UNIT-1

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 fundamentalcharacteristics:

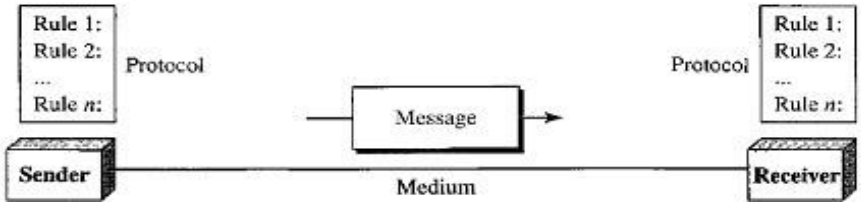
1. **Delivery** The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
2. **Accuracy** The system must deliver the data accurately. Data should not be altered. If the data is altered in transmission and left uncorrected 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.

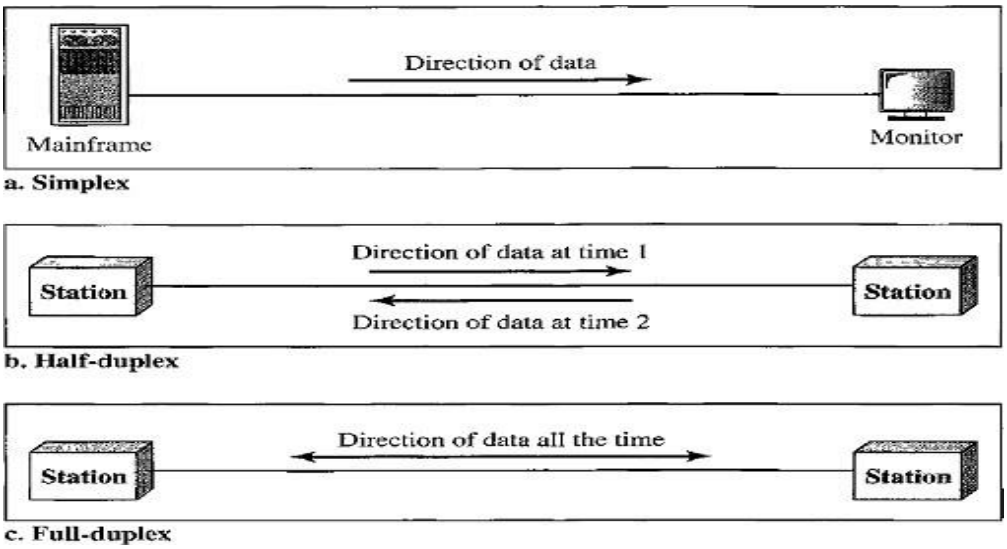
Five components of data communication



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

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, themonitor 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.

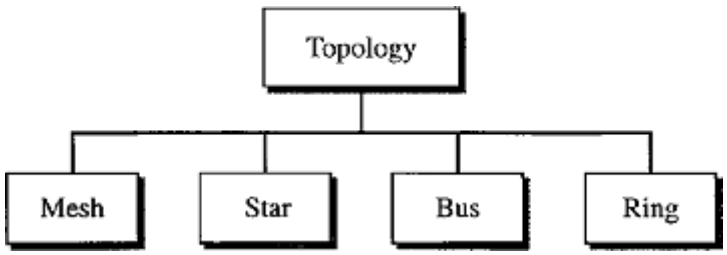
Full-Duplex

- 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.

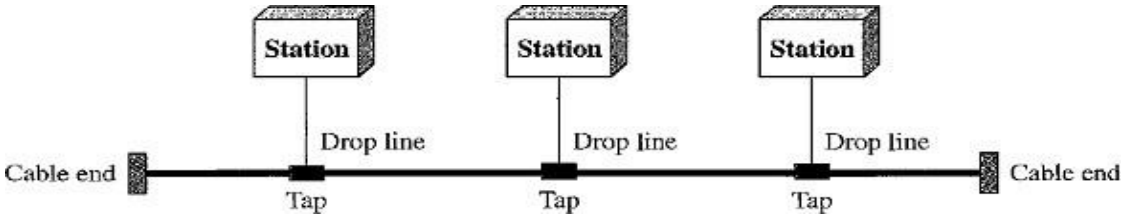
NETWORK TOPOLOGIES

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 a topology.
There are four basic topologies are present:



Bus Topology

- A **bus topology** is multipoint connection, one long cable acts as a **backbone** to link allthe 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:

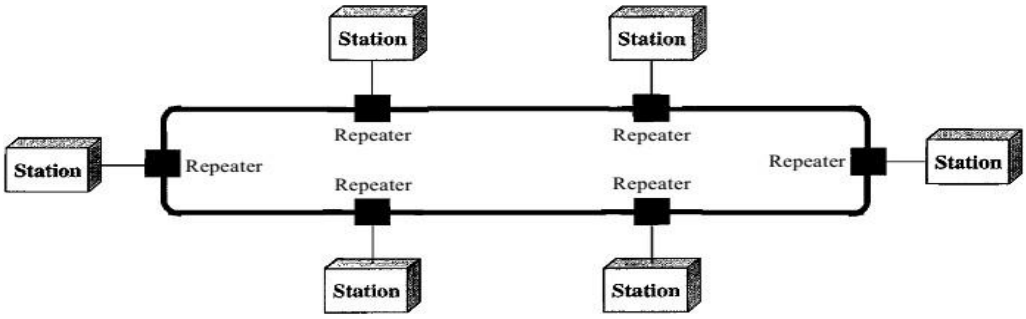
1. Installation is easy. Bus Backbone cable can be laid along the most efficient path and then connected to the nodes by drop lines of various lengths.
2. A bus uses less cabling than mesh or star topologies.

Disadvantages:

1. All the devices are connected to bus backbone cable, so that if the backbone cablefails 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 betweenthose taps.
4. More heat is generated if the number of taps are more. Heat degrades the quality ofsignal.

Ring Topology

- In a ring topology, each device has a dedicated point-to-point connection with only thetwo 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 intendedfor another device, its repeater regenerates the bits and passes them along.



Advantages:

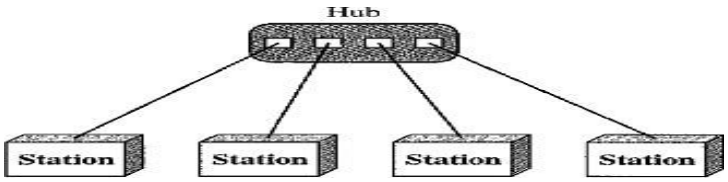
1. A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors (either physically or logically).
2. To add or delete a device requires changing only two connections.
3. The only constraints are media and traffic considerations (maximum ring length and number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

Disadvantage:

1. Unidirectional traffic can be a disadvantage.
2. In a simple ring, a 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: If hub fails entire processing will be stopped working.

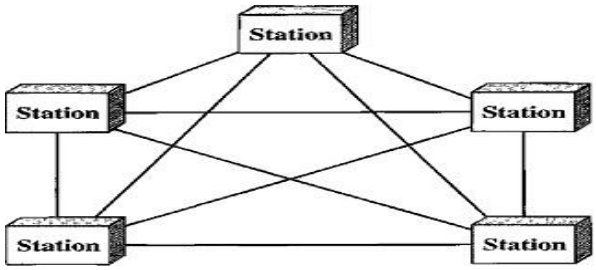
Uses: It is used in High-speed LAN's often use a star topology with a central hub.

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 accessto messages.
4. Point-to-Point links make **Fault Identification** and **Fault Isolation** easy.



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.

Usage: 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

PROTOCOL

A protocol is a set of rules that govern data communications. A protocol defines what is communicated, how it is communicated, and when it is communicated. For communication to occur, the entities must agree on a protocol.

The key elements of a protocol are: 1. Syntax 2. Semantics 3. Timing

Syntax

- The term *syntax* refers to the structure or format of the data, meaning the order in which they are presented.
- Example: a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.

Semantics

- The word *semantics* refers to the meaning of each section of bits. How are a particular pattern to be interpreted, and what action is to be taken based on that interpretation?
- For example, does an address identify the route to be taken or the final destination of the message?

Timing

- The term *timing* refers to two characteristics: when data should be sent and how fast theycan be sent.
- For example, if a sender produces data at 100 Mbps but the receiver can process data atonly 1 Mbps, the transmission will overload the receiver and some data will be lost.

NETWORK HARDWARE

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.

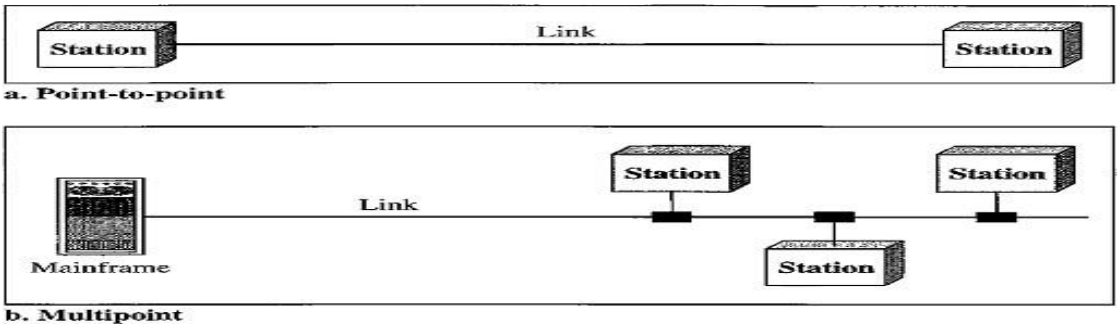
A **Node** can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

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 occurringof 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.

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)
4. Personal Area Networks (PAN)

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 butnow speeds are increased to 100 or 1000 Mbps.
- 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 small LAN to an Internet service provider (lSP).

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.

Personal Area Networks (PAN)

PAN is operable in an area the size of a room or a hall. Example: Bluetooth

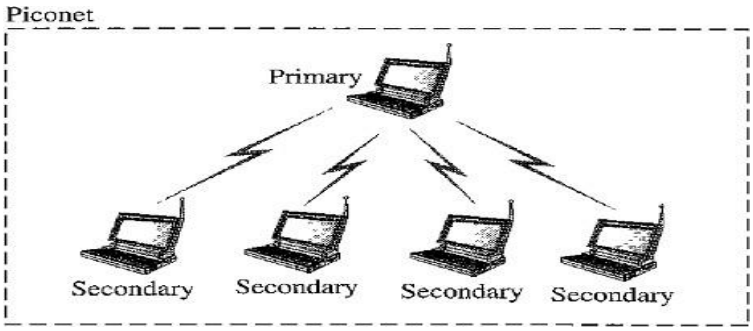
Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, desktop computers, laptop, cameras, printers, coffee makers, and so on.

- Peripheral devices such as a wireless mouse or keyboard can communicate with the computer through this technology.

- Bluetooth devices are called Gadgets. The devices find each other and make a network called Piconet.
- A Bluetooth LAN is an ad hoc network. An Ad-hoc network is a network that is formed spontaneously. A Bluetooth LAN is very small.

Piconet or Small-net

- A Bluetooth network is called a piconet, or a small net.



- A Piconet can have up to eight stations. in which only one station acts as primary station and other seven stations acts as Secondary stations.
- All the secondary stations synchronize their clocks and hopping sequence with the primary.
- The communication between the primary and the secondary can be one-to-one or one-to- many.
- A piconet can have a maximum of seven secondaries and an additional eight secondaries can be in the parked state.
- A secondary in a parked state is synchronized with the primary, but cannot take part in communication until it is moved from the parked state. Because only eight stations can beactive in a piconet.

CONNECTING DEVICES

Application layer	Application gateway
Transport layer	Transport gateway
Network layer	Router
Data link layer	Bridge, switch
Physical layer	Repeater, hub

Repeater

- Repeaters work at the physical layer.
- These are analog devices that work with signals on the cables to which they are connected.
- A signal appearing on one cable is cleaned up, amplified, and passed on to another cable.
- Repeaters do not understand frames, packets, or headers. They understand the symbols that encode bits as volts.
- Example: Classic Ethernet was designed to allow four repeaters that would boost the signal to extend the maximum cable length from 500 meters to 2500 meters.

Hubs

- Hub works at Physical layer (i.e) Hub doesn't understand Frames and MAC address.
- A hub has a number of input lines that it joins electrically.

