Intro, Physical layer - Detailed Notes

Data Communication is defined as exchange of data between two devices via some form of transmission media such as a cable, wire or it can be air or vacuum also. For occurrence of data communication, communicating devices must be a part of communication system made up of a combination of hardware or software devices and programs. Data Communication System Components : There are mainly five components of a data communication system:

1. **Message :** This is most useful asset of a data communication system. The message simply refers to data or piece of information which is to be communicated. A message could be in any form, it may be in form of a text file, an audio file, a video file, etc.

2. **Sender :** To transfer message from source to destination, someone must be there who will play role of a source. Sender plays part of a source in data communication system. It is simple a device that sends data message. The device could be in form of a computer, mobile, telephone, laptop, video camera, or a workstation, etc.

3. **Receiver :** It is destination where finally message sent by source has arrived. It is a device that receives message. Same as sender, receiver can also be in form of a computer, telephone mobile, workstation, etc.

4. Transmission Medium : In entire process of data communication, there must be something which could act as a bridge between sender and receiver, Transmission medium plays that part. It is physical path by which data or message travels from sender to receiver. Transmission medium could be guided (with wires) or unguided (without wires), for example, twisted pair cable, fiber optic cable, radio waves, microwaves, etc.

5. **Set of rules (Protocol) :** To govern data communications, various sets of rules had been already designed by the designers of the communication systems, which represent a kind of agreement between communicating devices. These are defined as protocol. In simple terms, the protocol is a set of rules that govern data communication. If two different devices are connected but there is no protocol among them, there would not be any kind of communication between those two devices. Thus the protocol is necessary for data communication to take place.

   A typical example of a data communication system is sending an e-mail. The user which send email act as sender, message is data which user wants to send, receiver is one whom user wants to send message, there are many protocols involved in this entire process, one of them is Simple Mail Transfer Protocol (SMTP), both sender

and receiver must have an internet connection which uses a wireless medium to send and receive email.

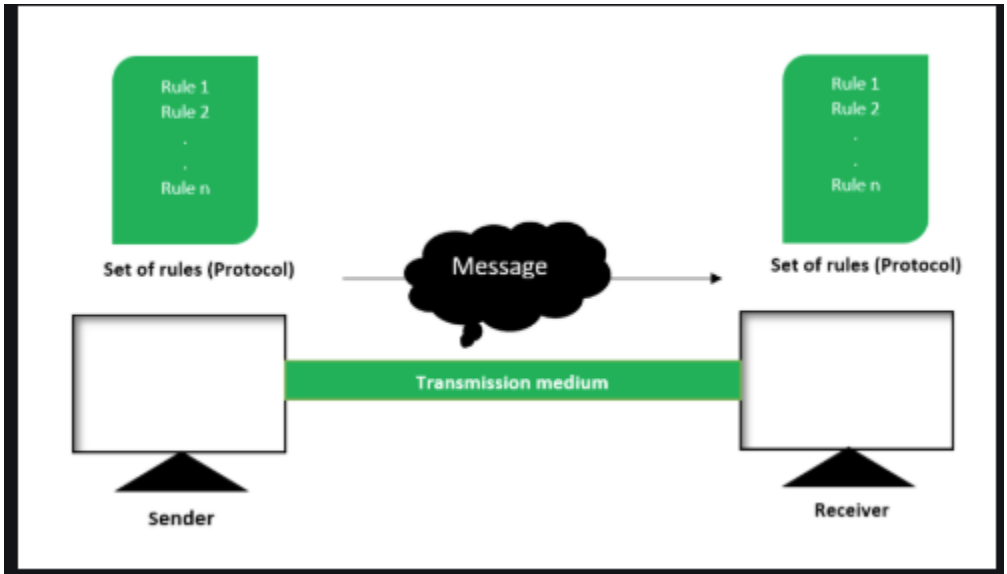


Figure - Components of Data Communication System

📡 Transmission Mode in Data Communication

◇ Definition:

Transmission mode (also known as communication mode) refers to the direction of signal flow between two connected devices in a communication system.

It determines how data is transmitted between the sender and the receiver: one-way, both ways but one at a time, or both ways simultaneously.

🔄 Types of Transmission Modes

There are three main types of transmission modes:

1. 🔘 Simplex Mode

- **Description:**
  - Data flows in **only one direction**.
  - One device is always the **sender**, and the other is always the **receiver**.
  - There is **no feedback** from the receiver.
- **Example:**
  - **Keyboard → Computer**
  - **TV broadcasting**
- **Advantages:**
  - Simple and low cost.
- **Disadvantages:**
  - **No two-way communication**.
  - **No error correction** possible.

---

2. 🌓 Half-Duplex Mode

- **Description:**
  - Data flows in **both directions**, but **one direction at a time**.
  - Devices can both **send and receive**, but **not simultaneously**.
- **Example:**
  - **Walkie-talkies**
  - **CB radios**
- **Advantages:**
  - Less complex than full-duplex.
  - Better utilization than simplex.
- **Disadvantages:**
  - Slower than full-duplex.
  - **Collision risk** if not well managed.

---

3. 🔘 Full-Duplex Mode

- **Description:**
  - Data flows in **both directions simultaneously**.
  - Sender and receiver can **transmit and receive at the same time**.
- **Example:**
  - **Telephones**
  - **Video calls**
  - **Chat applications**
- **Advantages:**
  - **Fastest and most efficient** mode.
  - Real-time communication.
  - Allows **error detection and correction**.
- **Disadvantages:**
  - More **complex and expensive** to implement.
  - Requires **more bandwidth**.

Networks and Various Connections

✅ **Definition**:
A **Computer Network** is an interconnection of multiple computing devices (computers, servers, printers, smartphones, etc.) that are linked together to share resources and exchange information.

🔗 **Key Features:**

- **Sharing of Resources** (printers, files, applications)
- **Communication** (emails, messages, video calls)
- **Data Access and Management**
- **Scalability and Flexibility**

Connections can be point-to-point or multipoint.

Types of networks: PAN (Personal Area Network), LAN (Local Area Network), MAN (Metropolitan Area Network), WAN (Wide Area Network).

Topology

What is Network Topology?

Network topology is the way devices are connected in a network. It defines how these components are connected and how data transfer between the network. Understanding the different types of network topologies can help in choosing the right design for a specific network.

There are two major categories of Network Topology i.e. Physical Network topology and Logical Network Topology. Physical Network Topology refers to the actual structure of the physical medium for the transmission of data. Logical network Topology refers to the transmission of data between devices present in the network irrespective of the way devices are connected. The structure of the network is important for the proper functioning of the network. one must choose the most suitable topology as per their requirement.

Types of Network Topology

Below mentioned are the types of Network Topology(see Kg pag no 20 to 26)

- Point to Point Topology
- Mesh Topology
- Star Topology
- Bus Topology
- Ring Topology
- Tree Topology
- Hybrid Topology

Difference between Physical and Logical Topology

Physical Topology	Logical Topology
Depicts physical layout of network.	Depicts logistics of network concerned with transmission of data.
The layout can be modified based on needs.	There is no interference and manipulation involved here.
This has major impact on cost, scalability and bandwidth capacity of network based on selection and availability of devices.	This has major impact on speed and delivery of data packets. It also handles flow control and ordered delivery of data packets.
It is actual route concerned with transmission.	It is a high level representation of data flow.
Physical connection of the network.	Data path followed of the network.

Protocols and Standards

☑ What is a Protocol?

A protocol is a set of rules and conventions that govern the communication between devices over a network.

💡 It defines how data is formatted, transmitted, and received to ensure successful communication.

🔑 Functions of Protocols

- Data encapsulation & formatting
- Addressing and routing
- Error detection and correction
- Flow control
- Session management

🔄 Common Protocols in Networking

Protocol	Full Form	Purpose
TCP	Transmission Control	Reliable, connection-oriented data

Protocol	Full Form	Purpose
	Protocol	delivery
IP	Internet Protocol	Addressing and routing of data
HTTP	HyperText Transfer Protocol	Web communication (browsing websites)
HTTPS	HTTP Secure	Secure web communication
FTP	File Transfer Protocol	Transfer of files between systems
SMTP	Simple Mail Transfer Protocol	Sending emails
POP3/IMAP	Post Office Protocol / IMAP	Receiving and managing emails
DNS	Domain Name System	Converts domain names to IP addresses
DHCP	Dynamic Host Configuration	Assigns IP addresses automatically
UDP	User Datagram Protocol	Fast, connectionless transmission (e.g., VoIP)
SNMP	Simple Network Management	Network monitoring and management

Protocol	Full Form	Purpose
ICMP	Internet Control Message	Diagnostics (e.g., ping)

☑ **What are Standards?**

Standards are documented agreements or specifications established by recognized organizations to ensure interoperability between different systems and devices.

💡 Standards ensure that equipment from different manufacturers can work together on a network.

📚 Types of Standards

1. De facto Standard
    - Developed through common usage and widespread acceptance.
    - Not officially approved by a standards body.
    - 📌 Example: HTML, early Ethernet.
2. De jure Standard

- Legally approved and published by recognized standards organizations.
- 📌 Example: IEEE 802.3 (Ethernet), ITU standards.

