Computer Network:

- Interconnected autonomous computers is called a computer network.
  Interconnected → able to exchange data through some valid interface.
  In systems, media must be there as an interface:
  - Wired media
  - Wireless media
- If the two systems are interconnected, they are able to exchange data.
- Autonomous → Independent computers.
  a) How to say they are independent:
  i) It is not ordered; communication operations are always in the form of *request-respond* only.
  Example: Phone call → signals not directly connected (only requests).
- In a computer network, communication is always in the form of *request-respond* only.
- There is no master-slave relation in computer networks.
  Example of master-slave: computer processors.
  OS → Master
  Processors → Slave

Uses of Computer Networks

Computer networks play a vital role in various fields. Here's a simplified explanation:

1. Business Applications

- **Resource Sharing**: Networks allow sharing of resources like printers, scanners, and data across a company. This saves costs and improves efficiency.
- **Information Sharing**: Companies rely heavily on computerized data like customer records, inventory, and financial information. Networks make this data accessible anytime, anywhere, enabling smooth operations.
- **Client-Server Model**: Employees (clients) use simple computers to access powerful servers that store company data. This model works whether employees are in the same office or spread across the globe.

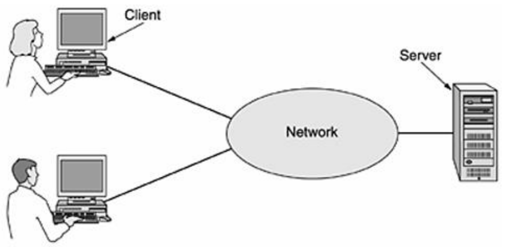
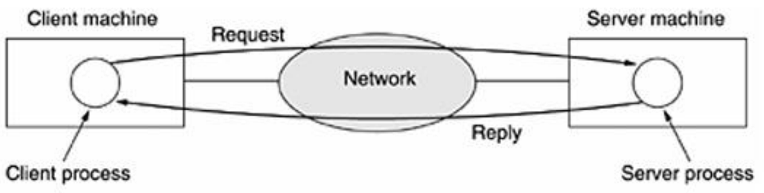


Figure 1-2. The client-server model involves requests and replies.



- **Improved Communication**:
  - **E-mail**: A fast and common way to communicate within companies.
  - **Collaboration**: Employees can edit shared documents in real time.
  - **Videoconferencing**: Distant teams can hold virtual meetings, saving time and travel costs.

- **E-commerce**: Companies sell products and services online, making shopping convenient for customers. This trend is growing rapidly.

2. Home Applications of Computer Networks

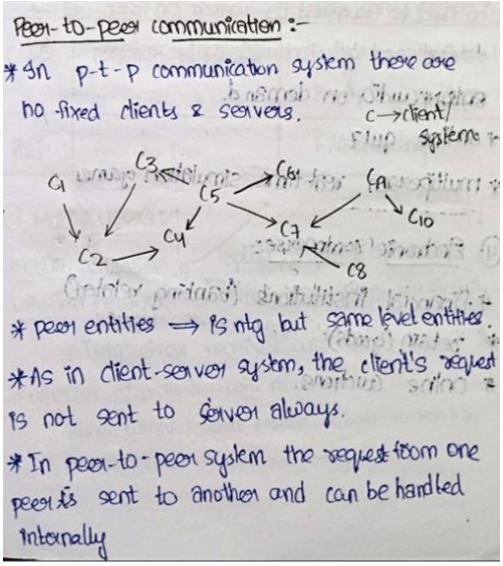
Computer networks have revolutionized home usage, enabling a variety of applications:

1. Access to Remote Information

- Surf the web for news, hobbies, health, or fun.
- Newspapers and digital libraries are now online, making information easier to access.

2. Person-to-Person Communication

- **E-mail and Messaging**: Quick and global communication, including multimedia.
- **Chat Rooms**: Real-time group discussions.
- **Peer-to-Peer Communication**: Direct sharing of files (e.g., music, photos).



Peer-to-peer communication :-

* In p-t-p communication system there are no fixed clients & servers.

c→client/

C1
C2
C3
C4
C5
C6
C7
C8
C9
C10

* peer entities ⇒ is ntg but same level entities.

* As in client-server system, the client's request is not sent to server always.

* In peer-to-peer system the request from one peer is sent to another and can be handled internally

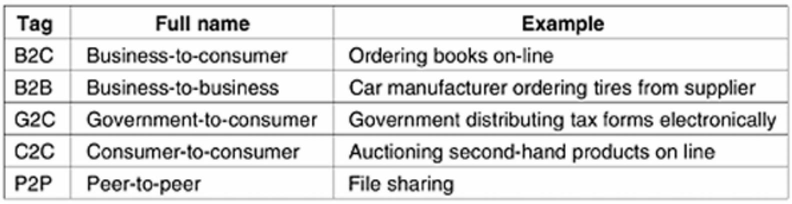
3. Interactive Entertainment

- **Games**: Multiplayer online games and virtual reality.
- **Video on Demand**: Stream movies or shows anytime.
- **Interactive TV**: Participate in live programs or quizzes.

4. E-Commerce

- **Online Shopping**: Browse and buy from digital catalogs.
- **Online Banking**: Pay bills and manage finances.
- **Auctions**: Platforms for buying and selling used items.

Figure 1-4. ***Some forms of e-commerce.***

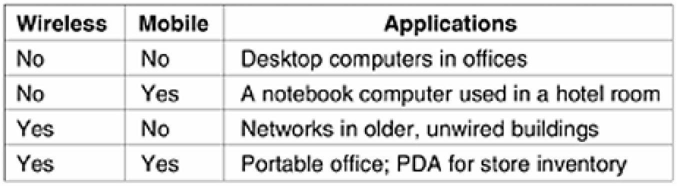


Tag	Full name	Example
B2C	Business-to-consumer	Ordering books on-line
B2B	Business-to-business	Car manufacturer ordering tires from supplier
G2C	Government-to-consumer	Government distributing tax forms electronically
C2C	Consumer-to-consumer	Auctioning second-hand products on line
P2P	Peer-to-peer	File sharing

3. Mobile Users and Wireless Networks

Mobile computers like laptops and PDAs are growing fast, allowing users to stay connected even while traveling.

Figure 1-5. Combinations of wireless networks and mobile computing.



Wireless	Mobile	Applications
No	No	Desktop computers in offices
No	Yes	A notebook computer used in a hotel room
Yes	No	Networks in older, unwired buildings
Yes	Yes	Portable office; PDA for store inventory

Uses of Wireless Networks

1. **Portable Office**:
   - Send/receive calls, emails, faxes, and access the internet from anywhere.
   - Example: At conferences or universities, wireless networks enable quick internet access.
2. **Business Applications**:
   - **Taxis**: Dispatch systems assign trips through wireless devices in taxis.
   - In some cities, taxi drivers have a small screen in their cabs. When a customer calls for a taxi, the central office sends the pickup and drop-off details to the screen. The first driver to press a button on their screen gets the job. This system works through wireless networks.
   - **Fleets**: Delivery vehicles and repair teams use wireless networks for updates and tracking.
3. **Military Use**:
   - Portable wireless networks support operations without relying on local infrastructure.

Other Applications

1. **Cost-Effective Connectivity**:
   - In old buildings, wireless networks avoid the expense of installing cables.
2. **Everyday Tasks**:
   - Wireless devices aid in inventory management, parking meters, and rental services.
   - Vending machines and utility meters report data wirelessly, reducing manual checks.
3. **Emerging Technologies**:
   - **M-Commerce**: Mobile devices enable banking, shopping, and payments.
   - **Smart Devices**: Watches and tiny computers (e.g., smart dust) connect users to the internet and track items.

4.Social Issues

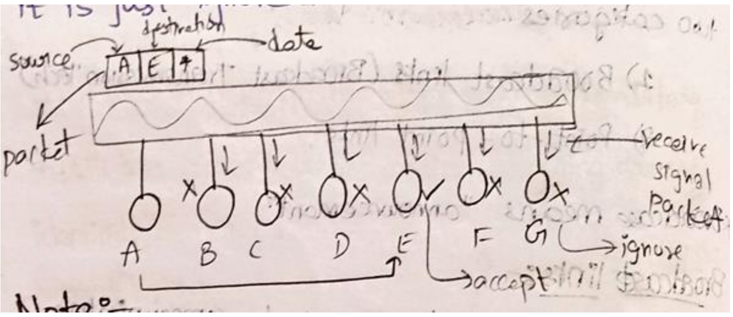
The rise of computer networks has brought social, ethical, and political issues

- **Offensive Content**: Controversial topics spark censorship debates.

