Introduction to Networks

A **network** is a system of interconnected devices that communicate and exchange data with each other over links – communication links.

A collection of two or more computers and devices connected together to share data, resources, and services.

Key components of a computer network include:

- **Nodes** (devices like computers, routers, switches)
- **Links** (wired or wireless connections)
- **Protocols** (rules for communication, like TCP/IP)

Each host/device/node has a unique address in the network. A host/device/node refers to any device that can send or receive information.

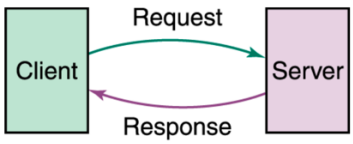
Data Communications is the movement of computer information from one point to another by means of electrical or optical transmission systems

Internet – A connection of multiple networks, or simply a network on networks. Each host has an address of the form n/h where n is the network number and h is the host number on network n.

Uses of computer networks

- **They have many uses**: Business Applications(client-server) » Home Applications » Mobile Users »
- **These uses raise**: Social Issues - Privacy Concerns, Digital Divide, Cybersecurity Threat, Ethical Dilemma
-

Client-server model –



The **client-server model** is a network architecture where **clients** request services or resources from a centralized **server**, which processes and responds to those requests.

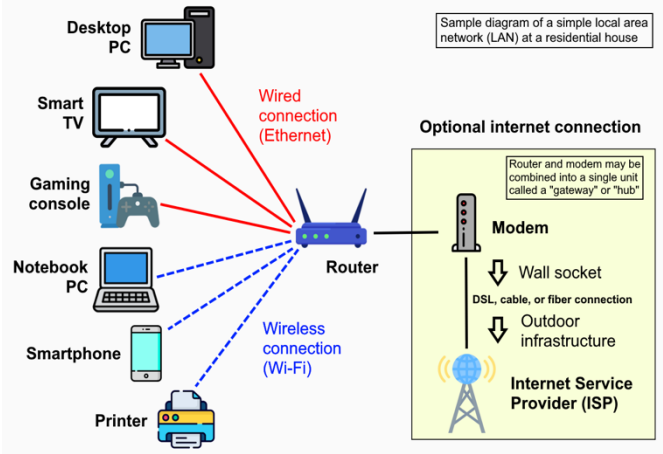
Component	Description
Client	A device or software (e.g., browser, mobile app) that sends requests to the server for services or data.
Server	A powerful computer or program that listens for requests and provides services or data to clients.

Categories of Networks

LAN(Local Area Networks) - Connect devices in a home or office building and it is called an enterprise network in a company.

Benefits

- **High-Speed Connectivity:** Fast data transfer within a localized area (e.g., building/campus).
- **Resource Sharing**: Enables file, printer, and device sharing among users.
- **Cost-Effective**: Lower infrastructure costs compared to wide-area networks.
- **Improved Security**: Easier to manage and secure within a confined network.
- **Reliability**: Consistent performance with fewer external interferences.



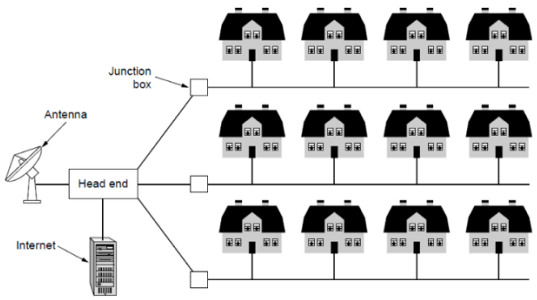
Drawbacks

- Limited Range: Restricted to a small geographic area (e.g., up to a few kilometers).
- Reconfiguration Challenges: Difficult to add or remove devices without disrupting the network.
- High Initial Cost: Significant investment in hardware and setup.
- Single Point of Failure: Central hub or server failure can disable the entire network.
- Maintenance Overhead: Requires regular updates and technical support.

MAN(Metropolitan Area Network) - a computer network that interconnects users with computer resources within a geographic region the size of a metropolitan area, typically a city or a large campus. It's larger than a local area network (LAN) but smaller than a wide area network (WAN). MANs are often used to connect multiple LANs and provide high-speed data transmission across a broader area.