🏛 Major Standard Organizations

Organization	Full Form	Role
ISO	International Organization for Standardization	Develops international standards
IEEE	Institute of Electrical and Electronics Engineers	Sets LAN/MAN standards (e.g., IEEE 802)
IETF	Internet Engineering Task Force	Develops and promotes internet protocols (e.g., TCP/IP)
ITU-T	International Telecommunication Union – Telecommunication	Develops telecommunication standards
ANSI	American National Standards Institute	Coordinates U.S. standards with global standards
W3C	World Wide Web Consortium	Standards for the web (HTML, CSS, XML, etc.)

📌 Why Protocols and Standards Are Important

- Enable interoperability between different hardware/software.
- Ensure reliability and security of communication.
- Promote scalability and compatibility of networks.
- Support efficient data transmission and network management.

OSI Model

📌 **Definition:**

The **OSI Model** is a **conceptual framework** developed by **ISO (International Organization for Standardization)** that standardizes the **functions of a telecommunication or computing system** into **seven abstract layers**.

🧩 Each layer serves a **specific purpose** and communicates with the **layers above and below** it.

📚 **7 Layers of the OSI Model (Bottom to Top)**

Layer Number	Layer Name	Function Summary
7	Application Layer	End-user interface, services like email, HTTP
6	Presentation Layer	Data format translation, encryption, compression
5	Session Layer	Session establishment, management, termination
4	Transport Layer	End-to-end delivery, error checking, flow control
3	Network Layer	Logical addressing, routing (IP)
2	Data Link Layer	Physical addressing, error detection (MAC)

Layer Number	Layer Name	Function Summary
1	Physical Layer	Transmission of bits over media

🔍 Layer-by-Layer Explanation

🔴 1. Physical Layer (Layer 1)

- **Function**: Transmits **raw bits** over a physical medium.
- **Deals with**: Voltage levels, timing, cables, connectors.
- **Devices**: Hubs, Repeaters, Cables.
- **Protocols**: Ethernet (physical specs), DSL, RS-232.

🟠 2. Data Link Layer (Layer 2)

- **Function**: Responsible for **node-to-node delivery** and **error detection**.
- **Divided into**:
  - **MAC (Media Access Control)**: Controls access to the physical medium.
  - **LLC (Logical Link Control)**: Error and flow control.
- **Devices**: Switches, Bridges.
- **Protocols**: Ethernet, PPP, Frame Relay.

🟡 3. Network Layer (Layer 3)

- **Function**: **Routes data** from source to destination across multiple networks.
- **Responsible for**: IP addressing and path selection.
- **Devices**: Routers.
- **Protocols**: IP (IPv4/IPv6), ICMP, ARP.

🟢 **4. Transport Layer (Layer 4)**

- **Function**: Ensures **reliable data transfer**, flow control, and error recovery.
- **Can be**:
  - **Connection-oriented** (TCP)
  - **Connectionless** (UDP)
- **Protocols**: TCP, UDP.

5. Session Layer (Layer 5)

- **Function**: Manages **sessions** between applications.
- **Responsible for**: Session setup, maintenance, and termination.
- **Examples**: API sessions, remote procedure calls (RPC).

🟣 **6. Presentation Layer (Layer 6)**

- **Function**: **Formats data** for the application layer.
- **Handles**: Encryption, decryption, compression, translation (e.g., ASCII to EBCDIC).
- **Examples**: SSL/TLS, JPEG, MPEG, GIF, XML.

⚫ **7. Application Layer (Layer 7)**

- **Function**: Closest to the user; provides **network services** to applications.
- **Examples**: Browsers, email clients, file transfer apps.
- **Protocols**: HTTP, FTP, SMTP, DNS, Telnet.

🎓 **Mnemonic to Remember OSI Layers**

From Layer 7 to 1:

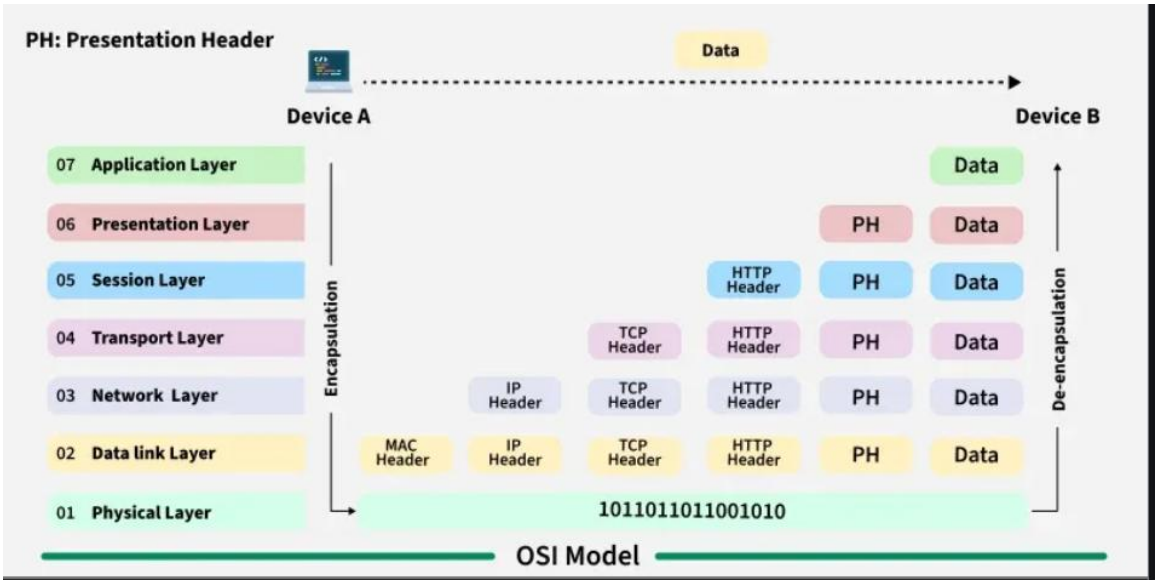
📚 "**All People Seem To Need Data Processing**"

From Layer 1 to 7:

📘 "**Please Do Not Throw Sausage Pizza Away**"

📌 Importance of OSI Model

- Encourages **modular design** and **standardization**.
- Aids in **troubleshooting** network issues layer by layer.
- Facilitates **interoperability** between vendors.
- Helps developers and engineers understand **data flow**.



TCP/IP Model (Transmission Control Protocol/Internet Protocol)

The **TCP/IP model** is a conceptual framework used to understand and design how data is transmitted over a network. It is the foundation of the modern Internet and is more practical than the OSI model.

It's composed of four interconnected layers compared to the seven layers in the OSI model. Each layer performs a specific task on the data that is being transmitted over the network channel, and data moves from one layer to another.

- Application Layer
- Transport Layer(TCP/UDP)
- Network/Internet Layer(IP)
- Network Access Layer

1. Application Layer

The Application Layer is the closest to the end user and is where applications and user interfaces reside. It serves as the bridge between user programs and the lower layers responsible for data transmission.

- **Function:** Provides services and interfaces for end-user applications to access network resources.
- **Key responsibilities:**
    - Supports application protocols like HTTP, FTP, SMTP, DNS, etc.
    - Enables communication between software applications across networks.
    - Handles data formatting, encryption, and session management.

2. Transport Layer

This layer ensures data is delivered reliably and in the correct order between devices. The two main protocols in this layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

- **Function:** Ensures reliable or unreliable delivery of data between hosts.
- **Key responsibilities:**
    - TCP (Transmission Control Protocol): Provides reliable, connection-oriented delivery with error checking, retransmission, and flow control.
    - UDP (User Datagram Protocol): Provides faster, connectionless transmission without guarantees.
    - Manages flow control and segmentation/reassembly of data.

3. Internet Layer

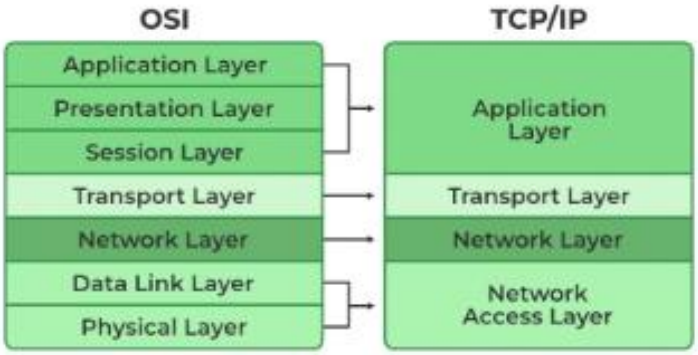
It handles the routing of data packets across networks. It uses the Internet Protocol (IP) to assign unique IP addresses to devices and decide the most efficient path for data to reach its destination.

- **Function:** Determines the best path for data to travel across networks.
- **Key responsibilities:**
    - IP (Internet Protocol)**:** Provides addressing and routing.
    - Handles packet forwarding, fragmentation, and logical addressing (IP addresses).
    - Involves protocols like IP, ICMP (for diagnostics), and ARP (for address resolution).

4. Network Access Layer

This layer is the lowest layer in the model and responsible for the physical connection between devices within the same network segment.

