COMPUTER NETWORKS (BCA-210)
UNIT – 1

DATA COMMUNICATION

DATA: are the raw facts, figures, concepts processed to be become information that is presented in a form which is understandable to the persons creating it and receiving it.

COMMUNICATION: defined as transfer of data, such as thoughts and messages between two entities. The invention of telegraph, radio, telephone, and television made possible instantaneous communication over long distances.

Eg:- humans, birds, animals communication etc.

Today computer is available in many offices and homes and therefore there is a need to share data and programs among various computers. With the advancement of data communication facilities the communication between computers has increased and thus it has extended the power of computer beyond the computer room. Now a user sitting at one place can communicate with computers of any remote site through communication channel.

In the context of computers, the data are represented by **bi**nary digi**t** or **bit** has only two values 0s and 1s. In fact any thing the computer deals with are 0s and 1s only. Due to this it is called discrete or digital.
Data communications concerns itself with the transmission (sending and receiving) of information between two locations by means of electrical signals. Data communication is the name given to the communication where exchange of information takes place in the form of 0s and 1s over some kind of medium.

The subject-Data Communications deals with the technology, tools, products and equipment to make this happen.

The systems which are used to achieve communication are called communication systems. Communication between two communication systems can either be in one direction or in both directions.

Components of data communication are:-

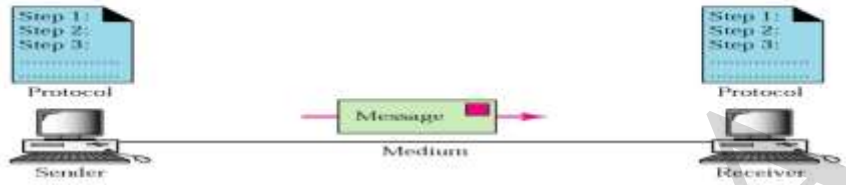
1. **Message** - It is the information to be communicated. Popular forms of information include text, pictures, audio, video etc.

2. **Sender** - It is the device which sends the data messages. It can be a computer, workstation, telephone handset etc.

3. **Receiver** - It is the device which receives the data messages. It can be a computer, workstation, telephone handset etc.

4. **Transmission Medium -** It is the physical path by which a message travels from sender to receiver.

5. **Protocol -** It is a set of rules that governs the data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating. ie. how, where and when of communication.



Elements of protocol are: syntax (structure or format of data to be communicated ie. The method in which data to be presented), semantics (meaning of data) and timing(when and how fast the data to be sent).

NETWORK: A set of devices (computers, printers etc) connected by a medium which is capable of sending data to other devices / receiving data from other devices.

DISTRIBUTED PROCESSING:

Networks use distributed processing and not centralized processing in which processing is divided among all devices over the network. Instead of a single large machine handling all the processing, separate computers are involved in the activities.

The features of distributed processing are :

1) Security
2) Faster problem solving
3) Collaborative processing
4) Distributed databases

Any **network** to be **efficient and effective** should meet some criteria. They are:

1) **Performance**: For a network, performance can be measured in respect to two aspects- transit time and response time. Transit time is the time taken to transfer message from one device to another. Response time is the time difference between request and response(question and answer).

The performance of network depends on factors like no. of users, devices, type of medium, devices capability and efficiency of software used.

2) **Reliability**: measured by the number of times the network fails, time it takes to recover from failure and how far the network support remains in case of calamities.
3) **Security**: means how the network is secure from unauthorized access and virus attacks. ie. The network should have security mechanisms at place like password protection, encryption techniques etc.

Some of the applications of data communication networks are in the areas of finance, marketing, entertainment, cable television, manufacturing, email and teleconferencing, world wide web etc.

Standards: These are required to govern the physical, electrical and procedural characteristics of communication devices. Advantages of standards are that they ensure a large market for a particular product, allows devices of different vendors to communicate with each other. Possible disadvantages are that the standards lock or freeze technology for some period of time, they take ample amount of time to get established and multiple standards for a same thing may exist.

Data communication standards is divided into 2 : de facto(by fact) and de jure(by law)

De facto(by fact) standards is divided into two: proprietary and nonproprietary. Proprietary standards are those given by an organization based on the operation of the products it supplies. Also called closed standards because it applies only to its own products.
Nonproprietary standards are those given by committees or interested groups and given to public. Also called open standards because applicable to all systems.

De jure standards are those officially given by some approved organizations.

Standards Organisations

(1) **International Standards Organisation (ISO)**:- Created in 1947, is a voluntary organization dedicated to worldwide international standards. It has members from 82 nations. ISO is into actively developing standards for the scientific, technological and economic areas. In the field of communications, they have given the Open system Interconnection model for network communication.

(2) **ITU-T**:- The United Nations formed the CCITT (Consultative Committee for International Telegraphy and Telephony) as part of ITU(International Telecommunications Union). This committee was devoted to the research and development of telecommunications standards. In 1993, CCITT was changed to ITU-T. Best known ITU-T standards are V series for communications over phone lines, X series for public digital networks, ISDN ie. International digital network.

The above two are the principal standards bodies internationally.

(3) **ANSI**:- (American National Standards Institute) is a private organization, all activities undertaken in compliance of the welfare of the US and its citizens. It is the representative in the ITU and ISO.
(4) **IEEE**:- Institute of Electrical and Electronics Engineers, is the largest professional engineering society in the world. Involved in developing standards for computing, communication, engineering and electronics. Important contribution is 802 series for LAN's.

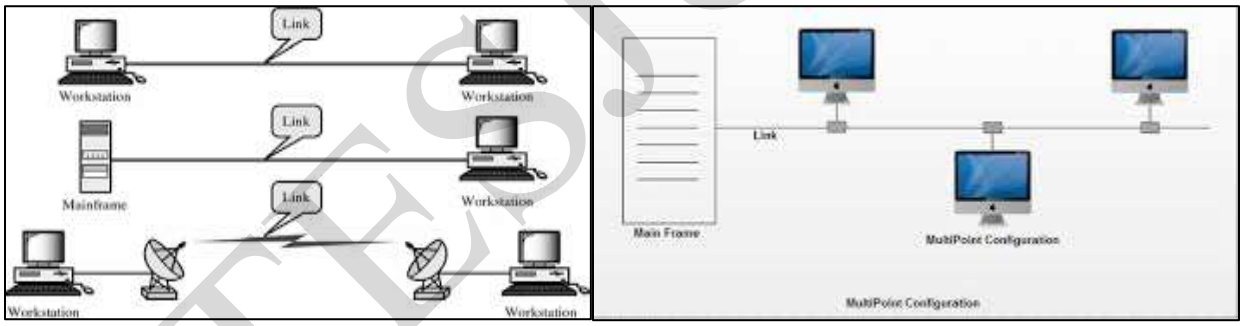
LINE CONFIGURATION (method of attachment of devices to a link)

LINK (is the physical communication method that transfers data from one device to another).

For data communication to occur the devices must be connected in some way to the same link at the same time.

There are 2 types of line configurations: **(point to point) and (multi-point).**

- Point to point line configuration means dedicated link between 2 devices. The entire link is for the transmission between the devices.
- Multipoint configuration means the two devices share their link with other devices.



NETWORK TOPOLOGY

The physical arrangement of links in a network is called as **TOPOLOGY. i**e. the way a network is laid out. Two or more devices connect to link, two or more links form part of topology.

- The topology defines how the devices (computers, printers.etc) are connected and how the data flows from one device to another.
- There are two conventions while representing the topologies. The physical topology defines how the devices are physically wired. The logical topology defines how the data flows from one device to another.

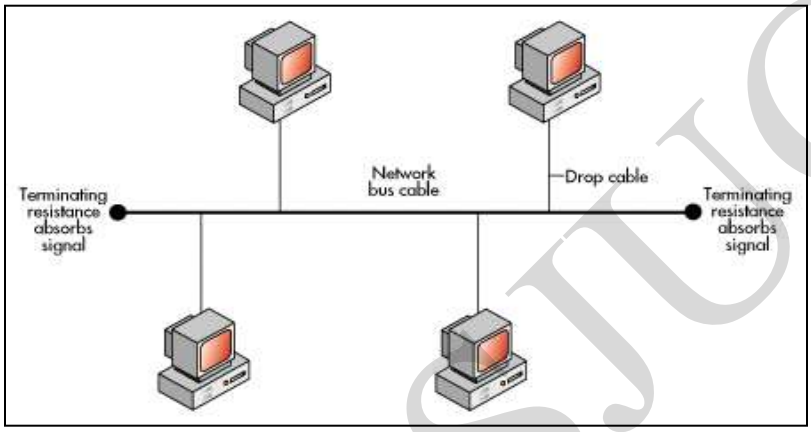
The Topologies are:

(a) Bus Topology

In bus topology all workstations are connected to a single communication line called bus. In this type of network topology there is no central server and all the computers can talk or communicate to all other systems connected to the cable. Transmission from any station travels the length of the bus in both directions and can be received by all workstations. The **advantage** of the bus topology is that

- It is quite easy to set up.
- If one station of the topology fails it does not affect the entire system.

The **disadvantage** of bus topology is that any break in the bus is difficult to identify and addition of more computers (nodes) slows down the network performance.

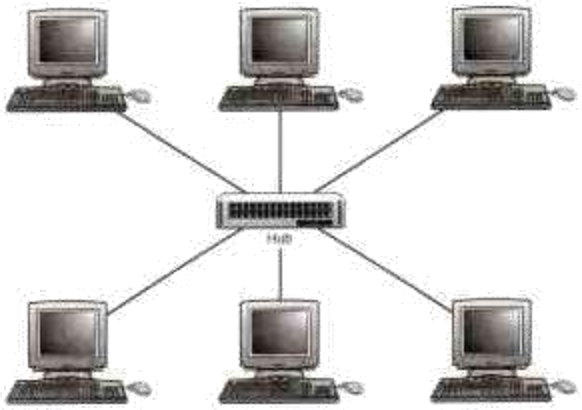


(b) Star topology

In star topology a number of workstations (or nodes) are directly linked to a central server. Any communication between stations in a star LAN must pass through the central server. There is bi-directional communication between various nodes. The central server controls all the activities of the nodes. The **advantages** of the star topology are:

- It offers flexibility of adding or deleting of workstations from the network.
- Breakdown of one station does not affect any other device on the network.