- Hub broadcast the Frames arriving on any of the lines are sent out on all the other stations that are connected to the Hub. Hence the data traffic is very high.
- If two frames arrive at the same time, they will collide.
- All the lines coming into a hub must operate at the same speed.
- Hubs differ from repeaters in that they do not amplify the incoming signals.
- As hubs works at physical layer, these devices does not examine the link layer addressesor use them in any way.

Bridge

- Bridge is data-link layer device that connects two or more LANs.
- Bridge works on data-link layer that can understand the MAC address of frame.
- When a frame arrives, the bridge extracts the destination MAC address from the frame header and looks it up in a table to see where to send the frame.
- The bridge only outputs the frame on the port where it is needed and can forward multiple frames at the same time.
- Bridges offer much better performance than hubs. Depends upon the network type, the bridge can run on different speeds. Bridge ports can supports different speeds.

Problem with Bridges

- Bridges were originally intended to be able to join different kinds of LANs such as an Ethernet and a Token Ring LAN.
- But this never worked well because of differences between the LANs. (i.e.) Different frame formats require copying and reformatting, which takes CPU time, requires a new checksum calculation, and introduces the possibility of undetected errors due to bad bits in the bridge's memory, and also different LANs will implement their own security mechanisms and Quality of service.
- Due to all these reasons practically Bridges can connect same type of LANs only.Note: To connect different LANs Routers are used now.

Switch

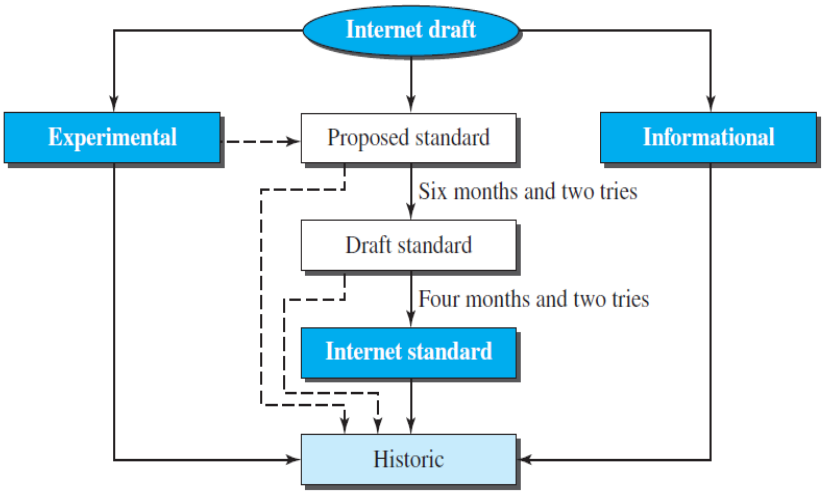
- **Switch** works at the physical and data link layers. Switch forwards the frames by usingMAC address.
- A Switch is a like a bridge with many ports gives better performance than bridge.
- Switches use point-to-point links, such as twisted-pair cables, so individual computers plug directly into a switch and thus the switch will tend to have many ports.
- Like bridge when a switch receives a frame, it extracts the destination MAC address from the frame header and looks it up in a table to see where to send the frame.
- Switches can have a buffer to hold the frames for processing. Switch forwards the frame faster than the bridge.

Routers

- Router is a network layer device. Router has Network layer, Datalink layer and Physical layer.
- Router understands logical address (IP address), it routes packets based on their logical addresses.
- A router normally connects two different networks in the Internet and has a routing table that is used for making decisions about the route.
- Example: The router can connect a Ethernet LAN and a Token Ring LAN or Router connects a LAN with a WAN.

- The routing tables are normally dynamic and are updated using routing protocols.

INTERNET STANDARDS

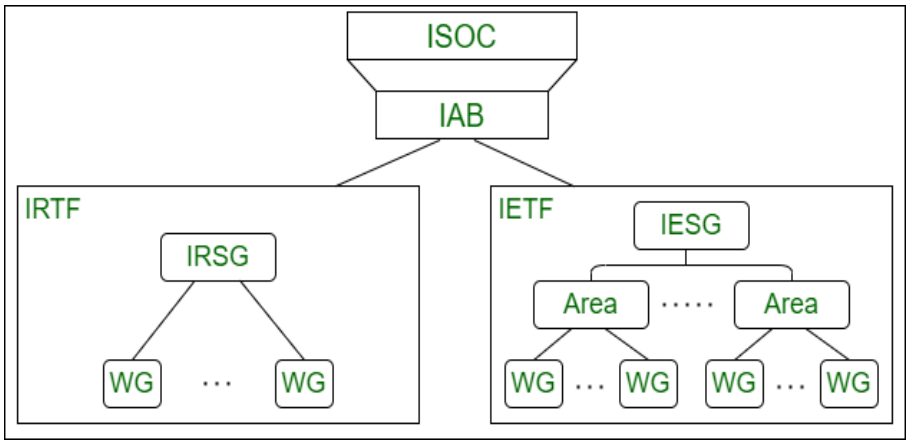


- An Internet standard is a thoroughly tested specification that is useful to and adhered to by those who work with the Internet. It is a formalized regulation that must be followed. There is a strict procedure by which a specification attains Internet standard status. A specification begins as an Internet draft. An Internet draft is a working document (a work in progress) with no official status and a six-month lifetime. Upon recommendation from the Internet authorities, a draft may be published as a Request for Comment (RFC). Each RFC is edited, assigned a number, and made available to all interested parties. RFCs go through maturity levels and are categorized according to their requirement level.
- **Maturity Levels:** An RFC, during its lifetime, falls into one of six maturity levels: proposed standard, draft standard, Internet standard, historic, experimental, and informational. Proposed Standard. A proposed standard is a specification that is stable, well understood, and of sufficient interest to the Internet community. At this level, the specification is usually tested and implemented by several different groups.
- **Draft Standard:** A proposed standard is elevated to draft standard status after at least two successful independent and interoperable implementations. Barring difficulties, a draft standard, with modifications if specific problems are encountered, normally becomes an Internet standard.
- **Internet Standard:** A draft standard reaches Internet standard status after demonstrations of successful implementation.
- **Historic:** The historic RFCs are significant from a historical perspective. They either have been superseded by later specifications or have never passed the necessary maturity levels to become an Internet standard.
- **Experimental**: An RFC classified as experimental describes work related to an experimental situation that does not affect the operation of the Internet. Such an RFC should not be implemented in any functional Internet service.
- **Informational:** An RFC classified as informational contains general, historical, or tutorial information related to the Internet. It is usually written by someone in a non-Internet organization, such as a vendor.
- **Requirement Levels:** RFCs are classified into five requirement levels: required, recommended, elective, limited use, and not recommended.
- **Required:** An RFC is labeled required if it must be implemented by all Internets systems to achieve minimum conformance. For example, IF and ICMP are required protocols.

- **Recommended:** An RFC labeled recommended is not required for minimum conformance; it is recommended because of its usefulness. For example, FTP and TELNET are recommended protocols.
- **Elective:** An RFC labeled elective is not required and not recommended. However, a system can use it for its own benefit.
- **Limited**: Use An RFC labeled limited use should be used only in limited situations. Most of the experimental RFCs fall under this category.
- **Not Recommended:** An RFC labeled not recommended is inappropriate for general use. Normally a historic (deprecated) RFC may fall under this category.

INTERNET ADMINISTRATION

Internet Administration is basically a group that coordinates and guides the Internet with its growth and development. It makes sure that all the protocols are followed by the devices and network for the smooth functioning of the internetwork. Some of the organizations that overlook the growth and development of the internet are –



- **Internet Society (ISOC) :**

  An international, non-profit organization, ISOC formed to provide support for the Internet standard process accomplishes its goals by maintaining and supporting other Internet administrative bodies such as IAB, IETF, IRTF, and IANA. It also promotes research and other activities relating to the Internet.

- **Internet Architecture Board (IAB) :**

  The technical advisor to the ISOC, the IAB's main purpose is to oversee the continuing development of the TCP/IP Protocol Suite and to serve in a technical advisory capacity to research members of the Internet community, which is accomplished by its two components, the Internet Engineering Task Force (IETF) and the Internet Research Task Force (IRTF). Additionally, IAB is also the editorial manager of the RFCs and is the external liaison between the Internet and the other standards, organizations, and forums.

- **Internet Engineering Task Force (IETF) :**

  Managed by the Internet Engineering Steering Group (IESG), the IETF is a forum of working groups responsible for identifying operational problems, proposing solutions to them, and developing and reviewing specifications intended as Internet Standards. The groups are collected into areas, like, applications, routing, security, protocols, and network management, and each area concentrates on a specific topic.

- **Internet Research Task Force (IRTF) :**

  Managed by the Internet Research Steering Group (IRSG), the IRTF is a forum of working groups focusing on long-term research topics related to Internet protocol, technology, applications, and architecture.

PROTOCOL LAYERING

In data communication and networking, a protocol defines the rules that both the sender and receiver and all intermediate devices need to follow to be able to communicate effectively. When communication is simple, we may need only one simple protocol; when the communication is complex, we may need to divide the task between different layers, in which case we need a protocol at each layer, or protocol layering.

A **protocol** is a set of rules and standards that primarily outline a language that devices will use to communicate. There are an excellent range of protocols in use extensively in networking, and that they are usually implemented in numerous layers.

It provides a communication service where the process is used to exchange the messages. When the communication is simple, we can use only one simple protocol.

When the communication is complex, we must divide the task between different layers, so, we need to follow a protocol at each layer, this technique we used to call protocol layering. This layering allows us to separate the services from the implementation.

Each layer needs to receive a set of services from the lower layer and to give the services to the upper layer. The modification done in any one layer will not affect the other layers.

Basic Elements of Layered Architecture:

The basic elements of the layered architecture are as follows −

Service − Set of actions or services provided from one layer to the higher layer.

Protocol − It defines a set of rules where a layer uses to exchange the information with its peer entity. It is concerned about both the contents and order of the messages used.

Interface − It is a way through that the message is transferred from one layer to another layer.

Reasons

The reasons for using layered protocols are explained below −

Layering of protocols provides well-defined interfaces between the layers, so that a change in one layer does not affect an adjacent layer.

The protocols of a network are extremely complicated and designing them in layers makes their implementation more feasible.

Advantages

The advantages of layered protocols are as follows −

- Assists in protocol style, as a result of protocols that operate at a particular layer have outlined information that they work and a defined interface to the layers on top of and below.
- Foster's competition because products from completely different vendors will work along.
- Prevents technology or capability changes in one layer from touching different layers above and below.
- Provides a typical language to explain networking functions and capabilities.

Disadvantages

The disadvantages of layered protocols are as follows −

- The main disadvantages of layered systems consist primarily of overhead each in computation and in message headers caused by the abstraction barriers between layers. Because a message typically should pass through several (10 or more) protocol layers the overhead of those boundaries is commonly more than the computation being done.

- The upper-level layers cannot see what is within the lower layers, implying that an application cannot correct where in an exceedingly connection a problem is or precisely what the matter is.

- The higher-level layers cannot control all aspects of the lower layers, so that they cannot modify the transfer system if helpful (like controlling windowing, header compression, CRC/parity checking, et cetera), nor specify routing, and should rely on the lower protocols operating, and cannot specify alternatives when there are issues.

NETWORK SOFTWARE

Service Primitives or Service Operations

A service is formally specified by a set of **primitives** (also called operations) available touser processes to access the service.

If the protocol stack is located in the operating system, the primitives are normally systemcalls.

There are Six basic service primitives which are used for a request-reply interaction in aclient-server Connection Oriented environment.