Metropolitan Area Networks

- Connect devices over a metropolitan area
- Example MAN based on Telephone Network
- , cable TV:



Advantages :
• **High Bandwidth**: Supports high-speed data transfer across a metropolitan area, ideal for cable TV and internet services.
• **Supports Large Number of Clients**: Handles numerous users within a city, such as businesses and residents.
• **Reduce the Errors**: Enhances data reliability over urban distances, minimizing transmission errors.

Disadvantages :
• **Large Space Requirements**: Needs extensive cabling or infrastructure (e.g., telephone lines), demanding significant urban space.
• **Slower Data Access**: Potential latency due to city-wide coverage and traffic, despite high bandwidth.
• **High Cost**: Expensive to deploy and maintain, including urban infrastructure and service agreements.

Another way to categorize networks is in terms of access:

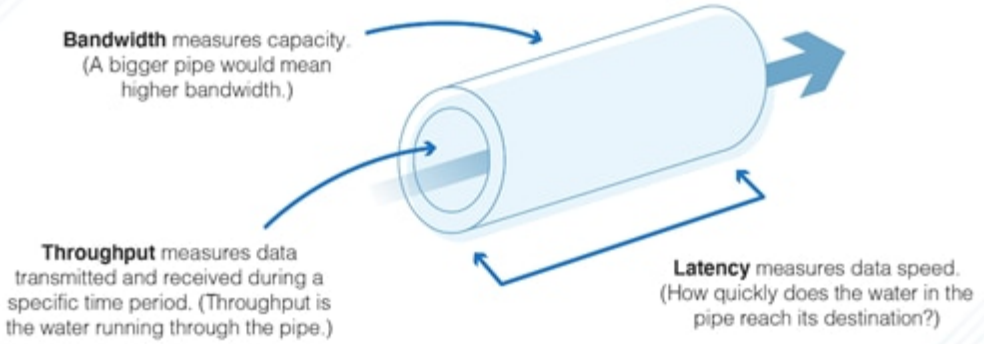
Intranet
• A network (often a LAN) that uses the Internet technologies to share information within an organization
• Open only to those inside the organization
• e.g., employees accessing budgets, calendars, and payroll information available through the organization's intranet

Extranet
• A network that uses the Internet technologies to share information between organizations
• Open only to those invited users outside the organization
• Accessible through the Internet
• e.g., suppliers and customers accessing the inventory information of a company over an extranet

Network Devices
- Router: Directs traffic between networks, choosing optimal routes.
- Hub: Connects multiple nodes in a network, broadcasting data.
- Switch: Efficiently forwards data to specific devices.
- Gateway: Links different networks (e.g., LAN to WAN), acting as a protocol converter.
- Node: Any device (e.g., computer) in the network.

Infrastructure & Performance
- Bandwidth: Capacity of the channel to carry data, affecting transmission speed.
- Traffic: Volume of data flow, managed by equipment like routers.
- Connection: Established via infrastructure (cables, fiber) and access points.
- System: Integrated components (e.g., hub, switch) ensuring signal integrity.

Network Latency vs. Throughput vs. Bandwidth



Bandwidth vs Latency – Key Differences

1 Bandwidth

Refers to the maximum amount of data that can be transferred over a network in a given time.Measured in Mbps (Megabits per second) or Gbps (Gigabits per second).

Think of it like the width of a highway; wider roads (more bandwidth) allow more cars (data) to travel at once.

Higher bandwidth means you can download or upload larger files faster.

2 Latency

Refers to the time delay it takes for data to travel from the source to the destination.Measured in milliseconds (ms).

Think of it like the travel time it takes for a car (data) to reach its destination. Lower latency means faster response time, which is important for real-time activities (like gaming, video calls, etc.)

3 Real-world Examples

- **High Bandwidth + High Latency**: Fast downloads, but lag in real-time apps.
- **Low Bandwidth + Low Latency:** Smooth real-time use, slow large transfers.
- **Best:** High Bandwidth + Low Latency for top performance.

4 Summary

- **Bandwidth = Speed/Capacity**
- **Latency = Delay/Response Time**
- **Both affect your network experience but in different ways.**

Communication model

Block Diagram for Communication Model:

When we talk about **data communication**, the goal is to ensure that data sent from a **sender** reaches the **receiver** correctly, quickly, and efficiently. Four major characteristics define the quality of communication.