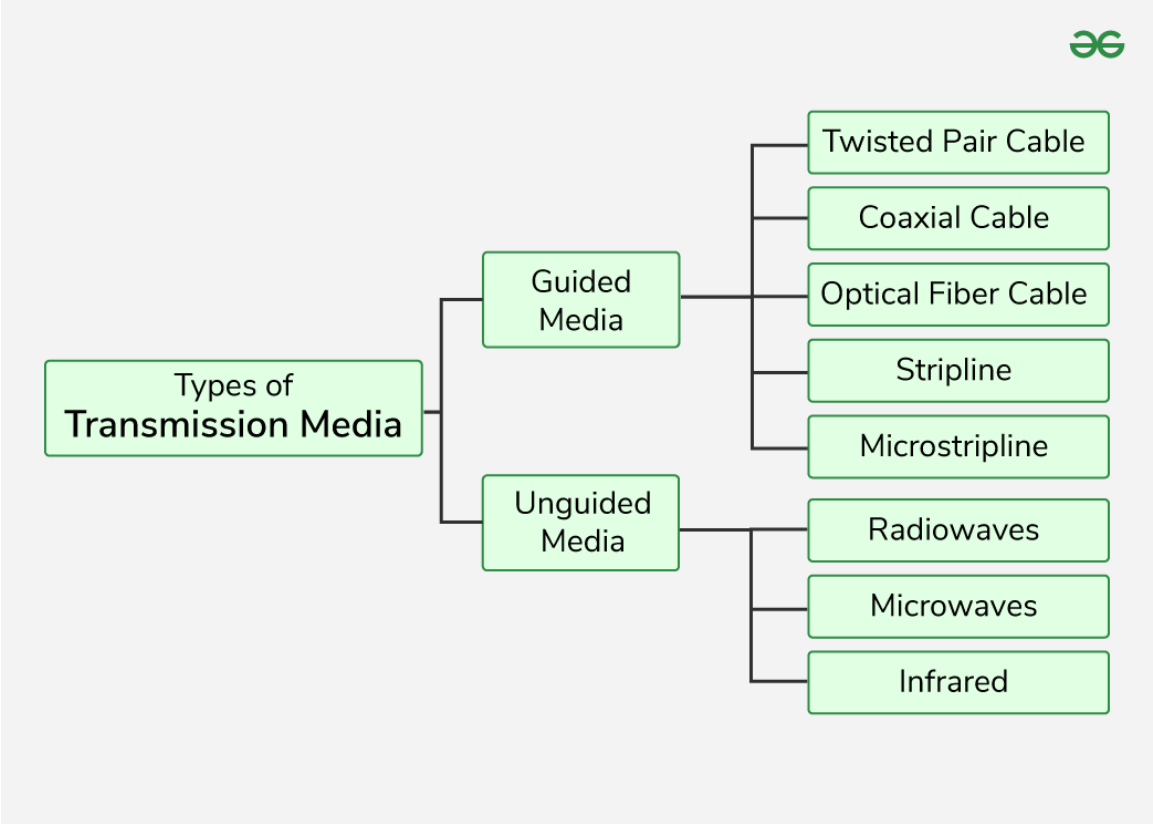
- **Function:** Manages the physical transmission of data over the network hardware.
- **Key responsibilities:**
    - Handles how data is physically sent over cables, Wi-Fi, etc.
    - Manages MAC addressing, framing, and error detection at the physical link.
    - Includes Ethernet, Wi-Fi, and other data link technologies.



OSI Model	TCP/IP Model
OSI stands for Open Systems Interconnection.	TCP/IP stands for Transmission Control Protocol/Internet Protocol.
OSI model has 7 layers.	TCP/IP model consists of 4 layers.
Package delivery is guaranteed in OSI Model.	Package delivery is not guaranteed in the TCP/IP Model.
In the OSI model, only layers 1,2 and 3 are necessary for data transmission.	All layers of the TCP/IP model are needed for data transmission.
Protocols at each layer is independent of the other layer.	Layers are integrated; some layers are required by other layers of TCP/IP model.
OSI Model is a conceptual framework, less used in practical applications.	Widely used in actual networks like Internet and Communication Systems.

Transmission Media

A transmission media is a physical path between the transmitter and the receiver i.e. it is the path along which data is sent from one device to another. Transmission Media is broadly classified into the following types:



Types of Transmission Media

1. Guided Media

Guided Media is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.

Features:

- High Speed

- Secure
- Used for comparatively shorter distances

There are 3 major types of Guided Media:

Twisted Pair Cable

It consists of 2 separately insulated conductor wires twisted about each other. Generally, several such pairs are bundled together in a protective sheath. They are the most widely used Transmission Media. Twisted Pair is of two types:

- Unshielded Twisted Pair (UTP):UTP consists of two insulated copper wires twisted around one another. This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.

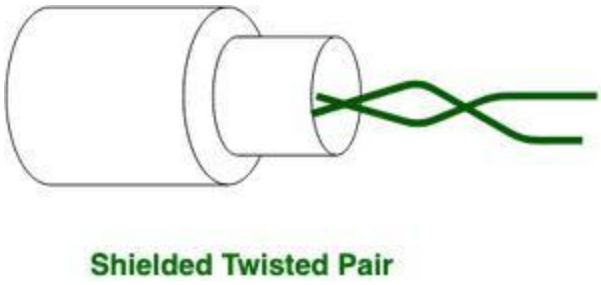
Unshielded Twisted Pair

Advantages of Unshielded Twisted Pair

- Least expensive
- Easy to install
- High-speed capacity

Disadvantages of Unshielded Twisted Pair

- Lower capacity and performance in comparison to STP
- Short distance transmission due to attenuation



Shielded Twisted Pair

Shielded Twisted Pair (STP): Shielded Twisted Pair (STP) cable consists of a special jacket (a copper braid covering or a foil shield) to block external interference. It is used in fast data rate Ethernet and in voice and data channels of telephone lines.

Advantages of Shielded Twisted Pair

- Better performance at a higher data rate in comparison to UTP
- Eliminates crosstalk
- Comparatively faster

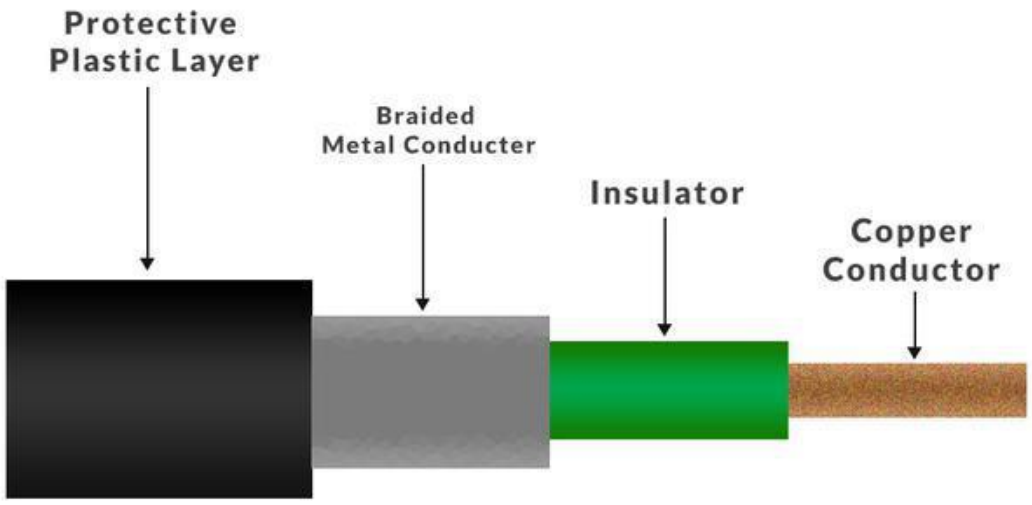
Disadvantages of Shielded Twisted Pair

- Comparatively difficult to install and manufacture
- More expensive

- Bulky

Coaxial Cable

Coaxial cable has an outer plastic covering containing an insulation layer made of PVC or Teflon and 2 parallel conductors each having a separate insulated protection cover. The coaxial cable transmits information in two modes: Baseband mode(dedicated cable bandwidth) and Broadband mode(cable bandwidth is split into separate ranges). Cable TVs and analog television networks widely use Coaxial cables.



Advantages of Coaxial Cable

- Coaxial cables has high bandwidth .
- It is easy to install.
- Coaxial cables are more reliable and durable.
- Less affected by noise or cross-talk or electromagnetic inference.

- Coaxial cables support multiple channels

Disadvantages of Coaxial Cable

- Coaxial cables are expensive.
- The coaxial cable must be grounded in order to prevent any crosstalk.
- As a Coaxial cable has multiple layers it is very bulky.
- There is a chance of breaking the coaxial cable and attaching a “t-joint” by hackers, this compromises the security of the data.

Optical Fiber Cable

Optical Fibre Cable uses the concept of total internal reflection of light through a core made up of glass. The core is surrounded by a less dense glass or plastic covering called the coating. It is used for the transmission of large volumes of data. The cable can be unidirectional or bidirectional. The WDM (Wavelength Division Multiplexer) supports two modes, namely unidirectional and bidirectional mode.

