UNIT-I

DATA COMMUNICATIONS

The word **Data** refers to **Information.**

Data Communications are the exchange of data between two devices via some form of transmission medium such as a wire cable. For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software(programs).

The effectiveness of a data communications system depends on four fundamental characteristics:

1. **Delivery** The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
2. **Accuracy** The system must deliver the data accurately. Data should not be altered. If the data is altered in transmission and left uncorrected are unusable.
3. **Timeliness** The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced and without significant delay. This kind of delivery is called *real-time* transmission.
4. **Jitter** It refers to the variation in the packet arrival time. Jitter is the uneven delay in the delivery of audio or video packets.

   Example: Let us assume that video packets are sent every 3ms. If some of the packets arrive with 3ms delay and others with 4ms delay, an uneven quality in the video is the result.

COMPONENTS

A data communications system has five components:

1. **Message**

   The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
2. **Sender**

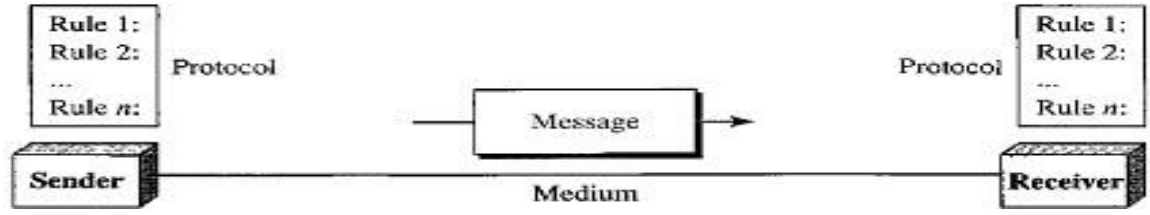
   The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
3. **Receiver**.

   The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
4. **Transmission medium**

   The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.
5. **Protocol**

   A protocol is **a set of rules** that govern data communications. It represents an **agreement** between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

Five components of data communication



Note: The term ***TELECOMMUNICATION*** includes telephony, telegraphy, and television, means communication at a distance *(tele* is Greek for "far").

DATA REPRESENTATION

Information comes in different forms such as text, numbers, images, audio, and video, where text numbers images can be represented in bit pattern.

Text

- In data communications, text is represented as a bit pattern, a sequence of bits (0's or1's).
- Different sets of bit patterns have been designed to represent text symbols. Each set is called a code, and the process of representing symbols is called coding.
- The prevalent coding system is called Unicode, which uses 32 bits to represent a symbol or character used in any language in the world.
- The American Standard Code for Information Interchange (ASCII) developed in the United States, now constitutes the first 127 characters in Unicode.

Numbers

- Numbers are also represented by bit patterns.
- A code such as ASCII is not used to represent numbers.
- The number is directly converted to a binary number to simplify mathematical operations.

Images

- Images are also represented by bit patterns. An image is composed of a matrix of pixels (picture elements) where each pixel is a small dot.
- The size of the pixel depends on the *resolution.* Example: An image can be divided into 1000 pixels or 10000pixels.
- If the number of pixels is more there is a better representation of the image (better resolution) but more memory is needed to store the image.
- After an image is divided into pixels, each pixel is assigned a bit pattern. The size and the value of the pattern depend on the image.
- There are several methods to represent color images. RGB and YCM
- In RGB each color is made of a combination of three primary colors: *red,* green and blue.
- In YCM a color is made of a combination of three other primary colors: yellow, cyan, and magenta.

Audio

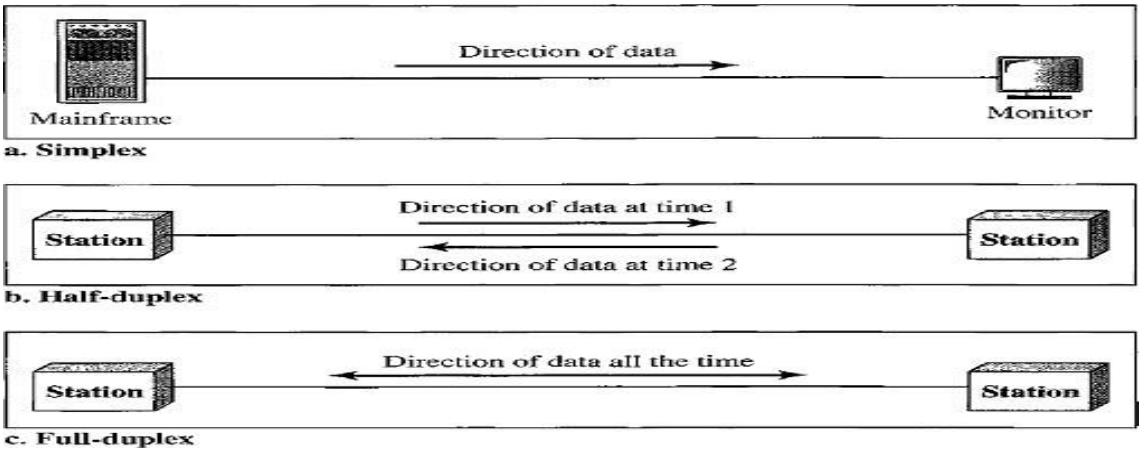
- Audio refers to the recording or broadcasting of sound or music.
- Audio is by nature different from text, numbers, or images. It is continuous, not discrete.
- Even when we use a microphone to change voice or music to an electric signal, we create a continuous signal.

Video

- Video refers to the recording or broadcasting of a picture or movie.
- Video can either be produced as a continuous entity (e.g., by a TV camera), or it can be a combination of images, each a discrete entity, arranged to convey the idea of motion.

DIRECTION OF DATA FLOW

Communication between two devices can be simplex, half-duplex, or full-duplex.



Simplex

- In simplex mode, the communication is unidirectional (i.e. one direction only).
- Only one of the two devices on a link can transmit; the other can only receive.
- The simplex mode can use the entire capacity of the channel to send data in one direction.
- Examples - **Keyboards** and **Monitors,** the keyboard can only introduce input, the monitor can only accept output.

Half-Duplex

- In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa.
- In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time.
- The half-duplex mode is used, where there is no need for communication in both directions at the same time. The entire capacity of the channel can be utilized for each direction.
- **Examples** - Walkie-talkies and CB (citizens band) radios are both half-duplex systems.

Full-Duplex

- In full-duplex mode (or duplex), both stations can transmit and receive simultaneously.
- In full-duplex mode signals going in one direction share the capacity of the link: with signals going in the other direction
- This sharing can occur in two ways: Either the link must contain two physically separate transmission paths, one for sending and the other for receiving, or the capacity of channel is divided between signals traveling in both directions.
- The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel must be divided between the two directions.
- **Example -** Telephone network. Two people talk and listen at the same time.

NETWORKS

A **Network** is a set of devices (also called as nodes) connected by communication links. (or)
A **Network** is two or more devices connected through links.

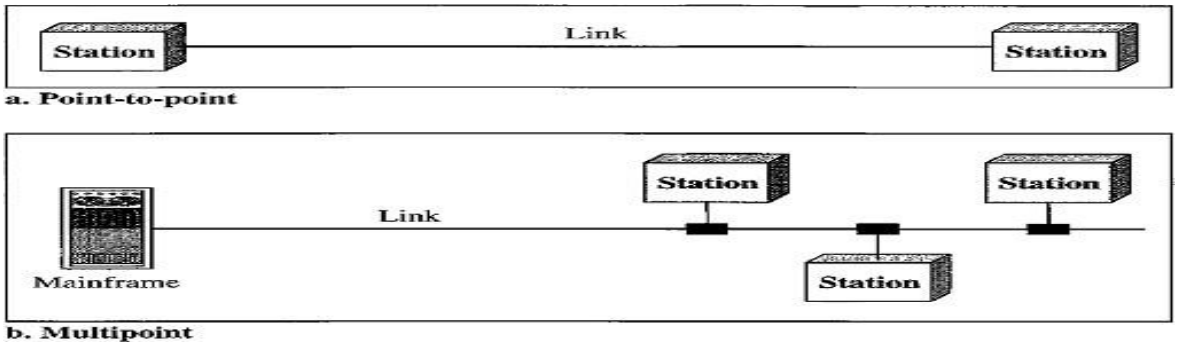
A **Node** can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

A **Link** is a communications pathway that transfers data from one device to another.

Type of Connection

Two devices must be connected in some way to the same link at the same time for occurring of communication. There are two possible types of connections:

1. Point-to-Point Connection
2. Multipoint Connection



Point-to-Point Connection

- A Point-to-Point connection provides a dedicated link between two devices.
- The entire capacity of the link is reserved for transmission between those two devices.
- Point-to-Point connections use an actual length of wire or cable to connect the two ends and microwave or satellite links.
- Example: When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.

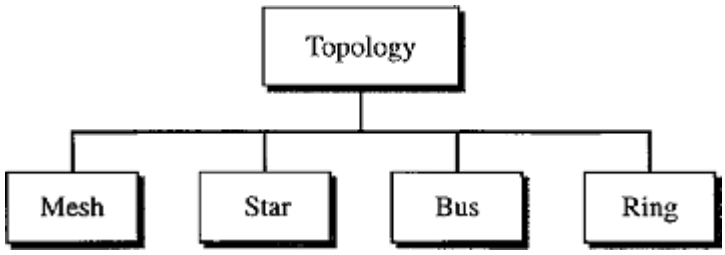
Multipoint (or) Multi-drop Connection

- A multipoint connection is more than two specific devices share a single link.
- In a multipoint environment, the capacity of the channel is shared, either spatially or temporally.
- If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.

NETWORK TOPOLOGIES

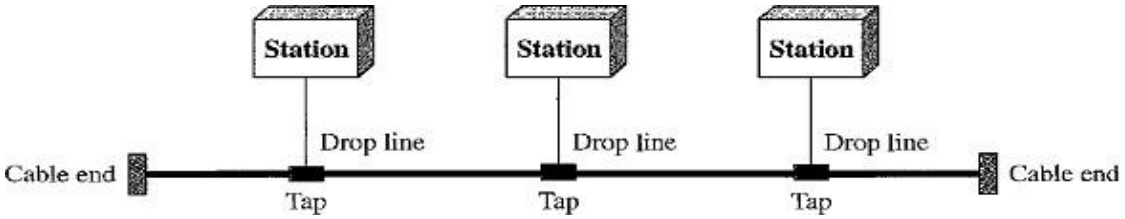
The term physical topology refers to the way in which a network is connected physically.
Two or more devices connect to a link. Two or more links form atopology.
There are four basic topologies are present:

1. Bus
2. Ring
3. Star
4. Mesh



Bus Topology

- A **bus topology** is multipoint connection, one long cable acts as a **backbone** to link all the devices in a network. Here the cable is called the bus.
- Bus topology was the one of the first topologies used in the design of early local area networks.
- Nodes are connected to the bus cable by drop lines and taps.
- A drop line is a connection running between the device and the main cable.
- A tap is a connector that splices into (attached to) the main cable.



Advantages:

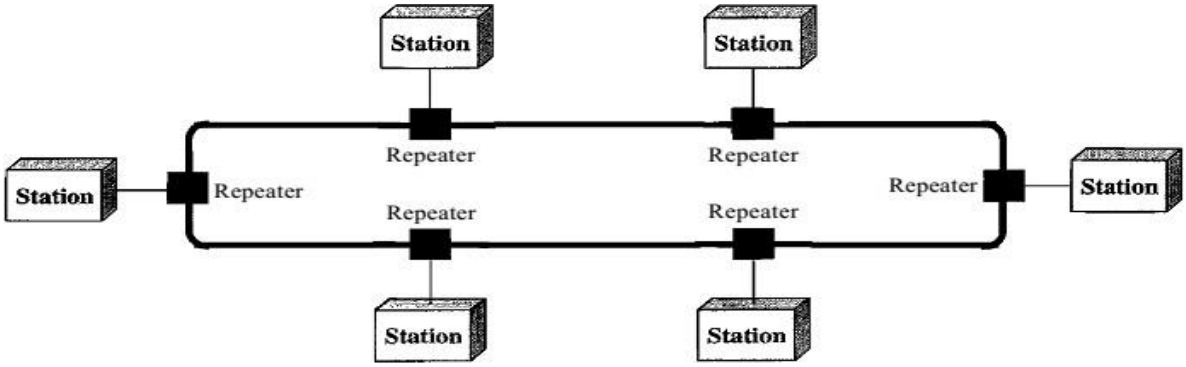
1. Installation is easy. Bus Backbone cable can be laid along the most efficient path and then connected to the nodes by drop lines of various lengths.
2. A bus uses less cabling than mesh or star topologies.

Disadvantages:

1. All the devices are connected to bus backbone cable, so that if the backbone cable fails the entire system fails.
2. Difficult Reconnection and Fault Isolation. It is difficult to add new devices.
3. There is a limit on the number of taps a bus can support and on the distance between those taps.
4. More heat is generated if the number of taps is more. Heat degrades the quality of signal.

Ring Topology

- In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it.
- A signal is passed along the ring in one direction from device to device, until it reaches its destination.
- Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.



Advantages:

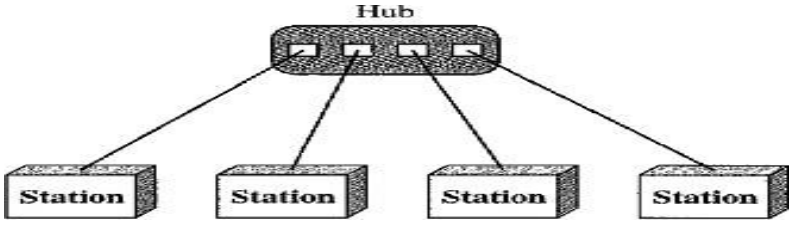
1. A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors (either physically or logically).
2. To add or delete a device requires changing only two connections.
3. The only constraints are media and traffic considerations (maximum ring length and number of devices).

Disadvantage:

1. Unidirectional traffic can be a disadvantage.
2. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network.

Star Topology

- In a star topology, each device has a dedicated point-to-point link only to a central controller called a Hub or Switch. The devices are not directly linked to one another.
- A star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, and the controller transfers the data to the other connected device.



Advantages:

1. A star topology is less expensive than a mesh topology. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure
2. Less cabling is required than mesh topology.
3. Star topology is robust, If one link fails, only that link is affected. All other links remain active.

Disadvantages:

1. If hub fails entire processing will be stopped working.

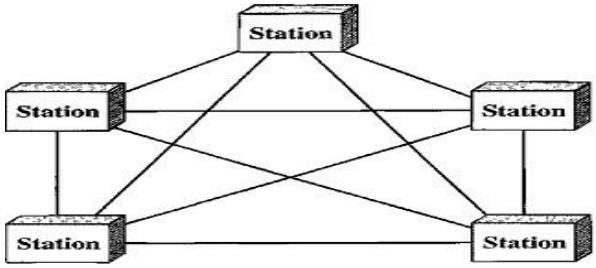
Uses:

1. It is used in High-speed LAN's often use a star topology with a central hub.

Mesh Topology

- In a mesh topology, every device has a **Dedicated Point-to-Point** link to every other device. (i.e.) for each node there is a link to all other nodes.
- The term **Dedicated** means that the link carries traffic only between the two devices it connects.