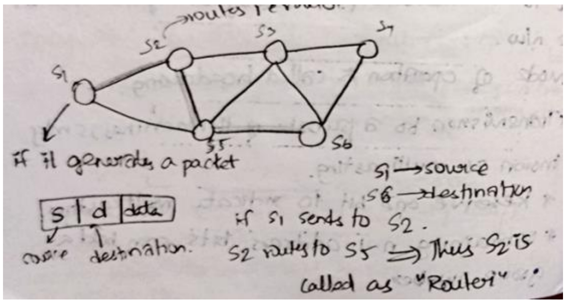
- **Employer Monitoring**: Privacy issues in workplace communication.
- **Government Surveillance**: Email spying vs. privacy rights.
- **Privacy Issues**: Cookies and data leaks online.
- **Anonymous Messaging**: Balancing anonymity and accountability.
- **Misinformation and Cybercrimes**: Spam, hacking, and identity theft.

Network Hardware – (transmission technology, scale)

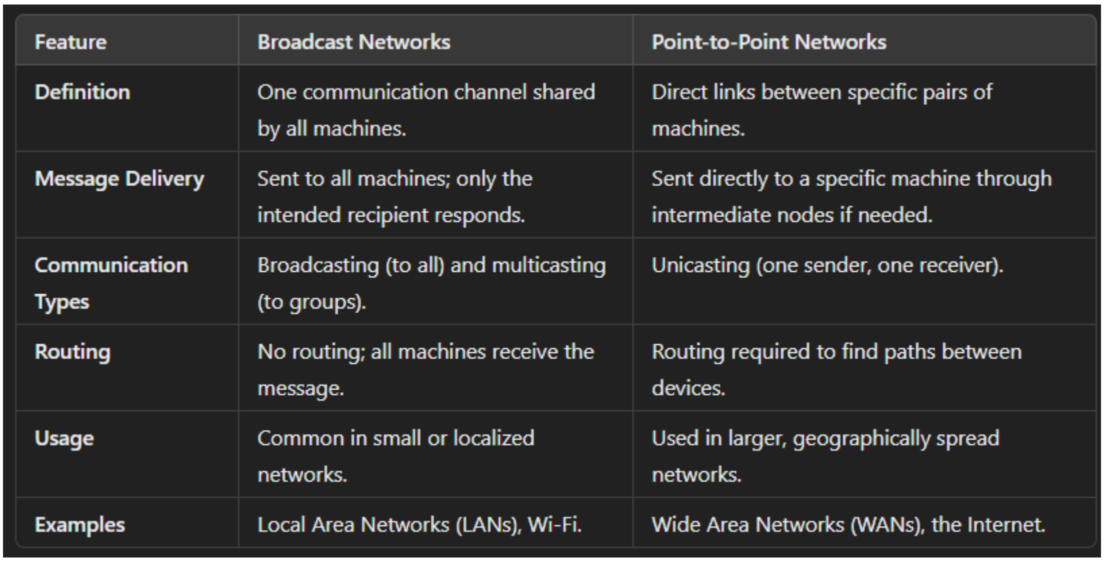
1. **Transmission Technology Types**:
   - **Broadcast Networks**: One communication channel shared by all machines.
   - **Point-to-Point Networks**: Direct links between specific pairs of machines.
2. **Broadcast Networks Features**:



   - Messages (packets) sent to all machines, but only intended recipients respond.
   - **Broadcasting**: Send to all machines.
   - **Multicasting**: Send to specific groups of machines.
3. **Point-to-Point Networks Features**:



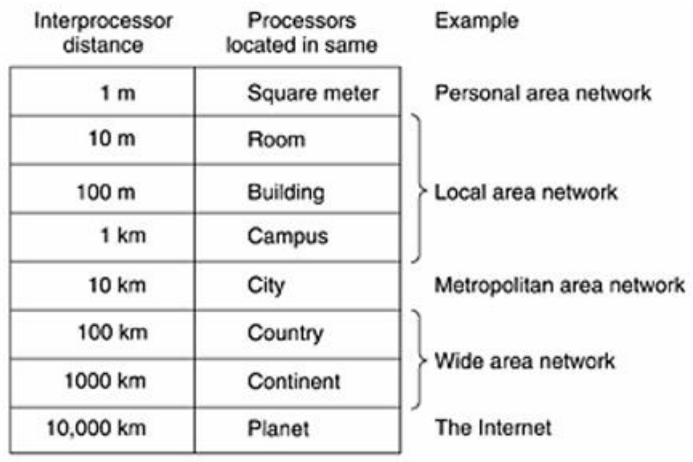
   - Packets may pass through multiple machines to reach the destination.
   - Used for larger, geographically spread networks.
   - **Unicasting**: One sender, one receiver.



Feature	Broadcast Networks	Point-to-Point Networks
Definition	One communication channel shared by all machines.	Direct links between specific pairs of machines.
Message Delivery	Sent to all machines; only the intended recipient responds.	Sent directly to a specific machine through intermediate nodes if needed.
Communication Types	Broadcasting (to all) and multicasting (to groups).	Unicasting (one sender, one receiver).
Routing	No routing; all machines receive the message.	Routing required to find paths between devices.
Usage	Common in small or localized networks.	Used in larger, geographically spread networks.
Examples	Local Area Networks (LANs), Wi-Fi.	Wide Area Networks (WANs), the Internet.

Network Classification by Scale:

- **Personal Area Networks (PANs)**: For a single person (e.g., connecting a mouse to a computer).
- **Local Area Networks (LANs)**: Small areas like offices.
- **Metropolitan Area Networks (MANs)**: Covers a city.
- **Wide Area Networks (WANs)**: Spans large distances.
- **Internetworks**: Connect multiple networks (e.g., the Internet).



Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

Personal Area Networks (PANs) are small networks for individual use, such as connecting a computer to its mouse, keyboard, and printer, or devices like a PDA controlling a hearing aid.

PAN is spread around the area of 1m.

Local Area Networks (LANs) are private networks within a small area (e.g., a building or campus), typically a few kilometers in size. They are used to connect personal computers and workstations to share resources (like printers) and exchange information. LANs have three main characteristics:

1. **Size**: They are restricted in size, making transmission times predictable and manageable.
2. **Transmission Technology**: LANs usually use cables to connect machines, with speeds ranging from 10 Mbps to 10 Gbps.

3. **Topology:** Topology in networking refers to the layout or arrangement of different elements (like computers, devices, and connections) in a network. It defines how devices are connected and how data flows between them. Examples include bus, star, ring, and mesh topologies.

   An **arbitration mechanism** is a method used in network communication to decide which device gets to use the shared communication channel when multiple devices want to transmit data at the same time. Since many devices may be connected to a single network medium (like a bus or ring), an arbitration mechanism ensures that only one device can transmit at any given moment to avoid data collisions.

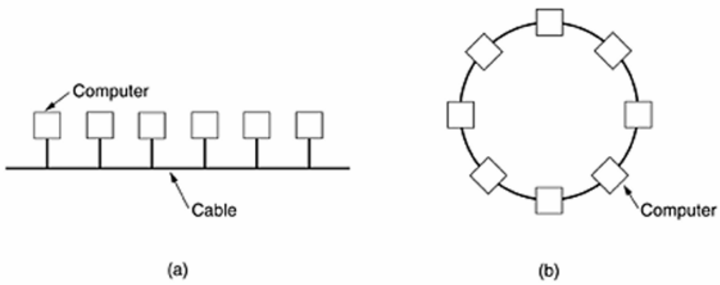
   There are two main types of arbitration mechanisms:

1. **Centralized Arbitration**: A central controller or entity decides which device can transmit at a time. It may accept requests from devices and grant permission based on certain rules or algorithms.
2. **Distributed Arbitration**: Each device independently determines when it can transmit. This method often uses algorithms like **CSMA/CD** (Carrier Sense Multiple Access with Collision Detection) in Ethernet, where devices listen to the channel, and if it's clear, they transmit. If a collision occurs, devices back off and try again later.

LANs can have different physical layouts, such as:

- **Bus (IEEE 802.3 -> Ethernet)**: A single cable connects all devices, and only one device can transmit at a time. Conflicts are resolved using a random retry mechanism (e.g., Ethernet).
- **Ring (IEEE 802.5)**: Devices are connected in a circle, and data travels around the ring. Arbitration is needed for accessing the ring.

Figure 1-7. Two broadcast networks. (a) Bus. (b) Ring.



LANs can use **static or dynamic allocation** for channel use:

- **Static**: Time is divided into intervals, and each device gets a turn to send.
- **Dynamic**: Devices share the channel based on demand, either through centralized or decentralized control.

These networks help simplify communication within a small, localized area.