Primitives	Meaning
Listen	Block waiting for an incoming connection
Connect	Establish a connection with a waiting peer
Accept	Accept an incoming connection from a peer
Receive	Block waiting for an incoming message
Send	Send a message to the peer
Disconnect	Terminate a connection

1. The server executes LISTEN to indicate that it is prepared to accept incoming connections. After executing the primitive, the server process is blocked until a requestfor connection appears.
2. The client process executes CONNECT to establish a connection with the server. The client process is suspended until there is a response.
3. When the packet arrives at the server, the server process can then establish the connection with the ACCEPT call. This sends a response back to the client process to accept the connection. The arrival of this response then releases the client. At this point the client and server are both running and they have established a connection.
4. Then the server to execute RECEIVE to prepare to accept the first request. The RECEIVE call blocks the server.
5. Then the client executes SEND to transmit its request followed by the execution of RECEIVE to get the reply. The arrival of the request packet at the server machine unblocks the server so it can handle the request.
6. Then the server uses SEND to return the answer to the client. The arrival of this packet unblocks the client, which can now inspect the answer. If the client has additionalrequests, it can make them now.
7. When the client is done, it executes DISCONNECT to terminate the connection.
8. When the server gets the packet, it also issues a DISCONNECT of its own, acknowledging the client and releasing the connection.
9. When the server's packet gets back to the client machine, the client process is released and the connection is broken.

NETWORK REFERENCE MODELS

There are two types of network models are used:

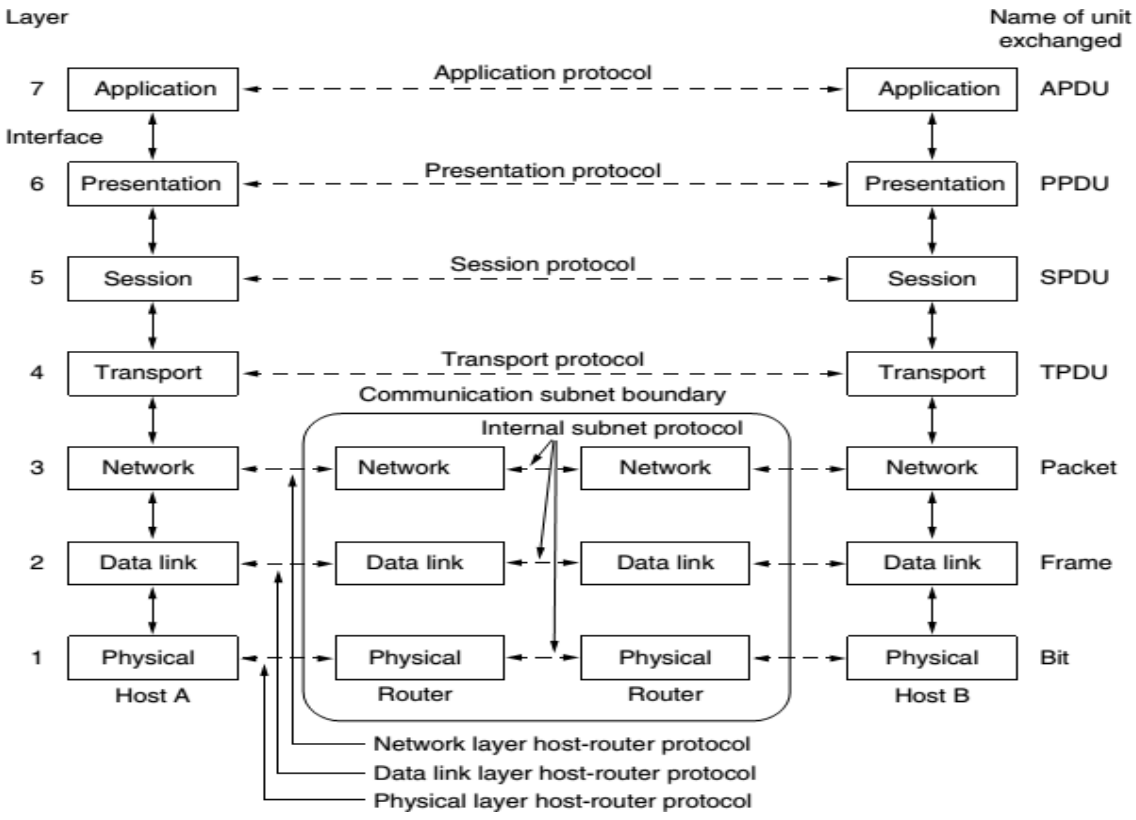
1. ISO/OSI Model.
2. TCP/IP protocol model

ISO/OSI Model

- **ISO** is the **Organization**. **OSI** is the **Model**. ISO was established in 1947. OSI was first introduced in 1970.
- 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 Framework** 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.



Above 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.
2. **Session, Presentation,** and **Application Layers** can be thought of as the user support layers.
3. **The Transport Layer** links the two subgroups and ensures that what the lower layershave 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.

Transport Layer

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 nextbut 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 atthe 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 bit 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 andsends the resulting message out over the network.
- Decryption reverses the original process to transform the message back to its originalform. Encryption and Decryption is done for privacy of the sensitive information.

Compression

- Data compression reduces the number of bits contained in the information at the time of transmission of multimedia data such as text, audio, and video.

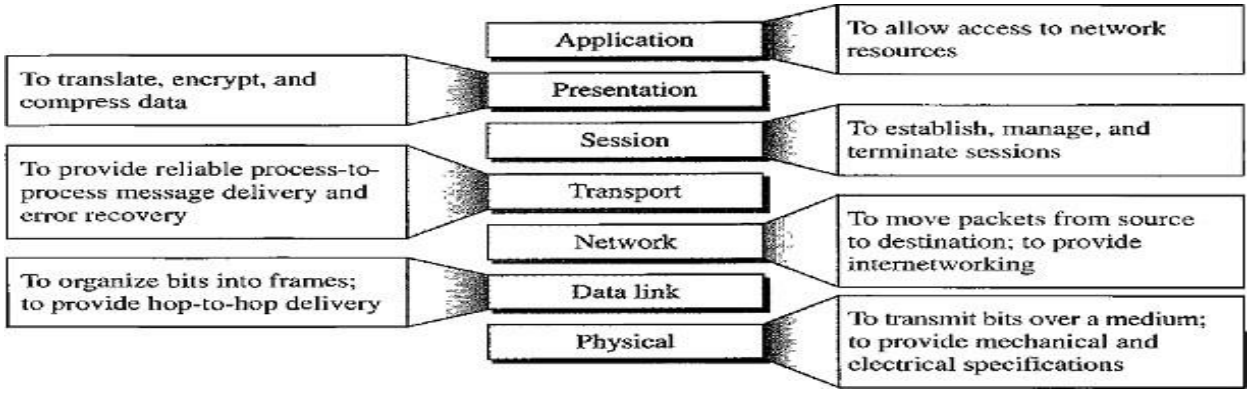
Application Layer

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:

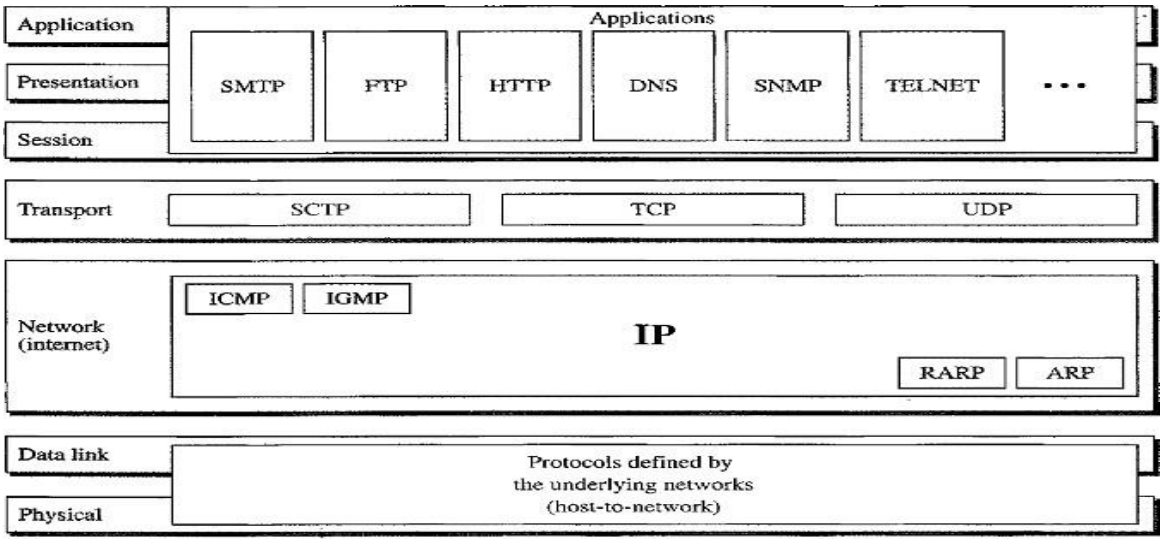
- **A network virtual terminal** is a software version of a physical terminal, and it allows auser to log on to a remote host.
- **File** transfer, access, and management in a remote host.
- **Mail services** such as email forwarding and mail storage.
- **Directory services** are an application provides distributed database sources and accessfor 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 takecare 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 inOSI 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 beduplicated.
- IP does not keep track of the routes and has no facility for reordering datagrams once theyarrive 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)

Transmission Control Protocol

- TCP provides full transport-layer services to applications. TCP is a reliable streamtransport 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

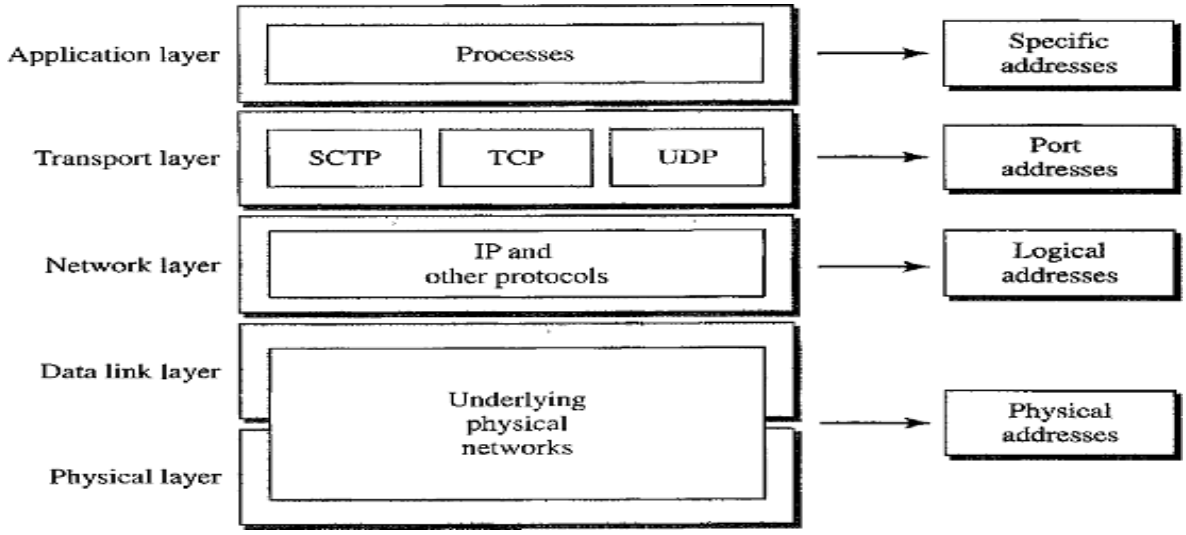
On top of the transport layer is the **application layer**. It contains all the higher-level protocols such as:

- **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 networkaddresses.
- **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. Ex: Computer A can communicate with computer B by using TELNET. At the same time, computer A communicates with computer C by using the File TransferProtocol (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 as www.google.com.

DATA & SIGNALS

To be transmitted, data must be transformed to electromagnetic signals.

Data can be Analog or Digital.

1. Analog data refers to information that is continuous; ex. sounds made by a human voice

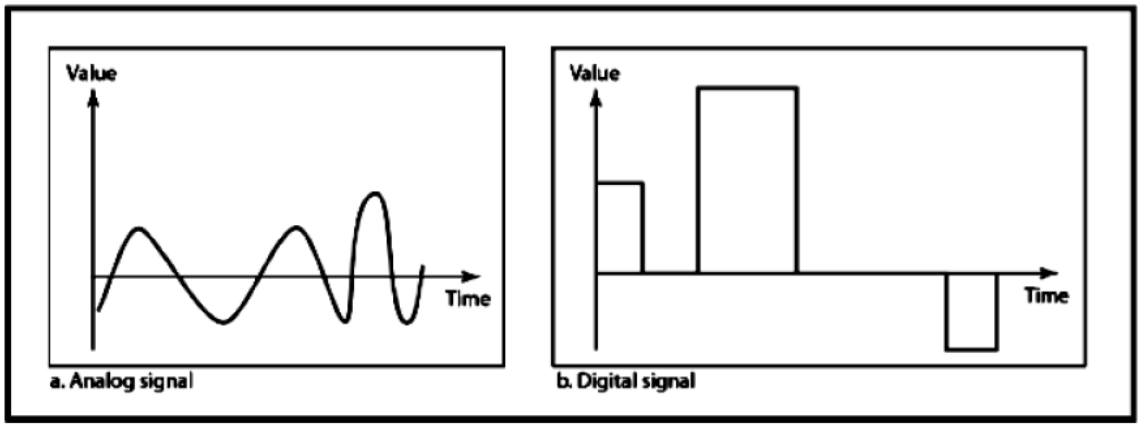
2. Digital data refers to information that has discrete states. Digital data take on discrete values.