Advantages:

1. A mesh topology is robust. If one link becomes unusable, it does not affect the entire system.
2. The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
3. **Privacy or Security.** When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages.
4. Point-to-Point links make **Fault Identification** and **Fault Isolation** easy.
5. 

Disadvantages:

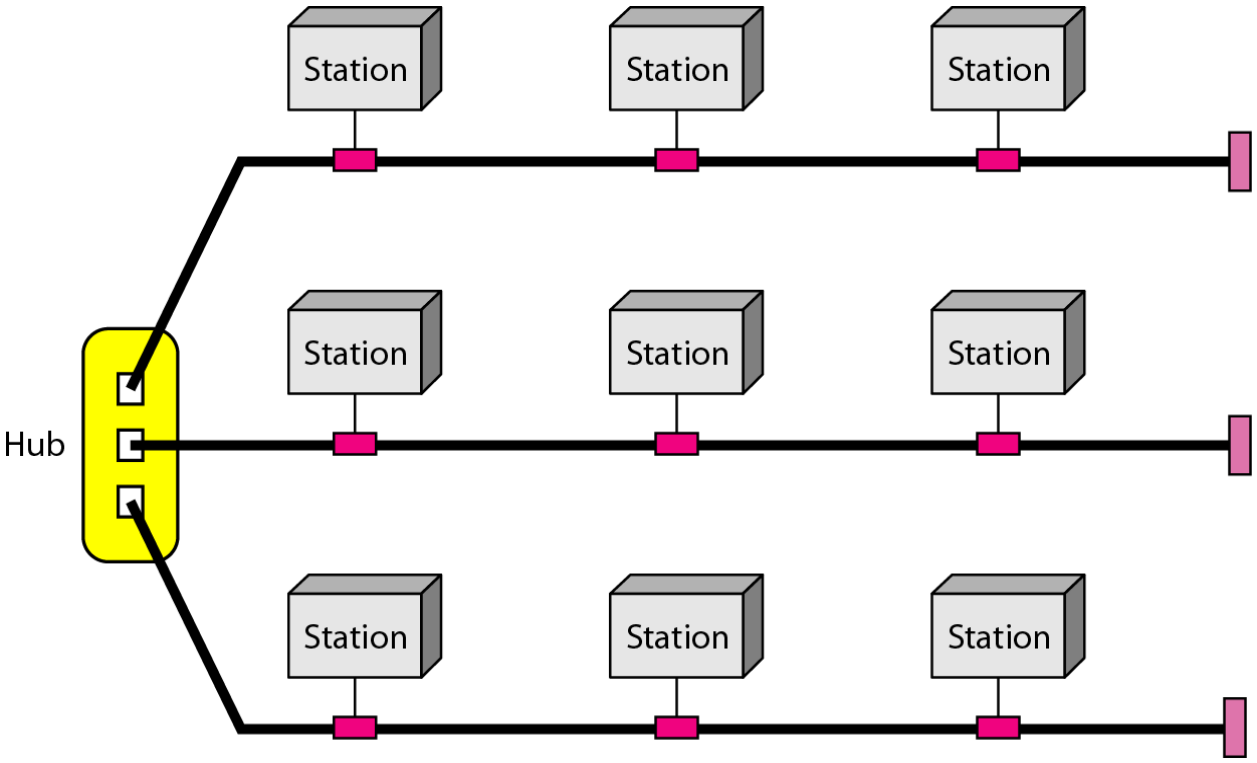
1. **High Cost:** Every device must be connected to every other device then there is a high amount of cabling and huge number of I/O ports required, this will make installation and reconnection are difficult.
2. The hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.
3. More hardware (i.e. cables) and space is required

Example: Telephone offices and Police stations.

Connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

Hybrid Topology

It is a combination of two or more topologies for example star topology with each branch connecting several stations in a bus topology



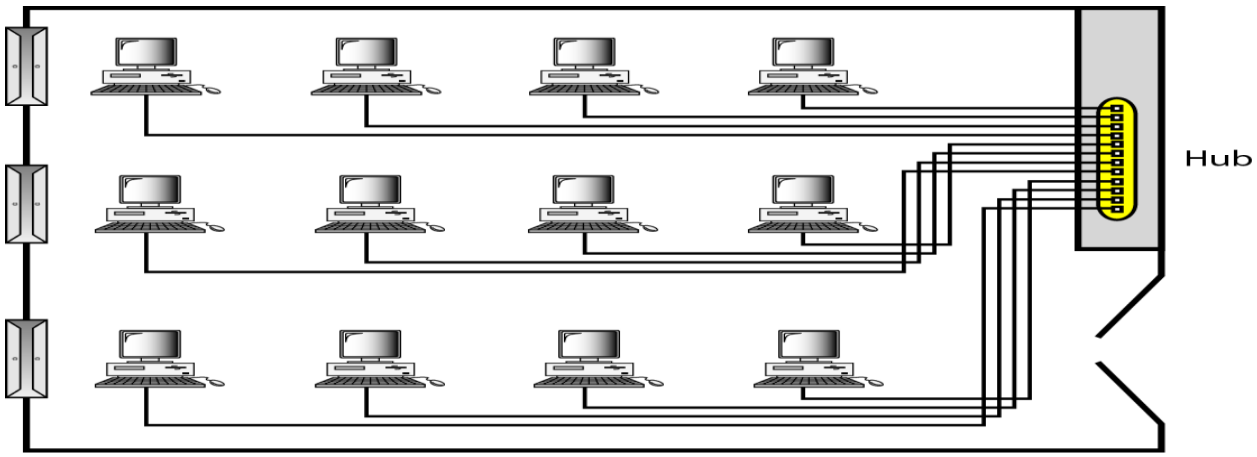
CATEGORIES OF NETWORKS

There are 3 categories of networks depend on its size:

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

Local Area Networks

- A Local Area Network (LAN) provides short-distance transmission of data over small geographic areas that may comprise a single office, building, or campus.
- **Size:** LAN size is limited to a few kilometers.
- **Speed:** Early LANs had data rates in the 4 to 16 megabits per second (Mbps) range but now speeds are increased to 100 or 1000Mbps.
- LANs are designed to allow resources to be shared between personal computers or workstations.
- The resources to be shared can include hardware (e.g., a printer), software (e.g., an application program), or data.
- A local area network (LAN) is usually privately owned.
- LAN will use only one type of transmission medium.
- The most common LAN topologies are bus, ring, and star.

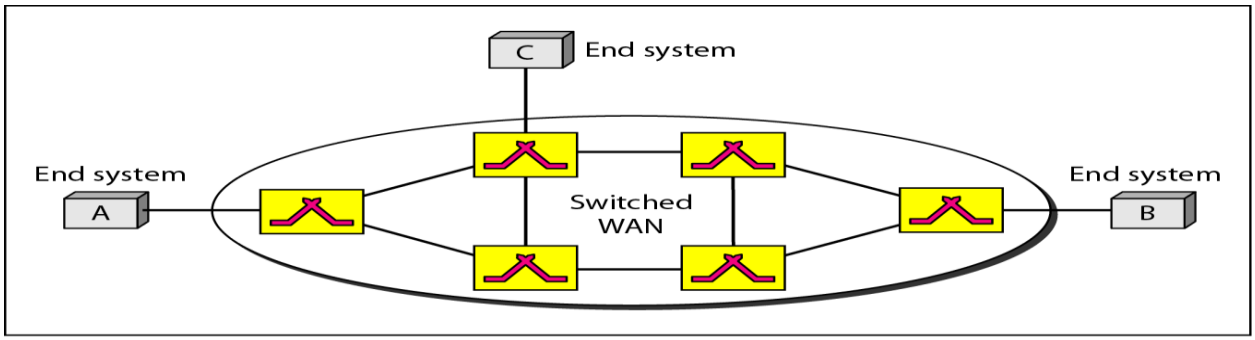


Wide Area Network

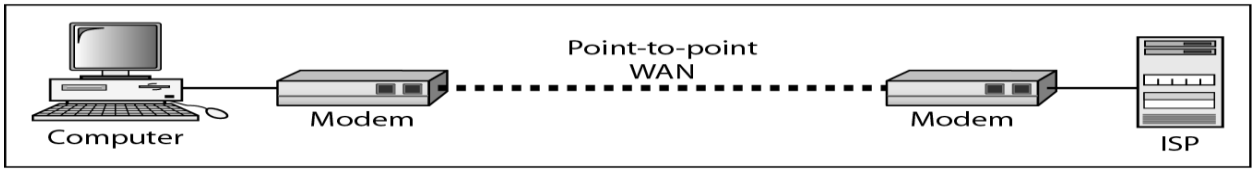
A Wide Area Network (WAN) provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world.

The switched WAN connects the end systems, which usually comprise a router (inter-networking connecting device) that connects to another LAN or WAN.

The point-to-point WAN is often used to provide Internet access. A line leased from a telephone provider that connects a home computer or a s mall LAN to an Internet service provider (lSP).



a. Switched WAN



b. Point-to-point WAN

Metropolitan Area Networks

A Metropolitan Area Network (MAN) is a network with a size between a LAN and a WAN. It normally covers the area inside a town or a city.

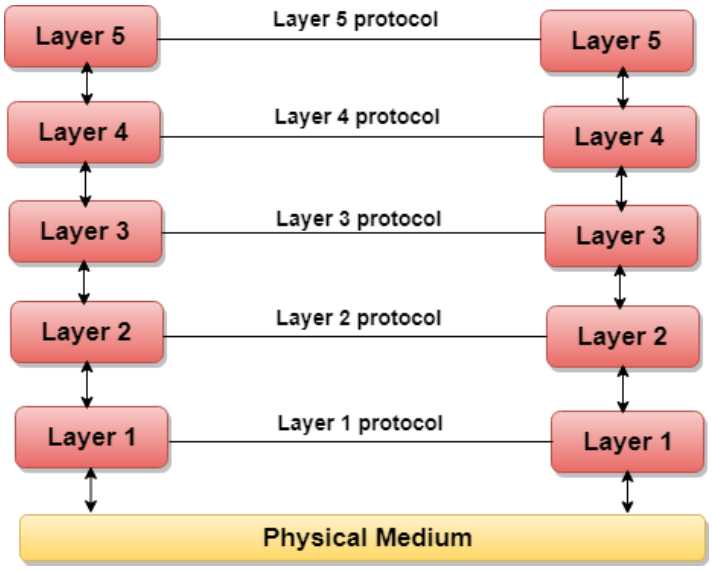
It is designed for customers who need a high-speed connectivity to the Internet, and have endpoints spread over a city or part of city.

Example of a MAN is the part of the telephone company network that can provide a high-speed DSL line to the customer.

Flow of Network layered architecture:

- The main aim of the layered architecture is to divide the design into small pieces.
- Each lower layer adds its services to the higher layer to provide a full set of services to manage communications and run the applications.
- It provides modularity and clear interfaces, i.e., provides interaction between subsystems.
- It ensures the independence between layers by providing the services from lower to higher layer without defining how the services are implemented. Therefore, any modification in a layer will not affect the other layers.
- The number of layers, functions, contents of each layer will vary from network to network. However, the purpose of each layer is to provide the service from lower to a higher layer and hiding the details from the layers of how the services are implemented.
- The basic elements of layered architecture are services, protocols, and interfaces.
    - **Service:** It is a set of actions that a layer provides to the higher layer.
    - **Protocol:** It defines a set of rules that a layer uses to exchange the information with peer entity. These rules mainly concern about both the contents and order of the messages used.
    - **Interface:** It is a way through which the message is transferred from one layer to another layer.
- In a layer n architecture, layer n on one machine will have a communication with the layer n on another machine and the rules used in a conversation are known as a layer-n protocol.

Let's take an example of the five-layered architecture.



- In case of layered architecture, no data is transferred from layer n of one machine to layer n of another machine. Instead, each layer passes the data to the layer immediately just below

it, until the lowest layer is reached.

- Below layer 1 is the physical medium through which the actual communication takes place.
- In a layered architecture, unmanageable tasks are divided into several small and manageable tasks.
- The data is passed from the upper layer to lower layer through an interface. A Layered architecture provides a clean-cut interface so that minimum information is shared among different layers. It also ensures that the implementation of one layer can be easily replaced by another implementation.
- A set of layers and protocols is known as network architecture.

Why do we require Layered architecture?

- **Divide-and-conquer approach:** Divide-and-conquer approach makes a design process in such a way that the unmanageable tasks are divided into small and manageable tasks. In short, we can say that this approach reduces the complexity of the design.
- **Modularity:** Layered architecture is more modular. Modularity provides the independence of layers, which is easier to understand and implement.
- **Easy to modify:** It ensures the independence of layers so that implementation in one layer can be changed without affecting other layers.
- **Easy to test:** Each layer of the layered architecture can be analyzed and tested individually.

NETWORK MODELS

There are two types of network models are used:

1. ISO/OSI Model.
2. TCP/IP protocol model

ISO/OSI Model

- **ISO** is the **Organization**. **OSI** is the **Model**. ISO was established in 1947. OSI was first introduced in1970.
- The **International Standards Organization (ISO)** is a multinational body dedicated to worldwide agreement on international standards.
- An ISO standard that covers all aspects of network communications is the **Open Systems Interconnection model**.
- An **Open System** is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.
- **The purpose** of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software.
- The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.