Characteristics of a Communications model

Delivery – The system must reliably deliver data to the correct destination
Accuracy – The system must deliver data in an accurate way
Timeliness – Data must be on delivers on time/Exact time
Jitter – Difference on the arrival time

Data transmission concepts and terminology **15 July 2025**

Components of Communication Model :

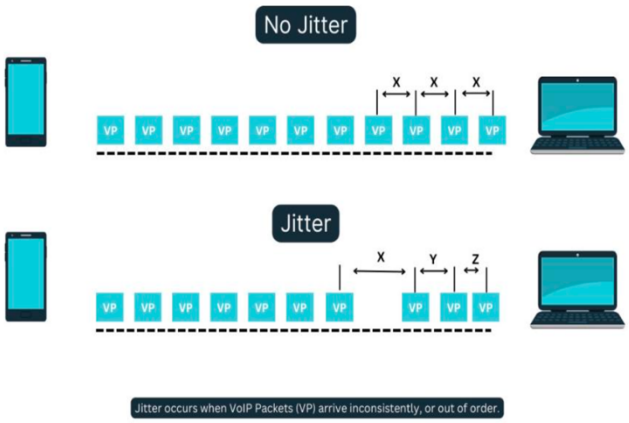
i) **Sender**

ii) **Receiver**

iii) **Medium**

iv) **Message**

v) **Protocol**



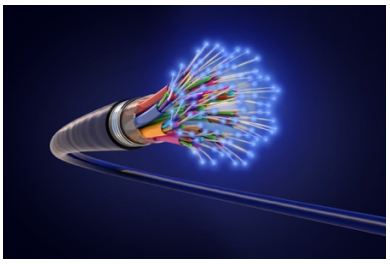
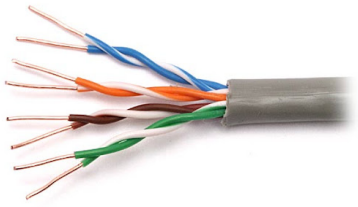
Data Transmission occurs between sender and receiver over some Transmission Medium or Transmission Media.

Transmission Media may be classified into Two Types **:**

- **Guided Media [Wired Technology]** - In Guided Media Signals are Passed in a physical path"

Example:

Optical fibre **Coaxial Cable** **Twisted pair Cable**

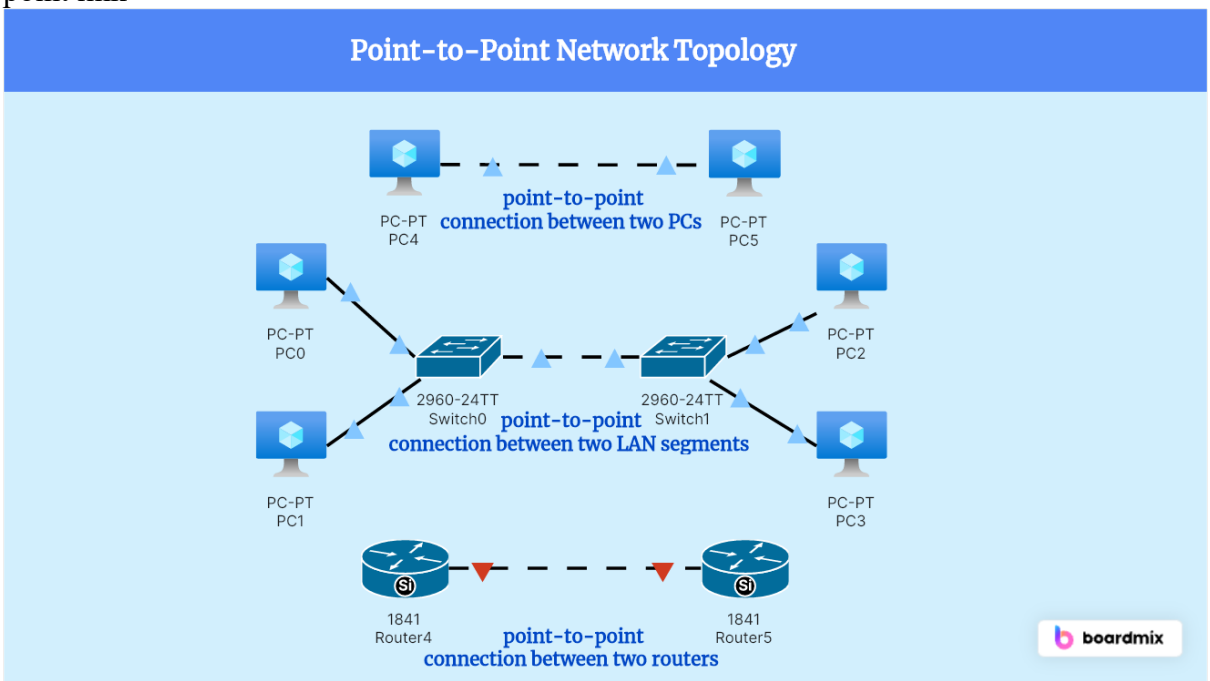




- **Unguided Media [Wireless Technology]** - Media Signals are Passed in the form of" Electromagnetic Waves"