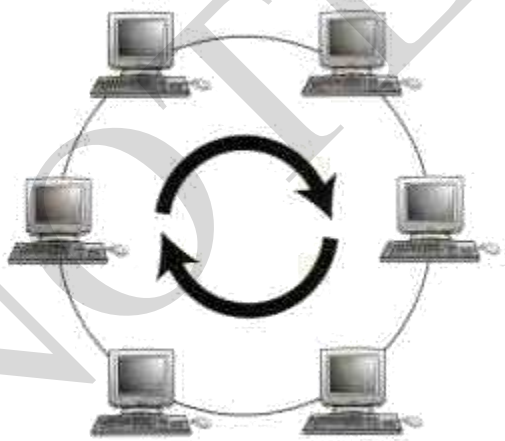
The major **disadvantage** of star topology is that failure of the central node disables communication throughout the whole network.



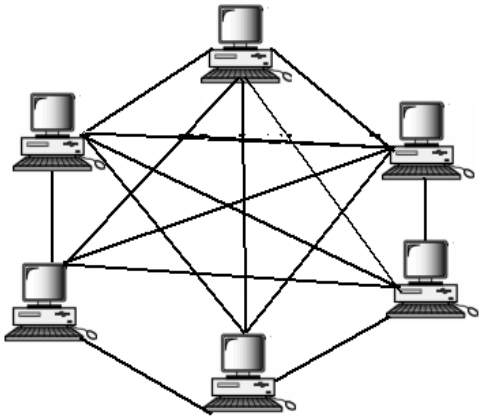
(c) Ring Topology

In ring topology each station is attached to nearby stations on a point-to-point basis so that the entire system is in the form of a ring. In this topology data is transmitted in one direction only. Thus the data packets circulate along the ring in either clockwise or anticlockwise direction. The **advantage** of this topology is that any signal transmitted on the network passes through all the LAN stations.

The **disadvantage** of ring network is that the breakdown of any one station on the ring can disable the entire system. The communication of data takes longer time as flow is only in one direction.



(d) Mesh Topology: In a full mesh network, each network node is connected to every other node in the network. Due to this arrangement of nodes, it becomes possible for a simultaneous transmission of signals from one node to several other nodes. In a partially connected mesh network, only some of the network nodes are connected to more than one node. This is beneficial over a fully connected mesh in terms of redundancy caused by the point-to-point links between all the nodes. It helps find the quickest route on the network; provides redundancy. Very expensive and not easy to set up.



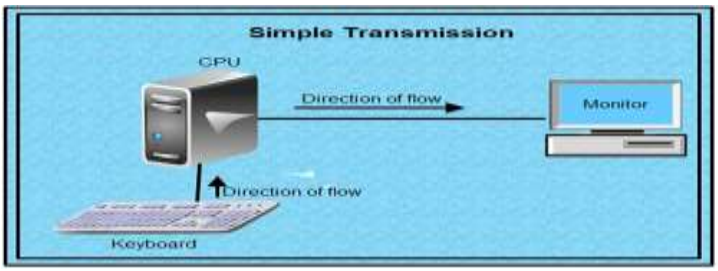
(e) Hybrid topology

A hybrid topology is a combination of any two or more network topologies in such a way that the resulting network does not have one of the standard forms. For example, a tree network connected to a tree network is still a tree network, but two star networks connected together is a hybrid network topology. A hybrid topology is always produced when two different basic network topologies are connected.

Data Transmission Modes

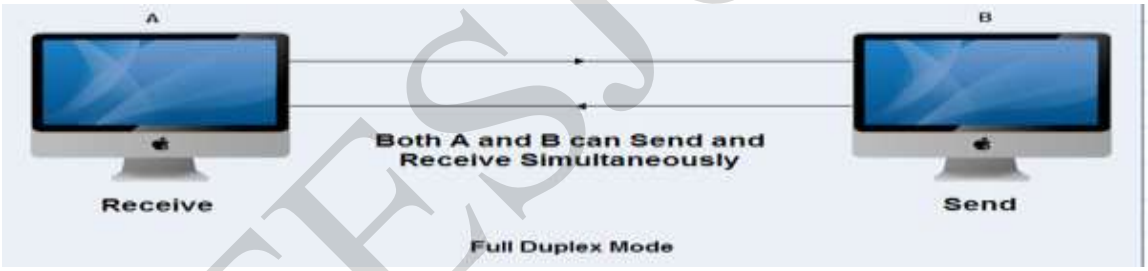
Based on the direction of transmission, there are three ways for transmitting data from one point to another.

1. **Simplex**: In simplex mode the communication can take place only in one direction. The receiver receives the signal from the transmitting device. This mode of flow of information is Unidirectional. Example: Radio, T.V., Pager transmission.



2. **Half-duplex**: In half-duplex mode the communication channel is used in both directions, but one direction at a time. Thus a half-duplex line can alternately send and receive data. Example is the walkie-talkie.

3. Full-duplex: In full duplex mode, the communication channel is used in both directions at the same time. Use of full-duplex line improves the efficiency as the line turn around time required in half-duplex arrangement is eliminated. Example of this mode of transmission is the telephone line.



COMPUTER NETWORK

A computer network is an interconnection of various computer systems located at different places. In computer network two or more computers are linked together with a medium and data communication devices for the purpose of communicating data and sharing resources. The computer that provides resources to other computers on a network is known as server. In the network the individual computers, which access shared network resources, are known as workstations or nodes.

Computer networks may be classified on the basis of geographical area in three broad categories.

1. Local Area Network (LAN)

2. Metropolitan Area Network (MAN)

3. Wide Area Network (WAN)

(a) Local Area Network

Network used to interconnect computers in a single room or rooms within a building or nearby buildings is called Local Area Network (LAN). LAN transmits data with a speed of several megabyte per second (106 bytes per second). The transmission medium is normally coaxial or twisted-pair cables. This usually spans about 0-5 kms and is generally a private network owned by an organization. For example: Office LAN, Hospital LAN, Campus-wide LAN, etc.

LAN links computers through software and hardware in the same area for the purpose of sharing information. Usually LAN links computers within a limited geographical area and are therefore connected by a cable. Addition of a new computer in the network therefore requires cabling to be done. People working in LAN get more capabilities in data processing, work processing and other information exchange compared to stand-alone computers. Because of this information exchange capability most of the business and government organizations are using LAN.

Major Characteristics of LAN

- Each computer has the potential to communicate with any other computer of the network.
- High degree of interconnection between computers
- Easy physical connection of computers in a network.
- Inexpensive medium of data transmission
- High data transmission rate

Advantages

- The reliability of network is high because the failure of one computer in the network does not effect the functioning of other computers.
- Addition of new computer to network is easy.
- High rate of data transmission is possible.
- Peripheral devices like magnetic disk and printer can be shared by other computers.

Disadvantages

- If the communication line fails, the entire network system breaks down.

Use of LAN

Following are the major areas where LAN is normally used: File transfers and Access, Word and text processing, Electronic message handling, Remote database access, Personal computing, Digital voice transmission and storage.

(b) Metropolitan Area Network

The MAN is used to describe a network of computers spanning a city usually 5-50 kms of range. A company having multiple offices in various parts of a city generally uses this type of network. Example is the Cellular or mobile Phone network.

(c) Wide Area Network

The term Wide Area Network (WAN) is used to describe a computer network spanning a regional, national or global area. For example, for a large company the head quarters might be at Delhi and regional branches at Bombay, Madras, Bangalore and Calcutta. Here regional centers are connected to head quarters through WAN. The distance between computers connected to WAN is quite large. Therefore the transmission medium used is normally telephone lines, microwaves and satellite links. Internet is an example of a WAN.

Characteristics of WAN

Followings are the major characteristics of WAN.

1. Communication Facility: For a big company spanning over different parts of the country the employees can save long distance phone calls and it overcomes the time lag in overseas communication. Computer conferencing is another use of WAN where users communicate with each other through their computer system.

2. Remote Data Entry: Remote data entry is possible in WAN. It means sitting at any location you can enter data, update data and query other information of any computer attached to the WAN but located in other cities or country. For example, supposeyou are sitting at Madras and want to see some data of a computer located at Delhi, you can do it through WAN.

3. Centralised Information: In modern computerized environment you will find that big organizations go for centralized data storage. This means if the organization is spread over many cities, they keep their important business data in a single place. As the data are generated at different cities, WAN permits collection of this data from different sites and save at a single site.

Examples of WAN

1. Ethernet: Ethernet developed by Xerox Corporation is a famous example of WAN. This network uses coaxial cables for data transmission. Special integrated circuit chips called controllers are used to connect equipment to the cable.

2. Arpanet: The Arpanet is another example of WAN. It was developed at Advanced Research Projects Agency of U.S. Department. This Network connects more than 40 universities and institutions throughout USA and Europe.

INTERNET

The Internet is a network of networks. Millions of computers all over the world are connected through the Internet. Computer users on the Internet can contact one another anywhere in the world. If your computer is connected to the Internet, you can connect to millions of computers. You can gather information and distribute your data. It is very much similar to the telephone connection where you can talk with any person anywhere in the world. In Internet a huge source of information is accessible to people across the world. Information in every field starting from education, science, health, medicine, history and geography to business, news, etc. can be retrieved through Internet. You can also download programs and software packages from anywhere in the world. Due to the tremendous information resources the Internet provides, it is now indispensable to every organization.

ISO-OSI MODEL (Very IMPORTANT)

The OSI Model provides a framework for describing what goes on when two computer systems communicate over a network. The framework divides the tasks involved with communicating into a series of layers. In 1977 ISO formed a working committee to develop standards for computer to computer communication. The result was the Open Systems Interconnection (OSI) Reference Model; a logical method for dividing up the task of system to system communication and a framework for understanding all the pieces of that task.

The OSI Model

The Open Systems Interconnection Reference Model, or OSI Model, breaks the job of system to system communication over a network into seven layers. Each layer represents a different portion of the task.
The bottom layer of the OSI model is closest to the hardware in the computer or other networked device. The top layer is closest to the application software that you interact with.