3. For example, data are stored in computer memory in the form of Os and 1s

Signals can be of two types:

1. Analog Signal: They have infinite values in a range.

2. Digital Signal: They have limited number of defined values



Signals which repeat itself after a fixed time period are called Periodic Signals.

Signals which do not repeat itself after a fixed time period are called Non-Periodic Signals.

In data communications, we commonly use periodic analog signals and non-periodic digital signals.

ANALOG SIGNAL

- An analog signal has infinitely many levels of intensity over a period of time.

- As the wave moves from value *A* to value *B*, it passes through and includes an infinite number of values along its path as it can be seen in the figure below.
- A simple analog signal is a sine wave that cannot be further decomposed into simpler signals.

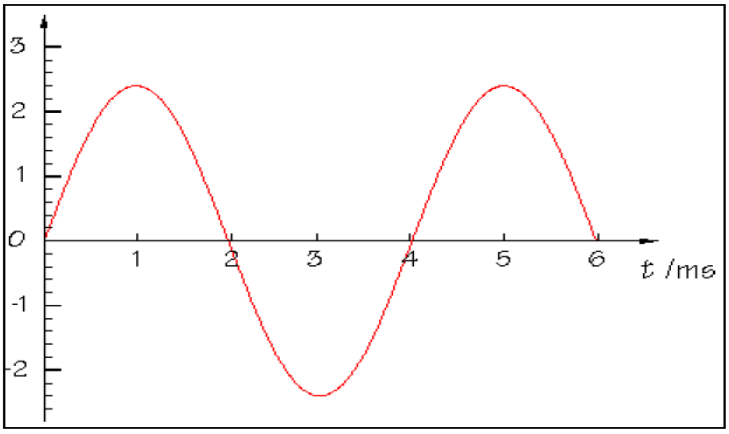


Fig. Sine wave

A sine wave is characterized by three parameters:
1. Peak Amplitude
2. Frequency
3. Phase

Characteristics of an Analog Signal

Peak Amplitude

The amplitude of a signal is the absolute value of its intensity at time t.
The peak amplitude of a signal is the absolute value of the highest intensity.
The amplitude of a signal is proportional to the energy carried by the signal.

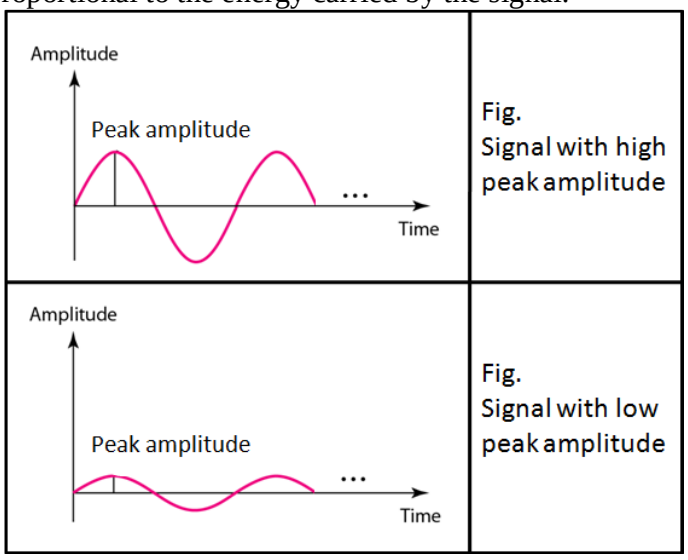


Fig. Amplitude of a sine wave

Frequency
Frequency refers to the number of cycles completed by the wave in one second.
Period refers to the time taken by the wave to complete one second.

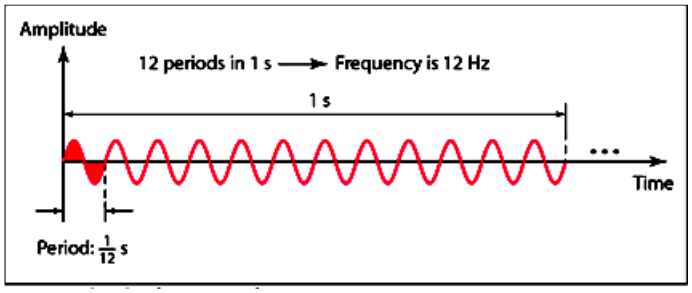


Fig: Frequency & Period of a sine wave

Phase

Phase describes the position of the waveform with respect to time (specifically relative to time O).

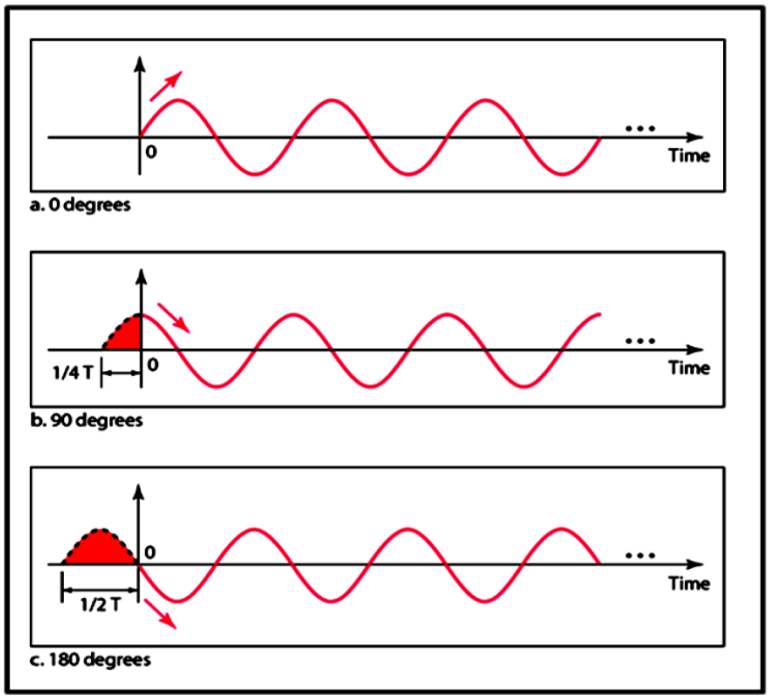


Fig: Phase of a sine wave*

Phase indicates the forward or backward shift of the waveform from the axis.

It is measured in degrees or radian.

The figure above shows the sine waves with same amplitude and frequency but different phases.

Relation between Frequency & Period Frequency & Period are inverse of each other.

It is indicated by the following formula:

$$T = 1/f$$

Or

$$f = 1/T$$

Wavelength

The wavelength of a signal refers to the relationship between frequency (or period) and propagation speed of the wave through a medium.

The wavelength is the distance a signal travels in one period.

It is given by

Wavelength = Propagation Speed X Period

OR

Wavelength =Propagation Speed X 1

Frequency: It is represented by the symbol : λ (pronounced as lamda) It is measured in micrometers

It varies from one medium to another.

Composite Signal

A composite signal is a combination of two or more simple sine waves with different frequency, phase and amplitude.

Composite signals can be periodic or non periodic.

- A periodic composite signal can be decomposed into a series of signals with discrete frequencies.
- A non-periodic signal when decomposed gives a combination of sine waves with continuous frequencies.

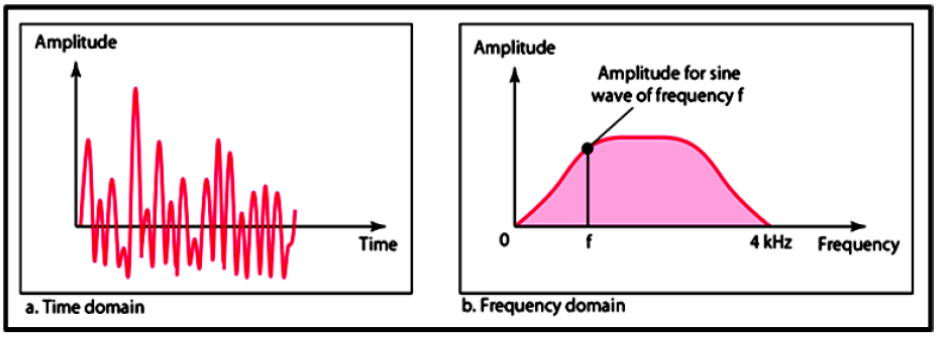


Fig The time and frequency domains of a non-periodic composite analog signal

Digital Signal

Information can also be explained in the form of a digital signal.

A digital signal can be explained with the help of following points:

Definition:-

A digital is a signal that has discrete values.

The signal will have value that is not continuous.

LEVEL

Information in a digital signal can be represented in the form of voltage levels.

Ex. In the signal shown below, a _1‘ is represented by a positive voltage and a _0‘ is represented by a Zero voltage.

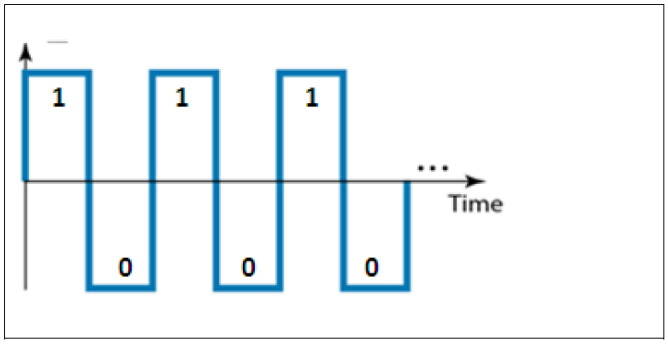
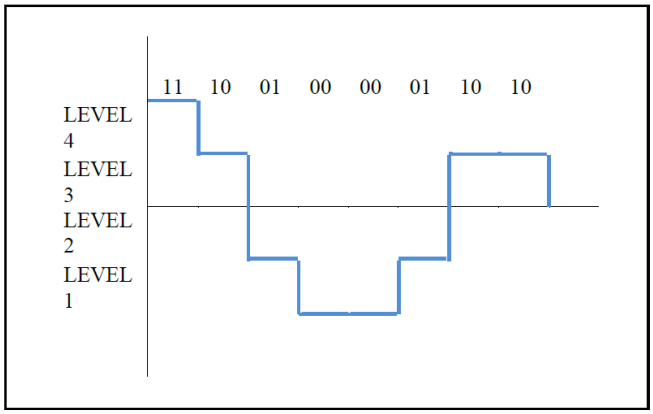


Fig: A digital signal with Two levels. „1“ represented by a positive voltage and „0“ represented by a negative voltage

A Signal can have more than two levels.



BIT LENGTH or Bit Interval (T_b)

It is the time required to send one bit. It is measured in seconds.

BIT RATE

It is the number of bits transmitted in one second. It is expressed as bits per second (bps).

Relation between bit rate and bit interval can be as follows Bit rate = 1 / Bit interval.

Baud Rate

It is the rate of Signal Speed, i.e the rate at which the signal changes.

A digital signal with two levels _0' & _1' will have the same baud rate and bit rate & bit rate.

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.