Example:

i) Mobile phones
ii) Satellite microwave
iii) Infrared

Point-to-point Connection - It Provides a dedicated links between two devices. For example, a wired system that connects two computers together can be thought of a point-to-point link



Multi-point Connection - It is a link between two or more devices. It is also known as Multi-Point configuration. The networks having multipoint configuration are called a broadcast network. It is a type of communication setup in which more than two devices share a single communication link.

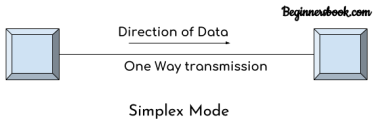
Key Features:

- One link is **shared** by multiple devices.
- Only **one device** can transmit at a time (to avoid collisions).
- Used to **save resources** (cables, ports).

Transmission Mode
It refers to the direction of information flow between two devices. Data flow is the flow of data between 2 points.

The direction of the data flow can be described as:

Simplex Mode



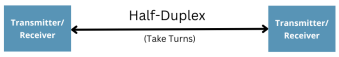
Simplex Mode

Direction: One-way communication only. Only one device can send, the other only receives.

Example:

Keyboard to Computer: You press a key, and the keyboard sends input to the computer. The keyboard never receives data back from the computer.

Half-Duplex Mode



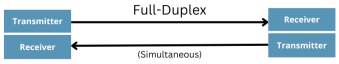
Direction: Two-way communication, but only one direction at a time**.**

Like a walkie-talkie — **you speak, then wait for the reply**.

Example: Walkie-Talkies

Person A talks, Person B listens. Then they switch roles — not at the same time.

Full-Duplex Mode



Direction: Two-way communication **at the same time**. Both devices can send and receive **simultaneously**.

Example: Mobile Phone Call

You can talk and listen at the same time.

No need to take turns.

Protocol Architecture

A protocol architecture is a layered structure of hardware and software that enables the exchange of data between computer systems**.**

Key Characteristics:

Structured in **layers** — each layer handles a specific function. Layers interact with:

- The **layer above** (receiving requests).
- The **layer below** (sending requests).

There are 2 widely used protocol architecture:

- TCP/IP Architecture
- OSI Model

Protocol
Protocol is a set of rules that govern data communication
It represents **what** is communicated, **when** it is communicated and **how** it is communicated.

There are 3 key elements
Syntax - It represents **structure**, Format of the data order in which it is presented

Data may contain:

- First 8 bit -> Sender Address
- Second 8 bit -> Receiver Address
- Remaining bits-> message stream

Semantics - It refers the **meaning** of each section of bit.

Timing - It refers when data sent and how fast it is sent.

Protocol standards

Protocol standards are **agreed-upon rules** that ensure different computer systems and devices can communicate properly. They define how data is **formatted, transmitted, and received** over a network.

De Facto Standards (Latin: *by fact*)

These are **unofficial but widely used** standards.

They become standards through **popular use**, **market dominance**, or **common acceptance** — even without formal approval.

Examples

- **PDF** – Developed by Adobe, now a global format
- **Windows OS file formats**
- **TCP/IP** – Became standard before it was formally recognized

De Jure Standards (Latin: *by law*)

These are **formal, official standards** developed and approved by **recognized international organizations**.

Reviewed, tested, and accepted through a structured process.