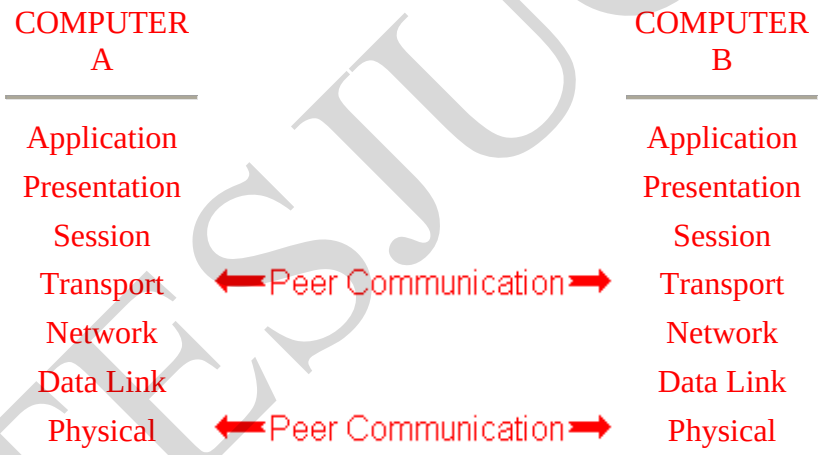
The outline of the model is shown below.

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

- Tasks and information move down from the top layers until they reach the bottom layer where they are sent out over the network media from the source system to the destination.
- At the destination the task or information rises back up through the layers until it reaches the top.
- Each layer is designed to accept work from the layer above it, and pass work down to the layer below it. The interfaces between layers are standardized. This permits several things that would not be possible without a layered design for communications.
- Each layer can be designed independently of the others. This means that the overall task of communicating on the network can be divided up between several design teams who can all work on the problem simultaneously.
- Also, the functioning of a layer can be changed without affecting the functioning of the layers above and below it.

Peer Communication

While each layer provides services to the layer above it, and sends work requests down to the layer below it, each layer *communicates* with its peer layer on the remote computer.



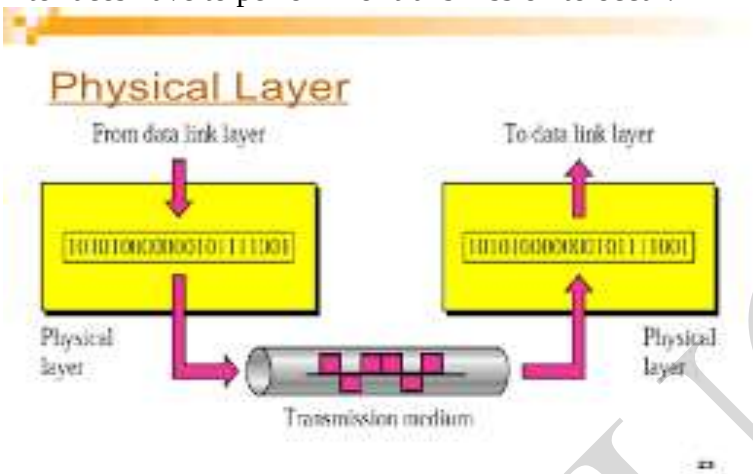
In the diagram above, the Transport layer on Computer A has a message for its peer -- the Transport layer on Computer B. Transport Layer on Computer A hands its message down to Network Layer on Computer A, requesting that it be sent to Computer B.

The message is handed down through the layers until it reaches layer 1 -- the Physical layer -- and is transmitted across the network media to Computer B. Once at Computer B the message rises layer by layer until it reaches Transport Layer. There, Transport Layer on Computer B reads the message from its peer -- Transport Layer on Computer A -- and takes whatever action is appropriate for the message.

Note: The OSI Model itself doesn't get any communicating done. It is not a piece of hardware or software. Rather, the OSI Model serves as a guideline for defining *protocols*.

Layer One – Physical Layer

The physical layer coordinates the functions required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission medium. It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur.



The physical layer is also concerned with the following:

Physical characteristics of interfaces and medium: The physical layer defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.

Representation of bits. The physical layer data consists of a stream of bits (sequence of Os or 1s) with no interpretation. To be transmitted, bits must be encoded into signals--electrical or optical. The physical layer defines the type of encoding .

Data rate. The transmission rate-the number of bits sent each second-is also defined by the physical layer. In other words, the physical layer defines the duration of a bit, which is how long it lasts.

Synchronization of bits. The sender and receiver not only must use the same bit rate but also must be synchronized at the bit level. In other words, the sender and the receiver clocks must be synchronized.

o Line configuration. The physical layer is concerned with the connection of devices to the media. In a point-to-point configuration, two devices are connected through a dedicated link. In a multipoint configuration, a link is shared among several devices. o Physical topology. The physical topology defines how devices are connected to make a network.

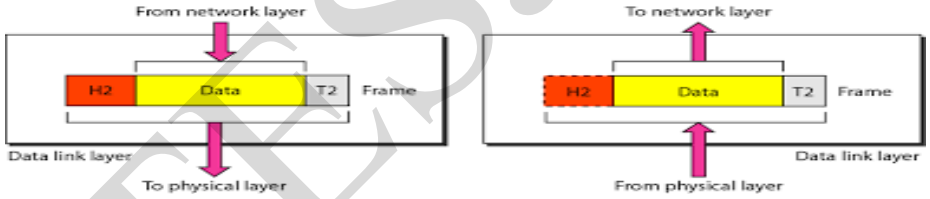
o Transmission mode. The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex

Services - ISDN, ADSL, ATM, FDDI,
CAT 1-5, Coaxial cable

Layer Two - Data Link Layer

The Data Link layer performs several tasks. It compiles the stream of ones and zeros coming from the Physical layer into bytes, and then into *frames* -- units of information that have a logical meaning. Data Link can add its own header to the information it passes down to the Physical layer. Information in the header usually includes the destination and source physical addresses of the frame. Actions performed of DLL are:

- Framing
- 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/or receiver of the frame
- Flow control: Managing the flow of data ie. If the rate at which the data received by receiver is slow, then the flow from sender is controlled.
- Error control: imposes mechanisms to detect and retransmit damaged or lost frames.
- Access control: when devices are attached to the same link, it the duty of this layer to determine which device has the access to the link at any point of time.



Services **–** SLIP/PPP, 802.2 SNAP, Ethernet

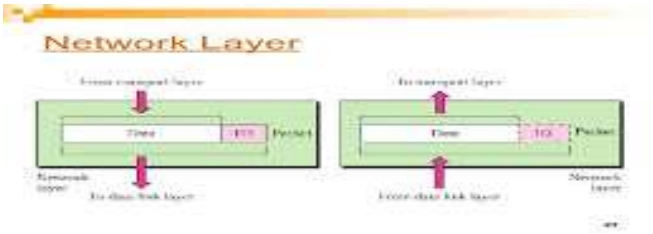
Layer Three – Network Layer

The Network Layer deals with moving packets of information across the network.

Devices that operate on layer three of the network forward packets from one network to the next based on the destination network address of the packet. They choose how to forward the packet based on either dynamically determining the best route, or by looking up a route from a static routing table. Through this method a packet is routed one hop at a time from its source, across the network, to its destination.

Ie. This layer is responsible for source to destination delivery of packets across multiple links.

Other responsibilities of the network layer include the following: o Logical addressing. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver. o Routing. When independent networks or links are connected to create intemetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.

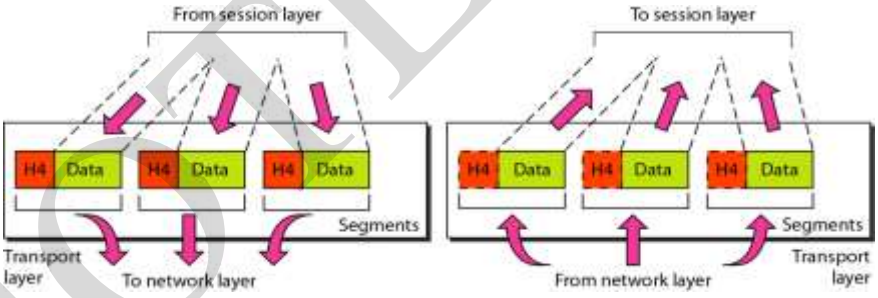


Layer Four – Transport Layer

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

The objective of the transport layer is to provide reliable data transmission for the layers above it.

Transport Layer does this by ordering the process of setting up and tearing down communications between two systems. It uses sequence numbers and flow control to keep information moving at the right rate, and to make sure that the recipient knows how to reassemble a stream of packets in the right order.



Functions of this layer are:

- Segmentation and reassembly: Dividing messages into packets while transmitting and repackaging messages while receiving.
- Connection control: ie either connectionless or connection oriented. A connection oriented transport layer makes a connection with the transport layer of destination

machine before sending the packets. After transfer, connection terminated. A connectionless transport layer directly sends the packets into the network.

- Flow control: similar to data link layer. But flow control on end to end rather than across a single link.
- Error control: similar to data link layer. But error control on end to end rather than across a single link, transport layer on sender makes sure that the entire message arrives at the receiver without error.

Layer Five – Session Layer

The bottom four layers -- Physical, Data Link, Network, and Transport -- all look "down" toward the bottom of the network. Their focus is on getting the job of moving data from point A to point B done.

The Session layer, in a sense, looks *up* toward the top layers. Session is responsible for regulating the flow of information between applications. It synchronizes their communication, and takes care of such things as security and handling errors outside the scope of network communications (such as a server with a full disk drive, or a tape that needs to be mounted).

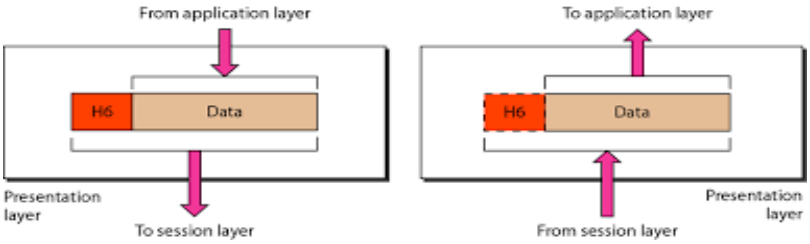
- Dialog control: The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half duplex (one way at a time) or full-duplex (two ways at a time) mode.
- Synchronization: adding sync bits (checkbits) to stream of data. For a Huge file size, add checkbits after interval of certain bits.

