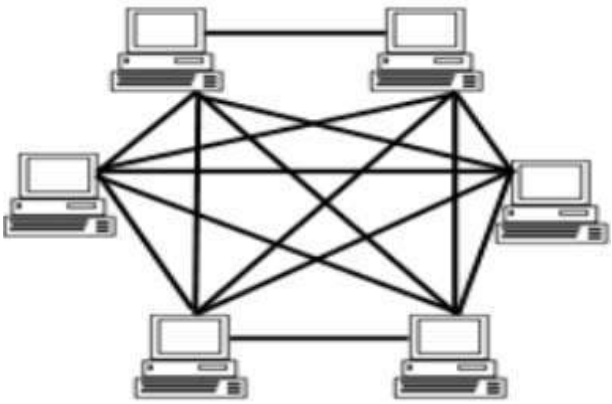
❌ **Disadvantages:**

- If one device fails, the entire network is affected
- Adding new devices can disrupt the network
- Troubleshooting is difficult
- Slower compared to star topology

---

3. Mesh Topology

📌 **Definition**: Every device is connected to every other device, ensuring multiple communication paths.



✅ **Advantages:**

- Highly reliable (no single point of failure)
- Fast data transmission with multiple routes
- Handles high traffic efficiently
- Strong security and privacy

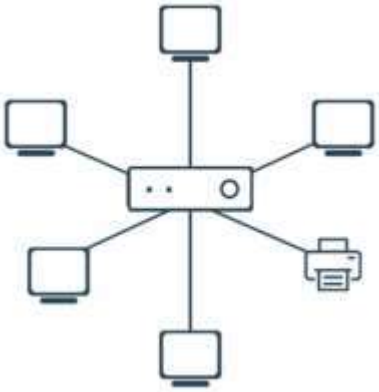
❌ **Disadvantages:**

- Very expensive due to many cables
- Complex installation and configuration
- Requires more maintenance
- Difficult to scale

---

4. Star Topology

📌 **Definition**: All devices connect to a central hub or switch, which manages network communication.



✅ **Advantages:**

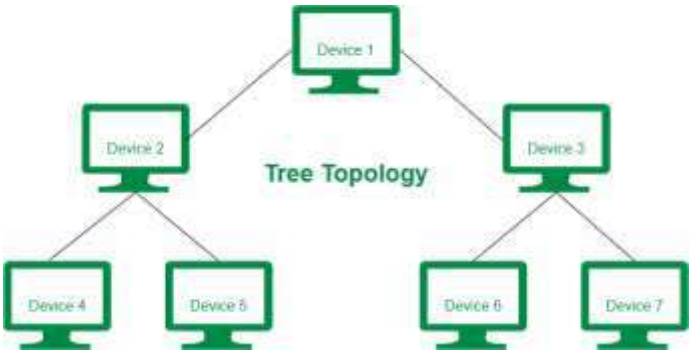
- Easy to install and manage
- If one device fails, others are unaffected
- High speed and performance
- Easy to add new devices

❌ **Disadvantages:**

- If the central hub fails, the network stops
- Expensive due to the hub and extra cables
- Performance depends on hub capacity
- Requires more cable than bus topology

5. Tree Topology

📌 **Definition**: A combination of star and bus topology, where groups of star networks connect via a main bus.



✅ **Advantages:**

- Scalable (easy to expand)
- Centralized control
- Hierarchical structure simplifies management
- Supports multiple devices efficiently

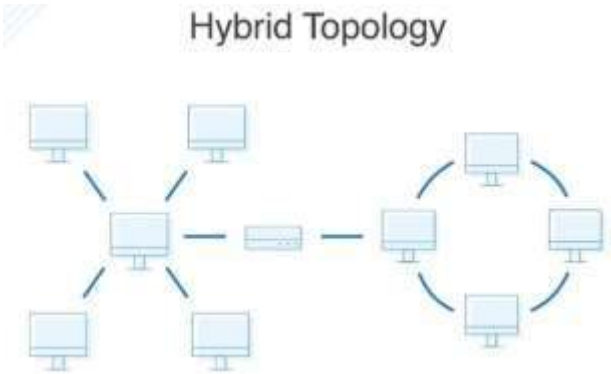
❌ **Disadvantages:**

- If the main bus fails, the entire network is affected
- Requires more cabling
- Complex to configure and maintain
- Expensive setup

---

6. Hybrid Topology

📌 **Definition**: A mix of two or more topologies (e.g., star + mesh, ring + bus).