The OSI model is a **Layered Frame work** for the design of network systems that allows

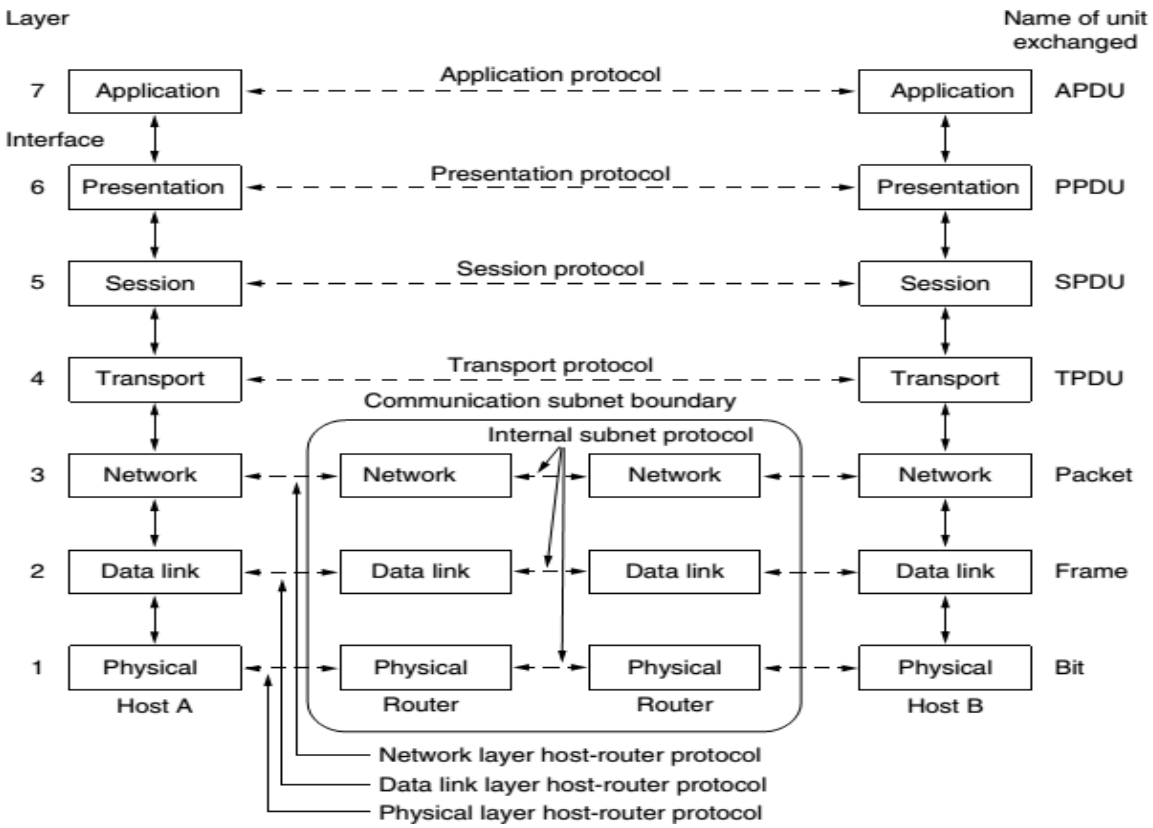
communication between all types of computer systems.

It consists of seven ordered layers. Each layer defines a part of the process of moving information across a network.

Below figure shows the layers involved when a message is sent from host A to host B. A host may be a device or node or a computer. Within a single machine, each layer calls upon the services of the layer just below it.

Each layer in the sending device adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it.

APDU, PPDU, SPDU, TPDU are packet data units of Application, Presentation, Session, Transport layers respectively.

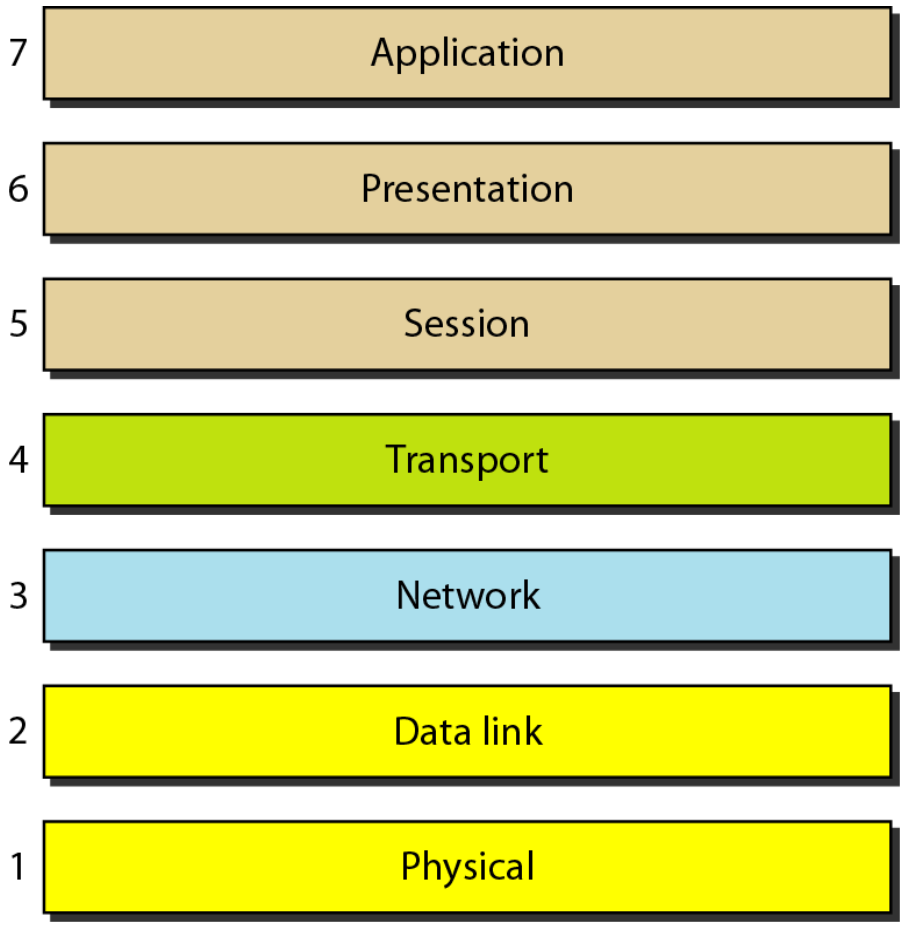


Interfaces Between Layers

- The passing of the data and network information between the layers in the device is made possible by an interface between each pair of adjacent layers.
- Each interface defines the information and services a layer must provide for the layer above it. These interfaces provide modularity to the network.

The Seven Layers in OSI Model are:

1. Physical Layer
2. Data link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer



These seven layers can be categorized into 3 groups:

1. **Physical, Data Link,** and **Network Layers** are the network support layers: they deal with the physical aspects of moving data from one device to another such as electrical specifications, physical connections, physical addressing, and transport timing and reliability.

   Note: Physical layer is implemented in hardware whereas Data link and Network layers are combination of hardware and software.
2. **Session, Presentation,** and **Application Layers** can be thought of as the user support layers. These are almost always implemented in software. They allow interoperability among unrelated software systems.

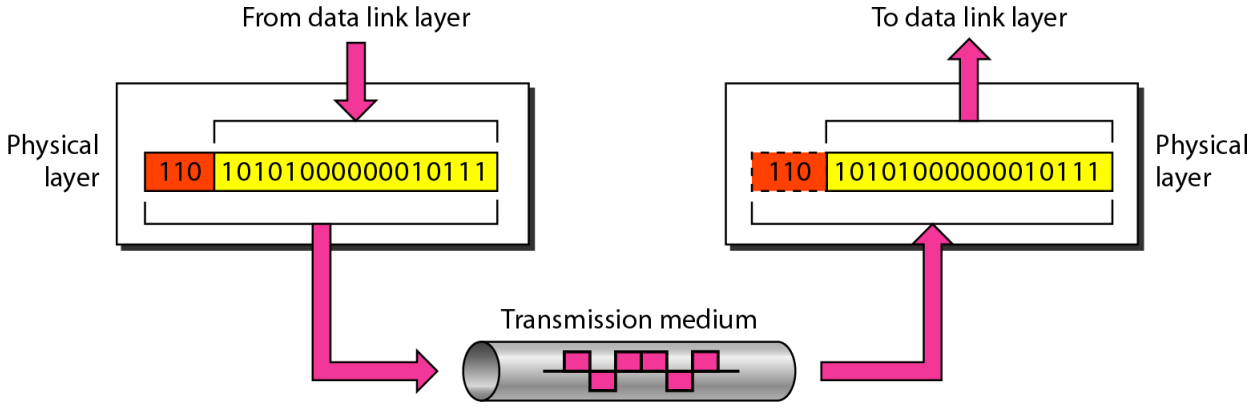
3. **The Transport Layer** links the two subgroups and ensures that what the lower layers have transmitted is in a form that the upper layers can use.

Physical Layer

The **Physical Layer** is concerned with transmitting raw bits over a communication channel.

Physical Layer is responsible for:

- It defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur.
- It also defines the type of transmission medium.
- It defines the data transmission rate, synchronization of data between sender and receiver.
- It defines type of connection (point-to-point or multipoint), type of topology, type of transmission mode, type of dataflow (simplex, half duplex, duplex).



The Data Link Layer

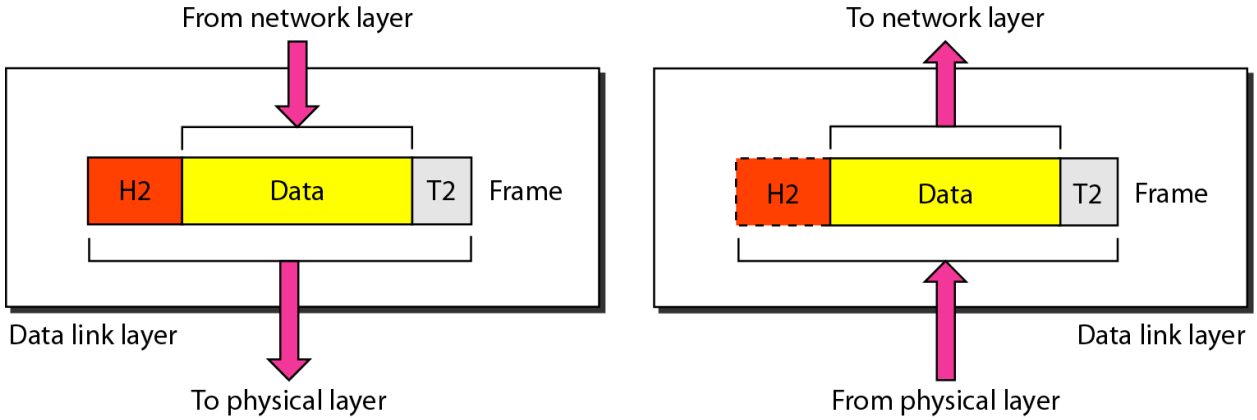
The data link layer is responsible for moving frames from one node to the next node.

The **main task** of the Data link layer is **Error Free Transmission**. At the sender the data link layer break up the input data into **data frames** and transmits the frames sequentially.

Frame is typically a few hundred or a few thousand bytes.

Other responsibilities of the data link layer include the following:

- **Framing** - The data link layer divides the stream of bits received from the network layer into manageable data units called frames
- **Physical addressing -** If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and receiver of the frame.
- **Flow control** - If the rate at which the data are received by the receiver is less than the rate at which data sent by the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.
- **Error control** - The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.
- **Access control** - When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.



Network Layer

The network layer is responsible for the delivery of individual packets from the source host to the destination host through single or multiple networks.

Note: If two systems are connected to the same network then there is usually no need for a network layer.

If the two systems are connected to different networks with connecting devices between the networks then there is a need for the network layer to accomplish source-to-destination delivery.

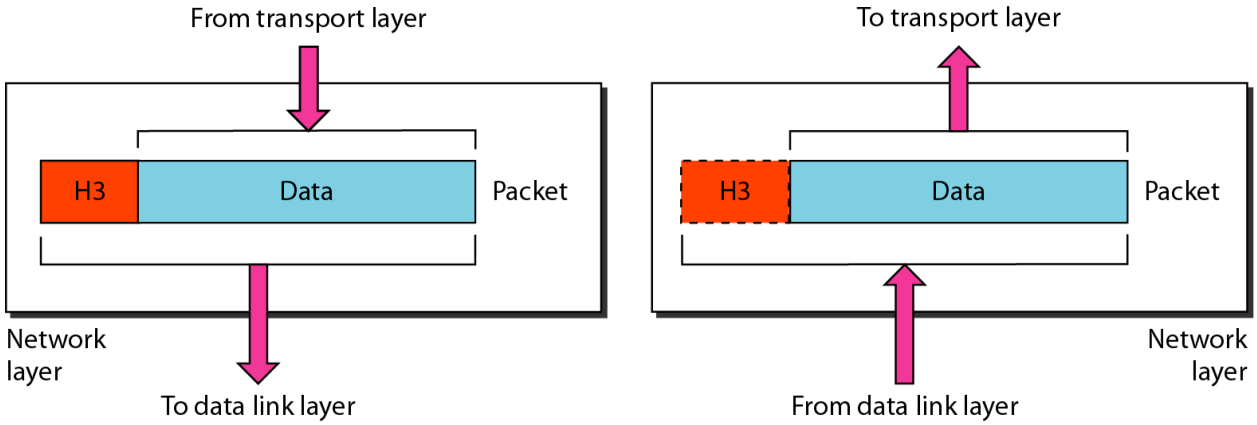
Responsibilities of the Network layer include the following:

Logical addressing

- The physical addressing is implemented by Data- link layer, whereas logical addressing is implemented by network layer.
- Data- link layer handles the addressing problem locally, but if packets passes the network boundary there is a need for logical addressing system to help distinguish source and destination systems.
- The network layer adds a header to the packet coming from the upper layer that includes the logical addresses of the sender and receiver.

Routing

- When independent networks or links are connected to create inter- networks (network of networks) or a large network, the connecting devices (called *routers* or *switches)* route the packets to their final destination.



<u>Transport Layer</u>

The transport layer is a true end-to-end layer; it carries from the source to the destination.

The transport layer is responsible for the delivery of a message from one process to another. A process is an application program running on a host.

Responsibilities of the Transport Layer Include:

Port addressing (or) Service point addressing

- Source-to-Destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other.
- The transport layer header must therefore include a type of address called a *service-point address* (or port address).
- The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.

Segmentation and Reassembly

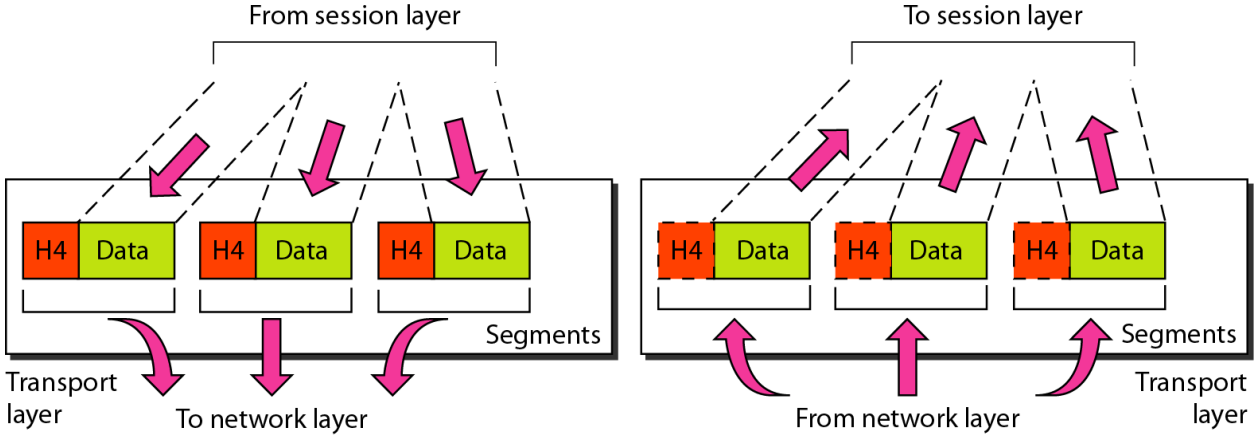
- A message is divided into transmittable segments, with each segment containing a sequence number.
- These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and the sequence numbers are used for identifying and replace packets that were lost during transmission.