Layer Six – Presentation Layer

The primary job of the Presentation layer is that of translator. It takes care of translating ACSII into EBCDIC, and vice versa; compression, decompression; encryption and decryption. Essentially, the Presentation layer works to transform data into the form that the Application layer can accept.
ie. Concerned with the syntax and semantics of the information exchanged between 2 systems.

Functions of this layer are:

- Translation: translates information into a form usable by the application layer. Changes from sender dependent format to receiver format.
- Encryption / Decryption: transforming the sender information into another form and vice-versa.
- Compression: compresses the bits to be transmitted.

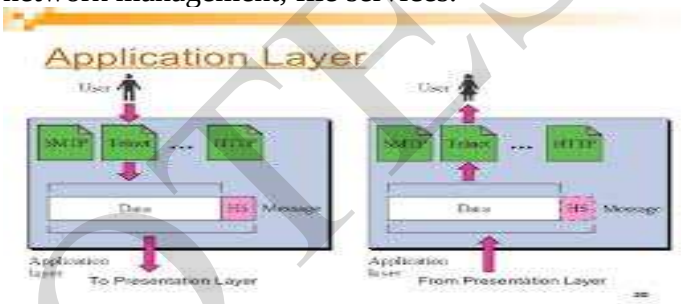


Layer Seven – Application Layer

This is the layer closest to the user. The Application layer deals with printing, file transfer, remote terminal services, directory browsing. Some user applications exist directly at the Application layer, such as Telnet and FTP. Other user applications have Application layer functions built into them. A word processing program that can print to a network printer has Application layer functions built into it. Watching the status bar of your web browser is a good place to see Application layer functions at work.

Enables the user to access the network. Provides the user interfaces and support for services such as email, remote file access / transfer, data base access etc.

Services **–** e-mail, news groups, web applications, file transfer, remote host, directory services, network management, file services.



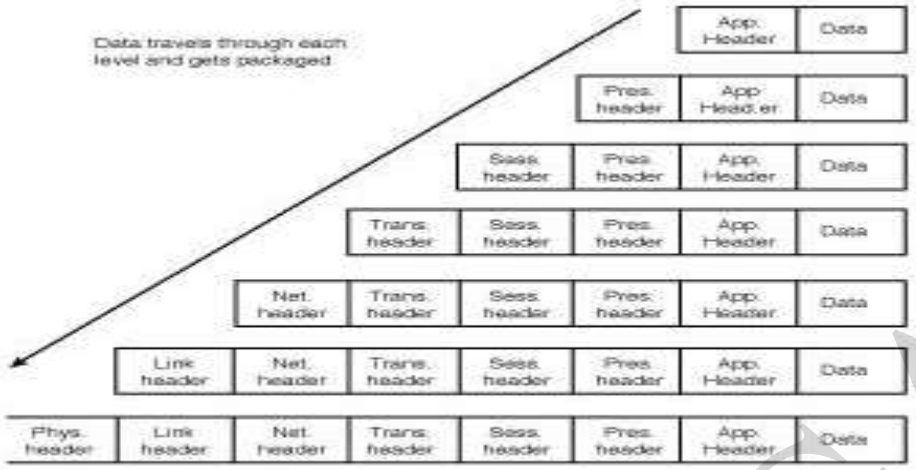
LAYERING OF OSI Model

Layering the communication process invokes breaking down the communication puzzle into smaller and easier to handle interdependent pieces. Each layer deals with a specific aspect of communication & provides an interface to the layer above.

The set of operations define the service provided by that layer.

As a message sent by the top layer is passed on to the next lower layer ,a header may be appended to the message. Some layers add both a header and a trailer. Each layer then strips the header (trailer), handles the message using the protocol provided by the layer and passes it on to the next higher layer.

The lowest layer transmits the message over the network to the receiving machine. It communicates with the most bottom layer of the receiver.



OSI in Action

- A message begins at the top application layer and moves down the OSI layers to the bottom physical layer.
- As the message descends, each successive OSI model layer adds a header to it.
- A header is layer-specific information that basically explains what functions the layer carried out.
- Conversely, at the receiving end, headers are striped from the message as it travels up the corresponding layers.

SUMMARY:

Application Layer: Provides network services to user applications. It is responsible for exchanging information between programs running on the machine, such as an e-mail program, and other services running on a network, such as a print server or another computers' application.

Presentation Layer: Concerned with how data is converted and formatted for data transfer. Examples of format conversions include ASCII text for documents and .gif and JPG for images. This layer performs code conversion, data translation, compression and encryption.

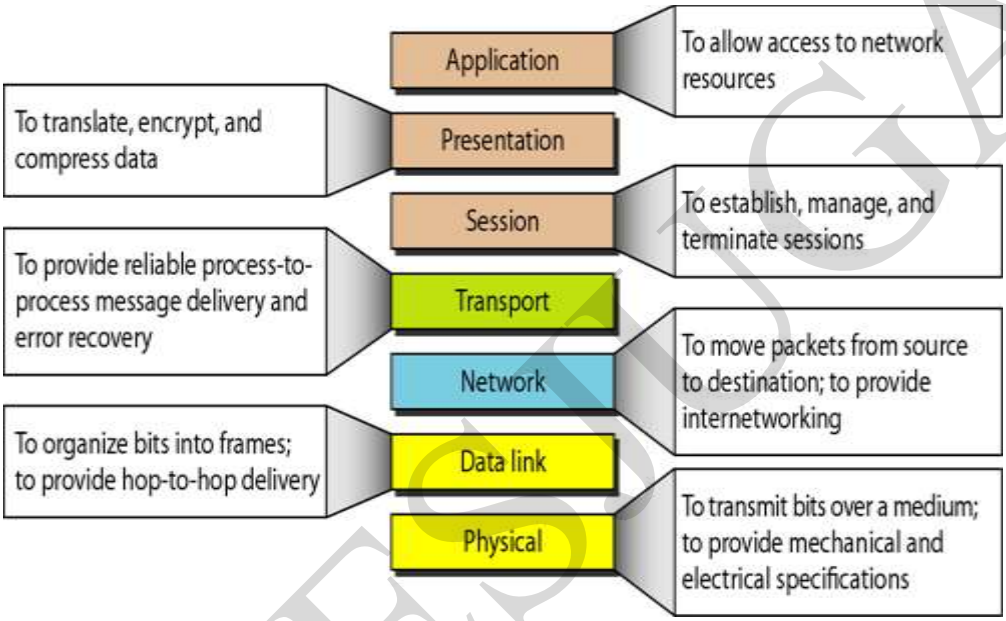
Session Layer: Determines how two devices establish, maintain and manage a connection - how they talk to each other. These connections are called sessions.

Transport Layer: Responsible for breaking the data into segments, establishing an end-to-end logical connection between machines, and providing for error handling.

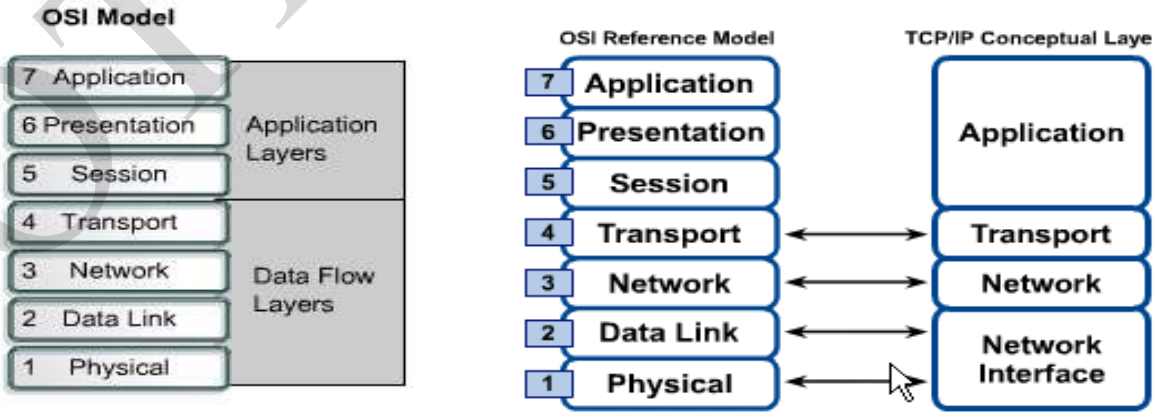
Network Layer: Responsible for determining addressing on the network, determining the routes that information will take on its journey, and managing network traffic congestion. Data at this level is packaged into packets.

Data Link Layer: Provides the link for how data, packaged into frames is communicated through hardware to be transported across a medium. It communicates with network cards, manages physical layer communications between connecting systems and handles error notification.

Physical Layer: Specifies how data is processed into bits and physically transferred over medium, such as cables. It's responsible for activating and maintaining the physical link between systems.



OSI & TCP/IP Models



The main **differences** between the two models are as follows:

1.OSI is a reference model and TCP/IP is an implementation of OSI model.

2.TCP/IP Protocols are considered to be standards around which the internet has developed. The OSI model however is a "generic, protocol-independent standard."

3.TCP/IP combines the presentation and session layer into its application layer.

4.TCP/IP combines the OSI data link and physical layers into the network access layer.

5.TCP/IP appears to be a simpler model and this is mainly due to the fact that it has fewer layers.

6.The OSI model consists of 7 architectural layers whereas the TCP/IP only has 4 layers.

7.The TCP/IP design generally favors decisions based on simplicity, efficiency and ease of implementation.

TCP/IP Model Layers Explained: It is a suite of protocols which is named after its most significant pair of protocols. That is Transmission Control Protocol and Internet Protocol.

- TCP/IP model are made up of layers. Each layer is responsible for a set of computer network related tasks. Every layer provides service to the layer above it.

- There are in all four layers in the TCP/IP reference model.

Host to Network Layer
It is the bottom layer of TCP/IP model & lies below the internet layer. It is also known as Network Interface Layer. Function of this layer is to connect the host to the network & inform the upper layers so that they could start sending the data packets. This layer varies from network to network.