✅ **Advantages:**

- Flexible and scalable
- High reliability and efficiency
- Can be customized for different needs
- Faults in one topology don’t affect others

❌ **Disadvantages:**

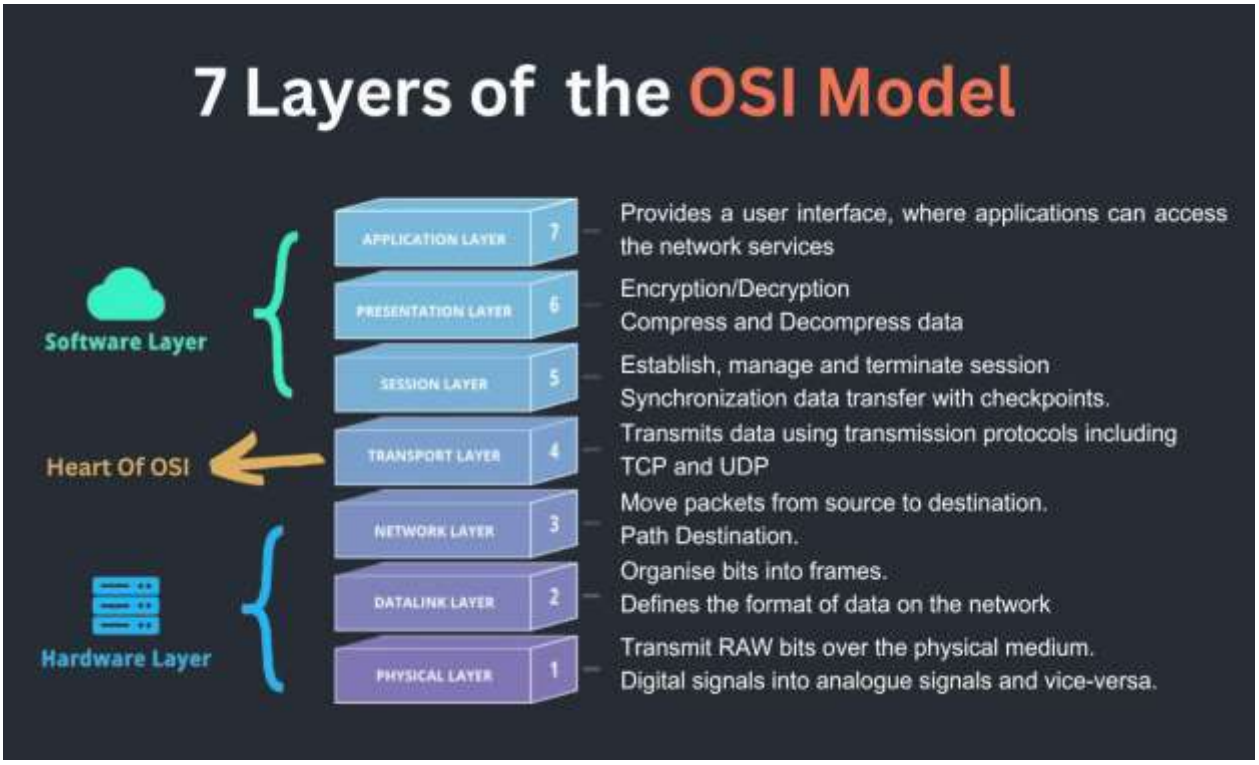
- Expensive due to multiple devices and cables
- Complex installation and configuration
- Requires expert management
- Difficult to troubleshoot