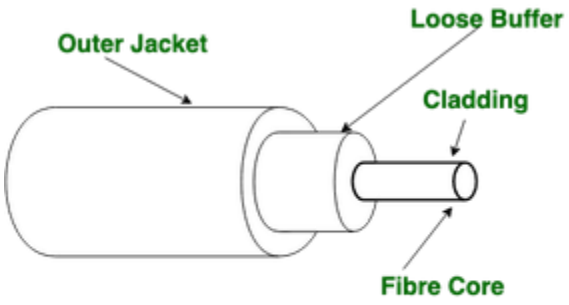


Figure of Optical Fibre Cable

Advantages of Optical Fibre Cable

- Increased capacity and bandwidth
- Lightweight
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials

Disadvantages of Optical Fibre Cable

- Difficult to install and maintain
- High cost

Applications of Optical Fibre Cable

- Medical Purpose: Used in several types of medical instruments.
- Defence Purpose: Used in transmission of data in aerospace.
- For Communication: This is largely used in formation of internet cables.
- Industrial Purpose: Used for lighting purposes and safety measures in designing the interior and exterior of automobiles.

LAN: Wired and Wireless

Networks can be classified based on their geographical coverage area. Here are the main types:

---

1. 🏠 PAN (Personal Area Network)

- **Coverage:** Very small area, typically a few meters (within a room).
- **Purpose:** Connects personal devices such as smartphones, tablets, laptops, and wearable devices.
- **Technology:** Bluetooth, Infrared, USB.
- **Example:** Wireless connection between a smartphone and a Bluetooth headset.

Advantages:

- Convenient for personal device communication.
- Low power consumption.

Disadvantages:

- Limited range.
- Limited number of devices.

---

2. 🏢 LAN (Local Area Network)

- **Coverage:** Small geographical area such as a home, office, or building.
- **Purpose:** Connects computers and devices within a local area to share resources like files, printers, and internet access.
- **Technology:** Ethernet, Wi-Fi.
- **Example:** Network within an office or school building.

Advantages:

- High data transfer speed.
- Easy resource sharing.
- Low setup cost.

Disadvantages:

- Limited to small areas.
- Requires physical infrastructure (cables, switches).

---

3. 🌆 MAN (Metropolitan Area Network)

- **Coverage:** Covers a city or metropolitan area (several kilometers to tens of kilometers).
- **Purpose:** Connects multiple LANs within a city to form a bigger network.
- **Technology:** Fiber optics, microwave links.
- **Example:** City-wide Wi-Fi networks, cable TV networks.

Advantages:

- Covers larger area than LAN.
- Useful for connecting several LANs.

Disadvantages:

- More complex and costly than LAN.
- Requires specialized equipment.

---

4. 🌍 WAN (Wide Area Network)

- **Coverage:** Very large geographic area, spanning countries or continents.
- **Purpose:** Connects multiple LANs and MANs over long distances.
- **Technology:** Internet, leased lines, satellite links.
- **Example:** The Internet is the largest WAN.

Advantages:

- Connects remote locations globally.
- Supports long-distance communication.

Disadvantages:

- Expensive to set up and maintain.
- Slower data transfer compared to LAN/MAN.

---

5. 🏫 CAN (Campus Area Network)

- **Coverage:** Limited to a campus like a university, industrial complex, or military base.
- **Purpose:** Connects multiple LANs within a campus for resource sharing.
- **Example:** University campus network.

Advantages:

- Efficient communication within campus.
- Easier to manage than WAN.

Disadvantages:

- Limited to campus size.
- Infrastructure cost.

---

6. 🏢 SAN (Storage Area Network)

- **Coverage:** Network dedicated to storage devices.
- **Purpose:** Provides block-level storage to servers.
- **Technology:** Fibre Channel, iSCSI.
- **Example:** Data centers using SAN for centralized storage.

Advantages:

- High-speed data access.
- Scalable and centralized storage management.

Disadvantages:

- Expensive setup.
- Complex management.

Encoding Techniques in Data Communication

Introduction

Encoding is the process of converting data — such as characters, symbols, or alphabets — into a specified format suitable for secure and efficient transmission over communication channels. Decoding is the reverse process, where the received encoded signal is converted back into the original data.

Data Encoding

Encoding involves representing binary data (1s and 0s) using various voltage or current patterns on the transmission medium. This representation ensures reliable data transfer between sender and receiver.

Common Types of Line Encoding

- Unipolar
- Polar
- Bipolar
- Manchester

Categories of Encoding Techniques

Based on the nature of data conversion, encoding techniques can be classified as follows:

1. Analog Data to Analog Signals

Uses modulation techniques to convert analog data into modulated analog signals.

- Amplitude Modulation (AM)
- Frequency Modulation (FM)
- Phase Modulation (PM)

---

2. Analog Data to Digital Signals

Known as digitization, this process converts analog signals into digital signals using techniques such as:

- Pulse Code Modulation (PCM): Sampling + Quantization + Encoding.
- Delta Modulation (DM): A simpler alternative to PCM with better performance in some cases.

---

3. Digital Data to Analog Signals

Modulates digital data onto analog carriers using methods like:

- Amplitude Shift Keying (ASK)
- Frequency Shift Keying (FSK)
- Phase Shift Keying (PSK)

---

4. Digital Data to Digital Signals

Maps digital bits to digital signals using line encoding schemes.

Detailed Digital-to-Digital Encoding Techniques

Non-Return to Zero (NRZ)

- Represents '1' as a high voltage and '0' as a low voltage.
- Voltage level remains constant during the bit interval.
- No signal transition if consecutive bits are the same, which may cause synchronization issues.

Variations:

- NRZ-L (Level): Polarity changes only when the bit value changes.
- NRZ-I (Inverted): A transition occurs at the beginning of a bit interval if the bit is '1'; no transition for '0'.

Disadvantage: Long sequences of 0s or 1s cause clock synchronization problems, often requiring a separate clock line.

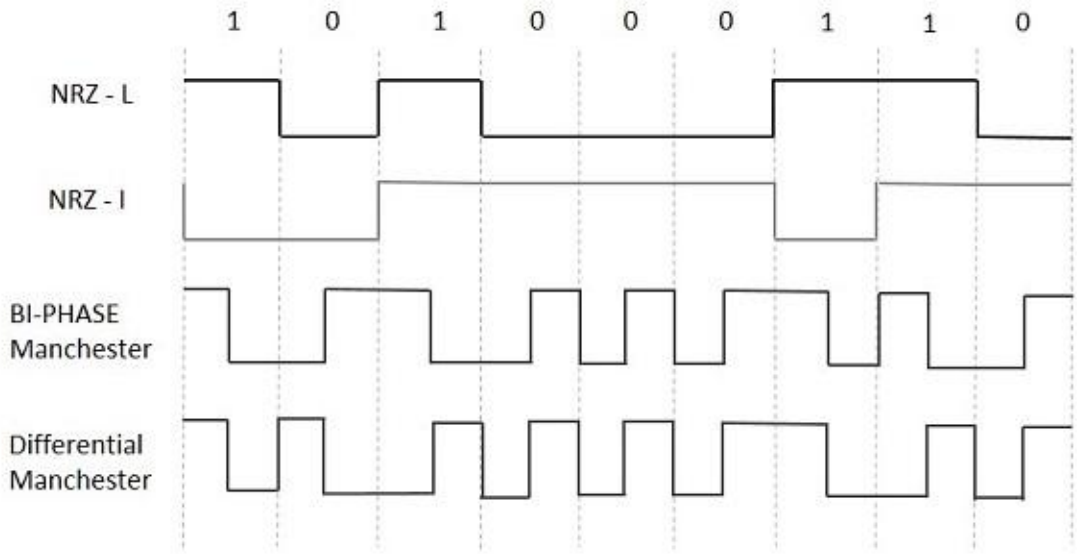
Bi-Phase Encoding

In this method, the signal is checked twice during each bit interval (start and middle), effectively doubling the clock rate and bandwidth.

Two main types:

- Bi-phase Manchester Encoding:
    - Transition in the middle of the bit interval.
    - '1' is represented by a high-to-low transition.

    - '0' is represented by a low-to-high transition.
    - Self-clocking, easy synchronization.
- Differential Manchester Encoding:
    - Always a transition at the middle of the bit interval.
    - Transition at the beginning of the bit interval indicates '0'.
    - No transition at the beginning indicates '1'.



Digital Modulation Techniques: QPSK, QAM, FSK

---

1. QPSK (Quadrature Phase Shift Keying)

- A phase modulation technique that conveys data by changing the phase of the carrier wave.
- Uses 4 different phase shifts to represent 2 bits per symbol: 00, 01, 10, 11.
- Each symbol represents 2 bits, effectively doubling the data rate compared to BPSK (which uses 1 bit per symbol).
- Phases typically: 0°, 90°, 180°, 270°.

Advantages:

- Efficient bandwidth usage (transmits 2 bits per symbol).
- Better noise immunity than ASK.
- Widely used in wireless and satellite communications.

Disadvantages:

- More complex receiver design than BPSK.
- Sensitive to phase noise and synchronization errors.