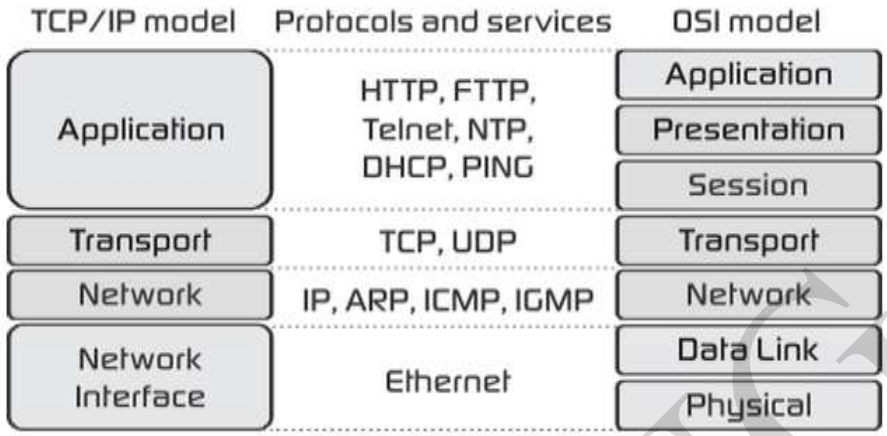
Internet Layer
It is similar to Network Layer of OSI model in functionality. It allow the hosts to submit the packets to the network & Packets should travel independently using any possible route. The order in which the packets arrive at destination can be different from the order in which they were sent. In such cases it is the responsibility of higher layer to arrange these packets in proper order.

Transport Layer

It is similar in functionality to transport layer of OSI model. It allows the two processes on source & destination machines to communicate with each other. It divides the byte stream into messages. It handles the flow control so that a fast sender should not overflow a slow receiver. Transport Layer also provides two types of services: connection oriented & connectionless services.

Application Layer

It is the topmost of TCP/IP Model. It is responsible for data transfer between applications. It provides services such as e-mail, file transfer, access to the world wide web etc. to the user applications. It uses the protocols like FTP, SNTP & TELNET to transfer the data between applications.



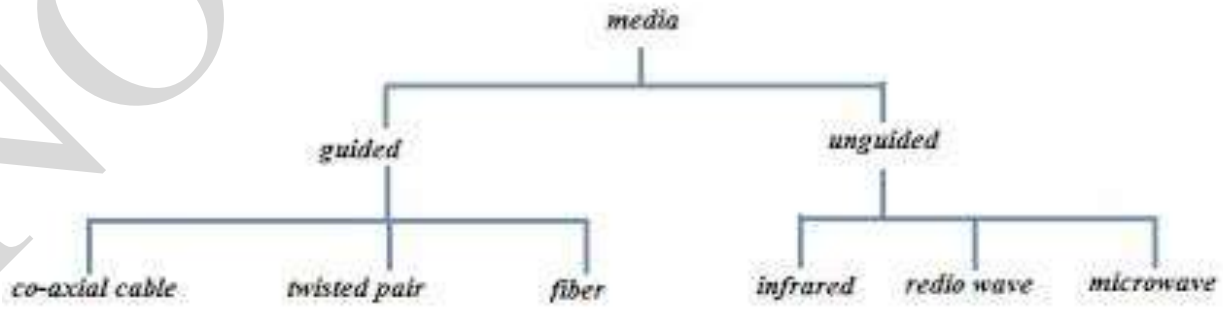
TRANSMISSION MEDIA

Transmission media can be defined as physical path between transmitter and receiver in a data transmission system.

There are 2 basic categories of Transmission Media: Guided and Unguided.

Guided Transmission Media uses a "cabling" system that guides the data signals along a specific path. The data signals are bound by the "cabling" system. Guided Media is also known as Bound Media.

Unguided Transmission Media consists of a means for the data signals to travel but nothing to guide them along a specific path. The data signals are not bound to a cabling media and as such are often called Unbound Media.

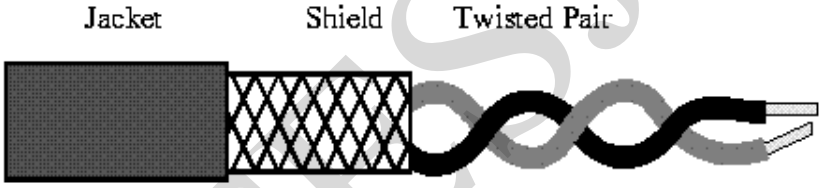


The types of Guided Media are: Twisted Pair , Coaxial Cable , Optical Fibre

Twisted Pair Cable : The least expensive and most widely used guided transmission media.

CAT5 cable (twisted cable)

Construction: A twisted pair cable consists of two insulated copper wires arranged in a spiral pattern. A wire pair acts as a communication link.
Two copper wires are typically ``twisted" together in a helix to reduce interference between the two conductors as shown in Fig.. Twisting decreases the cross-talk interference between adjacent pairs in a cable. Typically, a number of pairs are bundled together into a cable by wrapping them in a tough protective sheath.
They carry analog signals, commonly used in telephone networks. Now-a-days it is also used for digital signals, for LAN's. They spans distances of several kilometers. The data rate is determined by wire thickness and length. In addition, shielding is done to eliminate interference from other wires and ultimately, the data rate. For analog signals, amplifiers are used every 5 to 6 km. For digital transmission, repeaters are used every 2 or 3 km.



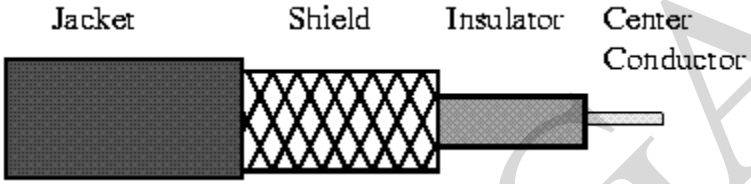
Cables with a shield are called Shielded Twisted Pair and commonly abbreviated STP. Cables without a shield are called Unshielded Twisted Pair or UTP.

UTP or Unshielded Twisted Pair cable is used on Ethernet LAN's . It uses the RJ line of connectors (RJ45, RJ11, etc..)

Coaxial Cable:

The coaxial cable or ``coax", consists of a copper core surrounded by insulating material and a braided outer conductor as shown in Fig. The outer conductor is covered with a jacket or shield. It operates over wider range of frequencies. It is of two types : baseband and broadband.
Applications of coaxial cable are: Long-distance telephone communication, Television distribution, LAN's.

Characteristics: Co-axial cable has superior frequency characteristics compared to twisted-pair and can be used for both analog and digital signaling. In baseband LAN, the data rates lies in the range of 1 KHz to 20 MHz over a distance in the range of 1 Km. This cable offers bandwidths of 300 to 400 MHz facilitating high-speed data communication with low bit-error rate.
In broadband signaling, signal propagates only in one direction, in contrast to propagation in both directions in baseband signaling. Because of the shielded, concentric construction, co-axial cable is less susceptible to interference and cross talk than the twisted-pair. For long distance communication, repeaters are needed for every kilometer or so. Data rate depends on physical properties of cable, but 10 Mbps is typical.



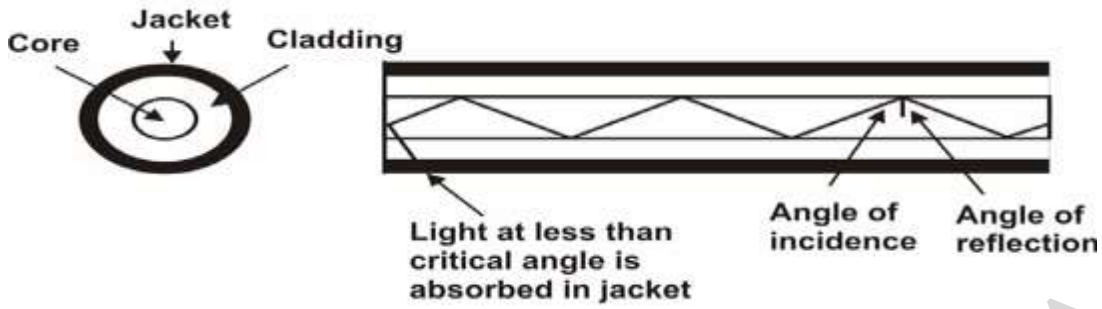
Fiber Optics Cable / Optical Fibre

An optical fibre is a thin flexible medium capable of guiding a light ray. Glass or plastic is used to make optical fibres. The fiber optic cable has a cylindrical shape and consists of three concentric sections: core, cladding and jacket.
Core consists of the innermost section and has the very thin strands or fibres made of glass. The fibre is surrounded by cladding , a glass or plastic coating that has a different density than core.
As a consequence, the light is propagated through multiple total internal reflections.
The interface between core and cladding acts as a reflector to confine light inside the medium. The outermost layer surrounding one or more bundle of cladded wires is the jacket. It is composed of plastic, or other material to protect it. The jacket is used to protect against moisture, abrasion, crushing and other environmental hazards.

The signal consists of pulses of light. For instance, a pulse of light means ``1", lack of pulse means “0”. An important characteristic of Fibre Optics is Refraction. Refraction is the characteristic of a material to either pass or reflect light. When light passes through a medium, it "bends" as it passes from one medium to the other. An example of this is when we look into a pond of water.

If the angle of incidence is small, the light rays are reflected and do not pass into the water. If the angle of incident is great, light passes through the media but is bent or refracted.

Optical Fibres work on the principle that the core refracts the light and the cladding reflects the light. The core refracts the light and guides the light along its path. The cladding reflects any light back into the core and stops light from escaping through it - it bounds the media!



Optical Fiber

Three components are required:

1. Fiber medium: Current technology carries light pulses for tremendous distances (e.g., 100s of kilometers) with virtually no signal loss.