Connection control

- The transport layer can be either connectionless or connection oriented.
- A **Connectionless** transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine.
- A **Connection-Oriented** transport layer makes a connection with the transport layer at the destination machine first before delivering the packets.
- After all the data are transferred, the connection is terminated.

Flow control and Error control

- Like the data link layer, the transport layer is responsible for flow control.
- Flow control at this layer is performed end to end rather than across a single link.
- Like the data link layer, the transport layer is responsible for error control.
- Error control at this layer is performed Process-to-Process rather than across a single link.
- Error control achieved through **Retransmission.**

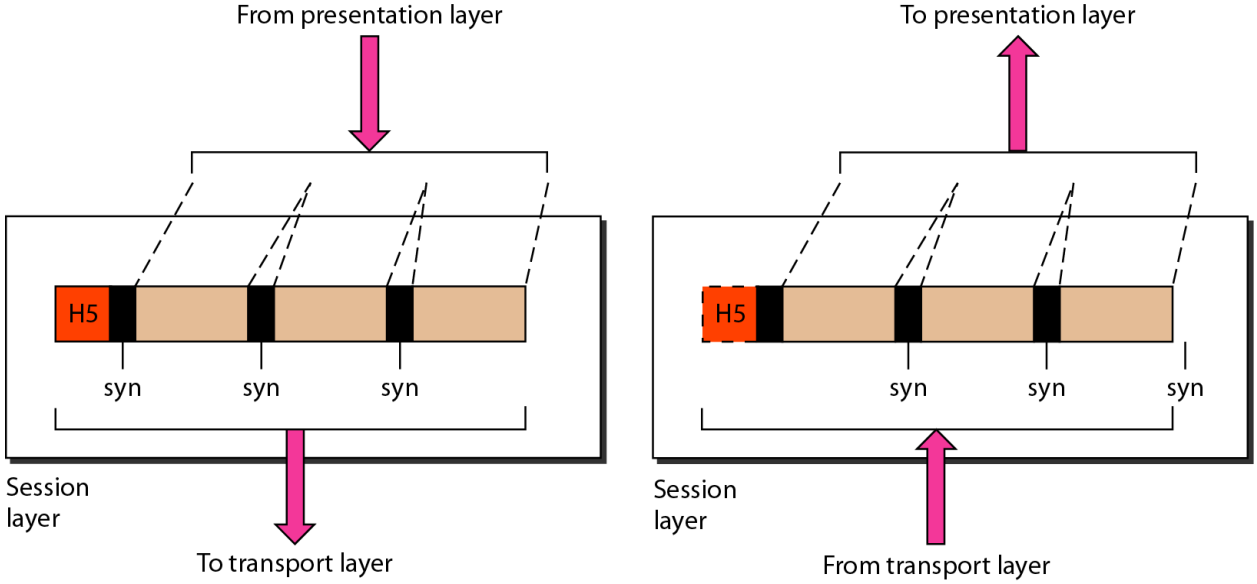


Session Layer

The session layer allows users on different machines to establish **sessions** between them. The session layer is the network *dialog controller*. It establishes, maintains, and synchronizes the interaction among communicating systems.

Responsibilities of the session layer include the following

- **Dialog Control** The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half-duplex (one way at a time) or full-duplex (two ways at a time) mode.
- **Synchronization** The session layer allows a process to add checkpoints, or synchronization points, to a stream of data. Check-Pointing long transmissions to allow them to pick up from where they left off in the event of a crash and subsequent recovery
- **Token management** prevents two parties from attempting the same critical operation simultaneously.



Presentation Layer

The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.

The presentation layer is responsible for **Translation, Compression, and Encryption**.

Translation

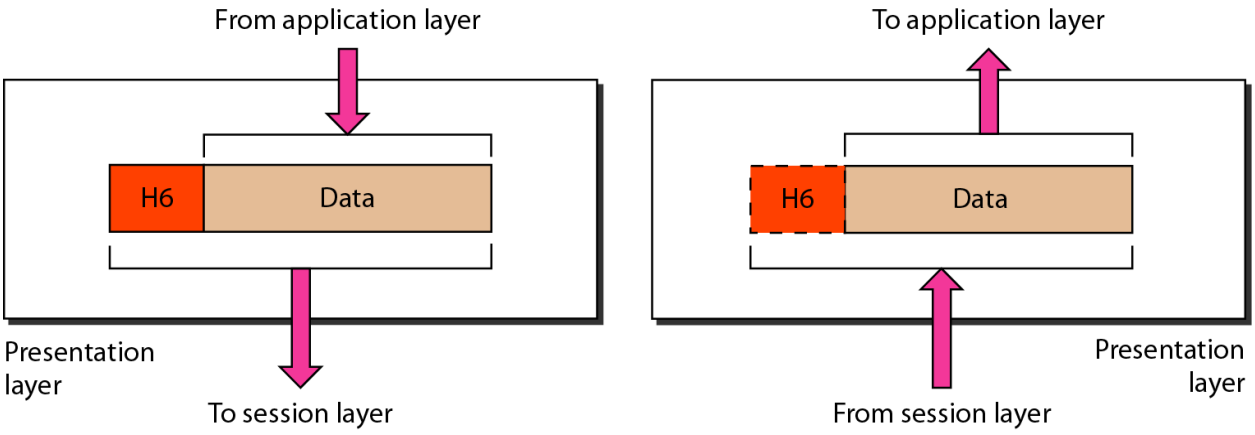
- The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers etc. The information must be changed to bits streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods.
- The presentation layer at the sender changes the information from its sender-dependent format into a common format.
- The presentation layer at the receiving machine changes the common format into its receiver-dependent format.

Encryption

- Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network.
- Decryption reverses the original process to transform the message back to its original form. Encryption and Decryption is done for privacy of the sensitive information.

Compression

- Data compression reduces the number of bits contained in the information.
- Data compression becomes particularly important in the transmission of multimedia such as text, audio and video.



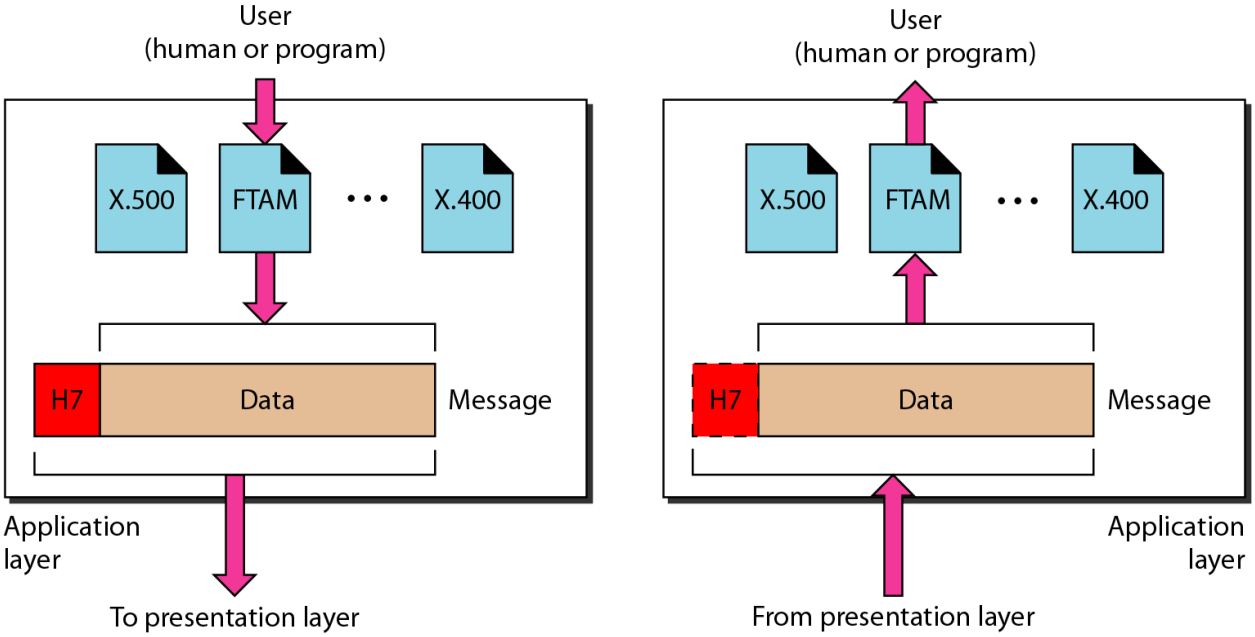
Application Layer

The application layer is responsible for providing services to the user.

The **application layer** contains a variety of protocols that are commonly needed by users. The application layer enables the user to access the network.

Specific services provided by the application layer include the following:

- **A network virtual terminal** is a software version of a physical terminal, and it allows a user to log on to a remote host.
- **File** transfer, access, and management in a remote host.
- **Mail services** such as email forwarding and mail storage.
- **Directory services** are an application provides distributed database sources and access for global information about various objects and services.



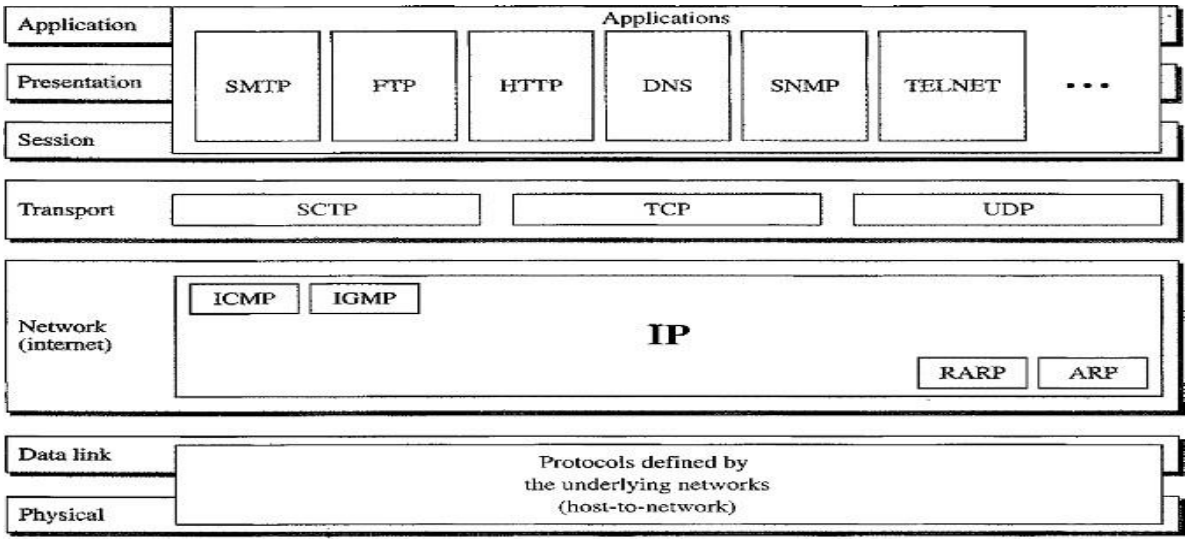
TCP/IP PROTOCOL SUITE

The TCP/IP protocol suite was developed prior to the OSI model.

The original TCP/IP protocol suite was defined as having four layers:

1. Host-To-Network Layer
2. Internet Layer
3. Transport Layer

4. Application Layer



Layers comparison in TCP/IP and OSI:

- **Host-to-Network** layer is equivalent to the combination of the **Physical** and **Data link** layers.
- The **Internet Layer** is equivalent to the **Network layer**.
- The **Transport layer** is similar in both OSI and TCP/IP, except that in TCP/IP it will take care of part of the duties of the session layer.
- The **Application Layer** is roughly doing the job of the **Session, Presentation** and **Application** layers.

Functionality in TCP/IP and OSI:

- ***TCP/IP*** is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality; however, the modules are not necessarily interdependent.
- **OSI model** specifies which functions belong to each of its layers, the layers of the *TCP/IP* protocol suite contain relatively independent protocols that can be mixed and matched depending on the needs of the system.
- The term *hierarchical* means that each upper- level protocol is supported by one or more lower-level protocols.

Host-to- Network Layer

- At the Host-to-Network layer is a combination of Physical Layer and Data-link layer in OSI model.
- It is an interface between hosts and transmission links.
- **TCP/IP** does not define any specific protocol. It supports all the standard and proprietary protocols.
- A network in a TCP/IP internetwork can be a local-area network or a wide-area network.

Internet Layer(or) **Network Layer**

- In this layer *TCP/IP* supports the Internetworking Protocol (IP). The Internetworking Protocol (IP) is the transmission mechanism used by the TCP/IP protocols.
- It is an unreliable and connectionless protocol-a best-effort delivery service.
- The term *best effort* means that IP provides no error checking or tracking.

- The transmission is unreliable (i.e.) there is no guarantee for the data.
- IP transports data in packets called *datagrams,* each of which is transported separately.
- Datagrams can travel along different routes and can arrive out of sequence or be duplicated.
- IP does not keep track of the routes and has no facility for reordering datagrams once they arrive at their destination.

IP uses four supporting protocols

1. ARP (Address Resolution Protocol)
2. RARP(Reverse Address Resolution Protocol)
3. ICMP(Internet Control Message Protocol)
4. IGMP(Internet Group Message Protocol)

Address Resolution Protocol (ARP)

- ARP is used to associate a logical address with a physical address. ARP is used to find the physical address of the node when its Internet address is known.
- On a typical physical network, such as a LAN, each device on a link is identified by a physical or station address, usually imprinted on the network interface card (NIC).

Reverse Address Resolution Protocol (RARP)

- RARP allows a host to discover its logical address when it knows only physical address.
- It is used when a computer is connected to a network for the first time or when a diskless computer is booted.

Internet Control Message Protocol (ICMP)

- ICMP is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender.
- ICMP sends query and error reporting messages.

Internet Group Message Protocol (IGMP)

- IGMP is used to facilitate the simultaneous transmission of a message to a group of recipients.

Transport Layer

Transport layer in *TCP/IP* has three protocols:

1. **TCP** (*Transmission Control Protocol)*
2. **UDP**(*User Datagram Protocol)*
3. **SCTP**(Stream Control Transmission Protocol)

Note: UDP and TCP are transport level protocols responsible for delivery of a message from one device to another device, whereas IP is a host-to- host protocol meaning that it can deliver a packet from one physical device to another.

Transmission Control Protocol

- TCP provides full transport- layer services to applications. TCP is a reliable stream transport protocol.
- The term ***stream*** means connection-oriented: A connection must be established between both ends of a transmission before either can transmit data.
- At the sending side for each transmission TCP divides a stream of data into smaller units called *Segments.* Each segment includes a sequence number for reordering at the destination side. Segments are carried across the internet inside of IP datagrams.

- For every segment there is a corresponding acknowledgement to be sent from the destination to the source.
- At the receiving side TCP collects each datagram as it comes in and reorders the transmission based on sequence numbers.