---

2. QAM (Quadrature Amplitude Modulation)

- Combines both amplitude and phase modulation.
- Data is encoded by changing both the amplitude and phase of the carrier wave.
- Common QAM types: 16-QAM, 64-QAM, 256-QAM, where the number represents the total possible symbols (4 bits, 6 bits, 8 bits per symbol respectively).
- Each symbol represents multiple bits (e.g., 16-QAM = 4 bits per symbol).

Advantages:

- Very high spectral efficiency (transmits many bits per symbol).
- Used in modern broadband systems (Wi-Fi, LTE, cable modems).

Disadvantages:

- More sensitive to noise and distortion due to amplitude variation.
- Requires higher signal-to-noise ratio (SNR) for reliable communication.

---

3. FSK (Frequency Shift Keying)

- A frequency modulation technique where digital data is transmitted through discrete frequency changes of the carrier signal.
- Binary FSK uses two frequencies: one for ‘0’ and another for ‘1’.
- Variants include BFSK (binary FSK), MFSK (multiple frequencies for multiple bits).

Advantages:

- Simple to implement.
- Robust to noise, better than ASK.
- Used in low-speed data transmissions like RFID, caller ID.

Disadvantages:

- Requires more bandwidth than PSK or QAM.
- Lower spectral efficiency compared to phase or amplitude modulation.

Techniques for Bandwidth Utilization: Multiplexing

Multiplexing is the sharing of a medium or bandwidth. It is the process in which multiple signals coming from multiple sources are combined and transmitted over a single communication/physical line. **Multiplexing in computer networks** is done using a device Multiplexer called MUX that takes 'n' input lines to generate a single output line. On the other hand, there is a device called DEMUX(Demultiplexer) that takes a single input line and generates 'n' output lines.

The 'n' input lines shown above are transmitted via a multiplexer and it combines the signals to form a composite signal. Now, these signals are passed through DEMUX and it transfers those signals to their respective destinations.

Types of Multiplexing in Computer Networks

Multiplexing can be classified as:

- Frequency Division Multiplexing (FDM)
- Time-Division Multiplexing (TDM)
- Wavelength Division Multiplexing (WDM)

TDM	FDM
TDM stands for Time division multiplexing.	FDM stands for Frequency division multiplexing.
TDM works with digital signals as well as analog signals.	While FDM works with only analog signals.
TDM has low conflict.	While it has high conflict.
Wiring or chip of TDM is simple.	While it's wiring or chip is complex rather than simple.
TDM is efficient.	While it is inefficient.
In TDM, time sharing takes place.	While in this, frequency sharing takes place.
In TDM, synchronization pulse is necessary.	While in it Guard band is necessary.

ORGANISER SPECIAL PROBLEMS:

1. ❌ Disadvantages of NRZ Encoding:

1. **Lack of Synchronization:**
    - Long sequences of 0s or 1s lead to no voltage changes.
    - This makes it difficult for the receiver to detect bit boundaries (where one bit ends and the next begins).
    - Causes **loss of synchronization** between transmitter and receiver.
2. **No Clock Information:**
    - NRZ signals do **not contain clock information**.
    - External clocking is required for synchronization, which increases complexity.
3. **Baseline Wander:**
    - Continuous stream of similar bits may shift the average voltage level.
    - This can lead to difficulty in determining what voltage level represents 0 or 1.
4. **DC Component:**
    - Long periods of constant voltage introduce a **DC component**.
    - Not suitable for systems that use AC coupling or magnetic media (e.g., audio tape, some communication channels).

2.How RZ (Return to Zero) Encoding Solves These Problems:

Advantages of RZ over NRZ:

1. Better Synchronization:
    - Frequent transitions (returning to zero) help receivers stay synchronized.
    - Easier to detect bit boundaries.
2. Clear Clock Recovery:
    - The regular return to zero helps in clock extraction from the data stream.
3. Less DC Component:
    - Because the signal returns to zero often, it reduces the average DC level.
    - Better for channels that cannot pass DC signals.

3.Standard Sampling Rate for Human Voice:

- For **telephone-quality audio**, the standard sampling rate is **8000 samples per second** (8 kHz).
  This is sufficient because human speech typically ranges from 300 Hz to 3400 Hz.

🎛️ **Bit Rate Calculation:**

$$\text{Bit Rate} = \text{Sampling Rate} \times \text{Bits per Sample}$$

$$= 8000 \text{ samples/second} \times 8 \text{ bits/sample} = \boxed{64,000 \text{ bps } (64kbps)}$$

4.🛰️ FDM (Frequency Division Multiplexing) – for Analog Signals

📌 **Why FDM is suited for Analog:**

1. **Analog Nature of Carriers:**
   - Analog signals can be modulated to different frequency bands (using AM, FM, etc.).
   - FDM assigns **a unique frequency band** (channel) to each analog signal.
   - These channels are combined and transmitted simultaneously over a single medium.
2. **Continuous Transmission:**
   - Analog signals are **continuous** in nature.
   - FDM allows continuous transmission without needing synchronization between users.
3. **Examples:**
   - **Radio broadcasting** (different stations at different frequencies)
   - **Cable TV**
   - **Traditional telephone networks**

⏱️ **TDM (Time Division Multiplexing) – for Digital Signals**

📌 **Why TDM is suited for Digital:**

1. **Discrete Time Slots:**
    - Digital signals consist of **discrete bits or symbols**.
    - TDM assigns a **time slot** to each signal in a round-robin fashion.
    - In each time slot, the signal sends its data bits.
2. **Precise Synchronization:**
    - Digital systems can be **easily synchronized**, making time slot allocation possible.
    - Clock signals ensure correct interpretation of bits in correct time slots.
3. **Efficient for Digital Circuits:**
    - TDM matches well with digital electronics and processors.
    - No need for guard bands (as in FDM), so bandwidth is used more efficiently.
4. **Examples:**
    - **Digital telephony (e.g., T1/E1 lines)**
    - **Computer networks**
    - **Digital TV broadcasting**

5. 📘 **1. Signaling Rate (Symbol Rate or Baud Rate)**

- It is the **number of signal changes (symbols)** transmitted **per second** in a communication channel.
- Measured in **baud** (symbols per second).
- Each symbol may represent **one or more bits**, depending on the modulation technique.

🧠 **Example**: If one symbol carries 2 bits, and the signaling rate is 1000 baud, then the bit rate is 2000 bps.

📘 **2. Guard Band**

- A **small frequency band** left unused between two frequency channels in **FDM systems**.

- Prevents **overlapping** and **interference** between adjacent channels.
- Acts as a **buffer zone** to ensure clear signal separation.

🧠 **Example**: In FM radio, stations are spaced apart by guard bands to avoid mixing signals.

📘 **3. Bandwidth of Media**

- Refers to the **capacity of a transmission medium** to carry data.
- Measured in **Hz (for analog)** or **bps (for digital)**.
- The **greater the bandwidth**, the **more data** can be transmitted in a given time.

🧠 **Example**: A cable with a bandwidth of 100 MHz can carry more data than one with 10 MHz.

📘 **4. Bit Rate**

- The **number of bits transmitted** per second.
- Measured in **bps (bits per second)**.
- Directly related to **data speed** and **efficiency**.

🧠 **Example**: A 1 Mbps link can transmit 1 million bits per second.

📘 **5. Baud Rate (Symbol Rate)**

- Baud rate = Number of **symbols/changes per second**.
- May or may not be equal to bit rate, depending on **how many bits each symbol represents**.

🧠 **Example**:

- If 1 symbol = 1 bit → baud rate = bit rate
- If 1 symbol = 2 bits → bit rate = 2 × baud rate

📘 **6. Inverse TDM (ITDM)**

- A **variant of Time Division Multiplexing**.
- Instead of combining multiple low-speed inputs into one high-speed channel (as in regular TDM), **Inverse TDM splits a high-speed data stream into multiple low-speed channels**.
- Used when **a single high-bandwidth line is unavailable**, but multiple lower-bandwidth lines are.

🧠 **Example**: Splitting a 10 Mbps stream across five 2 Mbps lines.

📘 7. Baseband Transmission

- Uses the **entire bandwidth** of the channel to send **a single signal at a time**.
- Transmits **digital signals** directly.
- Requires **time-division** or some switching method if multiple users share the channel.

✅ **Used in:** Ethernet LANs

🧠 **Example**: Sending digital data over a coaxial cable without converting it to analog.

📘 8. Broadband Transmission

- Allows **multiple signals** to be transmitted **simultaneously** using **different frequency ranges** (FDM).
- Suitable for **analog signals** or **digitally modulated analog signals**.

✅ **Used in:** Cable TV, DSL

🧠 **Example**: Watching multiple cable TV channels simultaneously.

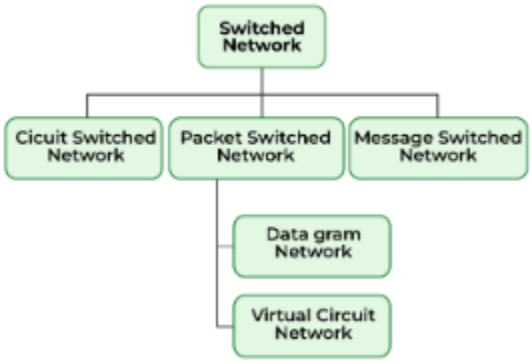
🔁 What is Switching?