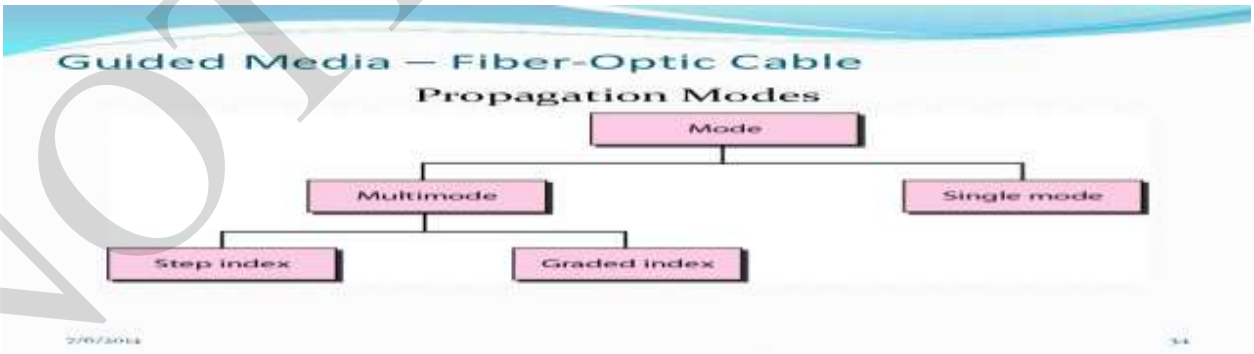
2. Light source: typically a Light Emitting Diode (LED) or laser diode. Running current through the material generates a pulse of light.

3. A photo diode light detector, which converts light pulses into electrical signals.

Fiber Uses: Because of greater bandwidth (2Gbps), smaller diameter, lighter weight, low attenuation, immunity to electromagnetic interference and longer repeater spacing, optical fiber cables are finding widespread use in long-distance telecommunications. Fiber optic cables are also used in high-speed LAN applications.
Rural exchange trunks-link towns and villages

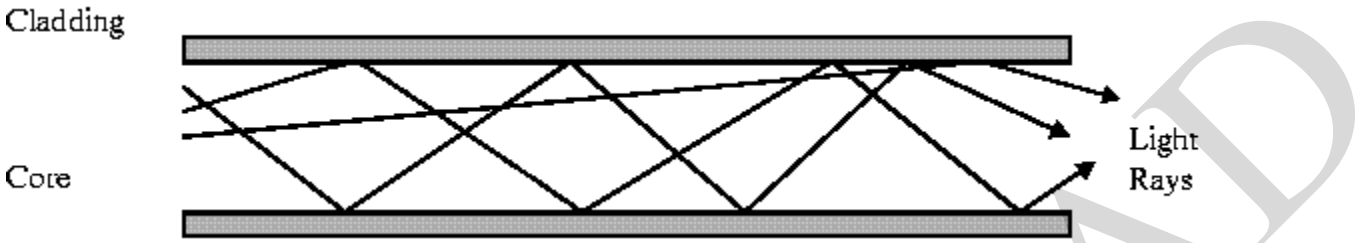
Optical Transmission Modes

There are 3 primary types of transmission modes using optical fibre.

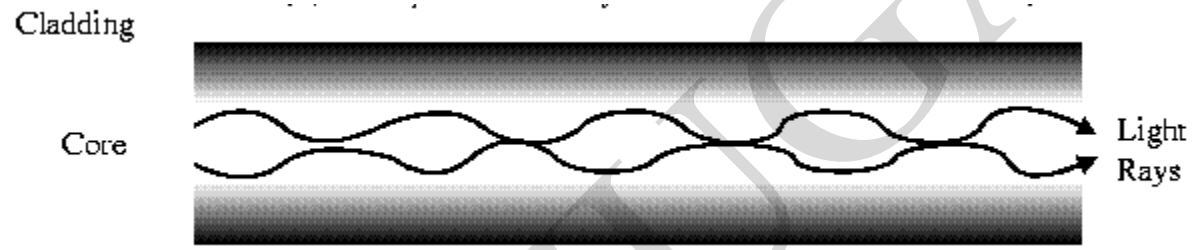


Step Index has a large core , the density of core from center to the edge is the same. The light rays tend to bounce around, reflecting off the cladding, inside the core. This causes some rays to take a longer or shorted path through the core. Some take the direct path with hardly any

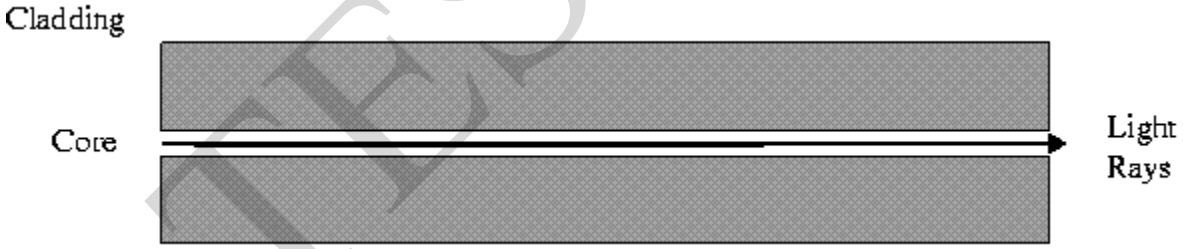
reflections while others bounce back and forth taking a longer path. The result is that the light rays arrive at the receiver at different times. The signal becomes longer than the original signal.



Grade Index has a gradual change in the Core's Refractive Index. Ie. The density of the core varies from center to the edge. This causes the light rays to be gradually bent back into the core path. This is represented by a curved reflective path in the attached drawing. The result is a better receive signal than Step Index.



Single Mode has separate distinct Refractive Indexes for the cladding and core. The light ray passes through the core with relatively few reflections off the cladding. Single Mode is used for a single source of light (one colour) operation.



Advantages of Optical Fibre:

- Noise immunity
- Security: cannot tap into cable.
- Large Capacity due to BW (bandwidth)
- No corrosion
- Longer distances than copper wire
- Smaller and lighter than copper wire
- Faster transmission rate

Disadvantages of Optical Fibre:

- Physical vibration will show up as signal noise.
- Limited physical arc of cable. Bend it too much & it will break.
- Difficult to splice.

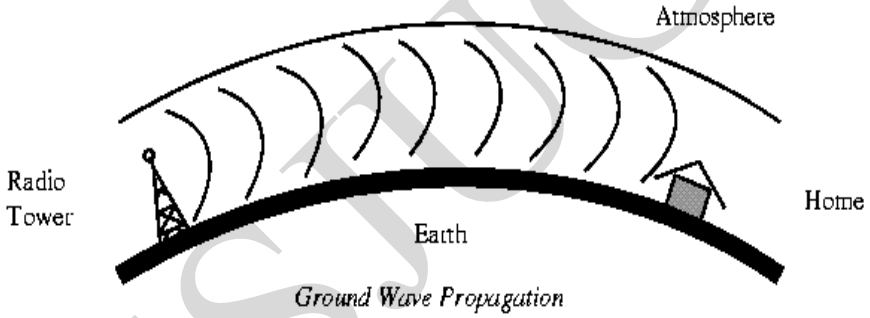
Transmission Media - Unguided

Unguided Transmission Media is transmission of data signals through the air. They are not guided or bound to a channel to follow. Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.

Unguided signals can travel from the source to destination in several ways:

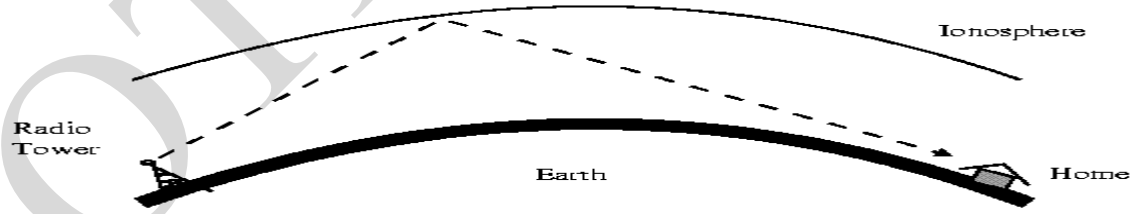
ground propagation, sky propagation, and line-of-sight propagation

Ground Propagation follows the curvature of the Earth. Ground Waves have carrier frequencies up to 2 MHz. AM radio is an example of Ground Wave Propagation.

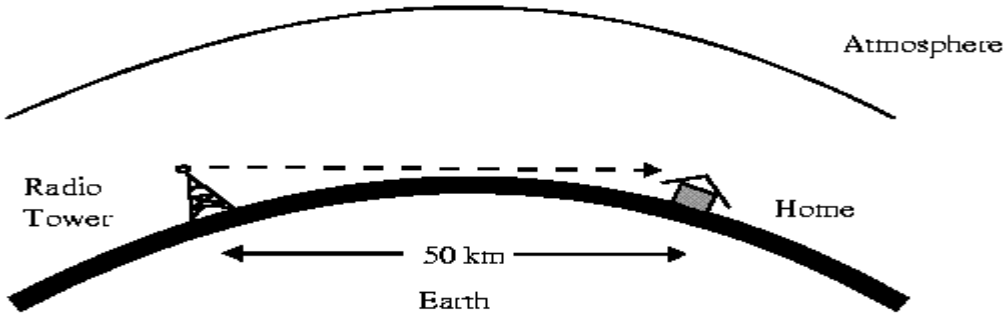


Ground Wave Propagation

Ionospheric or Sky Propagation bounces off of the Earths Ionospheric Layer in the upper atmosphere. The signal bounces off of the ionosphere and back to earth.



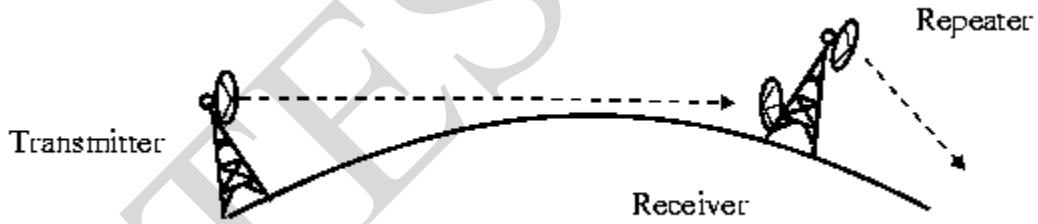
Line of Sight Propagation transmits exactly in the line of sight. The receive station must be in the view of the transmit station. Examples of Line of Sight Propagation are: FM Radio.



Radio Frequencies are in the range of 300 kHz to 10 GHz. We are seeing an emerging technology called wireless LANs. Some use radio frequencies to connect the workstations together, some use infrared technology.