Reason for Multiplexing

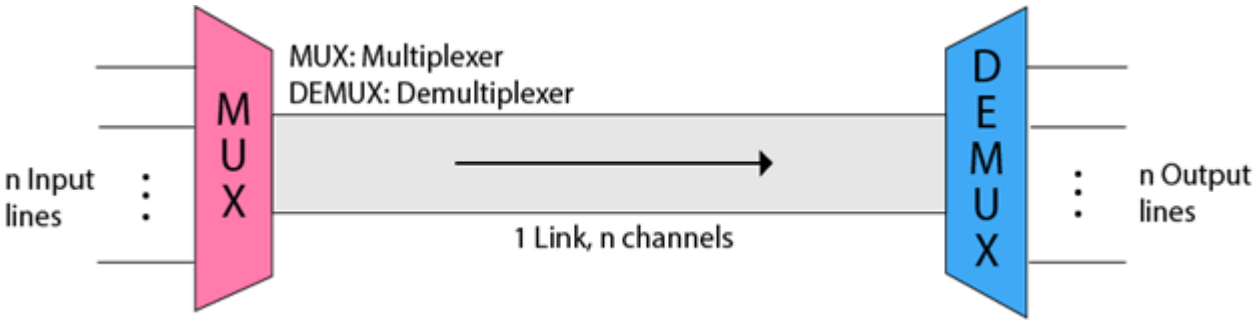
- The transmission medium is used to send the signal from sender to receiver. The medium can only have one signal at a time.
- If there are multiple signals to share one medium, then the medium must be divided in such a way that each signal is given some portion of the available bandwidth. For example: If there are 10 signals and bandwidth of medium is100 units, then the 10 unit is shared by each signal.
- When multiple signals share the common medium, there is a possibility of collision. Multiplexing concept is used to avoid such collision.
- Transmission services are very expensive.

History of Multiplexing

- Multiplexing technique is widely used in telecommunications in which several telephone calls are carried through a single wire.

- Multiplexing originated in telegraphy in the early 1870s and is now widely used in communication.
- George Owen Squier developed the **telephone carrier multiplexing** in 1910.

Concept of Multiplexing



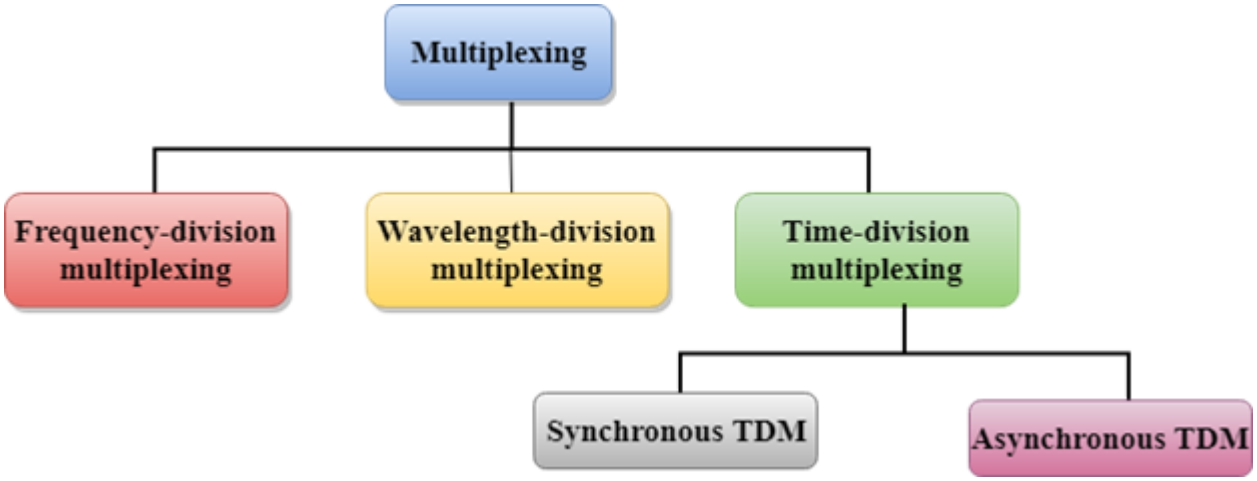
- The 'n' input lines are transmitted through a multiplexer and multiplexer combines the signals to form a composite signal.
- The composite signal is passed through a Demultiplexer and demultiplexer separates a signal to component signals and transfers them to their respective destinations.

Advantages of Multiplexing:

- More than one signal can be sent over a single medium.
- The bandwidth of a medium can be utilized effectively.

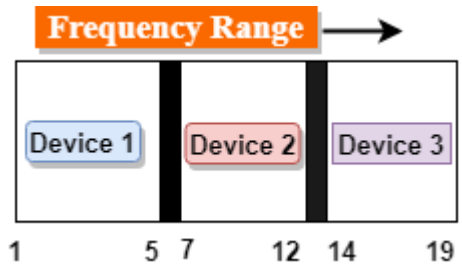
Multiplexing Techniques

Multiplexing techniques can be classified as:

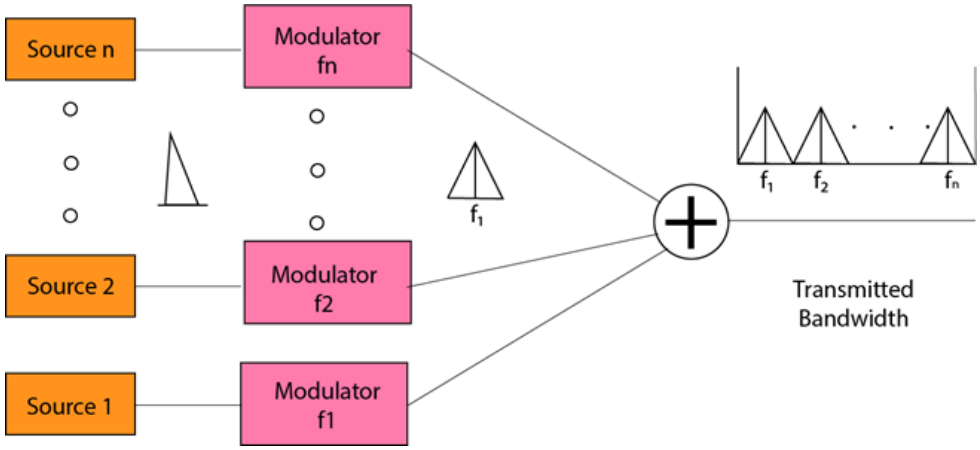


Frequency-division Multiplexing (FDM)

- 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.

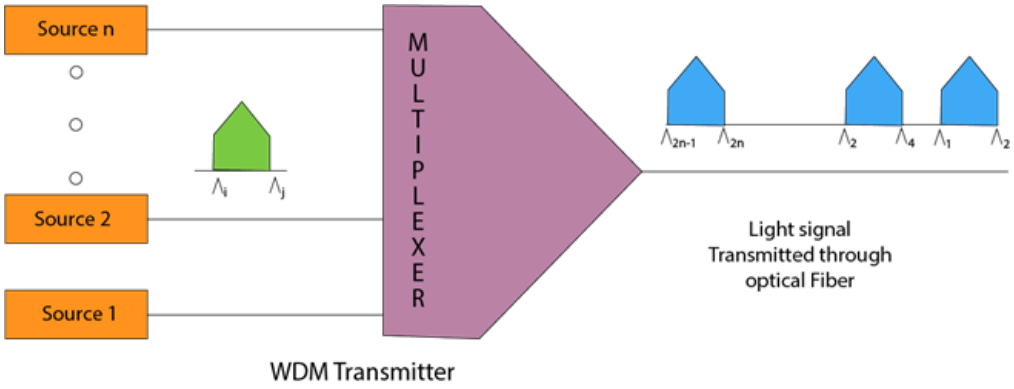
Disadvantages Of FDM:

- 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:

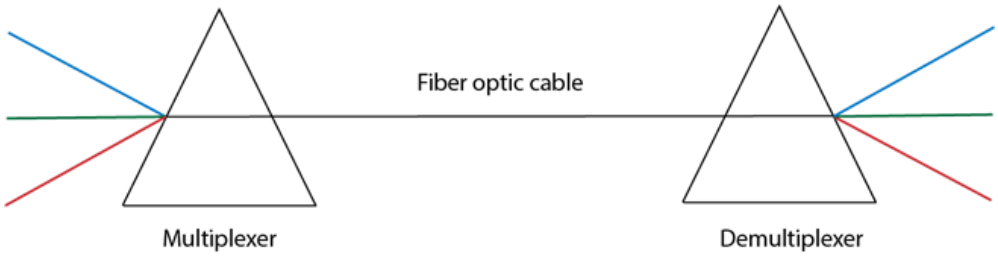
- FDM is commonly used in TV networks.
- It is used in FM and AM broadcasting. Each FM radio station has different frequencies, and they are multiplexed to form a composite signal. The multiplexed signal is transmitted in the air.

Wavelength Division Multiplexing (WDM)



WDM Transmitter

- 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.

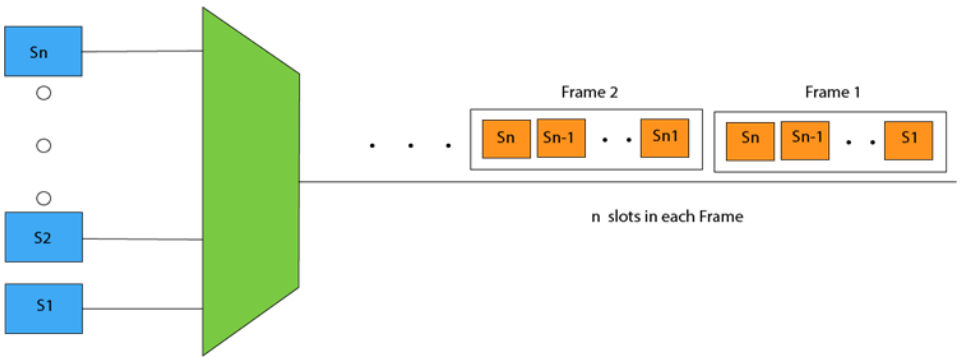
- In **Time Division Multiplexing technique**, the total time available in the channel is distributed among different users. Therefore, each user is allocated with different time interval known as a Time slot at which data is to be transmitted by the sender.
- A user takes control of the channel for 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:

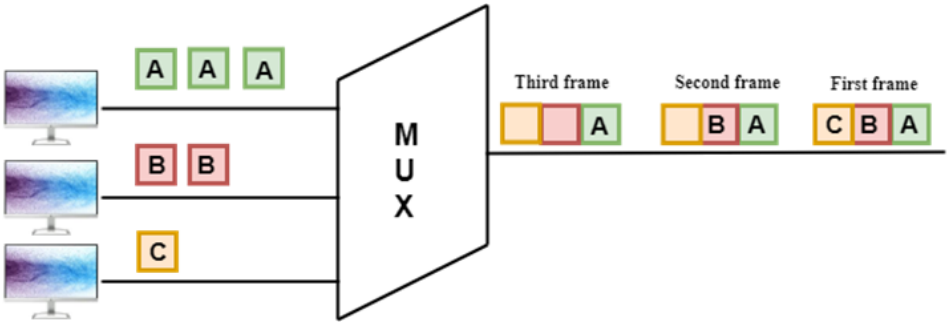
- Synchronous TDM
- Asynchronous TDM

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:

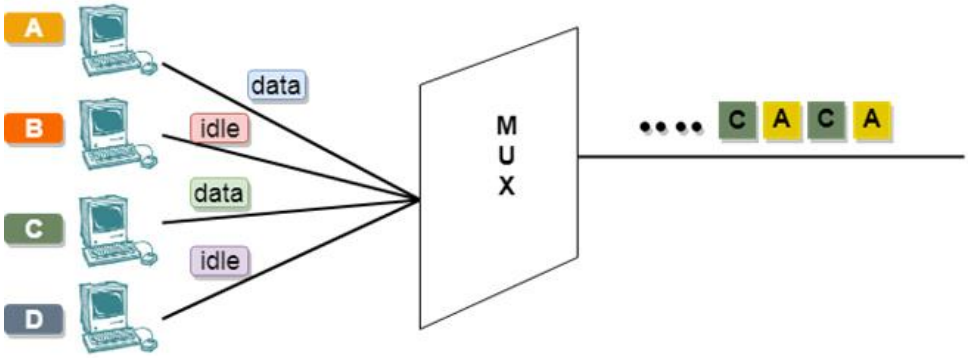
- The capacity of the channel is not fully utilized as the empty slots are also transmitted which is having no data. In the above figure, the first frame is completely filled, but in the last two frames, some slots are empty. Therefore, we can say that the capacity of the channel is not utilized efficiently.
- 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.