Switching is the process of **forwarding data** (packets, messages, or signals) from a source to a destination across a network using **intermediate devices** like switches or routers.

It enables **efficient use of network resources** by dynamically choosing paths for data based on availability and performance.

🧭 Why Switching is Needed?

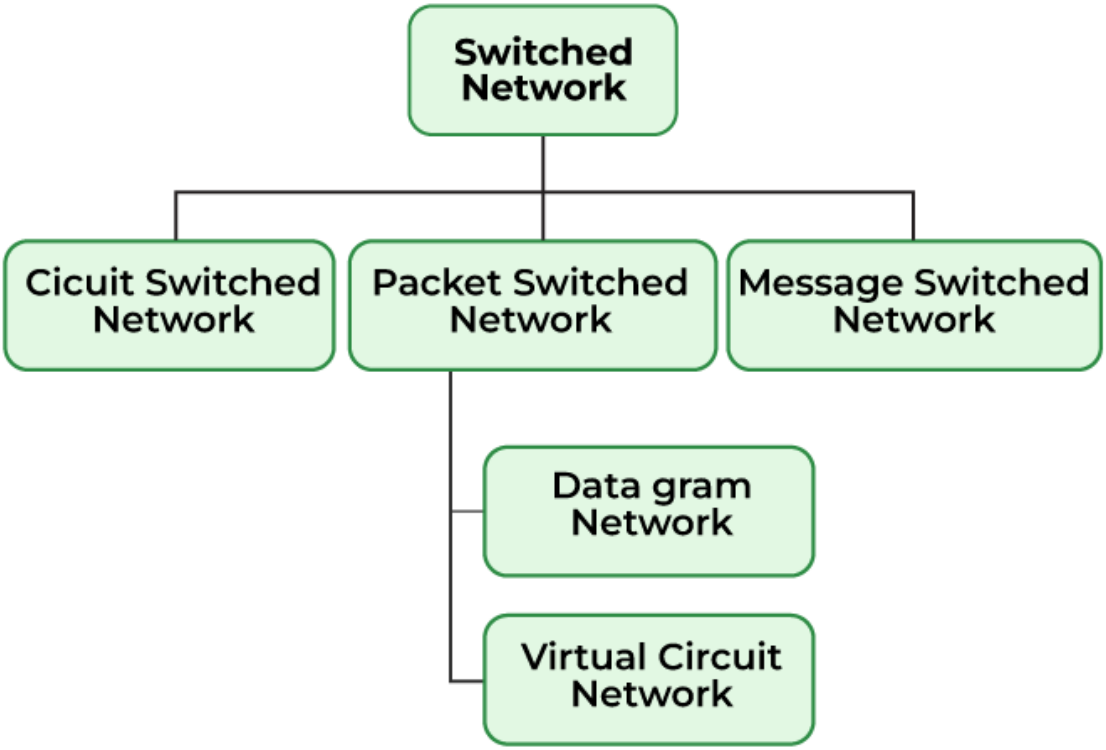
- Direct connection between every sender and receiver is impractical.
- Reduces the number of required communication links.
- Manages traffic efficiently in **large networks**.
- Allows **multiple communications** simultaneously.



Types of Switching

There are three types of switching methods:

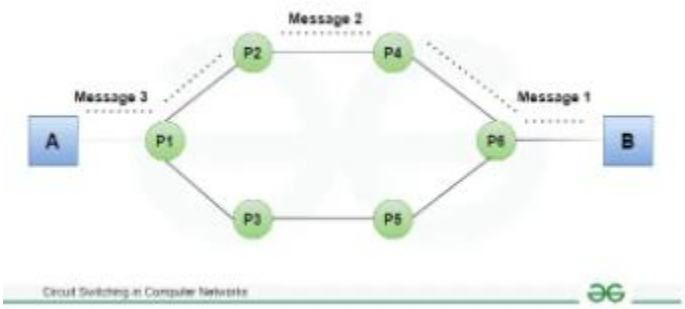
- Message Switching
- Circuit Switching
- Packet Switching
    - Datagram Packet Switching
    - Virtual Circuit Packet Switching



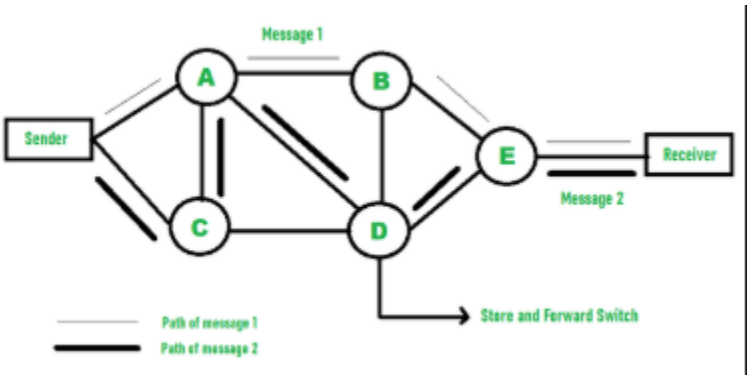
Let us now discuss them individually:

Message Switching: This is an older switching technique that has become obsolete. In message switching technique, the entire data block/message is forwarded across the entire network thus, making it highly inefficient.

Circuit Switching: In this type of switching, a connection is established between the source and destination beforehand. This connection receives the complete bandwidth of the network until the data is transferred completely.
This approach is better than message switching as it does not involve sending data to the entire network, instead of its destination only.



Packet Switching: This technique requires the data to be broken down into smaller components, data frames, or packets. These data frames are then transferred to their destinations according to the available resources in the network at a particular time. This switching type is used in modern computers and even the Internet. Here, each data frame contains additional information about the destination and other information required for proper transfer through network components.



📦 Difference Between Datagram and Virtual Circuit Switching

Aspect	Datagram Packet Switching	Virtual Circuit Packet Switching
Connection Setup	❌ No connection is established before sending data.	✅ A logical connection is established before data transfer.
Routing	Each packet is routed independently.	All packets follow the same predetermined path.
Packet Sequence	Packets may arrive **out of order.**	Packets arrive **in the correct order.**
Reliability	Less reliable; extra effort needed at receiver for ordering.	More reliable; order is preserved automatically.
Overhead	More routing information (header) in each packet.	Less overhead; only virtual circuit ID is needed.
Error Handling	Handled at the receiver side.	Easier error detection and correction due to fixed path.
Efficiency	Better for bursty data and dynamic networks.	Better for consistent, steady data flow.
Failure Recovery	More fault tolerant (can reroute packets dynamically).	Failure of a single link breaks the circuit; reconnection needed.
Used In	Internet (e.g., **UDP protocol**).	ATM networks, Frame Relay, or protocols like **TCP/IP** (logical VC).
Example Analogy	Like **postal mail** – each letter may take a different route.	Like a **train on tracks** – all coaches follow the same track.

🔄 Difference Between Circuit Switching and Packet Switching

Aspect	Circuit Switching	Packet Switching
Definition	A dedicated communication path is established for the entire session.	Data is broken into packets, and each packet is routed independently.
Connection Setup	Required before data transfer (setup phase).	Not required (in datagram), or logical connection only (in virtual circuit).
Resource Allocation	Fixed and reserved resources (bandwidth) for the entire session.	Resources are shared dynamically based on availability.
Data Flow	Continuous and in sequence.	Packets may take different paths and arrive out of order.
Bandwidth Utilization	Inefficient – bandwidth is reserved even if idle.	Efficient – uses bandwidth as needed.
Transmission Delay	Low after setup, since path is fixed.	May have variable delay due to routing and queuing.
Reliability	High – predictable performance.	Requires mechanisms to handle errors, losses, or reordering.
Example Technologies	Traditional telephone networks (PSTN).	Internet, LANs, WANs.
Data Type Suitability	Best for continuous, real-time data (e.g., voice).	Best for bursty, non-real-time data (e.g., web, email).
Setup Time	High – circuit setup takes time before transmission starts.	Low – packets are sent as soon as ready.
Cost	Higher due to dedicated path.	Lower as resources are used on demand.

Data Link Layer and Medium Access Sub Layer

Introduction

The data link layer is the second layer from the bottom in the OSI (Open System Interconnection) network architecture model. It is responsible for the node-to-node delivery of data within the same local network. Its major role is to ensure error-free transmission of information. DLL is also responsible for encoding, decoding, and organizing the outgoing and incoming data.

This is considered the most complex layer of the OSI model as it hides all the underlying complexities of the hardware from the other above layers. In this article, we will discuss Data Link Layer in Detail along with its functions, and sub-layers.

Functions of the Data Link Layer

1. Framing

- **Definition**: Framing is the process of dividing a stream of bits into manageable data units called *frames*.
- **Purpose**: Ensures that the receiver can detect the beginning and end of each message.
- **Techniques**: Character count, flag bytes with byte stuffing, flag bits with bit stuffing, and physical layer coding violations.

---

2. Physical Addressing

- **Function**: Adds source and destination **MAC (Media Access Control)** addresses to each frame.
- **Purpose**: Ensures that the frame is delivered to the correct device on the local network segment.