Microwaves

Microwave transmission is line of sight transmission. The Transmit station must be in visible contact with the receive station. This sets a limit on the distance between stations depending on the local geography. Typically the line of sight due to the Earth's curvature is only 50 km to the horizon. Repeater stations must be placed so the data signal can hop, skip and jump across the country.



Microwaves operate at high operating frequencies of 3 to 10 GHz. This allows them to carry large quantities of data due to the large bandwidth.

Advantages:

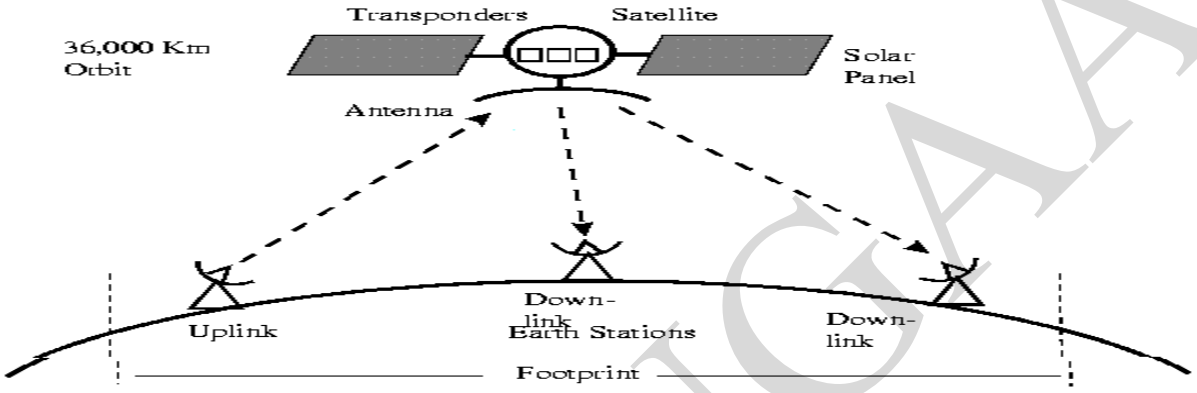
a. They can carry high quantities of information due to their high operating frequencies.
b. Each tower occupies small area.
c. High frequency/short wavelength signals require small antenna.

Disadvantages:

a. Attenuation by solid objects: birds, rain, snow and fog.
b. Reflected from flat surfaces like water and metal.
c. Refracted by atmosphere, thus causing beam to be projected away from receiver.

Satellite Transmission

Satellites are transponders that are set in a geostationary orbit. A transponder is a unit that receives on one frequency and retransmits on another.



The uplink is the transmitter of data to the satellite. The downlink is the receiver of data. Uplinks and downlinks are also called Earth stations due to be located on the Earth. The footprint is the "shadow" that the satellite can transmit to. The shadow being the area that can receive the satellite's transmitted signal.

Encoding and Modulation

Introduction

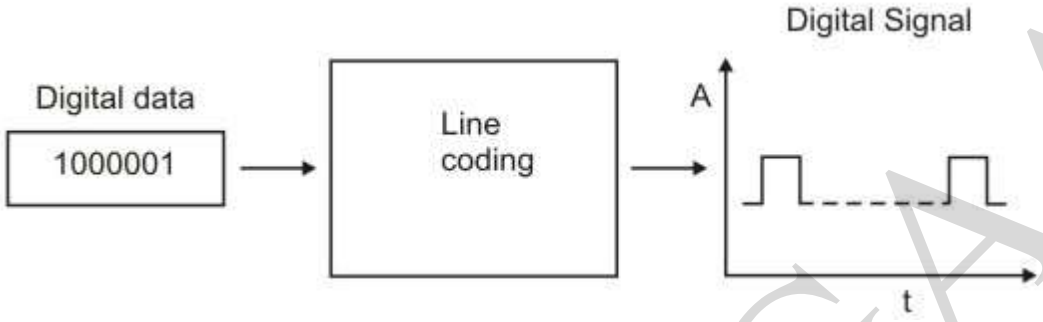
A computer network is used for communication of data from one station to another station in the network. Data traverses through a communication media in the form of a signal from the source to the destination. The channel between the transmitter and the receiver may be any transmission medium. But, irrespective of the medium, the signal traversing the channel becomes distorted with increasing distance. Hence a process is adopted to match the properties of the transmitted signal to the channel characteristics so as to efficiently communicate over the transmission media. There are two alternatives; the data can be either converted to digital or analog signal.

The basis of analog signaling is a constant frequency signal known as a **carrier signal**, which is chosen to be compatible with the transmission media being used, so that it can traverse a long distance. Data can be transmitted using these carrier signals by a process called modulation, where one or more fundamental parameters of the carrier wave, i.e. amplitude, frequency and

phase are being modulated by the source data. The resulting signal, called modulated signal traverses the media, which is demodulated at the receiving end and the original signal is extracted.

Encoding

The first approach converts **digital data to digital signal**, known as line coding, as shown in Fig.

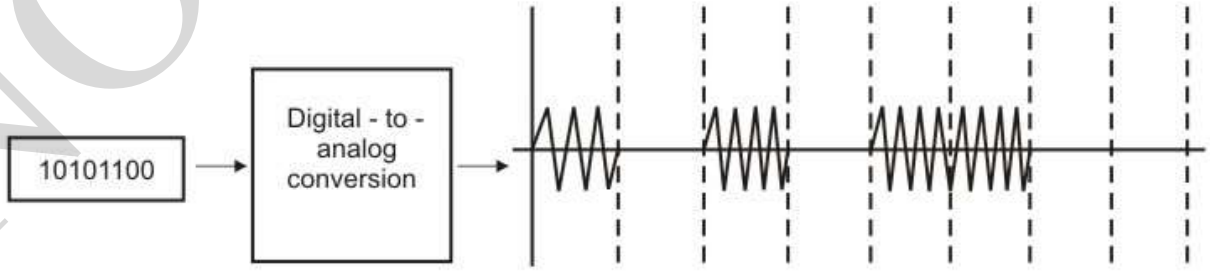


Bit rate versus Baud rate: The **bit rate** represents the number of bits sent per second, whereas the **baud rate** defines the number of signal elements per second in the signal.

Digital to Analog Encoding Techniques

Quite often we have to send digital data through analog transmission media such as a telephone network. In such situations it is essential to convert digital data to analog signal. This conversion is accomplished with the help of special devices such as modem (modulator-demodulator) that converts digital data to analog signal and vice versa.

Since modulation involves operations on one or more of the three characteristics of the carrier signal, namely amplitude, frequency and phase, three basic encoding or modulation techniques are available for conversion of digital data to analog signals. The three techniques, referred to as **amplitude shift keying (ASK), frequency shift keying (FSK) and phase shift keying (PSK).** There are many situations where ASK and PSK techniques are combined together leading to a modulation technique known as Quardrature Amplitude Modulation (QAM).

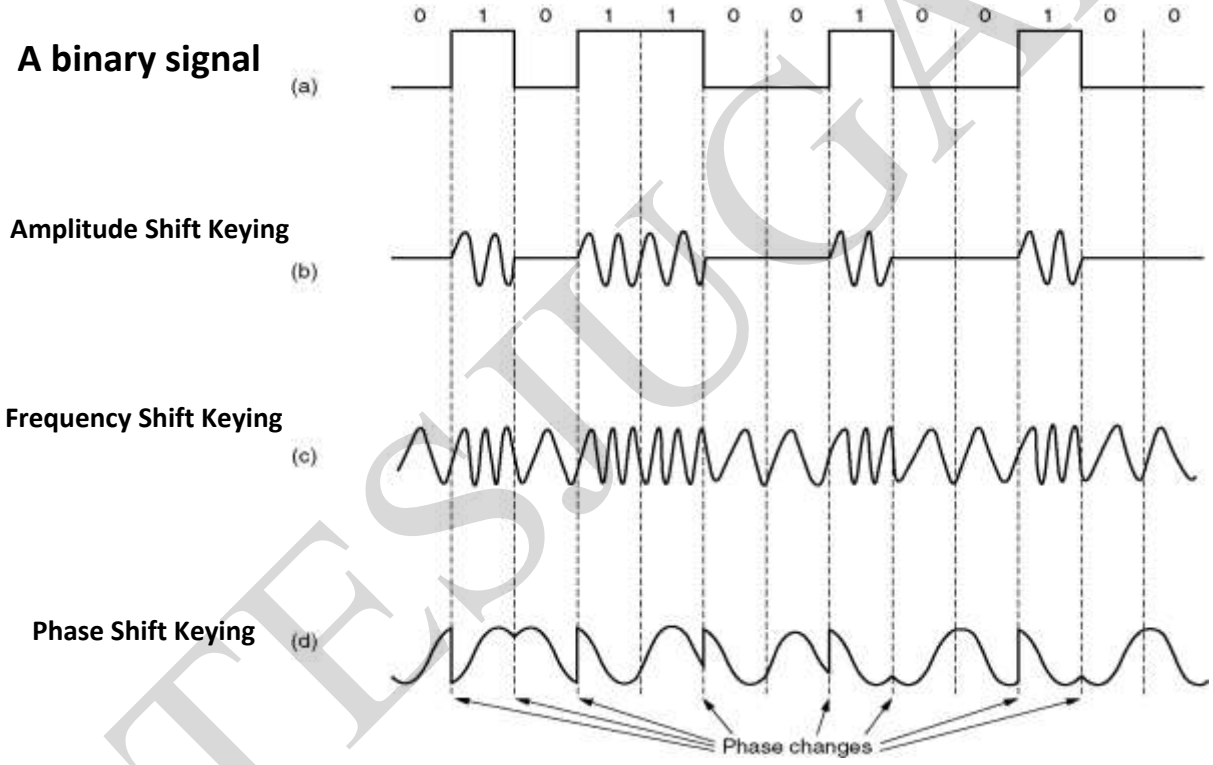


Amplitude-shift keying (ASK)

In ASK, two binary values are represented by two different amplitudes of the carrier signal. This method is very much prone to noise interference and hence considered as an inefficient modulation technique.

Frequency-shift keying (FSK)
In Frequency Shift Keying, the change in frequency define different digits. Two different frequencies near carrier frequency represent '0' ,"1'.