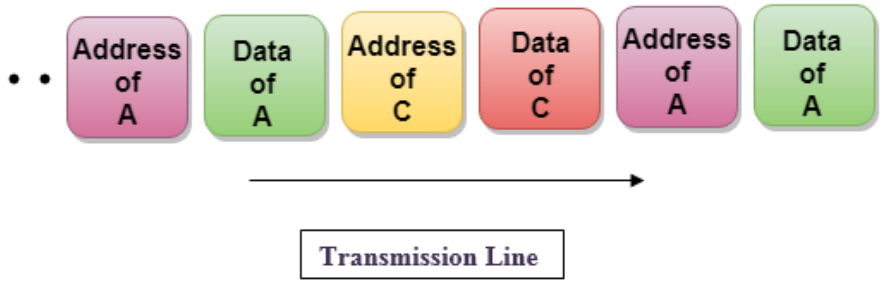
- The difference between Asynchronous TDM and Synchronous TDM is that many slots in Synchronous TDM are unutilized, but in Asynchronous TDM, slots are fully utilized. This leads to the smaller transmission time and efficient utilization of the capacity of the channel.
- In Synchronous TDM, if there are 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.

SPREAD SPECTRUM

- "Spread Spectrum is a technique in which the transmitted signals of specific frequencies are varied slightly to obtain greater bandwidth as compared to initial bandwidth."
- Spread spectrum technology is widely used in radio signals transmission because it can easily reduce noise and other signal issues.

In this conventional wireless communication model, you can face at least two problems:

1. A signal whose frequency is constant is subject to catastrophic interference. This interference occurs when another signal is transmitted on or near the frequency of a specified signal.
2. A constant-frequency signal can easily be intercepted. So, it is not suitable for the applications in which information must be kept confidential between the source (transmitting party) and the receiver.

- The spread spectrum model is used to overcome with this conventional communication model. Here, the transmitted signal frequency is deliberately varied over a comparatively large segment of the electromagnetic radiation spectrum.
- This variation is done according to a specific but complicated mathematical function. If the receiver wants to intercept the signal, it must be tuned to frequencies that vary precisely according to this function.

Reasons to use Spread Spectrum

- Spread spectrum signals are distributed over a wide range of frequencies and then collected and received back to the receiver. On the other hand, wide-band signals are noise-like and challenging to detect.
- Initially, the spread spectrum was adopted in military applications because of its resistance to jamming and difficulty intercepting.
- Now, this is also used in commercial wireless communication.
- It is most preferred because of its useful bandwidth utilization ability.

Usage of Spread Spectrum

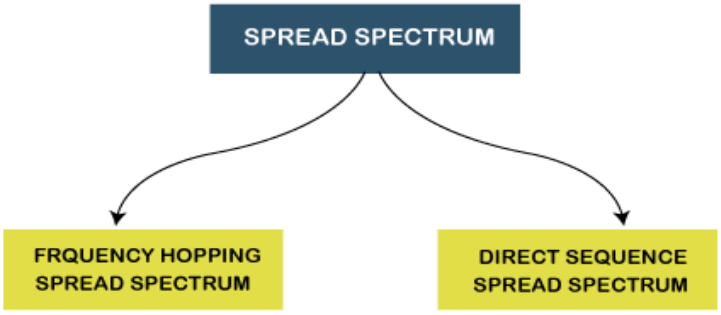
There are many reasons to use this spread spectrum technique for wireless communications. The following are some reasons:

- It can successfully establish a secure medium of communication.
- It can increase the resistance to natural interference, such as noise and jamming, to prevent detection.
- It can limit the power flux density (e.g., in satellite down links).
- It can enable multiple-access communications.

Types of Spread Spectrum

Spread Spectrum can be categorized into two types:

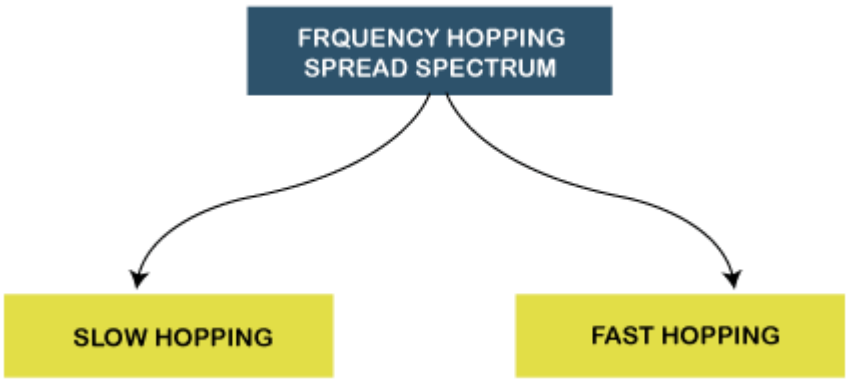
- Frequency Hopping Spread Spectrum (FHSS)
- Direct Sequence Spread Spectrum(DSSS)



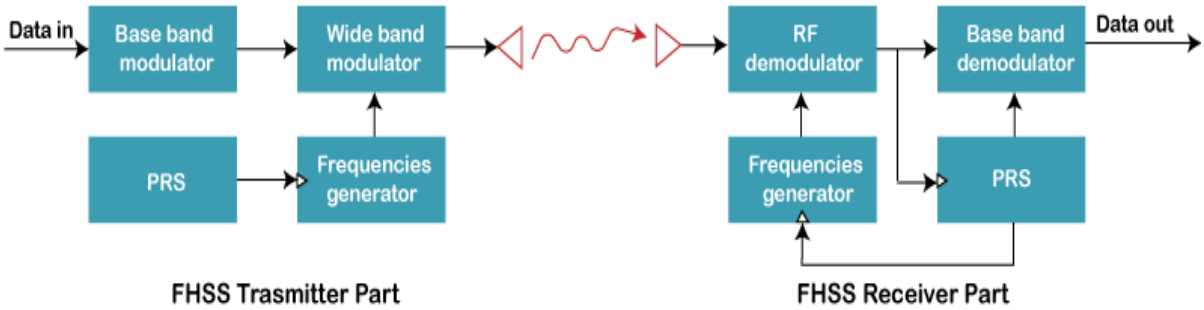
Frequency Hopping Spread Spectrum (FHSS)

- The Frequency Hopping Spread Spectrum or FHSS allows us to utilize bandwidth properly and maximum. In this technique, the whole available bandwidth is divided into many channels and spread between channels, arranged continuously.
- The frequency slots are selected randomly, and frequency signals are transmitted according to their occupancy.
- The transmitters and receivers keep on hopping on channels available for a particular amount of time in milliseconds.
- So, you can see that it implements the frequency division multiplexing and time-division multiplexing simultaneously in FHSS.

The Frequency Hopping Spread Spectrum or FHSS can also be classified into two types:



- **Slow Hopping:** In slow hopping, multiple bits are transmitted on a specific frequency or same frequency.
- **Fast Hopping:** In fast hopping, individual bits are split and then transmitted on different frequencies.



Advantages of Frequency Hopping Spread Spectrum (FHSS)

The following are some advantages of frequency hopping spread spectrum (FHSS):

- The biggest advantage of Frequency Hopping Spread Spectrum or FHSS is its high efficiency.
- The Frequency Hopping Spread Spectrum or FHSS signals are highly resistant to narrowband interference because the signal hops to a different frequency band.
- It requires a shorter time for acquisition.
- It is highly secure. Its signals are very difficult to intercept if the frequency-hopping pattern is not known; that's why it is preferred to use in Military services.
- We can easily program it to avoid some portions of the spectrum.
- Frequency Hopping Spread Spectrum or FHSS transmissions can share a frequency band with many types of conventional transmissions with minimal mutual interference. FHSS signals add minimal interference to narrowband communications, and vice versa.
- It provides a very large bandwidth.
- It can be simply implemented as compared to DSSS.

Disadvantages of Frequency Hopping Spread Spectrum (FHSS)

The following are some disadvantages of Frequency Hopping Spread Spectrum (FHSS):

- FHSS is less Robust, so sometimes it requires error correction.
- FHSS needs complex frequency synthesizers.
- FHSS supports a lower data rate of 3 Mbps as compared to the 11 Mbps data rate supported by DSSS.
- It is not very useful for range and range rate measurements.
- It supports the lower coverage range due to the high SNR requirement at the receiver.

- Nowadays, it is not very popular due to the emerging of new wireless technologies in wireless products.

Applications of Frequency Hopping Spread Spectrum (FHSS)

Following is the list of most used applications of Frequency Hopping Spread Spectrum or FHSS:

- The Frequency Hopping Spread Spectrum or FHSS is used in wireless local area networks (WLAN) standard for Wi-Fi.
- FHSS is also used in the wireless personal area networks (WPAN) standard for Bluetooth.

Direct Sequence Spread Spectrum (DSSS)

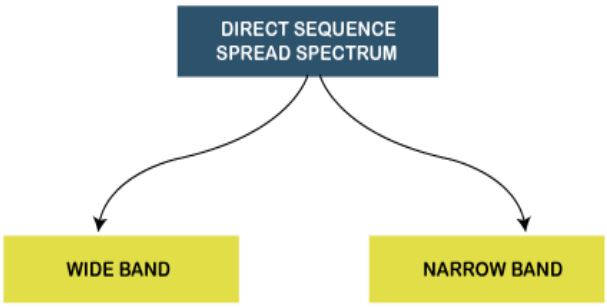
- The Direct Sequence Spread Spectrum (DSSS) is a spread-spectrum modulation technique primarily used to reduce overall signal interference in telecommunication.
- The Direct Sequence Spread Spectrum modulation makes the transmitted signal wider in bandwidth than the information bandwidth.
- In DSSS, the message bits are modulated by a bit sequencing process known as a spreading sequence. This spreading-sequence bit is known as a chip. It has a much shorter duration (larger bandwidth) than the original message bits.

Following are the features of Direct Sequence Spread Spectrum or DSSS.

- In Direct Sequence Spread Spectrum or DSSS technique, the data that needs to be transmitted is split into smaller blocks.
- After that, each data block is attached with a high data rate bit sequence and is transmitted from the sender end to the receiver end.
- Data blocks are recombined again to generate the original data at the receiver's end, which was sent by the sender, with the help of the data rate bit sequence.
- If somehow data is lost, then data blocks can also be recovered with those data rate bits.
- The **main advantage** of splitting the data into smaller blocks is that it reduces the noise and unintentional inference.

The Direct Sequence Spread Spectrum or DSSS can also be classified into two types:

- Wide Band Spread Spectrum
- Narrow Band Spread Spectrum



Advantages of Direct Sequence Spread Spectrum (DSSS)

The following are some advantages of Direct Sequence Spread Spectrum or DSSS:

- Direct Sequence Spread Spectrum or DSSS is less reluctant to noise; that's why the DSSS system's performance in the presence of noise is better than the FHSS system.
- In Direct Sequence Spread Spectrum or DSSS, signals are challenging to detect.
- It provides the best discrimination against multipath signals.
- In Direct Sequence Spread Spectrum, there are very few chances of jamming because it avoids intentional interference such as jamming effectively.

Disadvantages of Direct Sequence Spread Spectrum (DSSS)

The following are some disadvantages of Direct Sequence Spread Spectrum or DSSS:

- The Direct Sequence Spread Spectrum or DSSS system takes large acquisition time; that's why its performance is slow.
- It requires wide-band channels with small phase distortion.
- In DSSS, the pseudo-noise generator generates a sequence at high rates.

Applications of Direct Sequence Spread Spectrum (DSSS)

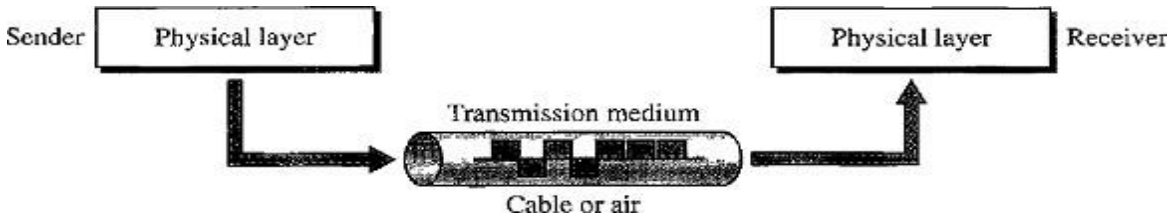
Following is the list of most used applications of Direct Sequence Spread Spectrum or DSSS:

- Direct Sequence Spread Spectrum or DSSS is used in LAN technology.
- Direct Sequence Spread Spectrum or DSSS is also used in Satellite communication technology.
- DSSS is used in the military and many other commercial applications.
- It is used in the low probability of the intercept signal.
- It supports Code division multiple access.