---

3. Error Detection

- **Purpose**: Identifies errors that may occur during transmission due to noise, attenuation, or interference.
- **Mechanisms**:
    - **Parity Bit**

- **Checksum**
- **Cyclic Redundancy Check (CRC)**

---

4. Error Correction

- **Function**: Corrects detected errors using additional redundant data.
- **Methods**:
  - **Hamming Code**
  - **Forward Error Correction (FEC)** techniques
- **Note**: Error correction may be done at the receiver or by requesting retransmission.

---

5. Flow Control

- **Definition**: Manages the rate of data transmission between sender and receiver.
- **Purpose**: Prevents a fast sender from overwhelming a slow receiver.
- **Protocols**:
  - **Stop-and-Wait**
  - **Sliding Window**

---

6. Access Control (Medium Access Control - MAC)

- **Function**: Controls how devices share the communication medium.
- **Purpose**: Prevents collision and ensures orderly access when multiple devices attempt to transmit.
- **Techniques**:
  - **CSMA/CD** (Used in Ethernet)
  - **CSMA/CA** (Used in Wi-Fi)
  - **Token Passing**

---

7. Frame Synchronization

- **Function**: Ensures that the sender and receiver are synchronized and can identify frame boundaries correctly.

- **Implementation**: Using start and end flags in framing schemes.

---

8. Acknowledgment and Retransmission

- **Purpose**: Confirms successful frame reception.
- **If not received**: Retransmission mechanisms like ARQ (Automatic Repeat reQuest) are triggered.

---

9. Link Management

- **Function**: Establishes, maintains, and terminates logical links between devices.
- **Purpose**: Ensures that both ends of the communication are properly coordinated during data exchange.

Sub-Layers of The Data Link Layer

The data link layer is further divided into two sub-layers, which are as follows:

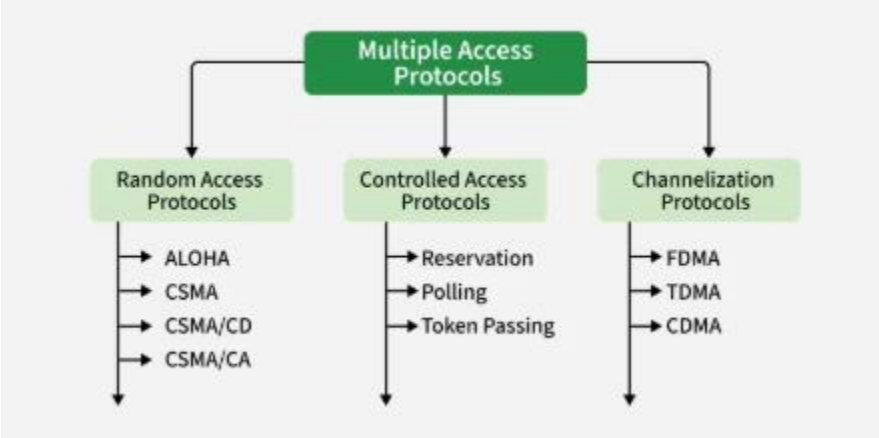
Logical Link Control (LLC)

This sublayer of the data link layer deals with multiplexing, the flow of data among applications and other services, and LLC is responsible for providing error messages and acknowledgments as well.

Media Access Control (MAC)

MAC sublayer manages the device's interaction, responsible for addressing frames, and also controls physical media access. The data link layer receives the information in the form of packets from the Network layer, it divides packets into frames and sends those frames bit-by-bit to the underlying physical layer.

Feature	LLC Sublayer (Logical Link Control)	MAC Sublayer (Media Access Control)
Position	Upper sublayer of the Data Link Layer	Lower sublayer of the Data Link Layer
Interface With	Network Layer (above) and MAC sublayer (below)	LLC sublayer (above) and Physical Layer (below)
Primary Role	Provides logical link services, multiplexing, and optional flow/error control.	Manages access to the physical medium and physical addressing.
Addressing	Uses Service Access Points (SAPs) for protocol multiplexing.	Uses MAC addresses (physical addresses) for device identification.
Medium Awareness	Medium-independent.	Medium-dependent (deals with how to access the specific physical medium).
Error Handling	Can provide connection-oriented error control (optional).	Primarily detects errors (FCS) and handles collision resolution.
Key Protocols	IEEE 802.2	CSMA/CD (Ethernet), CSMA/CA (Wi-Fi)



The main types of Random Access Protocols are:

a. ALOHA

The ALOHA protocol was developed at the University of Hawaii in the early 1970s for wireless LANs but can be used on any shared medium. It's very simple: a station transmits a frame whenever it has one to send.

- **Pure ALOHA:**
    - **Mechanism:** When a station has data to send, it transmits the frame immediately, without checking if the channel is busy.

    - **Collision Detection:** If an acknowledgment (ACK) is not received from the receiver within a timeout period, the sender assumes a collision occurred.
    - **Retransmission:** If a collision occurs, the station waits for a random amount of time (called a "back-off time") before retransmitting the frame. This randomness helps to avoid repeated collisions between the same frames.
    - **Vulnerable Time:** The "vulnerable time" for a frame in Pure ALOHA is $2 \times T_{fr}$, where T_{fr} is the frame transmission time. This means a frame can collide with other frames that start T_{fr} before it or T_{fr} after it.
    - **Efficiency:** The maximum theoretical throughput for Pure ALOHA is approximately 18.4% (or $1/(2e)$).
- **Slotted ALOHA:**
    - **Mechanism:** To improve efficiency, Slotted ALOHA divides time into discrete intervals called "slots." Stations are only allowed to transmit at the beginning of a time slot.
    - **Collision Reduction:** If a station misses the beginning of a slot, it must wait for the next slot. This synchronization significantly reduces the chances of partial collisions, as frames either collide entirely or not at all within a slot.
    - **Vulnerable Time:** The vulnerable time for a frame in Slotted ALOHA is T_{fr}.
    - **Efficiency:** The maximum theoretical throughput for Slotted ALOHA is approximately 36.8% (or $1/e$), which is twice that of Pure ALOHA.

b. CSMA (Carrier Sense Multiple Access)

CSMA improves upon ALOHA by adding a "carrier sense" mechanism. Before transmitting, a station *listens* to the medium to determine if it is busy.

- **"Listen Before Talk":** The core idea is that a station first senses the channel.
    - If the channel is *idle*, the station transmits.
    - If the channel is *busy*, the station waits.
- **Collision Possibility:** Collisions can still occur in CSMA due to propagation delay. If two stations sense the channel as idle at nearly the same time (before the first station's signal reaches the second), they might both transmit, leading to a collision.

There are several persistent methods in CSMA that define what a station does if the channel is busy:

- **1-Persistent CSMA:**

    - When a station has data to send, it senses the channel.
    - If idle, it transmits with a probability of 1 (i.e., immediately).
    - If busy, it continuously monitors the channel and transmits with a probability of 1 as soon as it becomes idle.
    - **Drawback:** High collision probability if multiple stations are waiting for the channel to become idle.
- **Non-Persistent CSMA:**
    - When a station has data to send, it senses the channel.
    - If idle, it transmits immediately.
    - If busy, it waits for a *random* amount of time, then re-senses the channel.
    - **Advantage:** Reduces collision probability compared to 1-persistent.
    - **Drawback:** Can lead to longer delays and lower channel utilization under light loads.
- **p-Persistent CSMA:**
    - Used with slotted channels.
    - When a station has data, it senses the channel.
    - If idle, it transmits with probability p.
    - With probability (1−p), it defers transmission to the next slot.
    - If busy, it waits until the next slot and re-senses.
    - This balances between 1-persistent and non-persistent, allowing for fine-tuning of performance.

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

CSMA/CD is an enhancement of CSMA, primarily used in **wired Ethernet networks**. It adds the capability to *detect* collisions while transmitting.

- **"Listen While Talk":**
    - A station senses the channel before transmitting.
    - If idle, it starts transmitting.
    - **Crucially:** While transmitting, the station *continues to listen* to the channel.

- **Collision Detection:** If a station detects a collision (e.g., by sensing an unexpected signal or an increase in voltage levels on the cable), it immediately stops its transmission.
- **Jam Signal:** Upon detecting a collision, the station transmits a short "jamming signal" to ensure that all other transmitting stations are aware of the collision.
- **Back-off Algorithm:** After transmitting the jam signal, each colliding station enters a random back-off period. This random delay helps to prevent the same stations from colliding again immediately. The back-off time usually increases with successive collisions (exponential back-off).
- **Efficiency:** CSMA/CD is much more efficient than pure ALOHA or even basic CSMA because it minimizes the time wasted on corrupted transmissions.

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

CSMA/CA is used in **wireless networks (like Wi-Fi - IEEE 802.11)** because collision detection is difficult or impossible in a wireless environment (a transmitting radio can't easily hear other transmissions over its own strong signal). Therefore, CSMA/CA focuses on *avoiding* collisions before they happen.