Examples

IEEE 802.11 – Wi-Fi standards

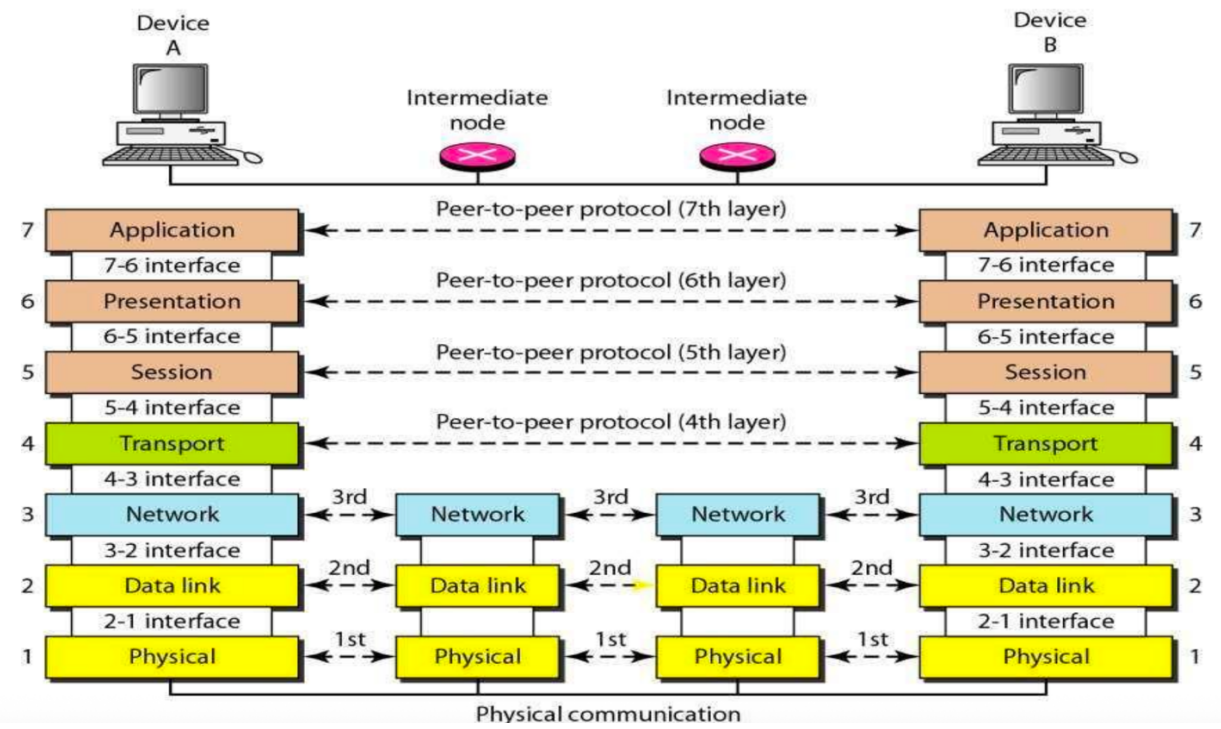
HTML, HTTP – Approved by W3C

OSI model – Developed by ISO (International Organization for Standardization)

The OSI Model

An ISO (International standard Organization) that covers all aspects of network communications is the

Open System Interconnection (OSI) model.
An open system is a model that allows any two different systems to communicate regardless of their underlying architecture (hardware or software). The OSI model is not a protocol; it is model for understanding and designing a network architecture that is flexible, robust and interoperable.

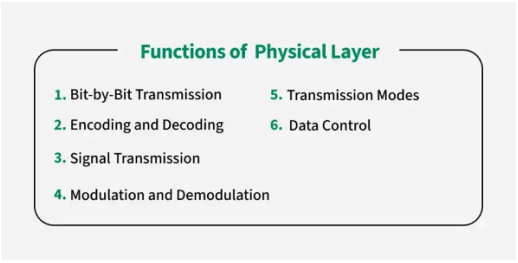


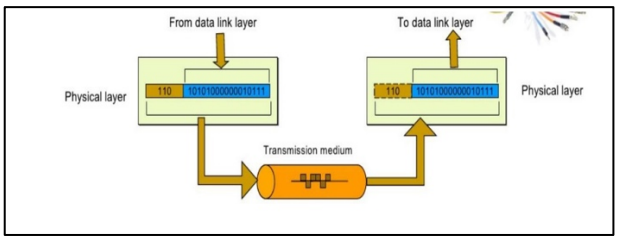
Peer-to-Peer Process

- Within a single machine, each layer calls upon services of the layer just below it.
- Layer 3, for example, uses the services provided by layer 2 and provides services for layer 4.
- Between machines, layer x on one machine communicates with layer x on another machine, by using a protocol (**this is Peer-to-Peer Process**).
- Communication between machines is therefore a peer-to-peer process using protocols appropriate to a given layer.
-

Physical Layer

- **What it does:** Transmits the **raw bits** (0s and 1s) over the physical medium (cable, fiber, etc.). *The physical layer is responsible for transmitting **individual bits** from one node to the next*
- Deals with **hardware**, like cables, switches, voltage levels.
- **Examples:** Ethernet cables, fiber optics, radio signals





Physical characteristics of interfaces and media: It define the type of transmission media

Representation of the bits: the physical layer data consist of a stream of bits(0,1). The transmitted bits must be encoded into signals–electrical or optical. The physical layer defines the type of encoding.