TRANSMISSION MEDIA

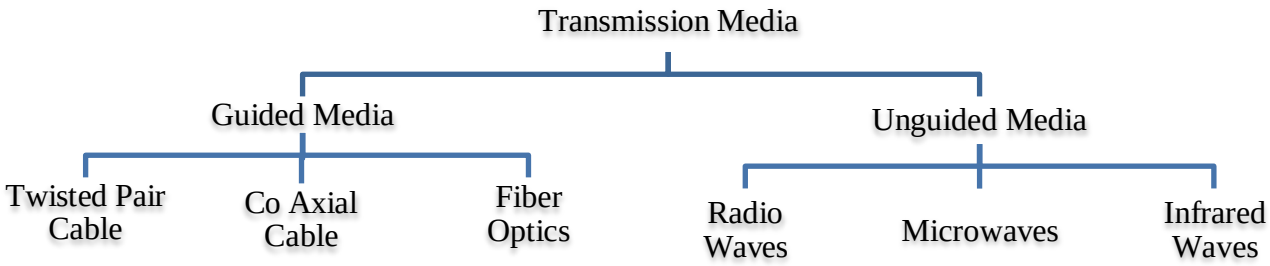
Transmission media are actually located below the physical layer and are directly controlled by the physical layer.

A transmission **medium** can be broadly defined as anything that can carry information from a source to a destination. In data communications the information is usually a signal.



Transmission media can be categorized into following ways:

- **Guided or Wired Media**: Twisted pair cable, Coaxial cable, Fiber Optic cable.
- **Unguided or Wireless Media**: Radio Waves, Micro waves, Infrared Waves.



Guided or Wired Media

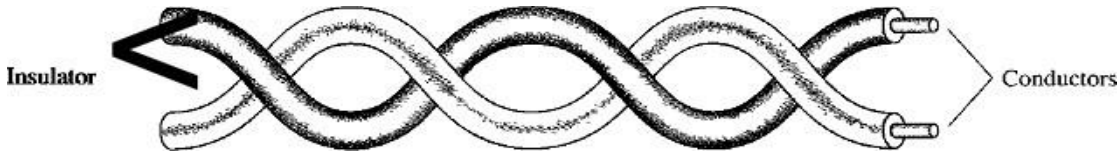
A signal traveling along this media is directed and contained by the physical limits of the medium. Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. Optical fiber is a cable that accepts and transports signals in the form of light.

Twisted-Pair Cable

A twisted pair consists of two conductors (normally copper), each with its own plastic

insulation, twisted together.

One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference.



The signal sent by the sender on one of the wires, interference (noise) and crosstalk may affect both wires and create unwanted signals.

STP v/s UTP

Shielded Twisted Pair (STP) cable has a **metal foil** or braided mesh covering that encases each pair of insulated conductors. A twisted-pair cable can pass a wide range of frequencies. Although metal casing improves the quality of cable by preventing the penetration of noise or crosstalk, it is bulkier and more expensive.

Unshielded Twisted pair (UTP) cables don't have the metal foil covering the cables. The most common UTP connector is RJ45 (Registered Jack 45).

Applications

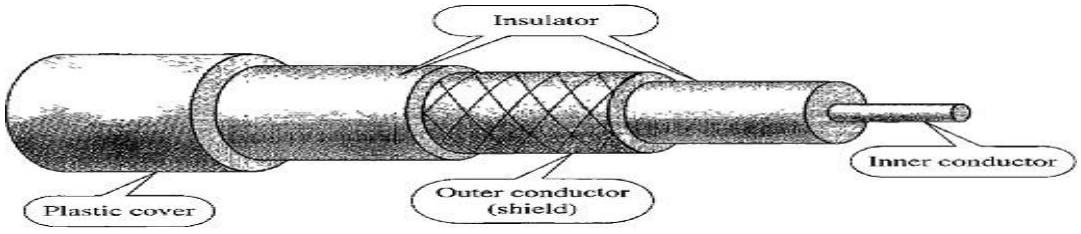
- Twisted-pair cables are used in telephone lines to provide voice and data channels. Most widely used in Internet connections.
- The DSL lines that are used by the telephone companies to provide high-data-rateconnections also use the high-bandwidth capability of unshielded twisted-pair cables.

Note: When there is an electric signal interference UTP signal performance is degraded.

Hence we use STP, the shield protects from interference of electric signals.

Coaxial Cable (Coax)

Coaxial cable carries signals of higher frequency ranges than those in twisted pair cable.



- Coaxial cable has a central core conductor of copper wire enclosed in an insulating sheath.

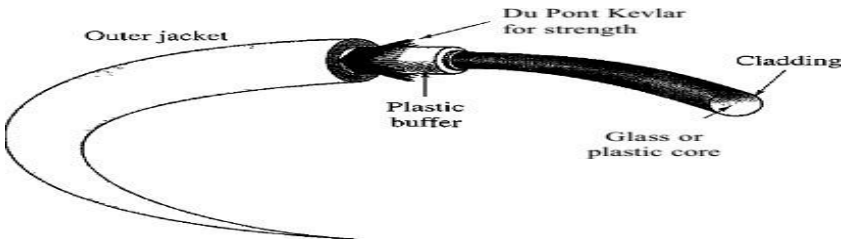
- Insulating sheath encased in an outer conductor of metal foil.
- The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit.
- This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover.
- Coaxial cables are categorized by their Radio Government (RG) ratings. Each RGnumber denotes a unique set of physical specifications. Ex: RG-59 is used for Cable TV.
- Although coaxial cable has a much higher bandwidth, the signal weakens rapidly and requires the frequent use of repeaters.

Applications

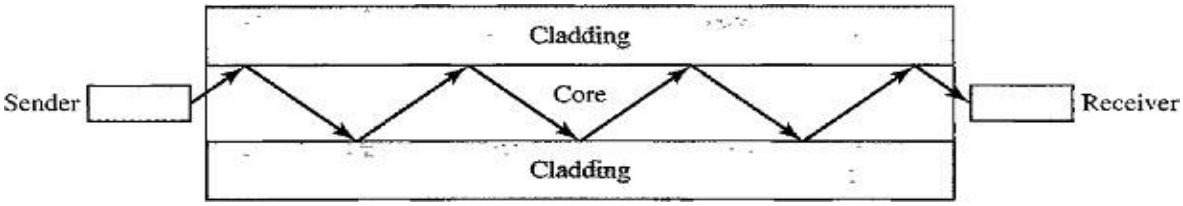
Coaxial cable was widely used in analog telephone networks, digital telephone networks, Cable TV networks, Ethernet LAN.

Fiber-Optic Cable

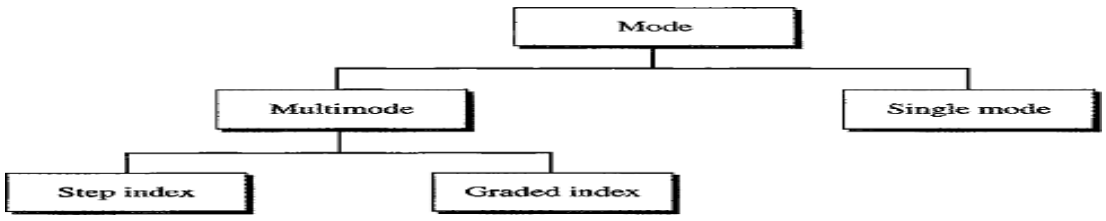
- A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.
- The outer jacket is made of either PVC or Teflon. Inside the jacket are Kevlar strands to strengthen the cable.
- Below the Kevlar is another plastic coating to cushion the fiber. The fiber is at the centerof the cable, and it consists of cladding and core.



- Optical fibers use reflection to guide light through a channel.
- A glass or plastic core is surrounded by a cladding of less dense glass or plastic.
- The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it.



Propagation Modes



Multimode Propagation

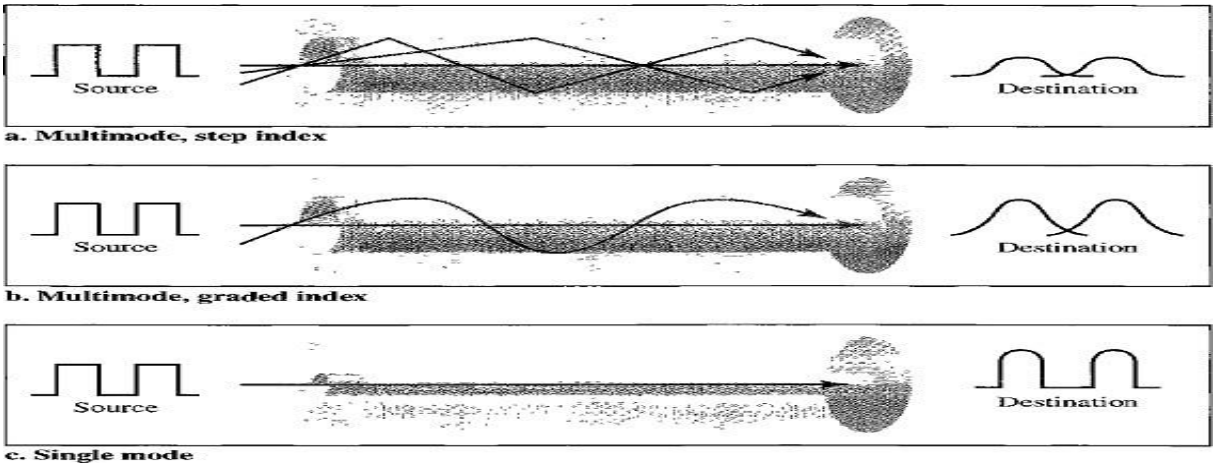
In this mode multiple beams from a light source move through the core in different paths.

Multimode Step-Index Fiber:

- The density of the core remains constant from the center to the edges.
- A beam of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding.
- At the interface, there is an abrupt change due to a lower density; this alters the angle ofthe beam's motion.
- The term *step index* refers to the suddenness of this change, which contributes to the distortion of the signal as it passes through the fiber.

Multimode Graded-Index Fiber:

- It decreases the distortion of the signal through the cable.
- The index of refraction is related to density. A graded-index fiber is one with varying densities.
- Density is highest at the center of the core and decreases gradually to its lowest at theedge.



Single-Mode Fiber:

- It uses step-index fiber and a highly focused source of light that limits beams to a smallrange of angles close to the horizontal.
- The single mode fiber is manufactured with a much smaller diameter than that ofmultimode fiber, and with substantially lower density (index of refraction).
- The decrease in density results in a critical angle that is close enough to 90° to make the propagation of beams almost horizontal.
- In this case, propagation of different beams is almost identical, and delays are negligible.
- All the beams arrive at the destination "together" and can be recombined with little distortion to the signal.

Fiber Optic Cable Connectors

- The **subscriber channel** (SC) **connector** is used for cable TV.
- The **straight-tip** (ST) **connector** is used for connecting cable to networking devices.

Performance: We need 10 times less repeaters when we use fiber-optic cable.

Application: Fiber-optic cable is often found in backbone networks because of its wide bandwidth is cost-effective.

Advantages

Fiber-optic cable has several advantages over metallic cable Twisted pair or coaxial.