- **"Listen Before Talk":** Similar to CSMA, stations sense the channel before transmitting.
- **Collision Avoidance Mechanisms:**
    - **Interframe Spacing (IFS):** After the channel becomes idle, stations wait for a specific short period of time (IFS) before transmitting. Different types of frames have different IFS values, providing priority.
    - **Contention Window (CW) / Random Back-off:** If the channel is busy, or after waiting an IFS, stations choose a random back-off time from a contention window. They then count down this back-off time while the channel remains idle. Only when the back-off counter reaches zero and the channel is still idle can the station transmit.
    - **Request to Send/Clear to Send (RTS/CTS):** (Optional, but commonly used in Wi-Fi)
        - A sending station can first send a short **RTS** (Request To Send) packet to the intended receiver.
        - If the receiver is ready, it sends a **CTS** (Clear To Send) packet.
        - All other stations that hear either the RTS or CTS know that the channel will be busy for the duration of the data transmission and defer their own transmissions. This helps to mitigate the **hidden**

node problem (where two stations can't hear each other but both can hear a central access point, leading to collisions at the access

-
- point).

- **Acknowledgment (ACK):** The receiver sends an explicit acknowledgment (ACK) for each successfully received frame. If the sender doesn't receive an ACK, it assumes a collision or loss and retransmits.

Aspect	Pure ALOHA	Slotted ALOHA
Time Structure	No specific time structure; data can be sent at any time.	Operates on time slots; data is sent at the beginning of a time slot.
Efficiency	Lower efficiency (~18.4%) due to higher probability of collisions.	Higher efficiency (~37%) as it reduces the chance of collisions.
Collision Handling	If a collision occurs, the message is resent after a random time interval.	Messages are sent in synchronized time slots, reducing the chance of collision but if a collision occurs, it is handled similarly to Pure ALOHA.
Complexity	Less complex as it doesn't require synchronization.	More complex due to the need for time synchronization.
Implementation	Easier to implement due to lack of synchronization requirements.	Implementation is moderately complex because of the synchronization of time slots.

Stop-and-Wait ARQ (Automatic Repeat reQuest)

(7 Marks)

◈ Introduction

Stop-and-Wait ARQ is a simple **flow control and error control protocol** used in the Data Link Layer to ensure reliable data transmission. It works by sending **one frame at a time** and waiting for an acknowledgment (ACK) before sending the next frame.

◈ Working Principle

- The sender transmits a single data frame.
- The sender then **waits for an ACK** from the receiver.
- If the ACK is received within a timeout period, the sender transmits the next frame.

- If no ACK is received (due to frame loss or error), the sender **retransmits the same frame**.
- The receiver sends ACK for each correctly received frame.

◈ Key Features

Feature	Description
Frame Transmission	One frame at a time
Acknowledgment	Positive ACK sent for correctly received frame
Timeout	Retransmission occurs if no ACK received
Sequence Numbers	Uses 1-bit sequence number (0 or 1) to avoid duplication
Efficiency	Low, because channel stays idle waiting for ACK

◈ Advantages

- Simple and easy to implement.
- Ensures reliable transmission.
- Suitable for low error and low delay networks.

◈ Disadvantages

- Inefficient for long propagation delays or high-speed links.
- Channel remains idle while waiting for ACK (low utilization).
- Throughput decreases significantly with high delay.

Go-Back-N ARQ Protocol

(7 Marks)

◈ Introduction

Go-Back-N ARQ (Automatic Repeat reQuest) is a **sliding window protocol** used for error control in the Data Link Layer. It allows the sender to transmit several frames before

needing an acknowledgment but requires retransmission of all frames following a lost or erroneous frame.

◈ Working Principle

- The sender can send **N frames** continuously without waiting for an acknowledgment, where **N** is the window size.
- Frames are numbered sequentially (using a finite sequence number space).
- The receiver **only accepts frames in order**.
- If a frame is lost or an error is detected, the receiver discards that frame and all subsequent frames.
- The sender **goes back** and retransmits the lost frame and all subsequent frames starting from that point.

◈ Key Features

Feature	Description
Window Size	N (max number of outstanding frames)
Acknowledgment	Cumulative ACK for the last correctly received frame
Retransmission	All frames from the erroneous/lost frame onward
Receiver Buffer	Only one frame buffer (in-order delivery)
Sequence Numbers	Used modulo 2k2^k2k where kkk is bits for sequence number

---

◈ Example

- Window size N=4N = 4N=4.
- Sender sends frames 1, 2, 3, 4.
- Frame 2 gets lost.
- Receiver discards frames 2, 3, 4.
- Sender retransmits frames 2, 3, 4.

◈ Advantages

- Efficient compared to Stop-and-Wait, as multiple frames are sent before waiting for ACK.
- Simpler than Selective Repeat ARQ.

◈ Disadvantages

- Inefficient when errors occur, because many correctly received frames after the lost frame are retransmitted unnecessarily.
- Receiver can only accept frames in sequence.

Selective Repeat ARQ Protocol

(7 Marks)

◈ Introduction

Selective Repeat ARQ is an enhanced **sliding window protocol** used for error control in data communication. Unlike Go-Back-N, it allows the sender to retransmit **only the erroneous or lost frames**, improving bandwidth efficiency.

◈ Working Principle

- The sender can send multiple frames (up to window size) without waiting for individual acknowledgments.
- Each frame is numbered, and acknowledgments (ACKs) are sent individually for each frame received correctly.
- The receiver **accepts frames out of order** and buffers them until any missing frames arrive.
- Only **the specific frames that are lost or corrupted are retransmitted** by the sender.

◈ Key Features

Feature	Description
Window Size	N≤2k−1N \leq 2^{k-1}N≤2k−1 (to avoid ambiguity)
Acknowledgment	Individual ACK for each correctly received frame
Retransmission	Only erroneous or lost frames are retransmitted
Receiver Buffer	Needs buffering for out-of-order frames
Sequence Numbers	Used modulo 2k2^k2k where kkk is bits for sequence number

---

◈ Example

- Window size N=4N = 4N=4.
- Sender sends frames 1, 2, 3, 4.
- Frame 2 is lost.
- Receiver buffers frames 3 and 4.
- Receiver sends a NAK or no ACK for frame 2.
- Sender retransmits frame 2 only.
- Receiver then delivers frames 2, 3, 4 in order to upper layer.

◈ Advantages

- More efficient than Go-Back-N in noisy environments.
- Reduces unnecessary retransmissions.
- Better bandwidth utilization.

◈ Disadvantages

- Complex implementation due to buffering and maintaining order.
- Requires larger receiver buffer.
- Higher processing overhead.

Framing in Data Link Layer

(7 Marks)

◈ Introduction

Framing is the process of dividing the continuous stream of bits received from the Network Layer into manageable data units called **frames** at the Data Link Layer. It is essential for reliable communication because it helps the receiver identify the start and end of each frame.

◈ Purpose of Framing

- To **delimit** the data into discrete frames.
- To provide **error detection** and **flow control** for each frame.
- To enable the receiver to correctly **extract** the transmitted frames from the bit stream.

◈ Methods of Framing

1. **Character Count Method**
    - The frame starts with a count field indicating the number of characters in the frame.
    - The receiver uses this count to extract the frame.
    - **Disadvantage:** If the count field is corrupted, synchronization is lost.
2. **Byte Stuffing (Character Stuffing)**
    - Special characters called **flags** mark the start and end of the frame.
    - If the data contains flag characters, an escape character is inserted to differentiate them.
    - Used in protocols like **HDLC**.
3. **Bit Stuffing**
    - Frames start and end with a special bit pattern (flag), usually 01111110.
    - Whenever five consecutive 1s appear in data, a 0 is stuffed to prevent confusion with the flag.

- Used in **HDLC** and similar protocols.

4. **Physical Layer Coding Violations**
    - Uses specific violations in physical layer encoding to indicate frame boundaries (used in some LANs).

◈ Importance of Framing

- Enables **error detection** and **flow control** on a per-frame basis.
- Helps maintain synchronization between sender and receiver.
- Fundamental for **reliable and organized data transmission** over noisy channels.

Piggybacking in Data Link Layer

(7 Marks)

◈ Introduction

Piggybacking is a technique used in **two-way communication systems** at the Data Link Layer to improve efficiency by combining data and acknowledgment (ACK) frames into a single frame.

◈ What is Piggybacking?

- When a device sends data frames, it also needs to send ACKs for frames it has received.
- Instead of sending separate ACK frames, piggybacking **attaches the ACK information to outgoing data frames**.
- This reduces the number of frames on the network, saving bandwidth.

◈ How Piggybacking Works

- The frame structure includes a special field for the acknowledgment number.
- When a device wants to acknowledge the receipt of a frame, it waits until it has data to send.
- It then sends its data frame along with the ACK for the received frame.
- If no data is ready to send, the device sends a standalone ACK frame after a timeout.

◆ Advantages

Advantage	Explanation
Bandwidth Efficient	Reduces the total number of frames sent
Reduces Overhead	Combines ACK and data in one frame
Improves Throughput	More data transmitted in less time

◆ Disadvantages

Disadvantage	Explanation
Increased Delay for ACK	ACK may be delayed if no data to send
Complexity	Requires more complex frame processing

◆ Example

- Station A sends data frame 1 to Station B.
- Station B receives frame 1 and wants to acknowledge it.
- Instead of immediately sending an ACK, Station B waits to send its own data.
- Station B sends its data frame 2 with the ACK for frame 1 piggybacked.
- Station A receives data frame 2 and ACK for frame 1 together.

Error Detection and Error Correction

Error Correction

Error Detection