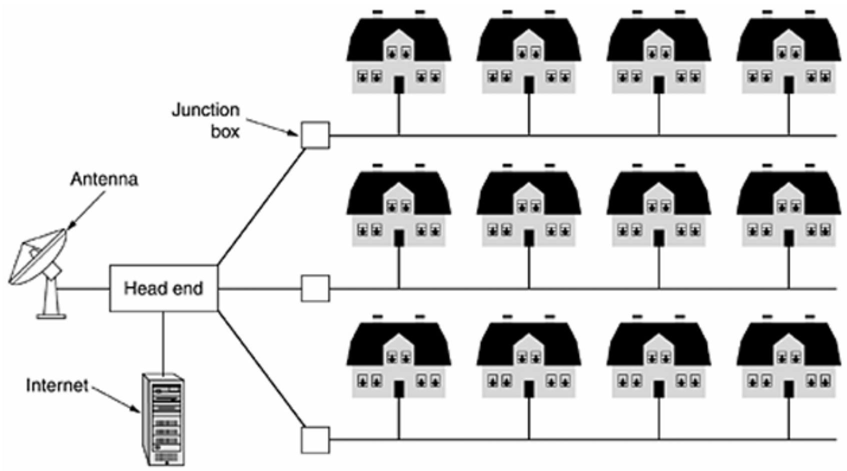
A **Metropolitan Area Network (MAN)** covers a city and is larger than a local area network (LAN) but smaller than a wide area network (WAN).

The most common example of a MAN is the **cable TV network**, which initially started as a way to improve TV reception in areas with poor signals. Over time, cable TV companies expanded to offer full city coverage. In the 1990s, these companies adapted their systems to provide **two-way Internet service**, turning the cable TV network into a **MAN**.

Another example of a MAN is **high-speed wireless Internet access**, which has been standardized as IEEE 802.16, IEEE 802.16 is a series of standards for wireless metropolitan area network

In short, a MAN connects various locations within a city and can provide services like TV, internet, and more.

Figure 1-8. A metropolitan area network based on cable TV.



A **Wide Area Network (WAN)** spans a large geographic area, like a country or continent. It connects multiple **hosts** (machines running application programs) through a **communication subnet**, which is typically owned by a **telephone company** or **Internet Service Provider (ISP)**. The subnet consists of **transmission lines** (copper wires, optical fiber, or radio links) and **switching elements** (routers) that forward data between hosts.

In most WANs, **data is transmitted in packets**, which are sent from one host to another. These packets may pass through multiple routers before reaching their destination, in a system called **store-and-forward**. Each router stores the packet until it can forward it to the next router or destination.

Routing algorithms determine how packets are sent through the network. In some WANs, like **satellite systems**, the communication is broadcast, where all routers can receive signals from a satellite, which is useful for certain applications.

Figure 1-9. Relation between hosts on LANs and the subnet.

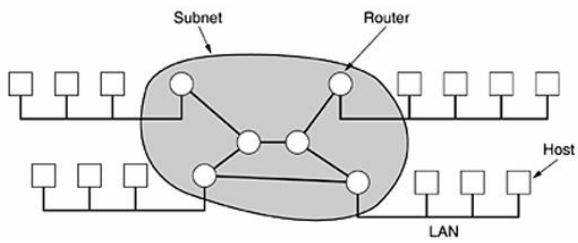
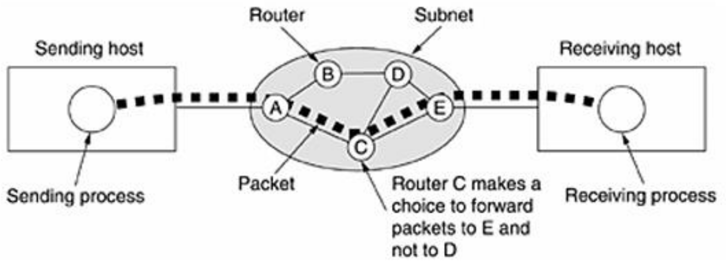


Figure 1-10. A stream of packets from sender to receiver.



<u>**Wireless Networks**</u>

Wireless networks enable communication without cables using radio signals. They can be categorized as:

1. **System Interconnection**
   - Connects computer components like keyboards, mice, and printers using short-range wireless (e.g., Bluetooth).
   - Operates in a **master-slave** setup where the main unit controls other devices.
2. **Wireless LANs (Local Area Networks)**

- Connect computers using radio modems and antennas within a small area, like homes or offices.
- Supports **peer-to-peer** communication or centralized communication through ceiling antennas.
- Commonly use the **IEEE 802.11 (Wi-Fi)** standard.

3. **Wireless WANs (Wide Area Networks)**
    - Examples include **cellular networks**, supporting voice and data over long distances (kilometers).
    - Evolved from **analog (1G)** to **digital (3G)** and beyond.
    - Wireless LANs are faster but operate over shorter distances compared to cellular networks.
4. **High-Bandwidth Wireless Networks**
    - Provide high-speed Internet access (e.g., **IEEE 802.16**).

Wireless networks often connect to wired networks for accessing files, databases, or the Internet. For example, in airplanes, wireless LANs link passenger devices to routers connected to ground stations.

Future of Wireless Networks

- Wireless technology is growing, with supporters seeing it as transformative.
- Some critics believe wired connections remain essential for certain settings.

Home Networks

1. Home networks connect devices like computers, appliances, and entertainment systems for communication and Internet access.
2. They need to be easy to install, simple to use, and affordable for everyone.
3. Security and reliability are important, especially to protect against misuse.
4. Wireless networks are cheaper, but wired ones provide better security.
5. Home networking has great potential but needs to be user-friendly for non-technical users.

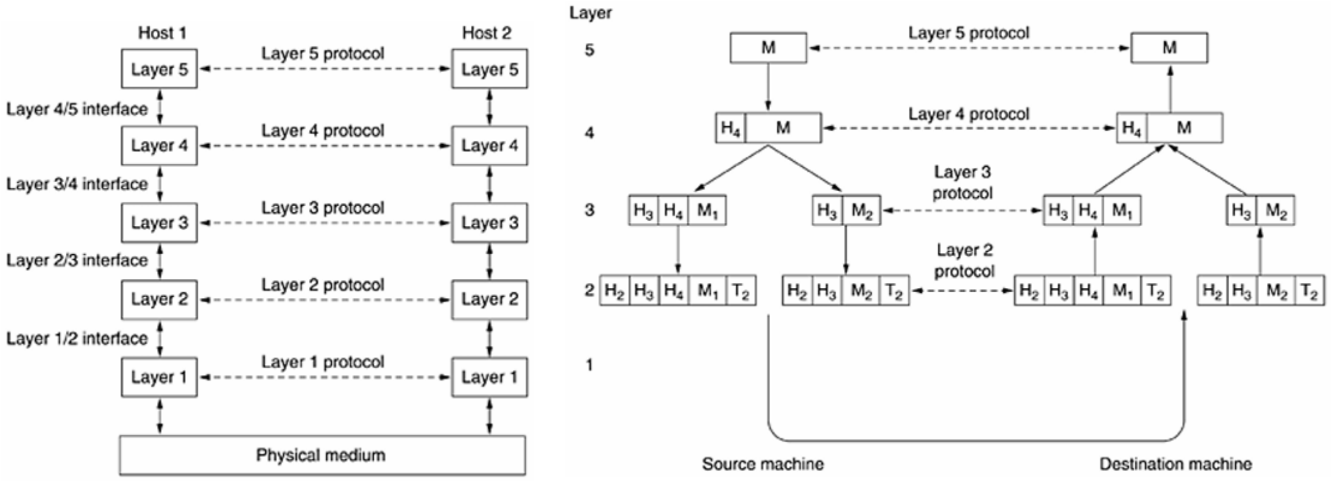
Internetworks

1. **Internetworks** connect different networks, often with different hardware and software, to enable communication between them.
2. Gateways are used to translate and connect these networks.
3. An **internetwork** is a collection of interconnected networks, while the **Internet** is a specific example of an internetwork.
4. LANs and WANs can be interconnected to form an internetwork.
5. A **subnet** refers to routers and lines owned by the network operator, while hosts and their connections form a network.
6. When distinct networks with different owners or technologies are linked, they create an internetwork.

Network Software

1. **Network Architecture:**
    - A set of layers and their corresponding protocols is called **network architecture**.
    - It is also referred to as the **network protocol stack** or simply the **protocol stack**.
2. **Layers and Protocols:**
    - **Breaking complexity:** Layering divides the network design into smaller, manageable parts, allowing easier design and troubleshooting.
    - Each layer has its **protocol** that facilitates **peer-to-peer communication**.
    - Protocols are sets of rules or mechanisms.
    - Layers on different devices communicate as peers using agreed rules, while each layer adds or removes headers during data transmission.
3. **Interface:**
    - The **interface** is the medium through which two **adjacent layers** within the same machine share information.
4. **Virtual Communication:**
    - **Protocols** enable **virtual communication** between two machines.
5. **Protocol Information:**
    - Protocol information is exchanged using a **header**.
6. **Layer Functionality:**
    - Each layer has a specific name and specific functionality.
    - Each layer provides services to the layer above it and uses the services of the layer below it.