User Datagram Protocol

- UDP is unreliable, connectionless protocols for applications that do not want TCP's sequencing or flow control and wish to provide their own.
- It is a process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from the upper layer.
- It is also widely used for client-server-type request-reply queries and applications in which prompt delivery is more important than accurate delivery such as transmitting speech or video.

Stream Control Transmission Protocol

- The Stream Control Transmission Protocol (SCTP) provides support for newer applications such as voice over the Internet. It is a transport layer protocol that combines the best features of UDP and TCP.

Application Layer

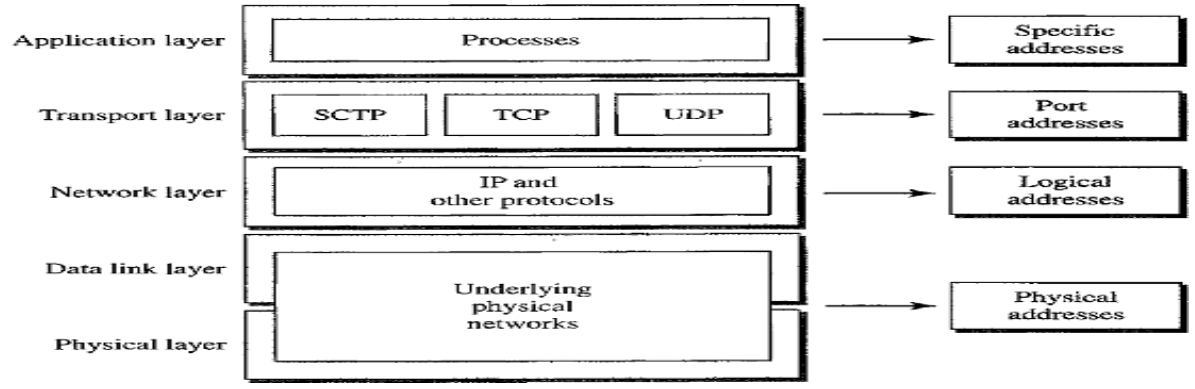
On top of the transport layer is the **application layer**. It contains all the higher-level protocols such as:

- **Telnet protocol** used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection.
- **File Transfer Protocol (FTP)** used for file transfer.
- **Simple Mail Transfer Protocol (SMTP)** used for mail services.
- **Domain Name System (DNS)** used for mapping host names onto their network addresses.
- **Hyper Text Transfer Protocol (HTTP)** used for fetching pages on the World Wide Web (WWW).
- **Real-time Transport Protocol (RTP)** used for delivering real-time media such as voice or movies.

ADDRESSING in TCP/IP

Four levels of addresses are used in an internet employing the *TCP/IP* protocols

1. Physical Addresses or Link Address
2. Logical Addresses or IP Address
3. Port Addresses
4. Specific Addresses



Physical Addresses (or) **Link address**

- The physical address is the address of a node as defined by its LAN or WAN.
- It is included in the frame used by the data link layer. It is the lowest-level address.
- The physical addresses have authority over the network (LAN or WAN). The size and format of these addresses vary depending on the network.
- **For example, Ethernet** uses a 6-byte (48-bit) physical address that is imprinted on the network interface card (NIC) such as **07:01:02:01 :2C:4B.**

Logical address

- Logical addresses are necessary for universal communications that are independent of underlying physical networks.
- Physical addresses are not adequate in an internetwork environment where different networks can have different address formats.
- Logical addressing is a universal addressing system in which each host can be identified uniquely, regardless of the underlying physical network.
- A logical address in the Internet is currently a 32-bit address that can uniquely define a host connected to the Internet. No two publicly addressed and visible hosts on the Internet can have the same IP address.

Example: **198.20.30.1** where each number is a 8 bit binary number.

127.0.0.1 is local host IP address.

Port Address

- The address assigned to a process is called a **Port Address**. A port address in TCP/IP is **16 bits** in length.
- The IP address and the physical address are necessary for a quantity of data to travel from a source to the destination host. However, arrival at the destination host is not the final objective of data communications on the Internet.
- Computers are devices that can run multiple processes at the same time.
- The end objective of Internet communication is a process communicating with another process.
- For example, computer A can communicate with computer C by using TELNET. At the same time, computer A communicates with computer B by using the File Transfer Protocol (FTP).
- For these processes to receive data simultaneously, we need to provide different addresses for different processes. The addresses which are assigned to different processes is called Port addresses.

Process	Port Number
FTP	21
TELNET	23
SMTP	25
DNS	53
HTTP	80
IMAP	143
SNMP	161
HTTPS	443

Specific Addresses

Some applications have user-friendly addresses that are designed for that specific address.

Examples: E- mail address such as dccn@gmail.com, Universal Resource Locator (URL) such aswww.google.com

1.2 Transmission Media, Techniques for Bandwidth utilization: Line configuration, Multiplexing – Frequency division, Time division and Wave division,

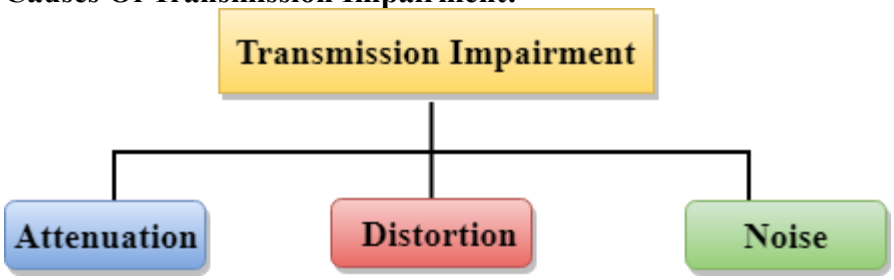
Transmission media

- Transmission media is a communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagnetic signals.
- The main functionality of the transmission media is to carry the information in the form of bits through **LAN**(Local Area Network).
- It is a physical path between transmitter and receiver in data communication.
- In a copper-based network, the bits in the form of electrical signals.
- In a fibre based network, the bits in the form of light pulses.
- In **OSI**(Open System Interconnection) phase, transmission media supports the Layer 1. Therefore, it is considered to be as a Layer 1 component.
- The electrical signals can be sent through the copper wire, fibre optics, atmosphere, water, and vacuum.
- The characteristics and quality of data transmission are determined by the characteristics of medium and signal.
- Transmission media is of two types are wired media and wireless media. In wired media, medium characteristics are more important whereas, in wireless media, signal characteristics are more important.
- Different transmission media have different properties such as bandwidth, delay, cost and ease of installation and maintenance.
- The transmission media is available in the lowest layer of the OSI reference model, i.e., **Physical layer**.

Some factors need to be considered for designing the transmission media:

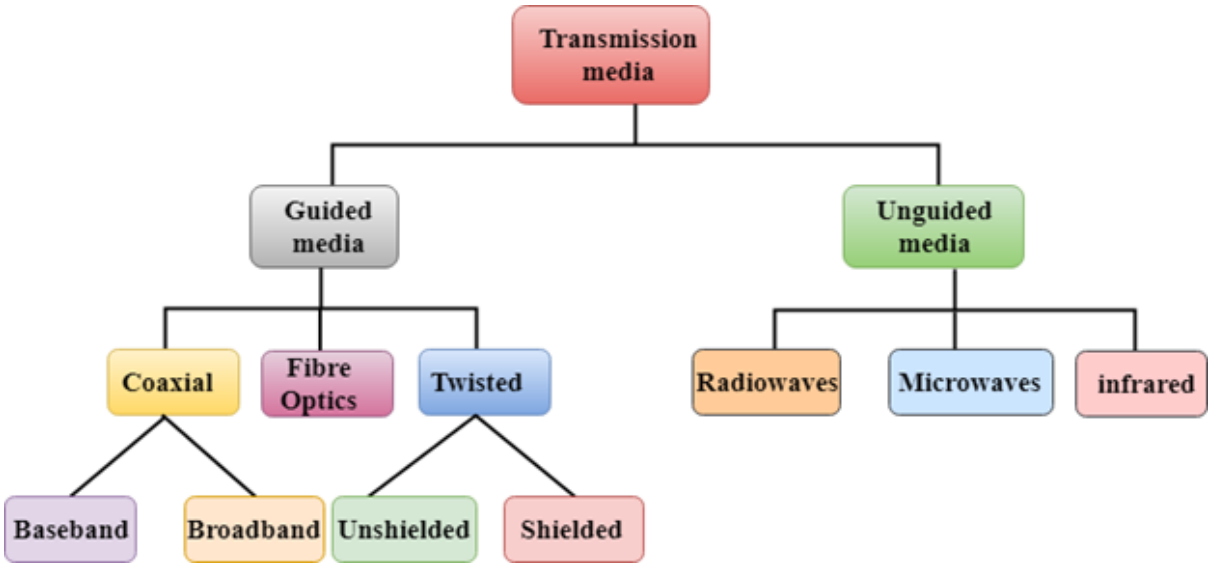
- **Bandwidth:** All the factors are remaining constant, the greater the bandwidth of a medium, the higher the data transmission rate of a signal.
- **Transmission impairment:** When the received signal is not identical to the transmitted one due to the transmission impairment. The quality of the signals will get destroyed due to transmission impairment.
- **Interference:** An interference is defined as the process of disrupting a signal when it travels over a communication medium on the addition of some unwanted signal.

Causes Of Transmission Impairment:



- **Attenuation:** Attenuation means the loss of energy, i.e., the strength of the signal decreases with increasing the distance which causes the loss of energy.
- **Distortion:** Distortion occurs when there is a change in the shape of the signal. This type of distortion is examined from different signals having different frequencies. Each frequency component has its own propagation speed, so they reach at a different time which leads to the delay distortion.
- **Noise:** When data is travelled over a transmission medium, some unwanted signal is added to it which creates the noise.

Classification Of Transmission Media:



Guided Media

It is defined as the physical medium through which the signals are transmitted. It is also known as Bounded media.

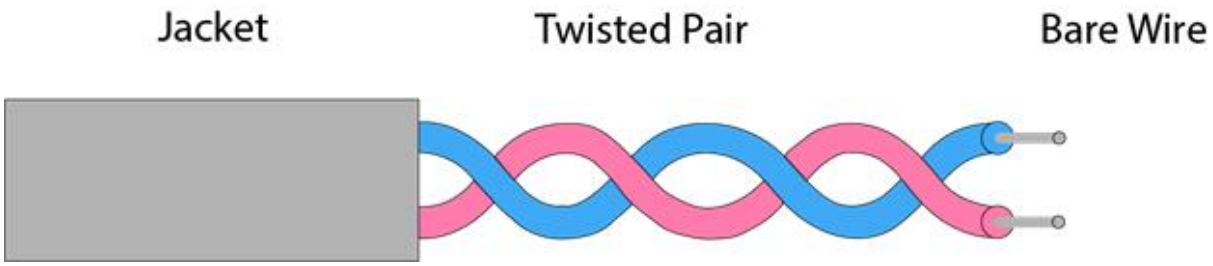
Types Of Guided media:

Twisted pair:

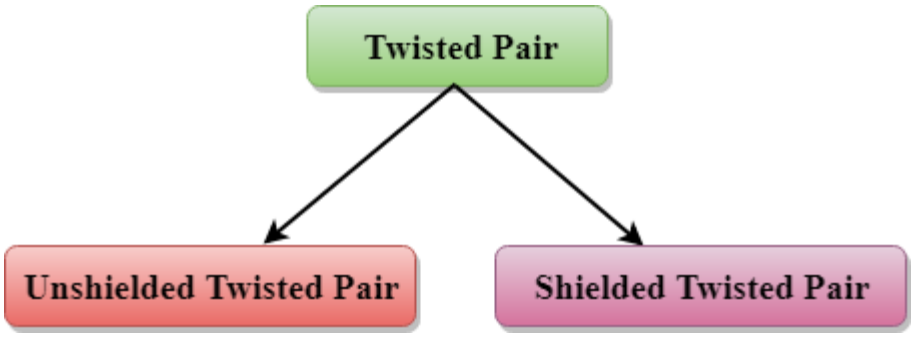
Twisted pair is a physical media made up of a pair of cables twisted with each other. A twisted pair cable is cheap as compared to other transmission media. Installation of the twisted pair cable is easy, and it is a lightweight cable. The frequency range for twisted pair cable is from 0 to 3.5KHz.

A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern.

The degree of reduction in noise interference is determined by the number of turns per foot. Increasing the number of turns per foot decreases noise interference.



Types of Twisted pair:



Unshielded Twisted Pair:

An unshielded twisted pair is widely used in telecommunication. Following are the categories of the unshielded twisted pair cable:

- **Category 1:** Category 1 is used for telephone lines that have low-speed data.
- **Category 2:** It can support upto 4Mbps.
- **Category 3:** It can support upto 16Mbps.
- **Category 4:** It can support upto 20Mbps. Therefore, it can be used for long-distance communication.
- **Category 5:** It can support upto 200Mbps.

Advantages Of Unshielded Twisted Pair:

- It is cheap.

- Installation of the unshielded twisted pair is easy.
- It can be used for high-speed LAN.

Disadvantage:

- This cable can only be used for shorter distances because of attenuation.

Shielded Twisted Pair

A shielded twisted pair is a cable that contains the mesh surrounding the wire that allows the higher transmission rate.

Characteristics Of Shielded Twisted Pair:

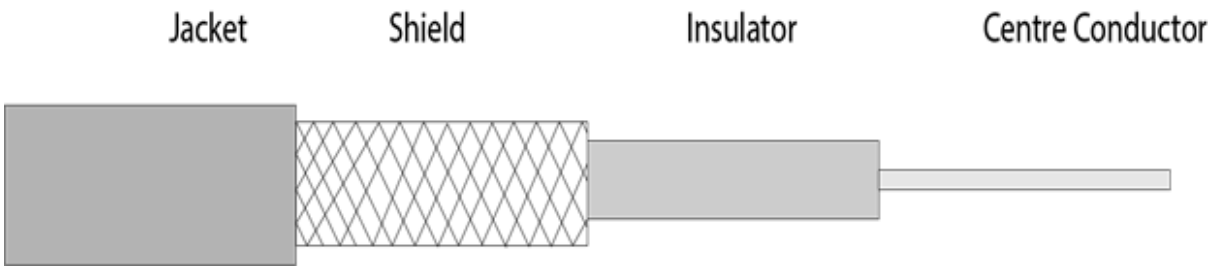
- The cost of the shielded twisted pair cable is not very high and not very low.
- An installation of STP is easy.
- It has higher capacity as compared to unshielded twisted pair cable.
- It has a higher attenuation.
- It is shielded that provides the higher data transmission rate.

Disadvantages

- It is more expensive as compared to UTP and coaxial cable.
- It has a higher attenuation rate.

Coaxial Cable

- Coaxial cable is very commonly used transmission media, for example, TV wire is usually a coaxial cable.
- The name of the cable is coaxial as it contains two conductors parallel to each other.
- It has a higher frequency as compared to Twisted pair cable.
- The inner conductor of the coaxial cable is made up of copper, and the outer conductor is made up of copper mesh. The middle core is made up of non-conductive cover that separates the inner conductor from the outer conductor.
- The middle core is responsible for the data transferring whereas the copper mesh prevents from the **EMI**(Electromagnetic interference).