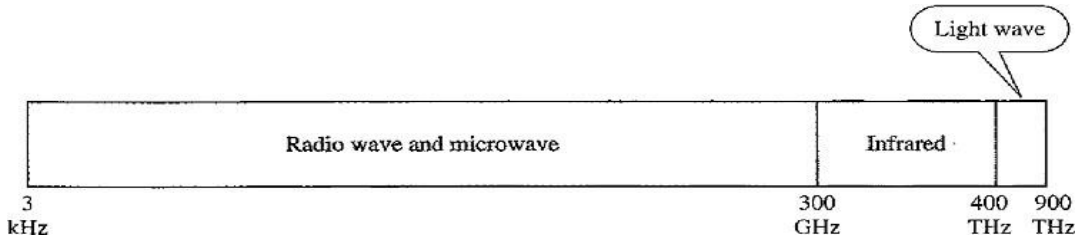
- **Higher bandwidth**. Fiber-optic cable can support higher bandwidths than either twisted- pair or coaxial cable.
- **Less signal attenuation**. Fiber-optic transmission distance is significantly greater than that of other guided media. A signal can run for 50 km without requiring regeneration. We need repeaters every 5 km for coaxial or twisted-pair cable.
- Electromagnetic noise cannot affect fiber-optic cables.
- **Resistance:** Glass is more resistant to corrosive materials than copper.
- **Light weight.** Fiber-optic cables are much lighter than copper cables.
- Fiber-optic cables are more **immune to tapping** than copper cables.

Disadvantages

- **Installation and maintenance:** Fiber-optic cable is a relatively new technology. Its installation and maintenance require expertise that is not yet available everywhere.
- **Unidirectional light propagation**: Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.
- **Cost:** The cable and the interfaces are relatively more expensive than those of other guided media. If the demand for bandwidth is not high the use of optical fiber cannot be justified.

UNGUIDED MEDIA (or) **WIRELESS COMMUNICATION**

Unguided media transport **Electromagnetic Waves** without using a physical conductor. This type of communication is often referred to as wireless communication. Electromagnetic spectrum ranging from **3 kHz to 900 THz** used for wireless communication.



Categories of Wireless Communication:

- Radio Waves (3kHz – 1GHz)
- Microwaves (1GHz- 300 GHz)
- Infrared Waves (300 GHz - 400 THz).

Radio Waves

- Radio waves ranges between 3 kHz and 1 GHz. Radio waves are Omni-directional.
- When an antenna transmits radio waves, they are propagated in all directions. Hence the sending and receiving devices don't have to be aligned.
- A sending antenna sends waves that can be received by any receiving antenna.
- Radio waves can travel long distances, hence it is used in long distance AM Radio broadcasting.
- Radio waves of low and medium frequencies can penetrate walls.

Disadvantage

- The Omni-directional property has a **disadvantage**; the radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using the same frequency or band.
- Radio waves leads to low data rate for digital communication.

Applications

- Radio waves are used in Multicasting applications such as AM Radio and FM radio, Television, Maritime Radio, Cordless Phones, and Paging.

Microwaves

- Electromagnetic waves having frequencies between 1GHz and 300 GHz are called microwaves.
- Microwaves are unidirectional. When an antenna transmits microwave waves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned.
- Microwaves need unidirectional antennas that send out signals in one direction. Two types of antennas are used for microwave communications: the parabolic dish and the horn.
- Microwave propagation is line-of-sight. Repeaters are often needed for long distance communication.
- Higher data rates are possible due to assigning of wider sub-bands.

Advantage: The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas.

Disadvantage: Very high-frequency microwaves cannot penetrate walls. This characteristic can be a disadvantage if receivers are inside buildings.

Applications: Microwaves used in Uni-casting communication between sender and receiver such as cellular phones, satellite networks and wireless LANs.

Infrared Waves

Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 nm), can be used for short-range communication upto few meters.

Advantages

Infrared waves having high frequencies cannot penetrate walls. This advantageouscharacteristic prevents interference between one system and another; a short-rangecommunication system in one room cannot be affected by another system in the next room.

Disadvantage

- We cannot use Infrared waves for long range communication.
- We cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.

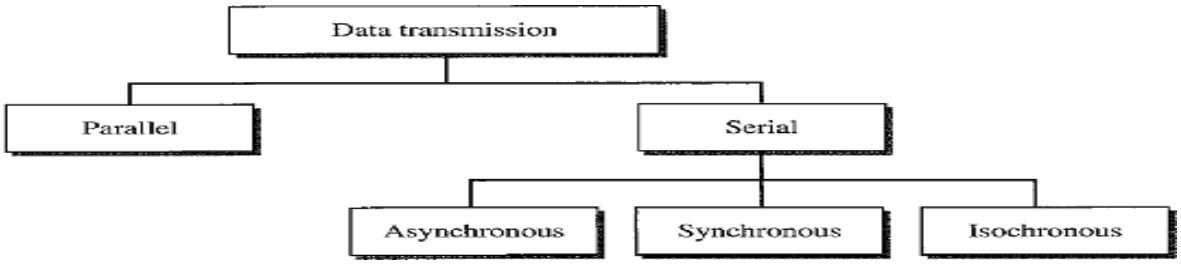
Applications

- Due to its wide bandwidth, it can be used to transmit digital data at high data rate.
- It can be used in Communication between devices such as keyboards, mice, PCs, and printers.

TRANSMISSION MODES

Transmission modes are two types:

1. Parallel Transmission
2. Serial Transmission

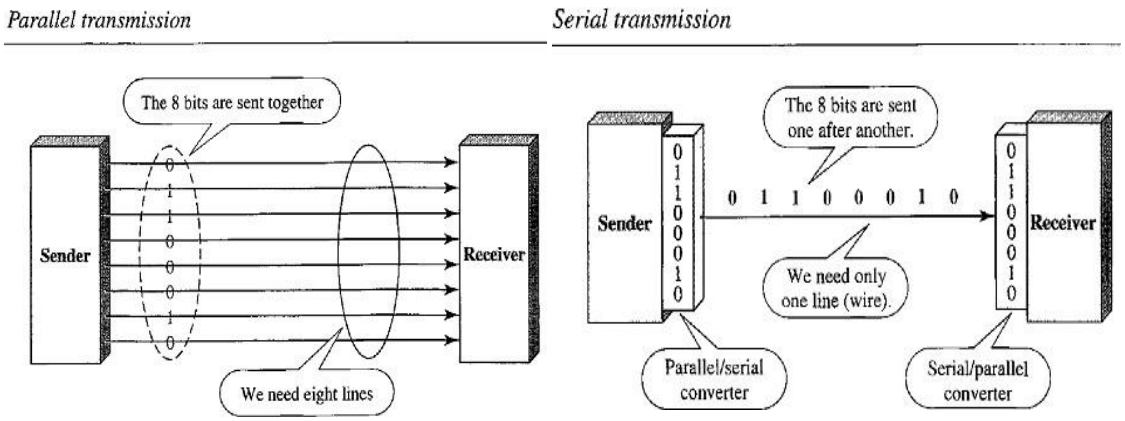


Parallel Transmission

- Parallel Transmission is defined as sending n bits of data at a time instead of transmittingone bit at a time.
- The mechanism for parallel transmission is a conceptually simple one: Use **n-wires** tosend **n-bits** at one time.
- **Advantage**: Speed of the transmission is increased.
- **Disadvantage**: Cost of equipment is increased for this reason parallel transmission is usually limited to short distances.

Serial Transmission

In serial transmission one bit follows another, so we need only one communication channel rather than **n channels** to transmit data between two communicating devices



Advantage: Reduces the cost transmission equipment because we need only one communication channel.

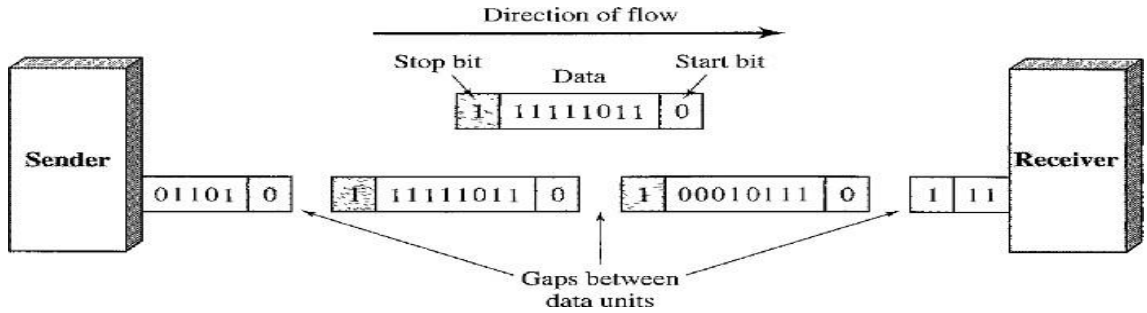
Since communication within devices is parallel, conversion devices are required at the interface between the sender and the line (parallel-to-serial) and between the line and the receiver (serial-to-parallel).

Serial transmission categorized into 3 types:

1. Asynchronous Transmission
2. Synchronous Transmission
3. Isochronous Transmission

Asynchronous Transmission

- The timing of signal is not important in Asynchronous transmission. Information isreceived and translated by agreed upon patterns.
- As long as those patterns are followed, the receiving device can retrieve the information without regard to the order in which it is sent.
- Patterns are based on grouping the bit stream into bytes. Each group contains 8 bits is sentalong the link as a unit.
- In asynchronous transmission, we send one start bit (0) at the beginning and one or morestop bits (1's) at the end of each byte. There may be a gap between each byte.
- The start and stop bits are used because the sending system handles each group independently whenever the group is ready it will transmitted through the link.



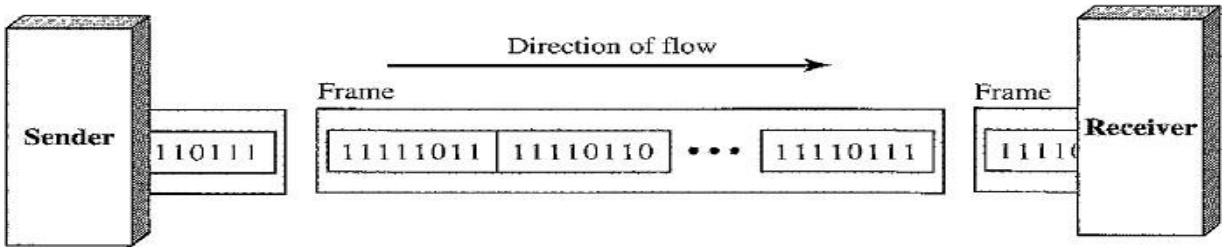
- Without synchronization, the receiver cannot use timing to predict when the next group will arrive.
- To alert the receiver to the arrival of a new group the extra bits 0 and 1 are added.
- At the receiver side when the receiver detects a start bit, it sets a timer and begins counting bits as they come in. After *n* bits, the receiver looks for a stop bit. As soon as it detects the stop bit, it waits until it detects the next start bit
- **Start** and **Stop** bits and the **Gap** alert the receiver to the beginning and end of each byte and allow it to synchronize with data stream. This mechanism is called **Asynchronous.**
- The transmission is slow because of addition of start, stops and gaps between bit streams. Hence it is used for low speed communications.
- Example: The connection to the keyboard to the computer is application of Asynchronous transmission.
- Apart from slower transmission Asynchronous transmission is cheap and effective.

Synchronous Transmission

In synchronous transmission, we send bits one after another without start or stop bits or gaps.It is the responsibility of the receiver to group the bits.

That means:

- The bit stream is combined into longer "**Frames**," which may contain multiple bytes.
- Each byte is introduced onto the transmission link without a gap between the byte and thenext byte.
- It is left to the receiver to separate the bit stream into bytes for decoding purposes.
- Data are transmitted as an unbroken string of 1s and 0's, and the receiver separates thatstring into the bytes, or characters and receiver needs to reconstruct the information.



In synchronous transmission **Timing** plays very crucial role. When the information comes from sender, the receiving device **accurately count the bits** and group them into 8 bits because we don't have any extra bits to identify starting and ending of byte. This process is called **Byte Synchronization**.

Advantage: Speed of the transmission is increased as compared to Asynchronous transmission because there are no extra bits to be add or remove at the sender side and receiver side respectively.

Usage: It is useful for **High Speed Application** such as transmission of data from one computer to another computer.

Note:

1. Byte Synchronization is accomplished at Receiver side.
2. Although there is no gap between characters in synchronous serial transmission, there may be uneven gaps between frames.

Isochronous Transmission

- The isochronous transmission guarantees that the data arrive at a fixed rate.
- In real-time audio and video, in which synchronous transmission fails such as uneven delays between frames, are not acceptable.
- For example, TV images are broadcast at the rate of 30 images per second; they must be viewed at the same rate. If each image is sent by using one or more frames, there should be no delays between frames.
- For this type of application, synchronization between characters is not enough; the entire stream of bits must be synchronized.