Figure 1-13. Layers, protocols, and interfaces.



- A message (**M**) is created at the top layer (Layer 5) and passed down through the layers.
- **Layer 4** adds a header with control info (like sequence numbers) to ensure proper order.
- **Layer 3** may split the message into smaller parts (e.g., **M1**, **M2**) and add its own header.
- **Layer 2** adds another header and trailer for error checking.

- **Layer 1** physically transmits the data.

On the receiving side:

- The data moves up through the layers, with headers/trailers removed at each step, until the complete message is reconstructed at Layer 5.

Key Points:

- Layers communicate logically (horizontal) but operate physically (vertical).
- Dividing tasks into layers simplifies network design.

Design Issues for Network Layers:

1. **Addressing**:
    - Each layer in a network must know **who is sending** and **who is receiving** the data.
    - Addressing helps pinpoint the exact destination when there are multiple options.
2. **Data Transfer**:
    - Data can flow in three ways:
        - **One-way** (Simplex): Data moves in only one direction.
        - **Two-way, not at the same time** (Half-duplex): Data goes both ways, but only one side at a time.
        - **Two-way simultaneously** (Full-duplex): Data flows both ways at the same time.
    - Decide whether data flows one-way or two-way.
    - Networks may use different channels for **normal data** and **urgent data**.
3. **Error Control**:
    - Errors can occur when sending data.
    - Systems detect errors, correct them, and ensure the receiver confirms that messages are received without issues.
4. **Message Order**:
    - Messages may arrive in the wrong order.
    - To fix this, pieces of messages are numbered so they can be reassembled correctly.
5. **Flow Control**:
    - Ensures a **fast sender** doesn’t overwhelm a **slow receiver** with too much data.
    - Techniques like feedback or speed limits are used to maintain balance.
6. **Message Size**:
    - Large messages are **broken into smaller pieces**, sent, and then reassembled.
    - Very small messages can be **combined into larger ones** for efficiency.

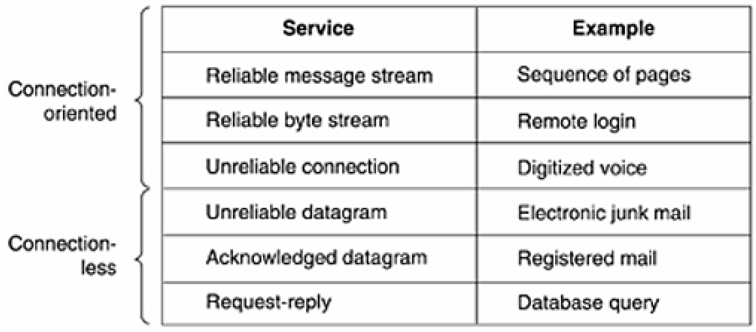
7. **Multiplexing**:
    - Multiple conversations can share a single connection, saving resources.
    - This is useful for efficiently using limited physical circuits.
    - For example, one internet connection can handle different streams like emails, calls, and web browsing simultaneously.
8. **Routing**:
    - When there are multiple paths to send data, the system chooses the **best route** based on factors like traffic or speed.
    - Routing decisions can be influenced by **current load** (low-level) or broader rules (like laws or policies, high-level).

Connection-Oriented vs. Connectionless Services

1. **Connection-Oriented Service:**
    - Works like a phone call:
        1. **Connect**
        2. **Send data in order**
        3. **Disconnect**
    - Reliable: ensures all data arrives correctly and in order.
    - Used for tasks like file transfers where accuracy is critical.
    - **Types:**
        - **Message sequences:** Sends data in separate pieces (e.g., book pages sent one by one).
        - **Byte streams:** Sends continuous data (e.g., typing commands to a server).
2. **Connectionless Service:**
    - Works like sending a letter:
        - No connection setup.
        - Each message has the full address and is sent separately.
    - May not guarantee delivery or order unless extra measures are added.
    - Used for short, fast communication like emails or live calls.
3. **Common Types of Services:**
    - **Unreliable Datagram:** No confirmation of delivery, used for non-critical tasks (e.g., junk mail).
    - **Acknowledged Datagram:** Confirms delivery, like registered mail.
    - **Request-Reply:** A single message request with a reply, used in client-server systems (e.g., library queries).
4. **Why Use Unreliable Communication?**

- Sometimes it's the only option (e.g., Ethernet).
- Reliable methods can be slower, which isn’t ideal for real-time tasks like video or voice calls.

Figure 1-16. Six different types of service.



	Service	Example
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Remote login
	Unreliable connection	Digitized voice
Connection-less	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Registered mail
	Request-reply	Database query

Connection-Oriented Services

These need a connection to be set up between sender and receiver before sending data.

1. **Reliable Message Stream**
   - Messages are sent and received as separate units.
   - Example: Sending pages of a book where each page stays separate.
2. **Reliable Byte Stream**
   - Data is sent as a continuous flow of bytes without splitting it into distinct parts.
   - Example: Typing commands during remote login.
3. **Unreliable Connection**
   - Data is sent over a connection, but it’s okay if some bits are lost.
   - Example: Voice calls where a little noise is fine.

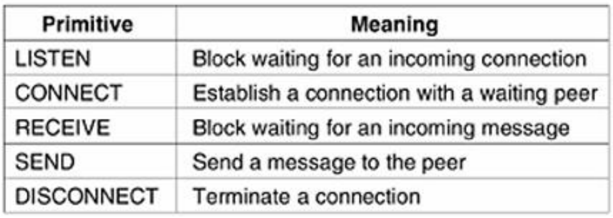
Connectionless Services

These send data directly without setting up a connection.

4. **Unreliable Datagram**
   - Data is sent without guarantees of delivery.
   - Example: Sending spam emails (no confirmation needed).
5. **Acknowledged Datagram**
   - Each message is confirmed by the receiver, ensuring it arrived.
   - Example: Registered mail where you get a delivery receipt.
6. **Request-Reply**
   - One message is sent as a request, and the receiver replies with an answer.
   - Example: A database query asking for specific information.

Service Primitives and Protocols

Figure 1-17. Five service primitives for implementing a simple connection-oriented service.



Primitive	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection

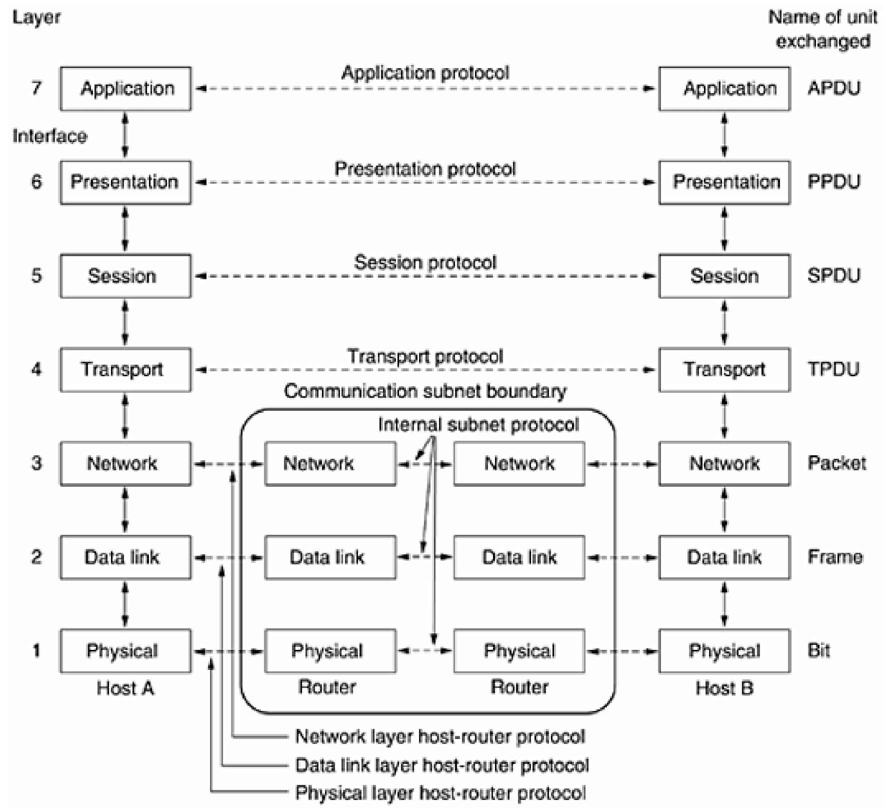
1. **What Are Service Primitives?**
   - **Primitives** are operations or actions provided by a layer for communication.
   - Examples in a **connection-oriented service**:
     - **LISTEN:** Server waits for a connection.
     - **CONNECT:** Client starts the connection.
     - **SEND:** Send data.
     - **RECEIVE:** Receive data.
     - **DISCONNECT:** End the connection.
2. **How It Works in Client-Server Communication:**
   - **Server:**
     - Calls LISTEN to wait for connections.
     - Calls RECEIVE to get data from the client.
     - Sends a reply with SEND.
   - **Client:**
     - Calls CONNECT to request a connection.
     - Sends data with SEND.
     - Waits for the reply with RECEIVE.
     - Calls DISCONNECT to close the connection.
   - Example: Like making a call—server waits for the call, client calls, they talk, then disconnect.
3. **Why Not Use Connectionless Protocols Always?**
   - Connectionless systems send fewer packets (request + reply).
   - However, for large files or reliable delivery, connection-oriented systems are better to handle errors and ensure data is delivered in the right order.
4. **Services vs. Protocols:**
   - **Services:**
     - What a layer offers to the layer above it (e.g., sending data).
     - Focuses on **what** can be done.
   - **Protocols:**