Coaxial cable is of two types:

1. **Baseband transmission:** It is defined as the process of transmitting a single signal at high speed.
2. **Broadband transmission:** It is defined as the process of transmitting multiple signals simultaneously.

Advantages Of Coaxial cable:

- The data can be transmitted at high speed.
- It has better shielding as compared to twisted pair cable.
- It provides higher bandwidth.

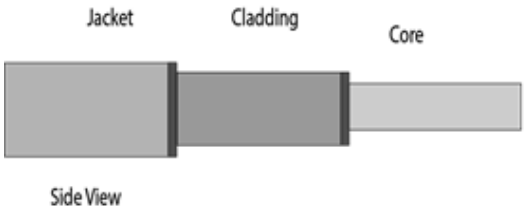
Disadvantages Of Coaxial cable:

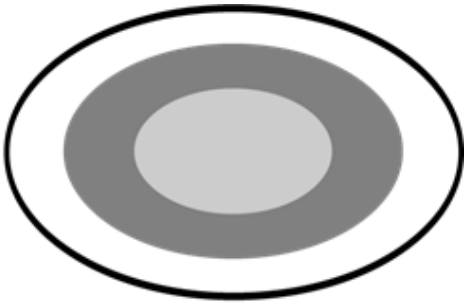
- It is more expensive as compared to twisted pair cable.
- If any fault occurs in the cable causes the failure in the entire network.

Fibre Optic

- Fibre optic cable is a cable that uses electrical signals for communication.
- Fibre optic is a cable that holds the optical fibres coated in plastic that are used to send the data by pulses of light.
- The plastic coating protects the optical fibres from heat, cold, electromagnetic interference from other types of wiring.
- Fibre optics provide faster data transmission than copper wires.

Diagrammatic representation of fibre optic cable:





Basic elements of Fibre optic cable:

- **Core:** The optical fibre consists of a narrow strand of glass or plastic known as a core. A core is a light transmission area of the fibre. The more the area of the core, the more light will be transmitted into the fibre.
- **Cladding:** The concentric layer of glass is known as cladding. The main functionality of the cladding is to provide the lower refractive index at the core interface as to cause the reflection within the core so that the light waves are transmitted through the fibre.
- **Jacket:** The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fibre strength, absorb shock and extra fibre protection.

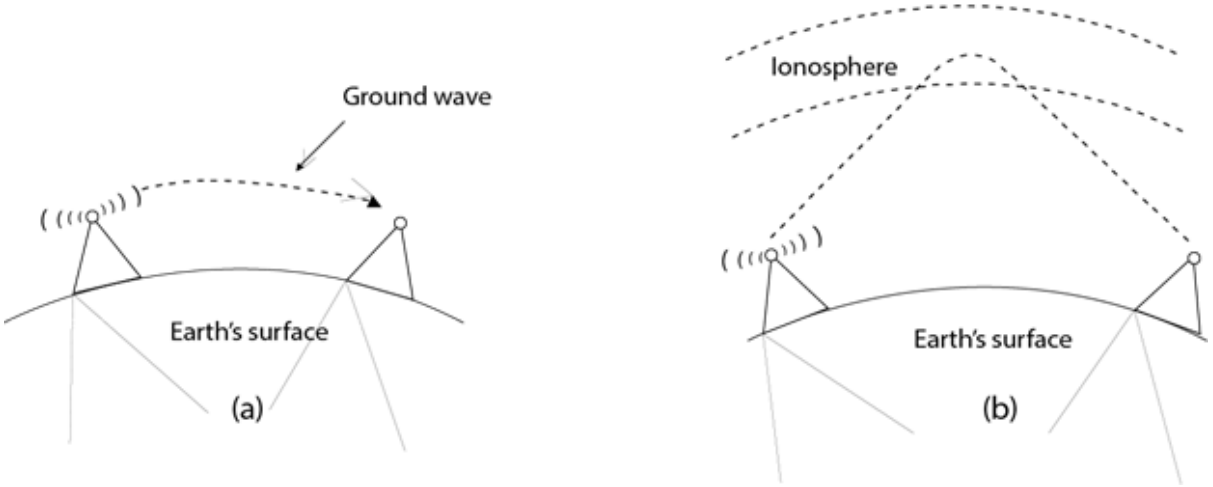
Following are the advantages of fibre optic cable over copper:

- **Greater Bandwidth:** The fibre optic cable provides more bandwidth as compared copper. Therefore, the fibre optic carries more data as compared to copper cable.
- **Faster speed:** Fibre optic cable carries the data in the form of light. This allows the fibre optic cable to carry the signals at a higher speed.
- **Longer distances:** The fibre optic cable carries the data at a longer distance as compared to copper cable.
- **Better reliability:** The fibre optic cable is more reliable than the copper cable as it is immune to any temperature changes while it can cause obstruct in the connectivity of copper cable.
- **Thinner and Sturdier:** Fibre optic cable is thinner and lighter in weight so it can withstand more pull pressure than copper cable.

UnGuided Transmission

- Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.

- Radio waves are omnidirectional, i.e., the signals are propagated in all the directions.
- The range in frequencies of radio waves is from 3Khz to 1 khz.
- In the case of radio waves, the sending and receiving antenna are not aligned, i.e., the wave sent by the sending antenna can be received by any receiving antenna.
- An example of the radio wave is **FM radio**.



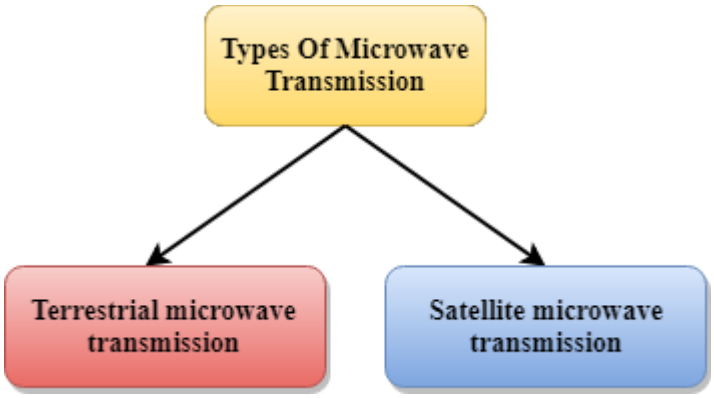
Applications Of Radio waves:

- A Radio wave is useful for multicasting when there is one sender and many receivers.
- An FM radio, television, cordless phones are examples of a radio wave.

Advantages Of Radio transmission:

- Radio transmission is mainly used for wide area networks and mobile cellular phones.
- Radio waves cover a large area, and they can penetrate the walls.
- Radio transmission provides a higher transmission rate.

Microwaves



Microwaves are of two types:

- Terrestrial microwave
- Satellite microwave communication.

Terrestrial Microwave Transmission

- Terrestrial Microwave transmission is a technology that transmits the focused beam of a radio signal from one ground-based microwave transmission antenna to another.
- Microwaves are the electromagnetic waves having the frequency in the range from 1GHz to 1000 GHz.
- Microwaves are unidirectional as the sending and receiving antenna is to be aligned, i.e., the waves sent by the sending antenna are narrowly focussed.
- In this case, antennas are mounted on the towers to send a beam to another antenna which is km away.
- It works on the line of sight transmission, i.e., the antennas mounted on the towers are the direct sight of each other.

Characteristics of Microwave:

- **Frequency range:** The frequency range of terrestrial microwave is from 4-6 GHz to 21-23 GHz.
- **Bandwidth:** It supports the bandwidth from 1 to 10 Mbps.
- **Short distance:** It is inexpensive for short distance.
- **Long distance:** It is expensive as it requires a higher tower for a longer distance.
- **Attenuation:** Attenuation means loss of signal. It is affected by environmental conditions and antenna size.

Advantages Of Microwave:

- Microwave transmission is cheaper than using cables.
- It is free from land acquisition as it does not require any land for the installation of cables.
- Microwave transmission provides an easy communication in terrains as the installation of cable in terrain is quite a difficult task.
- Communication over oceans can be achieved by using microwave transmission.

Disadvantages of Microwave transmission:

- **Eavesdropping:** An eavesdropping creates insecure communication. Any malicious user can catch the signal in the air by using its own antenna.
- **Out of phase signal:** A signal can be moved out of phase by using microwave transmission.
- **Susceptible to weather condition:** A microwave transmission is susceptible to weather condition. This means that any environmental change such as rain, wind can distort the signal.
- **Bandwidth limited:** Allocation of bandwidth is limited in the case of microwave transmission.

Satellite Microwave Communication

- A satellite is a physical object that revolves around the earth at a known height.
- Satellite communication is more reliable nowadays as it offers more flexibility than cable and fibre optic systems.
- We can communicate with any point on the globe by using satellite communication.

How Does Satellite work?

The satellite accepts the signal that is transmitted from the earth station, and it amplifies the signal. The amplified signal is retransmitted to another earth station.

Advantages Of Satellite Microwave Communication:

- The coverage area of a satellite microwave is more than the terrestrial microwave.
- The transmission cost of the satellite is independent of the distance from the centre of the coverage area.
- Satellite communication is used in mobile and wireless communication applications.
- It is easy to install.
- It is used in a wide variety of applications such as weather forecasting, radio/TV signal broadcasting, mobile communication, etc.

Disadvantages Of Satellite Microwave Communication:

- Satellite designing and development requires more time and higher cost.
- The Satellite needs to be monitored and controlled on regular periods so that it remains in orbit.
- The life of the satellite is about 12-15 years. Due to this reason, another launch of the satellite has to be planned before it becomes non-functional.

Infrared

- An infrared transmission is a wireless technology used for communication over short ranges.
- The frequency of the infrared in the range from 300 GHz to 400 THz.
- It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone resides in the same closed area.

Characteristics Of Infrared:

- It supports high bandwidth, and hence the data rate will be very high.
- Infrared waves cannot penetrate the walls. Therefore, the infrared communication in one room cannot be interrupted by the nearby rooms.
- An infrared communication provides better security with minimum interference.
- Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.

Techniques for Bandwidth utilization: Line configuration, Multiplexing - Frequency division, Time division and Wave division.

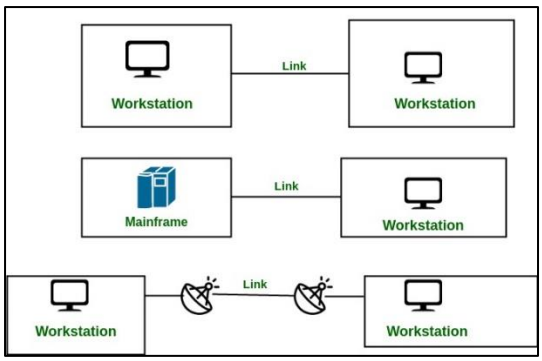
Line configuration:

A network is two or more devices connected through a link. A link is a communication pathway that transfers data from one device to another. Devices can be a computer, printer, or any other device that is capable to send and receive data. For visualization purposes, imagine any link as a line drawn between two points.

For communication to occur, two devices must be connected in some way to the same link at the same time. There are two possible types of connections:

1. **Point-to-Point Connection**
2. **Multipoint Connection**

Example: Point-to-Point connection between the remote control and Television for changing the channels.



Here are some features of different line configurations in computer networks:

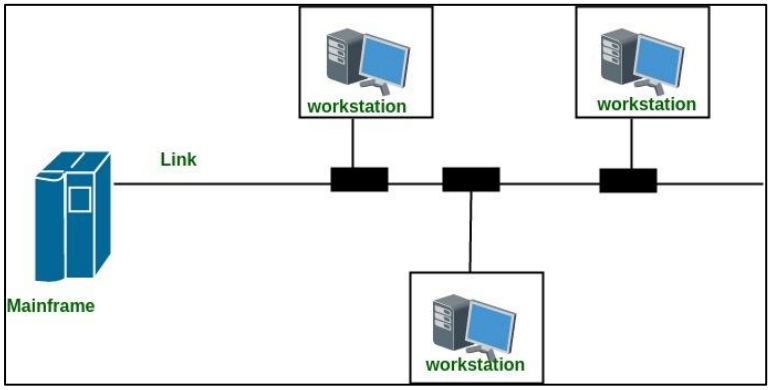
Point-to-Point:

- Uses a dedicated link to connect two devices
- Simple and easy to set up
- Limited to two devices only
- Does not require a network interface card (NIC) or a hub/switch
- Can become complex and difficult to manage as the network grows

Multipoint Connection :

1. It is also called Multidrop configuration. In this connection, two or more devices share a single link.
2. If more than two devices share the link then the channel is considered a 'shared channel'. With shared capacity, there can be two possibilities in a Multipoint Line configuration:

Spatial Sharing: If several devices can share the link simultaneously, it's called Spatially shared line configuration.
Temporal (Time) Sharing: If users must take turns using the link, then it's called Temporally shared or Time Shared Line configuration.



Multiplexing:

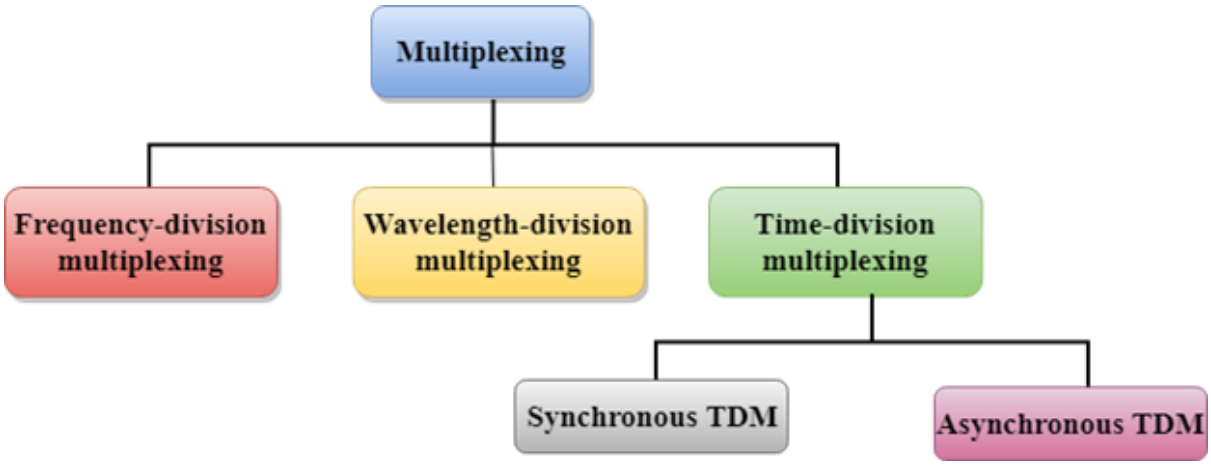
Multiplexing is a technique used to combine and send the multiple data streams over a single medium. The process of combining the data streams is known as multiplexing and hardware used for multiplexing is known as a multiplexer.