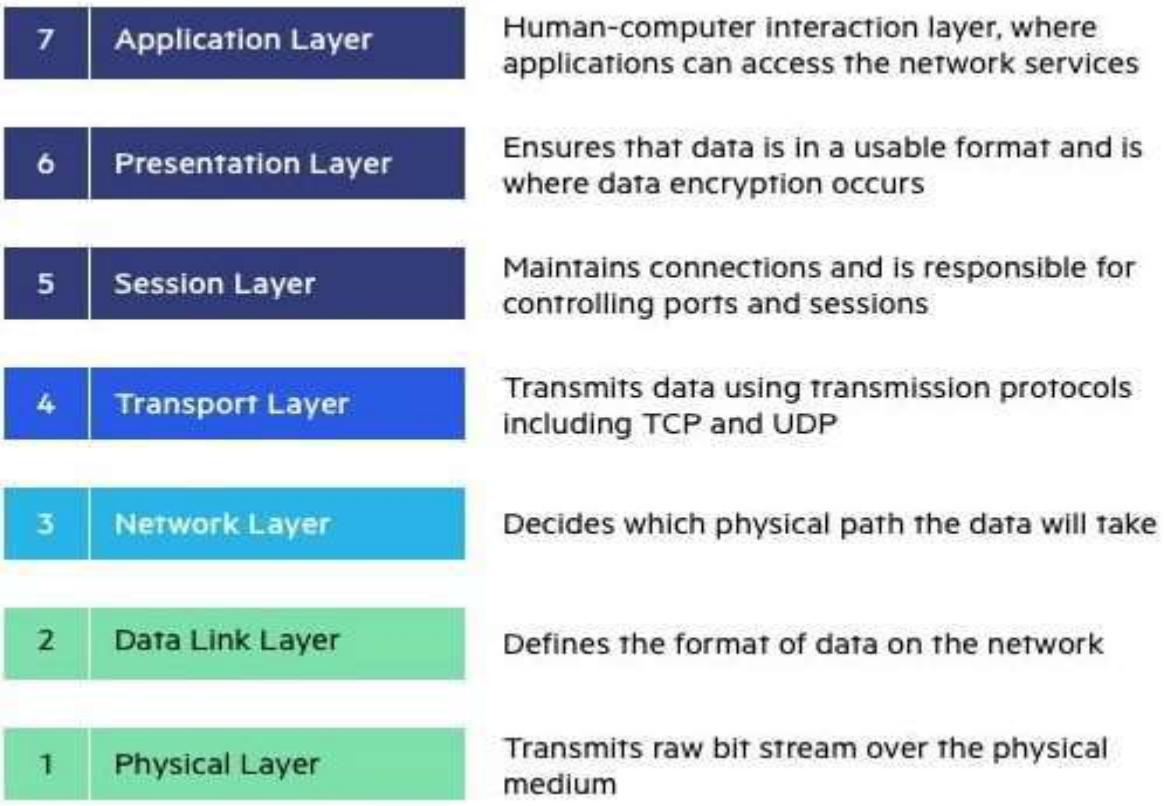
Selection Criteria for network

1. Cost
2. Data error rate
3. Simplicity
4. Data security
5. Transmission speed
6. Flexibility
7. Maintainability
8. Volume of data traffic

2.14 Basic Concept of OSI Reference Model

The OSI Model explains how data travels through a network in 7 steps, like layers: from physical connections to applications.





1. Physical Layer

The Physical Layer is the lowest layer of the OSI model and deals with the physical hardware of a network. It handles the transmission of raw binary data over a communication medium like cables, fibers, or wireless signals. This layer ensures that data bits are converted into electrical, optical, or radio signals for transmission. It defines the specifications for cables, connectors, and voltage levels, but it does not interpret the data being transmitted.

2. Data Link Layer

The Data Link Layer is responsible for organizing data into frames and ensuring error-free transfer between directly connected devices. It handles physical addressing (e.g., MAC addresses), detects and corrects errors, and manages flow control. This layer ensures that data reaches the correct device on a local network and manages access to the shared medium.

3. Network Layer

The Network Layer handles the routing of data between different networks. It assigns logical addresses (e.g., IP addresses) to devices and determines the best path for data to travel from the

sender to the receiver. This layer is essential for data delivery across multiple networks and ensures packets reach their destination, even in complex, interconnected systems.

4. Transport Layer

The Transport Layer ensures reliable data transfer between devices. It breaks data into smaller segments, numbers them for proper sequencing, and reassembles them at the destination. This layer handles error checking, retransmissions, and flow control to prevent data loss or congestion. Protocols like TCP (reliable) and UDP (fast but less reliable) operate at this layer.

5. Session Layer

The Session Layer manages and controls the dialogue between devices. It establishes, maintains, and terminates sessions or communication links between applications. This layer ensures that data streams from different applications are kept separate and synchronized, enabling smooth interactions during data exchanges.

6. Presentation Layer

The Presentation Layer focuses on the translation and formatting of data for the application layer. It ensures that data is presented in a readable format for the receiving system, handling tasks like data compression, encryption, and decryption. For example, it converts text into ASCII or JPEG images into binary streams.

7. Application Layer

The Application Layer is the topmost layer and directly interacts with user applications and software. It provides network services such as email, file transfer, and web browsing. This layer ensures that users can easily access and use network resources by providing interfaces for communication and data exchange.

These layers work together to ensure seamless data communication across networks.

2.15 Internet Protocol Addressing

Defines how devices are identified and located on the internet using IP addresses (e.g., IPv4 and IPv6). Devices communicate with each other over LAN using MAC address. But when they need to communicate over internet it uses IP address.IP address is used for connecting the compters for communiction . Once th are connected they share their MAC address and further communication takes place usin the MAC address.

Each ip address string is made up of two component:

- Network identifying component i.e is the left most part of address used by router for communication

- Device identifying component i.e. is the right most part of address.

IPv4

IPv4 (Internet Protocol version 4) is the fourth version of the Internet Protocol and the most widely used to date. It uses a 32-bit addressing system, which allows for approximately 4.3 billion unique IP addresses. These addresses are written in a dotted decimal format, such as 192.168.1.1. IPv4 supports features like subnetting, which divides a network into smaller segments, and uses methods like NAT (Network Address Translation) to extend address availability. However, due to the rapid growth of internet-connected devices, IPv4 addresses are running out, leading to the development of IPv6.

IPv6

IPv6 (Internet Protocol version 6) is the newer version of the Internet Protocol, designed to address the limitations of IPv4. It uses a 128-bit addressing system, providing an almost unlimited number of unique IP addresses—approximately 340 undecillion (a trillion trillion trillion). IPv6 addresses are written in hexadecimal and separated by colons, such as 2001:0db8:85a3:0000:0000:8a2e:0370:7334. In addition to more addresses, IPv6 offers features like improved security through mandatory encryption and more efficient routing. It is critical for the future of the internet as the number of connected devices continues to grow.