        - Rules for communication between machines in the same layer (e.g., message formats).
        - Focuses on **how** services are implemented.
    - Example:
        - A service is like a vending machine interface (buttons to select an item).
        - A protocol is the mechanism inside the machine that delivers the item.

OSI - Open Systems Interconnection

The **OSI (Open Systems Interconnection)** model is a framework to explain how data moves across a network. It splits the communication process into **7 layers**, each with a specific role. This makes it easier to understand, troubleshoot, and design networks.

Figure 1-20. The OSI reference model.



The 7 Layers of the OSI Model

1. Physical Layer

- **Purpose**: Handles the physical connection between devices and the actual transmission of raw data (bits: 0s and 1s) over a medium.

Functions:

1. **Data Encoding and Decoding**:
    - Converts binary data (0s and 1s) into signals like electrical voltages, light pulses, or radio waves that can travel through the medium.
    - Decodes signals back into binary at the receiving end.

2. **Transmission Medium and Connectors**:
    - Physical layer deals with data transfer – one way, two way – simultaneous, not simultaneous.
    - Specifies hardware, such as cables (Ethernet, HDMI), connectors, and their pin configurations.
    - Deals with how data physically flows through a medium like wires, fibre optics, or wireless.
3. **Bit Synchronization**:
    - Ensures that sender and receiver devices are in sync while transmitting data.
    - It deals with mechanical, electrical and timing interfaces over a communication medium.

---

2. Data Link Layer

- **Purpose**: Ensures error-free and reliable transmission of data over the physical layer.
- Data link layer deals with controlling the data over a “link”
- “link” is a communication path or communication between two adjacent terminals

Functions:

1. **Framing**:
    - It turns the raw data into frames and ensures data is correctly delivered without errors.
    - Breaks data into small chunks called **frames** for easier handling.
2. **Error Detection and Correction**:
    - Deals with transmission errors – error detection, error correction
    - Uses techniques like **Cyclic Redundancy Check (CRC)** to detect and correct errors – **Hamming code** in data transmission.
    - Error correction – self healing, feedback (ack)
3. **Flow Control**:
    - Ensures that a faster sender doesn’t overwhelm a slower receiver.
    - Flow control basically has two types of techniques – parameter negotiation(SLA – Service Level Agreement), Feedback (Stop and wait and continue algorithm).

Datalink layer has two modules – LLC (Logical link control), MAC (Medium Access Control).

4. **MAC (Media Access Control)**:
    - Manages access to the shared communication channel to prevent collisions (e.g., in Wi-Fi).
    - Collision means overlapping of transmission signals in a shared media.
    - Collision is due to simultaneous access.

    - Uses techniques like **CSMA/CD** (Collision Detection).

---

3. Network Layer

- **Purpose**: Handles routing and forwarding of data between networks to reach its destination.
- **Responsibility is host to host delivery**
- It belongs to Sub network – (physical layer + datalink layer + network layer).

Functions:

1. **Routing**:
    - Decides the best path for data to travel between networks.
    - Uses algorithms like Dijkstra's shortest path.
    - **Routing process** is defined as a decision-making process, which defines the best outcomes for a given incoming packet.
    - To do the routing process, there are 2 modules/algorithms:
        - Forwarding algorithms
        - Routing algorithms
    - **Forwarding Algorithm** is used to forward/shift the packet from one line to another using the routing table.
    - **Routing Algorithm** is used to design the routing tables based on topology.
    - Routing Algorithms are further divided into two types:
        - Static Routing Algo.
        - Dynamic Routing Algo.
    - **Static Routing:**
        - Routing decisions are not changed.
        - Static routing table.
    - **Dynamic Routing:**
        - Routing decisions are changed.
        - Periodically updated based on conditions on the network.
2. **Congestion Control:**
    - Congested → More density.
    - Congestion is defined as: If too many packets are present in the network, the performance of the network gradually decreases.
    - Thus, we require something to control congestion.
3. **Internetworking:**
    - It deals with the interconnection or integration of existing networks.
    - The networks may differ in packet size, hardware, software, protocols, etc.

---

4. Transport Layer

- **Purpose**: Ensures reliable data delivery from the source to the destination.
- Deals with transportation of data source to destination with the help of network layer, **process to process delivery**.

- It transports data from one process in one system to another process in another system.
- Functionality of transport layer is similar to the data link layer (error control, flow control).
- The **data link layer** generally works on the links, whereas **transport layer protocols** are applied on subnetworks.

Functions:

1. Multiplexing and demultiplexing.
2. Data recovery.
3. Buffering (queue management).
4. The transport layer basically offers two types of services:
   - Connection-oriented service.
   - Connectionless service.
5. **Error Detection and Retransmission**: Ensures lost or corrupted packets are resent.
6. **Flow Control**: Manages the rate of data flow to avoid overwhelming the receiver.
7. **End-to-End Communication**: Provides reliable delivery between devices, even across multiple networks.

Examples: Protocols like **TCP** (reliable) and **UDP** (faster but less reliable).

---

5. Session Layer

- **Purpose**: Manages communication sessions between devices.

Functions:

1. **Session Management**: Opens, maintains, and closes sessions.
2. **Synchronization**: Ensures communication can resume smoothly after interruptions.
3. **Dialog Control**: Manages who sends data at a given time to avoid conflicts.

---

6. Presentation Layer

- **Purpose**: Ensures data is in a format that the receiving application can understand.
- Deals with syntax and semantics of data representation

Functions:

1. **Data Translation**: Converts data between different formats (e.g., ASCII to UTF-8).
2. **Data Compression**: Reduces the size of data for faster transmission.
3. **Data Encryption and Decryption**: Secures data during transmission.

---

7. Application Layer

- **Purpose**: This is the topmost layer where users interact with the network.

Functions:

1. **Network Services**: Provides services like file transfers, email, and web browsing.
2. **Protocols**: Implements protocols like **HTTP** (web browsing), **FTP** (file transfer), and **SMTP** (email).

TCP/IP Reference Model

The **TCP/IP reference model** is the framework used to explain how devices communicate over the Internet. It evolved from the **ARPANET**, the first major wide-area computer network, developed by the U.S. Department of Defence (DoD). This model is the backbone of the modern Internet and has four key layers, each performing specific tasks to ensure smooth data transfer.

This model is called Internet model. The primary goal of the Internet model is to integrate or connect the existing networks.

The OSI model failed when we try to connect wired n/w with wireless n/w or satellite

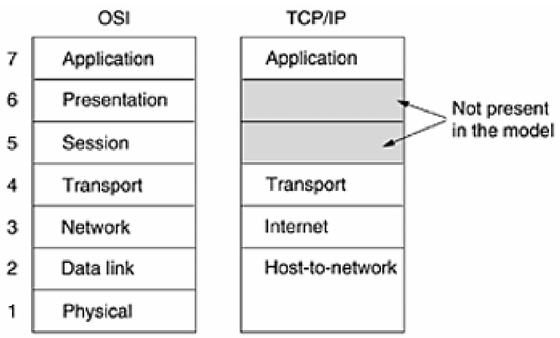
Key Goals of the TCP/IP Model:

1 **Connect multiple networks seamlessly**: The goal was to allow communication between different types of networks, like wired, satellite, and radio.