Multiplexing is achieved by using a device called Multiplexer (**MUX**) that combines n input lines to generate a single output line. Multiplexing follows many-to-one, i.e., n input lines and one output line.

Demultiplexing is achieved by using a device called Demultiplexer (**DEMUX**) available at the receiving end. DEMUX separates a signal into its component signals (one input and n outputs). Therefore, we can say that demultiplexing follows the one-to-many approach.

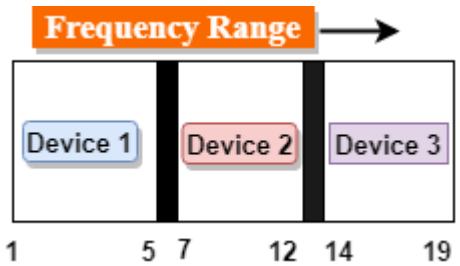
Multiplexing Techniques

Multiplexing techniques can be classified as:



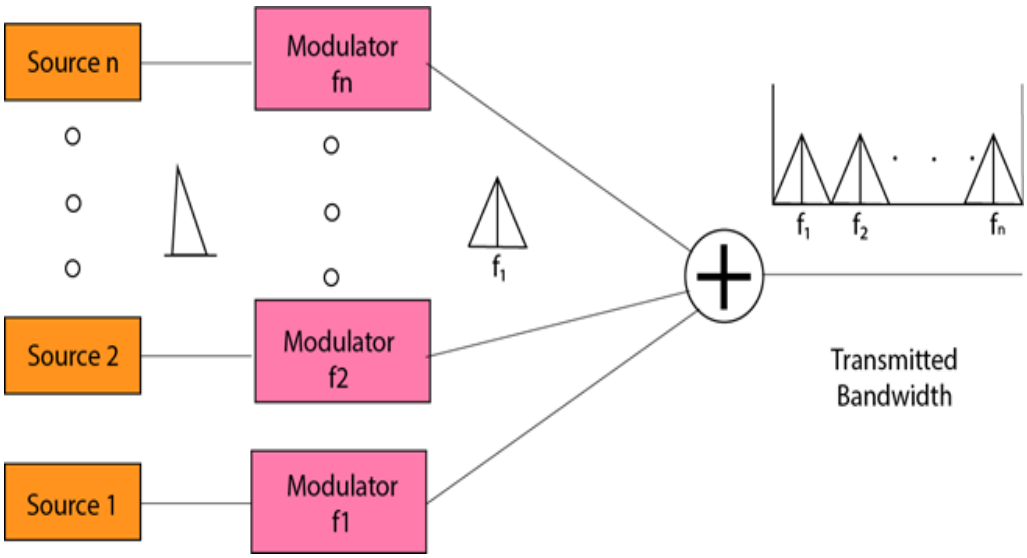
Frequency-division Multiplexing (FDM)

- It is an analog technique.
- **Frequency Division Multiplexing** is a technique in which the available bandwidth of a single transmission medium is subdivided into several channels.



- In the above diagram, a single transmission medium is subdivided into several frequency channels, and each frequency channel is given to different devices. Device 1 has a frequency channel of range from 1 to 5.

- The input signals are translated into frequency bands by using modulation techniques, and they are combined by a multiplexer to form a composite signal.
- The main aim of the FDM is to subdivide the available bandwidth into different frequency channels and allocate them to different devices.
- Using the modulation technique, the input signals are transmitted into frequency bands and then combined to form a composite signal.
- The carriers which are used for modulating the signals are known as **sub-carriers**. They are represented as f1,f2..fn.
- **FDM** is mainly used in radio broadcasts and TV networks.



Advantages Of FDM:

- FDM is used for analog signals.
- FDM process is very simple and easy modulation.
- A Large number of signals can be sent through an FDM simultaneously.
- It does not require any synchronization between sender and receiver.

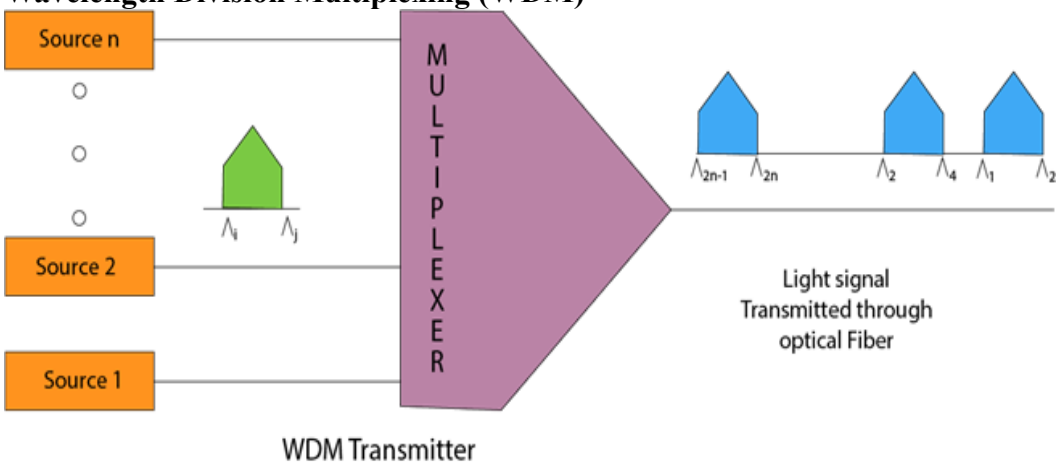
Disadvantages Of FDM:

- FDM technique is used only when low-speed channels are required.
- It suffers the problem of crosstalk.
- A Large number of modulators are required.
- It requires a high bandwidth channel.

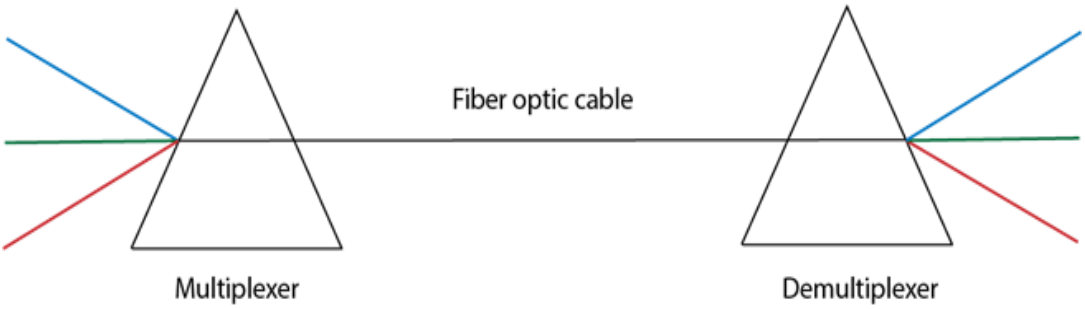
Applications Of FDM:

- FDM is commonly used in TV networks.
- It is used in FM and AM broadcasting. Each FM radio station has different frequencies, and they are multiplexed to form a composite signal. The multiplexed signal is transmitted in the air.

Wavelength Division Multiplexing (WDM)



- Wavelength Division Multiplexing is same as FDM except that the optical signals are transmitted through the fibre optic cable.
- WDM is used on fibre optics to increase the capacity of a single fibre.
- It is used to utilize the high data rate capability of fibre optic cable.
- It is an analog multiplexing technique.
- Optical signals from different source are combined to form a wider band of light with the help of multiplexer.
- At the receiving end, demultiplexer separates the signals to transmit them to their respective destinations.
- Multiplexing and Demultiplexing can be achieved by using a prism.
- Prism can perform a role of multiplexer by combining the various optical signals to form a composite signal, and the composite signal is transmitted through a fibre optical cable.
- Prism also performs a reverse operation, i.e., demultiplexing the signal.



Time Division Multiplexing

- It is a digital technique.
- In Frequency Division Multiplexing Technique, all signals operate at the same time with different frequency, but in case of Time Division Multiplexing technique, all signals operate at the same frequency with different time.
- In **Time Division Multiplexing technique**, the total time available in the channel is distributed among different users. Therefore, each user is allocated with different time interval known as a Time slot at which data is to be transmitted by the sender.
- A user takes control of the channel for a fixed amount of time.
- In Time Division Multiplexing technique, data is not transmitted simultaneously rather the data is transmitted one-by-one.
- In TDM, the signal is transmitted in the form of frames. Frames contain a cycle of time slots in which each frame contains one or more slots dedicated to each user.
- It can be used to multiplex both digital and analog signals but mainly used to multiplex digital signals.

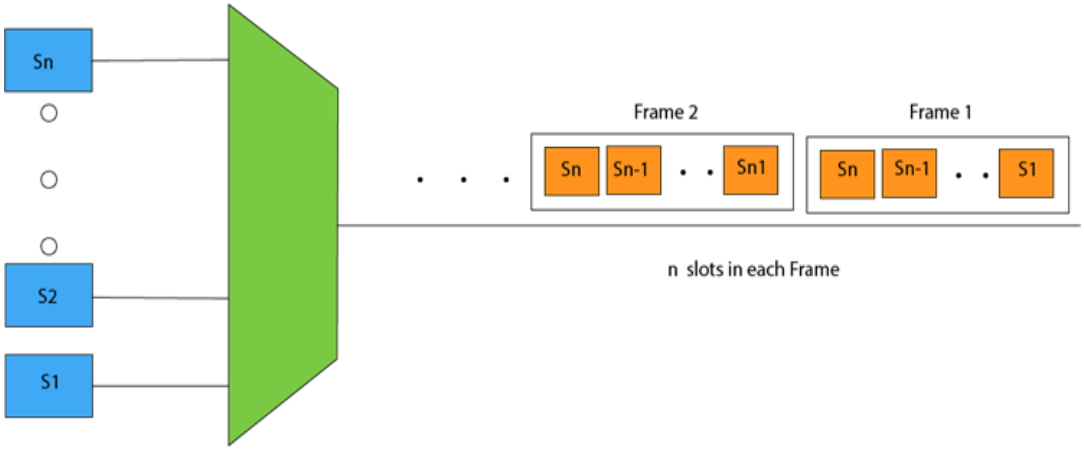
There are two types of TDM:

- Synchronous TDM
- Asynchronous TDM

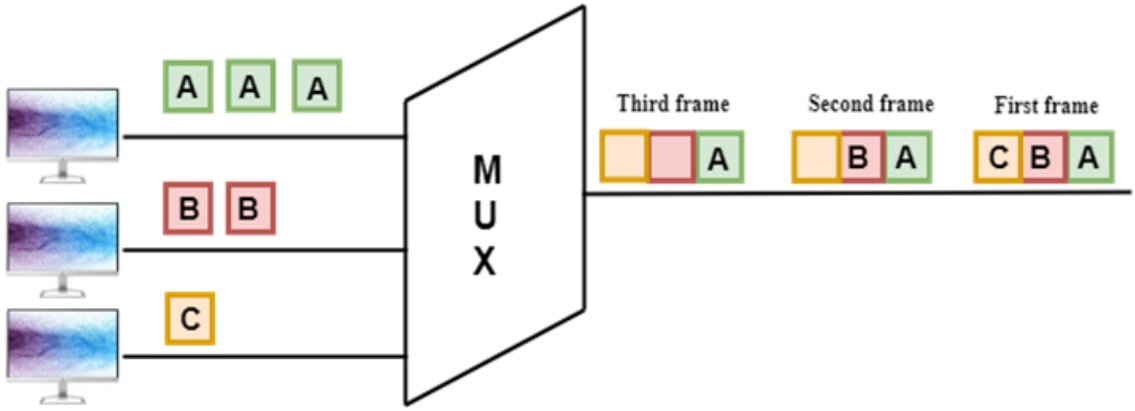
Synchronous TDM

- A Synchronous TDM is a technique in which time slot is preassigned to every device.
- In Synchronous TDM, each device is given some time slot irrespective of the fact that the device contains the data or not.
- If the device does not have any data, then the slot will remain empty.
- In Synchronous TDM, signals are sent in the form of frames. Time slots are organized in the form of frames. If a device does not have data for a particular time slot, then the empty slot will be transmitted.

- The most popular Synchronous TDM are T-1 multiplexing, ISDN multiplexing, and SONET multiplexing.
- If there are n devices, then there are n slots.



Concept Of Synchronous TDM



In the above figure, the Synchronous TDM technique is implemented. Each device is allocated with some time slot. The time slots are transmitted irrespective of whether the sender has data to send or not.

Disadvantages Of Synchronous TDM:

- The capacity of the channel is not fully utilized as the empty slots are also transmitted which is having no data. In the above figure, the first frame is completely filled, but in the last two frames, some slots are empty. Therefore, we can say that the capacity of the channel is not utilized efficiently.
- The speed of the transmission medium should be greater than the total speed of the input lines. An alternative approach to the Synchronous TDM is Asynchronous Time Division Multiplexing.

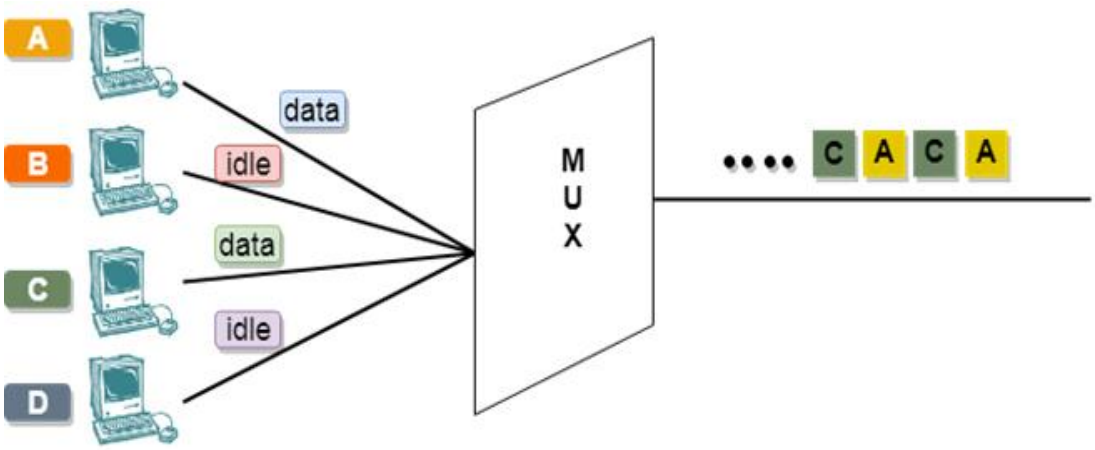
Asynchronous TDM

- An asynchronous TDM is also known as Statistical TDM.
- An asynchronous TDM is a technique in which time slots are not fixed as in the case of Synchronous TDM. Time slots are allocated to only those devices which have the data to send. Therefore, we can say that Asynchronous Time Division multiplexor transmits only the data from active workstations.
- An asynchronous TDM technique dynamically allocates the time slots to the devices.
- In Asynchronous TDM, total speed of the input lines can be greater than the capacity of the channel.
- Asynchronous Time Division multiplexor accepts the incoming data streams and creates a frame that contains only data with no empty slots.
- In Asynchronous TDM, each slot contains an address part that identifies the source of the data.