Data rate: The physical layer defines the transmission rate, the number of bits sent each second.

Line configuration: the physical layer is concerned with the connection of devices to the medium.

- Physical topology– Ring, star
- Transmission Mode - Simplex, Half duplex Full Duplex

Data Link Layer

- **What it does:** Ensures **error-free transfer** of data between two directly connected nodes. It is responsible for **node-to-node** delivery of data.
- Framing: The data link layer divides the **stream of bits** received from the network layer into data units called **frames**.
- Adds **MAC addresses** and **frames**.
- **Examples:** Ethernet, Wi-Fi (IEEE 802.11)

Physical addressing. If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the physical address of the sender (source address) and/or receiver (destination address) of the frame.

If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects one network to the next.

Flow Control. If the rate at which the data are absorbed by the receiver is less than the rate produced in the sender, the data link layer imposes a flow control mechanism to prevent overwhelming the receiver.

Error control. The data link layer adds reliability to the physical layer by adding mechanisms to retransmit damaged or lost frames. Error detect and control is normally achieved through a trailer to the end of the frame.

Access Control. When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any time.

Network Layer

- **What it does:** Handles **routing** and **forwarding** of data across networks.
- Adds **IP addresses** to the data.
- **Examples:** IP (Internet Protocol), routers

The Network layer is responsible for the **source-to-destination delivery of a packet** possible across multiple networks.
It converts **Frames into packets.**
If **two systems are connected to the same link**, there is usually **no need for a network layer**.
However, if the two systems are attached to different networks, there is often a need for the network layer to accomplish source-to-destination delivery.

Functions:
Logical addressing-Physical addressing (May change) handle addressing problem locally
If packet pass the network boundary, we need another addressing called logical addressing (Never change)
Routing - Route the packet to final destination

Transport Layer

- **What it does:** Ensures **reliable data transfer** with **error checking**, **flow control**, and **retransmission** if needed.
- **Breaks data into segments**.
- **Examples:** TCP (reliable), UDP (faster but less reliable)

The transport layer is responsible for **process-to-process or end-end** delivery of the entire message.

The network layer oversees host-to-destination delivery of individual packets, it does not recognize any relationship between those packets.

The transport layer ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the process-to-process level.

Session Layer

- **What it does:** Manages **sessions** or **connections** between applications.
- Handles **opening, maintaining, and closing** sessions.
- **Examples:** Logging into a website, video conferencing sessions

Presentation Layer

- **What it does:** Translates data into a **format the application can understand**, including **encryption, compression**, and **data conversion**.
- **Examples:** JPEG, MP3, SSL/TLS encryption

Application Layer

- **What it does:** Provides **services to the user** and handles **network-related application tasks**.
- **You interact with this layer.**
- **Examples:** Email (SMTP), Web browsing (HTTP), File transfer (FTP)

Easy Analogy – Sending a Letter:

OSI Layer	Role (in mail system)
Application	You write the letter
Presentation	You choose the language/encrypt it
Session	You open a chat or mailbox
Transport	You break it into pages and number them
Network	You decide the route to destination
Data Link	You write sender & receiver on envelope
Physical	You physically mail the letter

LAN Topologies

It defines the Physical (or) Logical arrangement of Links in a Network. Topology refers to the layout of connected devices in a network.

The Topology of the Network is Geometric Representation of the relationship between all Communication links.

Mesh Topology: N(N-1)/2 → n is the number of devices

Definition: Every device is **connected to every other device** in the network.
Advantages:
Very **reliable** – if one link fails, others still work.
Fast communication between devices.
Disadvantages:
Expensive – requires **lots of cables** and ports.
Complex to set up and manage.

Star Topology

Definition: All devices are **connected to a central hub or switch**.
Advantages:
Easy to install and manage.
If one device fails, others remain connected.
Disadvantages:
If the **central hub fails**, the whole network goes down.

Tree Topology
Bus Topology
Ring Topology
Hybrid Topology