2 **Survivability**: If part of the network fails (e.g., due to war or disasters), communication should still work as long as the source and destination are functional.

3 **Flexibility**: It needed to support various types of applications, from file transfers to real-time video or voice communication.

Figure 1-21. The TCP/IP reference model.



Layers of the TCP/IP Model

1. Host-to-Network Layer

- **Purpose**: This layer defines how a device connects to a network and sends data packets. It deals with the hardware and protocols needed for communication.
- It is similar to the physical and data link layer of OSI model
- The model doesn't specify how this connection should happen; it varies based on the network type (e.g., Ethernet, Wi-Fi).
- This layer is mostly concerned with making sure the device can send packets to the internet layer.

2. Internet Layer (Similar to the Network Layer in OSI)

- **Purpose**: This is the heart of the TCP/IP model. It ensures that data (packets) can travel independently through various networks and reach the destination.
- Internet layer defines one official protocol called as IP protocol(Internet Protocol)
- IP protocol is a connectionless and unreliable protocol.
- TCP/IP network are called datagram networks(uses Connectionless protocol)
- There are some other protocols
    - ICMP (Internet Control Management Protocol -offers services related to Internet Management)
    - ARP (Address Resolution Protocol – address translation Protocol)
    - RARP (Reverse Address Resolution Protocol-Address translation Protocol)
- **Key Points**:
    - **Packet Switching**: Data is broken into packets (PDU – Protocol Data Unit or Datagram packet) that travel independently and may take different paths to reach the destination. They might arrive out of order but will be rearranged later.
    - **IP (Internet Protocol)**: Defines the packet structure and ensures delivery to the right destination.
    - **Routing**: Decides the best path for the packets to travel.

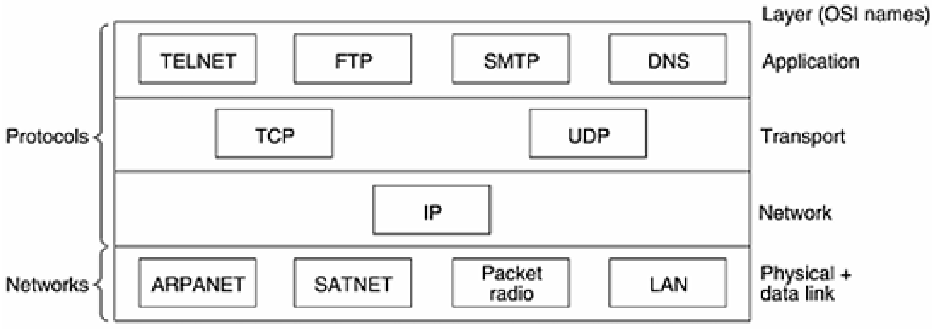
Users don't worry about how packets move across networks.

3. Transport Layer

- **Purpose**: This layer ensures that data sent between two devices is delivered reliably or quickly, depending on the application's needs. It manages the conversation between the sender and receiver.
- Functionality is similar to OSI model (error control, flow control, data recovery, buffering, multiplexing, demultiplexing, and transport services)
- In internet model, transport layer defines 2 standard protocols- TCP, UDP
    - **TCP (Transmission Control Protocol)**:
        - Reliable and connection-oriented.
        - Splits data into smaller packets - segments, ensures no packets are lost, and reassembles them at the destination.
        - Handles flow control so fast devices don't overwhelm slower ones.
        - Example: Used for tasks like file downloads, emails, and web browsing.
    - **UDP (User Datagram Protocol)**:
        - Unreliable, connectionless but faster.
        - Doesn't guarantee packet delivery or order, making it ideal for real-time data like video streaming or online games.

Think of TCP as a careful postman who checks if every package reaches its destination, while UDP is like a courier who delivers quickly without worrying about missing packages.

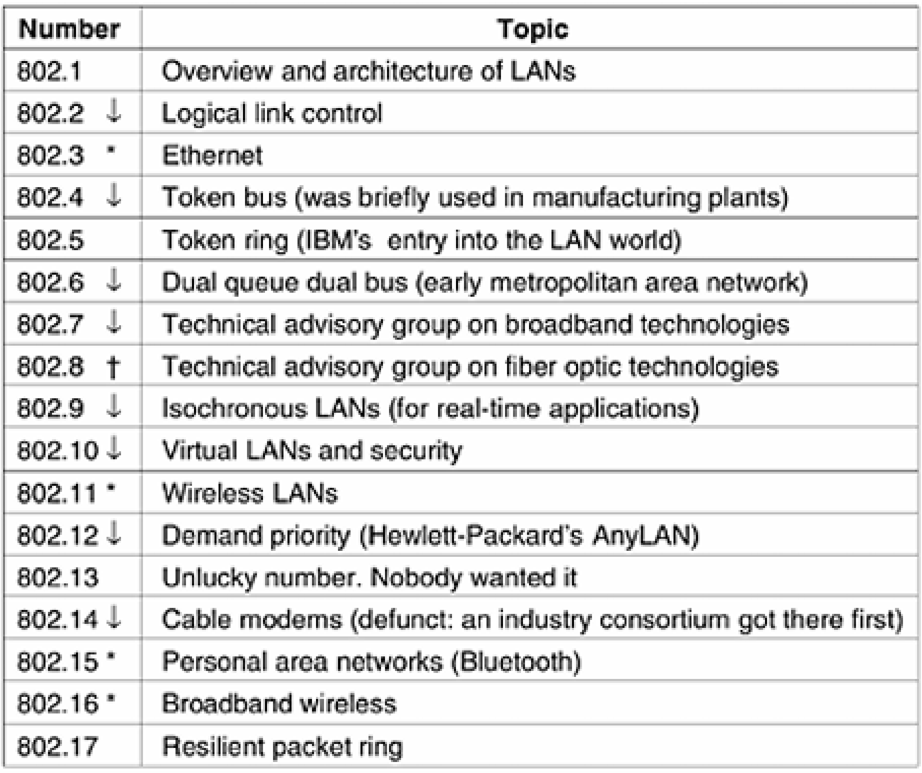
Figure 1-22. Protocols and networks in the TCP/IP model initially.