ADDRESS	DATA

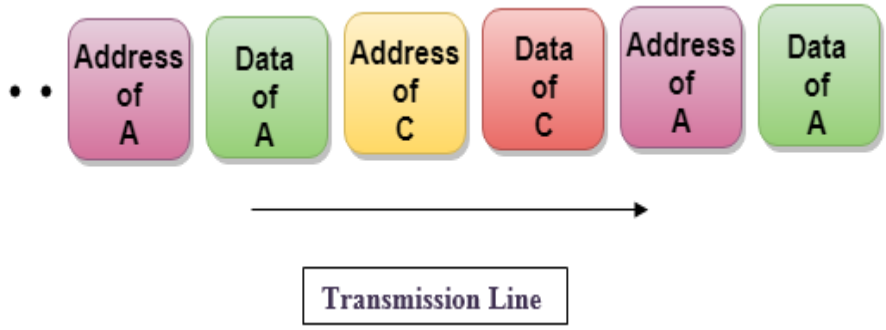
- The difference between Asynchronous TDM and Synchronous TDM is that many slots in Synchronous TDM are unutilized, but in Asynchronous TDM, slots are fully utilized. This leads to the smaller transmission time and efficient utilization of the capacity of the channel.
- In Synchronous TDM, if there are n sending devices, then there are n time slots. In Asynchronous TDM, if there are n sending devices, then there are m time slots where m is less than n (**m<n**).
- The number of slots in a frame depends on the statistical analysis of the number of input lines.

Concept Of Asynchronous TDM



In the above diagram, there are 4 devices, but only two devices are sending the data, i.e., A and C. Therefore, the data of A and C are only transmitted through the transmission line.

Frame of above diagram can be represented as:



The above figure shows that the data part contains the address to determine the source of the data.

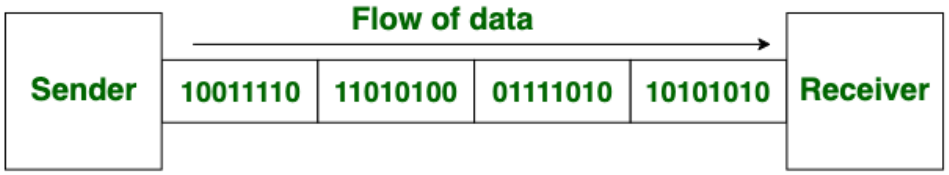
1.3 Asynchronous and Synchronous transmission , XDSL , Introduction to Wired and Wireless LAN

Asynchronous and Synchronous Transmission:

Synchronous Transmission: In Synchronous Transmission, data is sent in form of blocks or frames. This transmission is the full-duplex type. Between sender and receiver, synchronization is compulsory. In Synchronous transmission, There is no gap present between data. It is more efficient and more reliable than asynchronous transmission to transfer a large amount of data.

Example:

- Chat Rooms
- Telephonic Conversations
- Video Conferencing

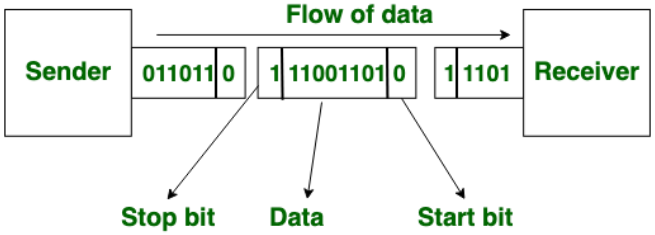


Synchronous Transmission

Asynchronous Transmission: In Asynchronous Transmission, data is sent in form of byte or character. This transmission is the half-duplex type transmission. In this transmission start bits and stop bits are added with data. It does not require synchronization.

Example:

- Email
- Forums
- Letters



Asynchronous Transmission

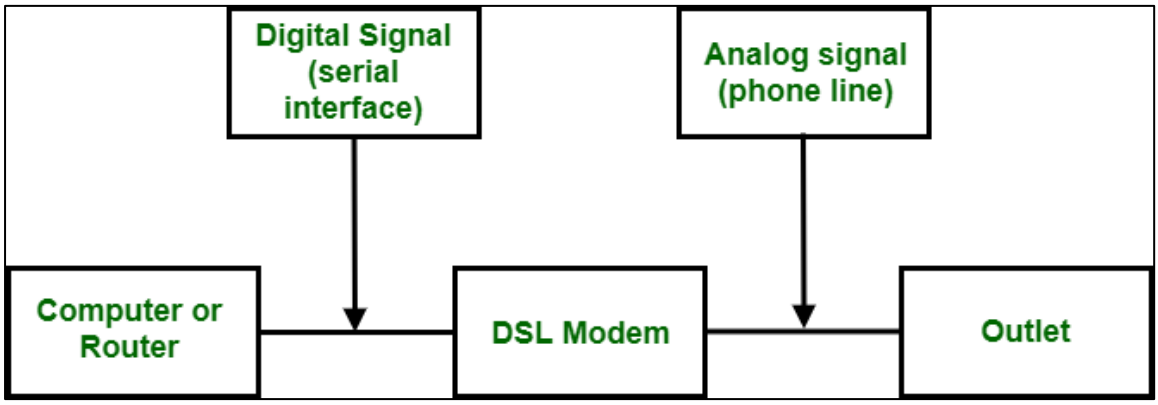
Difference between Synchronous and Asynchronous Transmission

S. No.	Synchronous Transmission	Asynchronous Transmission
1.	In Synchronous transmission, data is sent in form of blocks or frames.	In Asynchronous transmission, data is sent in form of bytes or characters.
2.	Synchronous transmission is fast.	Asynchronous transmission is slow.

S. No.	Synchronous Transmission	Asynchronous Transmission
3.	Synchronous transmission is costly.	Asynchronous transmission is economical.
4.	In Synchronous transmission, the time interval of transmission is constant.	In Asynchronous transmission, the time interval of transmission is not constant, it is random.
5.	In this transmission, users have to wait till the transmission is complete before getting a response back from the server.	Here, users do not have to wait for the completion of transmission in order to get a response from the server.
6.	In Synchronous transmission, there is no gap present between data.	In Asynchronous transmission, there is a gap present between data.
7.	Efficient use of transmission lines is done in synchronous transmission.	While in Asynchronous transmission, the transmission line remains empty during a gap in character transmission.
8.	The start and stop bits are not used in transmitting data.	The start and stop bits are used in transmitting data that imposes extra overhead.
9.	Synchronous transmission needs precisely synchronized clocks for the information of new bytes.	Asynchronous transmission does not need synchronized clocks as parity bit is used in this transmission for information of new bytes.
10.	Errors are detected and corrected in real time.	Errors are detected and corrected when the data is received.
11.	Low latency due to real-time communication.	High latency due to processing time and waiting for data to become available.
12.	Examples: Telephonic conversations, Video conferencing, Online gaming.	Examples: Email, File transfer, Online forms.

xDSL(DSL):

Digital Subscriber Line (DSL) is the most promising for the support of high-speed internet connection over the existing local loops. Basically, it is a set of technologies. **This set is also referred to as xDSL**, where x can be replaced by A, V, H, or S.



Digital Subscriber Line

Technologies of Digital Subscriber Line:

1. ADSL (Asymmetric DSL)
2. ADSL Lite or Universal ADSL or Splitterless ADSL
3. HDSL (High-bit-rate DSL)
4. SDSL (Symmetric DSL)
5. VDSL (Very high bit-rate DSL)

Summary: The following is summary table for technologies of DSL. The values in the following table are approximate and can vary from one implementation to another.

Technology	**Downstream Rate**	**Upstream Rate**	**Distance in feet**	**Twisted Pairs**	**Line Code**
ADSL	1.5-6.1 Mbps	16-640 kbps	12,000	1	DMT
ADSL Lite	1.5 Mbps	500 kbps	18,000	1	DMT
HDSL	1.5-2.0 Mbps	1.5-2.0 Mbps	12,000	2	2B1Q
SDSL	768 kbps	768 kbps	12,000	1	2B1Q
VDSL	25-55 Mbps	3,2 Mbps	3000-10,000	1	DMT

Features of DSL:

- It helps to meet the need for networks in different scenarios like DSL, Fiber/Cable, and 3G/4G Dongle.
- It supports ISP service providers, so we can that it is compatible with most of the service providers.

- It also supports high-quality telephone calls.
- There is an available app to manage the modem.

Introduction to wired and wireless LAN

A network consists of two or more computers that are linked in order to share all form of resources including communication. Both LAN and WLAN networks are interrelated and share moreover common characteristics.

Local Area Network (LAN):

A Local Area Network (LAN) is a type of network that connects devices in a small geographic area, such as a home, office, or school. LANs typically use wired connections, such as Ethernet cables, to connect devices to a central hub or switch. This allows devices to share data, resources, and devices such as printers and storage devices.

Advantages of LAN:

- Speed: LANs provide fast data transfer rates, typically 100 Mbps or 1 Gbps, allowing for quick data transfer between devices.
- Security: LANs are generally more secure than WLANs, as they are physically connected and less susceptible to outside interference.
- Cost: LANs can be less expensive to set up and maintain than WLANs, as they use wired connections that are often less expensive than wireless technology.

Disadvantages of LAN:

- Limited Mobility: LANs typically use wired connections, which limits device mobility and flexibility.
- Limited Range: The range of LANs is limited by the length of the Ethernet cable, which means that devices must be physically located within a small area.
- Installation: The installation of LANs can be complex, requiring the routing of cables and installation of switches.

Wireless Local Area Network (WLAN):

A Wireless Local Area Network (WLAN) is a type of network that uses wireless technology, such as Wi-Fi, to connect devices in the same area. WLANs use wireless access points to transmit data between devices, allowing for greater mobility and flexibility.

Advantages of WLAN:

- Mobility: WLANs provide greater device mobility and flexibility, as devices can connect wirelessly from anywhere within the network range.
- Easy Installation: WLANs are easier to install than LANs, as they do not require physical cabling and switches.
- Range: WLANs can cover a larger area than LANs, allowing for greater device connectivity and flexibility.

Disadvantages of WLAN:

- Security: WLANs are less secure than LANs, as wireless signals can be intercepted by unauthorized users and devices.
- Speed: WLANs provide slower data transfer rates than LANs, typically around 54 Mbps, which can result in slower data transfer between devices.

- Interference: WLANs are susceptible to interference from other wireless devices, which can cause connectivity issues.

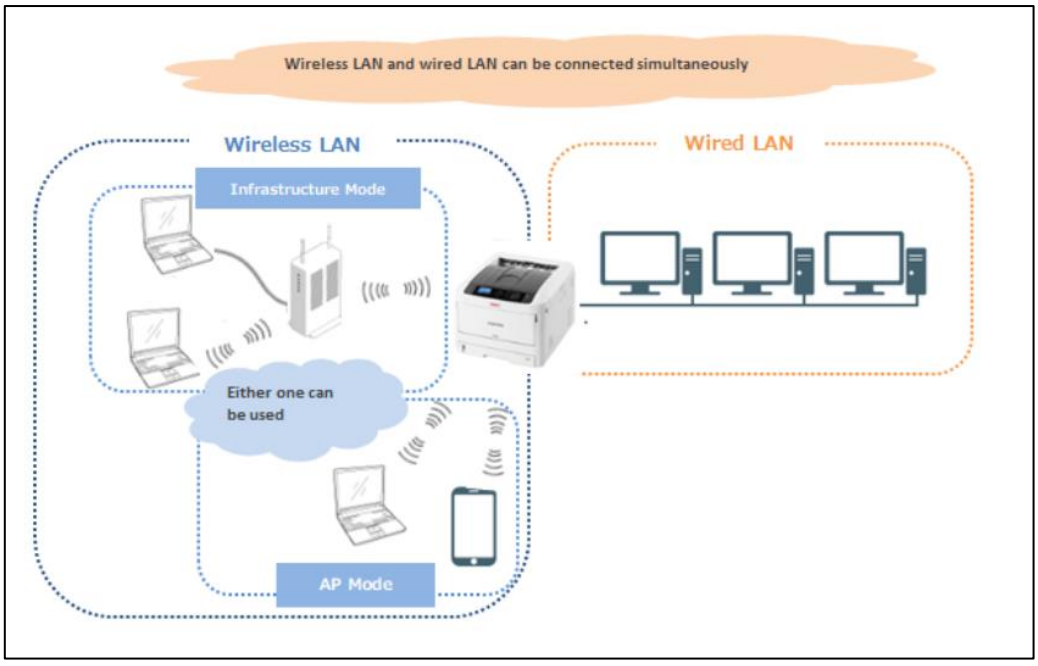
Similarities between LAN and WLAN:

- Both provide connectivity: The primary purpose of both LAN and WLAN is to provide connectivity between devices, allowing them to share data and resources.
- Both use the same protocols: LANs and WLANs use the same protocols for data transfer, such as TCP/IP and Ethernet, which ensures compatibility between devices.
- Both can support multiple devices: Both LANs and WLANs can support multiple devices simultaneously, allowing multiple users to share data and resources.
- Both can be secured: Both LANs and WLANs can be secured using encryption and authentication methods, ensuring that only authorized users have access to the network.
- Both require network hardware: Both LANs and WLANs require network hardware, such as routers, switches, and access points, to function properly.
- Both can be used for internet connectivity: Both LANs and WLANs can be used to connect to the internet, providing access to online resources and services.

Let's discuss about LAN and WLAN:

LAN	WLAN
LAN stands for Local Area Network.	WLAN stands for Wireless Local Area Network.
LAN connections include both wired and wireless connections.	WLAN connections are completely wireless.
LAN network is a collection of computers or other such network devices in a particular location that are connected together by communication elements or network elements.	WLAN network is a collection of computers or other such network devices in a particular location that are connected together wirelessly by communication elements or network elements.
LAN is free from external attacks like interruption of signals, cyber criminal attacks and so on.	Whereas, WLAN is vulnerable to external attacks.
LAN is secure.	WLAN is not secure.
LAN network has lost its popularity due to the arrival of latest wireless networks.	WLAN is popular.

LAN	WLAN
Wired LAN needs physical access like connecting the wires to the switches or routers.	Work on connecting wires to the switches and routers are neglected.
In LAN, devices are connected locally with Ethernet cable.	For WLAN Ethernet cable is not necessary.
Mobility limited.	Outstanding mobility.
It may or may not vary with external factors like environment and quality of cables.	It varies due to external factors like environment and quality of cables. Most of the external factors affect the signal transmission.
LAN is less expensive.	WLAN is more expensive.
Example: Computers connected in a college.	Example: Laptops, cell phones, tablets connected to a wireless router or hotspot.



Both LANs and WLANs have their advantages and disadvantages, depending on the specific requirements. LANs are generally faster and more secure, while WLANs provide greater mobility and flexibility. Choosing the right network for your needs depends on your specific requirements, such as speed, security, and device mobility.