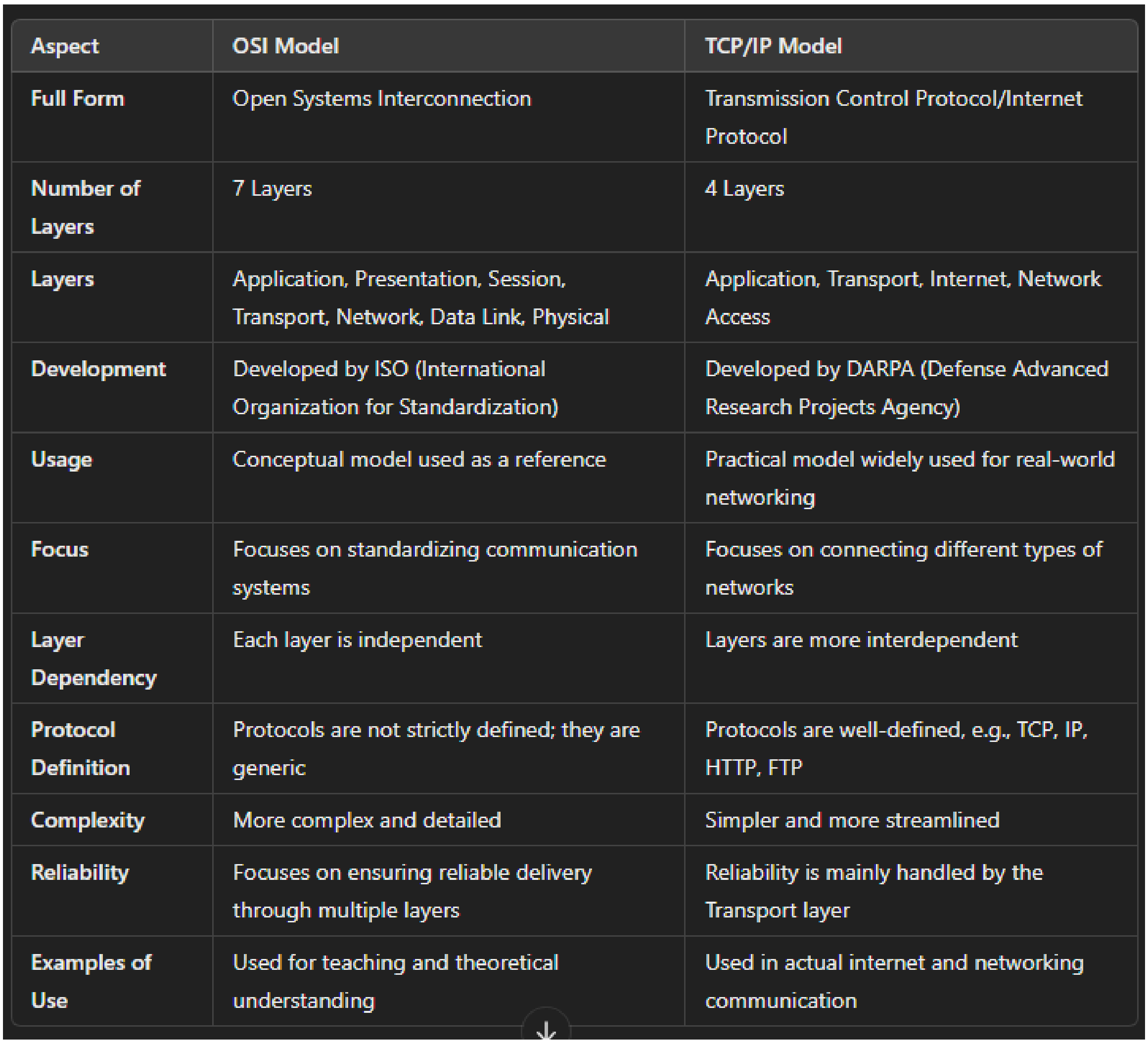
4. Application Layer

- **Purpose**: This is the layer where users interact with the network. It provides protocols that support services like web browsing, email, and file transfer.
- **Key Examples of Protocols**:
  - TELNET → Terminal Networking (virtual terminal/remote login).
  - FTP → File Transfer Protocol.
  - SMTP → Simple Mail Transfer Protocol (e-mail).
  - DNS → Domain Name System.
  - USENET → News protocol: It gathers news similar to Google homepage.
  - HTTP → World Wide Web protocol.
  - SNMP → Simple Network Management Protocol.

Unlike the OSI model, TCP/IP does not have separate **session** or **presentation layers**. These tasks are either handled by the application layer or considered unnecessary for most applications.



Number	Topic
802.1	Overview and architecture of LANs
802.2 ↓	Logical link control
802.3 *	Ethernet
802.4 ↓	Token bus (was briefly used in manufacturing plants)
802.5	Token ring (IBM's entry into the LAN world)
802.6 ↓	Dual queue dual bus (early metropolitan area network)
802.7 ↓	Technical advisory group on broadband technologies
802.8 †	Technical advisory group on fiber optic technologies
802.9 ↓	Isochronous LANs (for real-time applications)
802.10 ↓	Virtual LANs and security
802.11 *	Wireless LANs
802.12 ↓	Demand priority (Hewlett-Packard's AnyLAN)
802.13	Unlucky number. Nobody wanted it
802.14 ↓	Cable modems (defunct: an industry consortium got there first)
802.15 *	Personal area networks (Bluetooth)
802.16 *	Broadband wireless
802.17	Resilient packet ring



Aspect	OSI Model	TCP/IP Model
Full Form	Open Systems Interconnection	Transmission Control Protocol/Internet Protocol
Number of Layers	7 Layers	4 Layers
Layers	Application, Presentation, Session, Transport, Network, Data Link, Physical	Application, Transport, Internet, Network Access
Development	Developed by ISO (International Organization for Standardization)	Developed by DARPA (Defense Advanced Research Projects Agency)
Usage	Conceptual model used as a reference	Practical model widely used for real-world networking
Focus	Focuses on standardizing communication systems	Focuses on connecting different types of networks
Layer Dependency	Each layer is independent	Layers are more interdependent
Protocol Definition	Protocols are not strictly defined; they are generic	Protocols are well-defined, e.g., TCP, IP, HTTP, FTP
Complexity	More complex and detailed	Simpler and more streamlined
Reliability	Focuses on ensuring reliable delivery through multiple layers	Reliability is mainly handled by the Transport layer
Examples of Use	Used for teaching and theoretical understanding	Used in actual internet and networking communication

Internet Architecture

1. **How the Internet Works**:
   - A user connects to the **ISP (Internet Service Provider)** using a modem, which converts computer signals into a form that travels over telephone or fibre lines.
   - The data first reaches the ISP's **Point of Presence (POP)** and enters the ISP's network.
2. **Backbones**:
   - If the data needs to go to another network, it is sent to a **backbone**—a large, high-speed network connecting many regions or countries.
   - Big companies or server farms (websites storing lots of data) connect directly to these backbones.
3. **How Backbones Connect**:
   - **NAPs (Network Access Points)** are places where different backbone networks connect and exchange data.
   - Backbones also directly link some routers to speed up data transfer (private peering).

Connection-Oriented vs. Connectionless Networks

1. **Connectionless Networks** (e.g., the Internet):
   - Data is sent in small pieces (packets) that find their own way to the destination.

  - If a part of the network fails, packets take another path.
  - Example: Emails or web browsing.
2. **Connection-Oriented Networks** (e.g., Telephone Networks):
   - A fixed path is created before sending data.
   - Ensures smooth data flow but fails if the path breaks.
   - Example: Phone calls.

Ethernet

1. **What is Ethernet?**
   - A technology for connecting computers in a small area (e.g., offices or homes).
   - Developed in the 1970s to link computers using a single cable.
2. **How Ethernet Works**:
   - Computers check if the cable is free before sending data.
   - If two computers send data at the same time, they stop and try again after waiting for a random time.
3. **Why Ethernet is Popular**:
   - It's simple, reliable, and fast.
   - Over time, speeds have improved from 10 Mbps to 100 Mbps, 1 Gbps, and beyond.

In Summary

- The Internet connects users, ISPs, and backbones to send data globally.
- Connectionless networks like the Internet are flexible, while connection-oriented ones (like phone networks) ensure quality.
- Ethernet is a widely-used and efficient technology for small networks like homes and offices.

PART - 2

Purpose of the Physical Layer:

- It deals with transmitting raw bits (1s and 0s) from one device to another over a physical medium.
- Transmission media are broadly categorized as **guided** (like cables – copper wire, fibre optics) or **unguided** (like wireless signals).

In the physical layer of a network, transmission media refers to the **means or pathways used to carry data signals** from one device to another. It is classified into two main types:

1. Guided Media (Wired)

Signals travel through a physical medium like cables.

- **Examples**:

    - **Twisted Pair Cable**: Used in telephone lines and LANs.
    - **Coaxial Cable**: Used in TV networks and broadband connections.
    - **Fiber Optic Cable**: Uses light signals for high-speed, long-distance communication.

2. Unguided Media (Wireless)

Signals travel through air, water, or vacuum without a physical connection.

- **Examples**:
    - **Radio Waves**: Used for radio, Wi-Fi, and mobile communication.
    - **Microwaves**: Used for long-distance phone and TV transmission.
    - **Infrared**: Used for short-range communication like remote controls.
    - **Light waves**: Used for building-to-building communication via lasers.

GUIDED - WIRED

Types of Transmission Media:

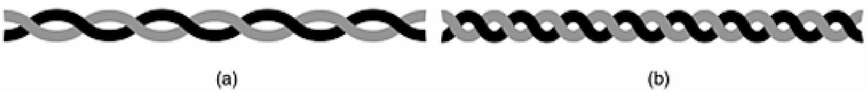
1. Magnetic Media

- Data is physically transferred using devices like tapes or disks.
- Example: A box of tapes can transfer huge data (e.g., 200 TB) faster than some networks for long distances.
- Cost-effective for backups but has a high delay (hours to transport).

2. Twisted Pair

- Commonly used in telephones and computer networks.
- Made of two insulated copper wires twisted to reduce interference.
- **Categories**:
    - **Category 3 (Cat 3):** Basic, supports older systems.
    - **Category 5 (Cat 5):** Better performance with fewer interferences.
    - **Cat 6 and 7:** Higher bandwidth, used for faster networks.
- Affordable and widely used, but prone to interference over long distances.

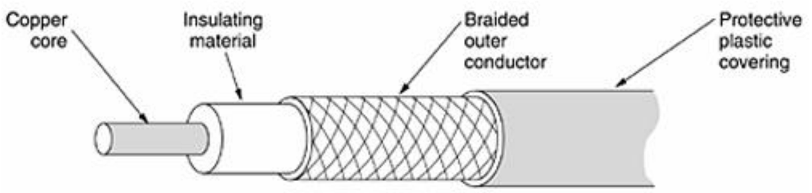
Figure 2-3. (a) Category 3 UTP. (b) Category 5 UTP.



3. Coaxial Cable (co-ax)

- Used in TV cables and some networks.
- Has a central copper core with insulation and shielding for better noise resistance.
- Bandwidth can reach up to 1 GHz.
- Less common now for long distances due to fibre optics replacing it.

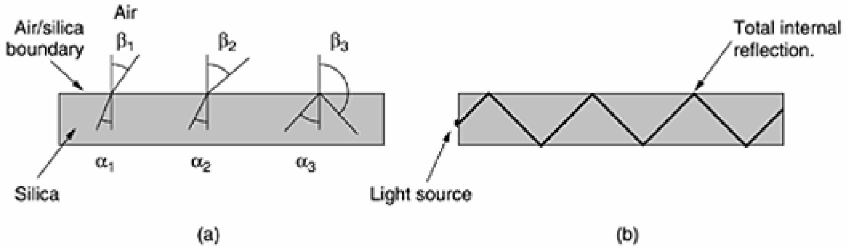
Figure 2-4. A coaxial cable.

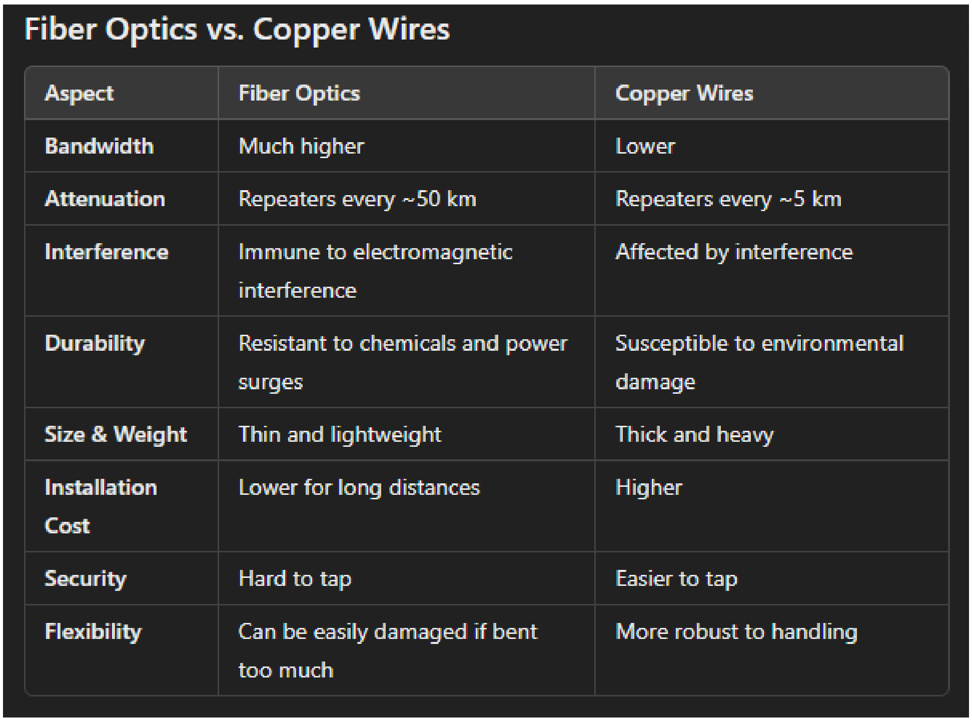


4. Fiber Optics

- Uses glass fibres to transmit light signals.
- **Advantages**:
  - Very high bandwidth (can handle 50 Tbps in theory).
  - Minimal signal loss over long distances.
  - Immune to electromagnetic interference and secure against wiretapping.
- **Drawbacks**:
  - Expensive and delicate.
  - Requires expertise to install and maintain.
- Used in high-speed networks, long-distance communication, and secure environments.

Figure 2-5. (a) Three examples of a light ray from inside a silica fiber impinging on the air/silica boundary at different angles. (b) Light trapped by total internal reflection.





Fiber Optics vs. Copper Wires

Aspect	Fiber Optics	Copper Wires
Bandwidth	Much higher	Lower
Attenuation	Repeaters every ~50 km	Repeaters every ~5 km
Interference	Immune to electromagnetic interference	Affected by interference
Durability	Resistant to chemicals and power surges	Susceptible to environmental damage
Size & Weight	Thin and lightweight	Thick and heavy
Installation Cost	Lower for long distances	Higher
Security	Hard to tap	Easier to tap
Flexibility	Can be easily damaged if bent too much	More robust to handling

Summary of Media Comparison:

- **Twisted Pair:** Low cost, low bandwidth, used for short distances.
- **Coaxial Cable:** Moderate cost, better shielding, suitable for TVs and moderate-speed networks.
- **Fiber Optics:** Expensive but offers unmatched speed, security, and reliability over long distances.

UNGUIDED - WIRELESS

Wireless Transmission Overview

- Wireless communication is crucial for mobile users (e.g., phones, laptops, smart devices) who can't rely on physical cables.
- It uses **electromagnetic waves** for data transmission, which don't require a physical medium.

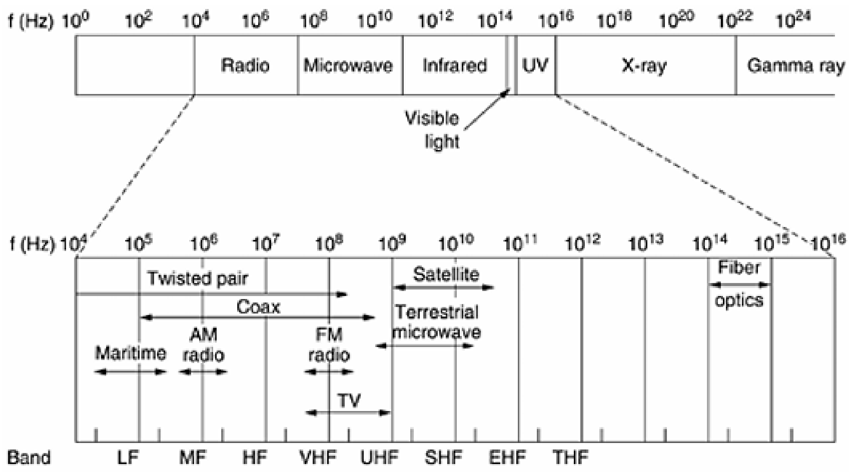
Key Concepts:

Electromagnetic Spectrum

- **Waves** are created by moving electrons which carry data.
- **Frequency (f):** How many wave cycles occur per second (measured in Hertz, Hz).
- **Wavelength (λ):** Distance between wave peaks.

  Related to frequency by $c=f\cdot\lambda$, where c is the speed of light.
- High frequencies = shorter wavelengths = more data capacity.

Figure 2-11. The electromagnetic spectrum and its uses for communication.



Types of Wireless Transmission:

1.Radio Waves

- **Advantages:**
  - Easy to generate and penetrate buildings.
  - Omnidirectional (spread in all directions).
- **Challenges:**
  - Interference from other devices.
  - Limited bandwidth at lower frequencies.

- **Applications:**
  - AM/FM radio, mobile phones, walkie-talkies.
  - Low frequencies travel far
  - high frequencies support more data.

2.Microwave Transmission

- **Characteristics:**
  - Travel straight, focused with antennas (like satellite dishes).
  - Need proper alignment of transmitter and receiver.
  - Cannot pass through buildings.
- **Challenges:**
  - Multipath fading (signals cancel due to delays).
  - Absorption by rain above 4 GHz.
- **Uses:** Widely used in long-distance communication (e.g., mobile phones, TV).

3.Electromagnetic Spectrum Politics

- Governments allocate frequency bands for specific purposes (radio, TV, mobile phones, etc.).
- **Allocation Methods**: Beauty contests, lotteries, or auctions (highest bidder gets rights).
- ISM (Industrial, Scientific, Medical) bands are unlicensed and used for devices like cordless phones and Wi-Fi.

4.Infrared and Millimetre Waves

- **Advantages:**
  - Cheap, directional, and do not pass through walls (no interference with neighbours).
  - Secure for short-range communication.
- **Uses**: Remote controls, connecting devices like printers and laptops.

5.Lightwave Transmission

- Uses lasers for high-speed communication between buildings.
- **Challenges:**
  - Beam alignment is difficult over long distances.
  - Weather conditions like fog or convection currents (hot air rising) can disrupt signals.
- **Example**: Rooftop laser links for temporary networks.

Spread Spectrum Techniques

Techniques to reduce interference:

- **Frequency Hopping:** Rapidly switching frequencies to avoid interference (used in Bluetooth, Wi-Fi).
- **Direct Sequence Spread Spectrum:** Spreads the signal over a wide frequency range (used in mobile networks).

Applications:

- Wireless communication for homes, offices, and cities.
- Key for mobile devices and remote locations.

Challenges:

- Weather sensitivity
- Interference
- spectrum licensing issues.

SAQ- Why are cables twisted together

Cables are twisted together to **reduce electromagnetic interference (EMI)** and **crosstalk**.