Phase-shift keying (ASK)
In this method, the phase of the carrier signal is shifted by phase measured relative to the previous bit interval. The binary 0 is represented by sending a signal of the same phase as the preceding one and 1 is represented by sending the signal with an opposite phase to the previous one.



Nyquist Theorem(NOT in SYLLABUS/But important for Network Basics): Sampling is done in accordance with the Nyquist Theorem that states that if sampling is performed at a rate two times the bandwidth of the signal, no signal information is lost.

Or, The sampling rate must be at least twice the highest frequency of the signal.

- The number of samples taken per second is called the sampling rate or sampling frequency.

Eg 1: ***Telephone companies digitize voice by assuming a maximum frequency of 4000 Hz. The sampling rate therefore is 8000 samples per second.***

Eg 2 : We want to digitize the human voice. What is the bit rate, assuming 8 bits per sample?

Solution

The human voice normally contains frequencies from 0 to 4000 Hz. So the sampling rate and bit rate are calculated as follows:

Sampling Rate = 4000 x 2 = 8000 samples /sec.

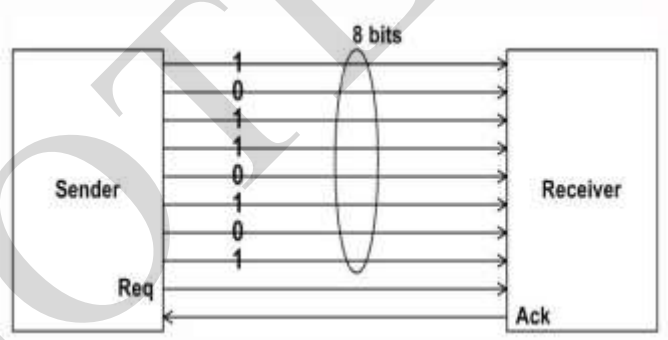
Bit Rate = 8000 x 8 = 64,000 bps = 64 kbps

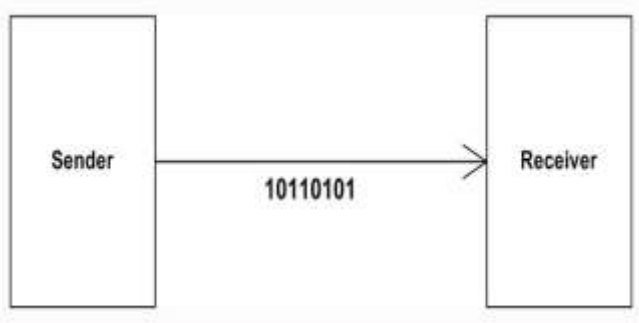
Digital Data Communication Techniques:

For two devices linked by a transmission medium to exchange data ,a high degree of co-operation is required. Typically data is transmitted one bit at a time. The timing (rate, duration, spacing) of these bits must be same for transmitter and receiver. There are two options for transmission of bits.

1. **Parallel:** All bits of a byte are transferred simultaneously on separate parallel wires. Synchronization between multiple bits is required which becomes difficult over large distance. Gives large band width but expensive. Generally bits sent in the group of 8.

2. **Serial:** Bits transferred serially one after other. Gives less bandwidth but cheaper.





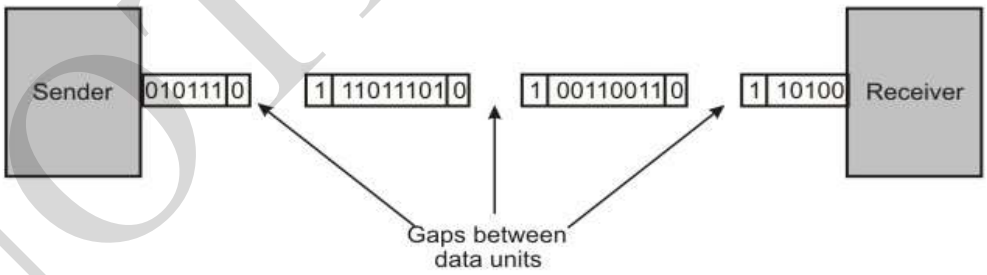
Transmission Techniques:

1. **Asynchronous:** Small blocks of bits(generally bytes) are sent at a time without any time relation between consecutive bytes .When no transmission occurs a default state is maintained corresponding to bit 1. Due to arbitrary delay between consecutive bytes, the time occurrences of the clock pulses at the receiving end need to be synchronized for each byte. This is achieved by providing 2 extra bits start and stop.

   Start bit: It is prefixed to each byte and equals 0. Thus it ensures a transition from 1 to 0 at onset of transmission of byte. Thus each start of a byte results in resynchronization of receiver clock.

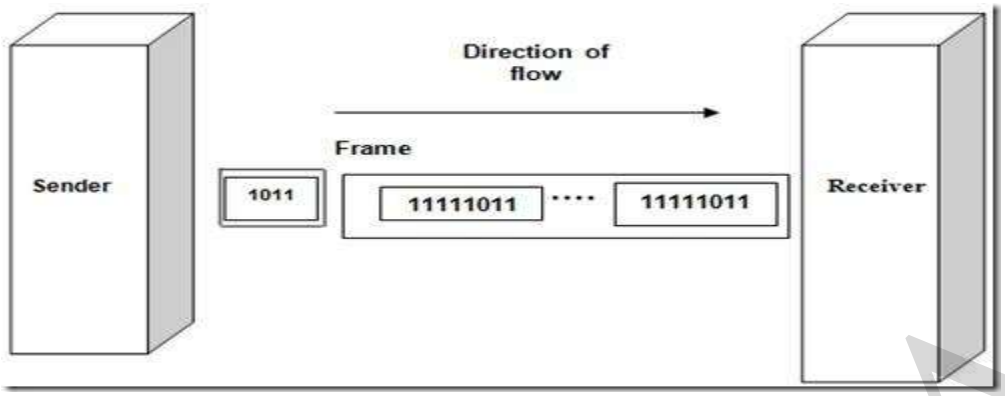
   Stop bit: To ensure that transition from 1 to 0 is always present at beginning of a byte it is necessary that default state be 1. But there may be two bytes one immediately following the other and if last bit of first byte is 0, transition from 1 to 0 will not occur . Therefore a stop bit is suffixed to each byte equaling 1.

Asynchronous transmission is simple and cheap but requires an overhead of 3 bits i.e. for 7 bit code 2 (start ,stop bits)+1 parity bit implying 30% overhead.



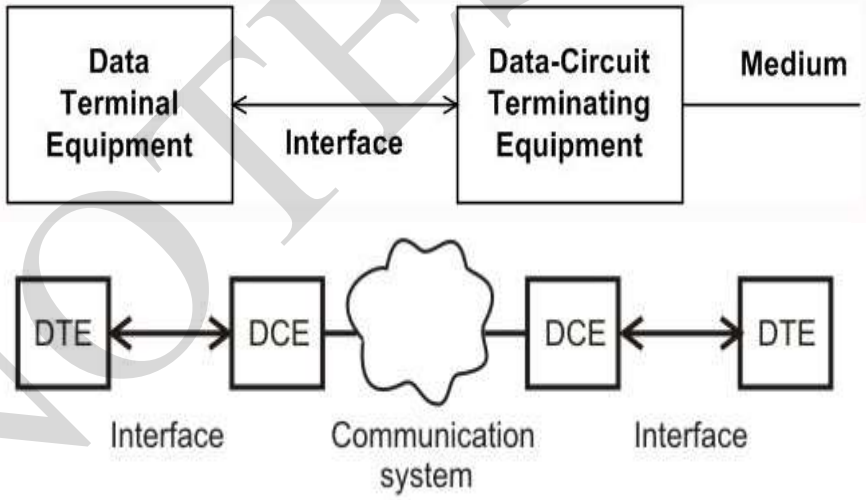
2. **Synchronous** - Larger blocks of bits are successfully transmitted. Blocks of data are either treated as sequence of bits or bytes. Still another level of synchronization is required so that receiver determines beginning or end of block of data. Hence each block begins with a start code and ends with a stop code. These are in general known as flag

that is unique sequence of fixed no. of bits .In addition some control characters encompass data within these flags. **Data+control information** is called a frame.



DTE-DCE Interface

To send signal through the transmission media, it is necessary to develop suitable mechanism for interfacing data terminal equipments (DTEs), which are the sources of data, to the data circuit terminating equipments (DCEs), which converts data to signal and interfaces with the transmission media. The way it takes place is shown in Fig. The link between the two devices is known as *interface*.



In case of two computers or a computer and an appliance, this understanding can be ensured with the help of a *standard*, which should be followed by both the parties. The EIA and ITU-T have

been involved in developing standards for the DTE-DCE interface known as EIA-232, EIA-442, etc and ITU-T standards are known as V series or X series. The standards should normally define the following four important specifications like mechanical, electrical, procedural and functional. A variety of standards exist, and the popular interface is given below:

The RS-232 C: The Electronic Industries Association (EIA) developed the standard RS-232C as an interface between the DTE and DCE. Although developed in 1960, it is still widely used for serial binary data interchange. A 25-pin connector (DB-25) or 9-pin connector (DB-9) is commonly used for establishing mechanical connection. It uses single-ended, bipolar voltage. The bipolar voltage levels are +3 to + 25V for bit 0 and –3 to –25V for bit 1. There are two data lines, one for each direction, facilitating full-duplex operation. There are several control and ground lines.

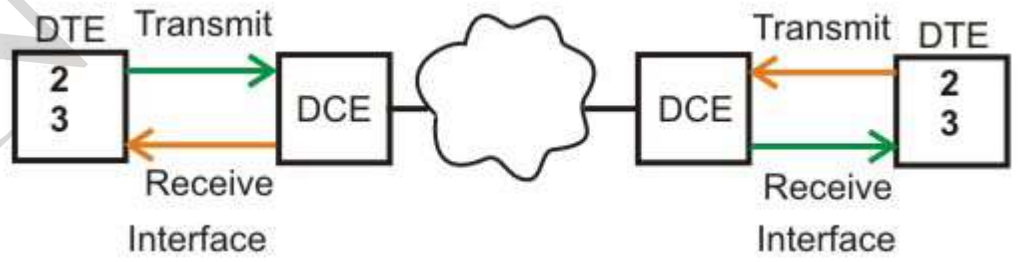
TABLE Important RS-232C Pins

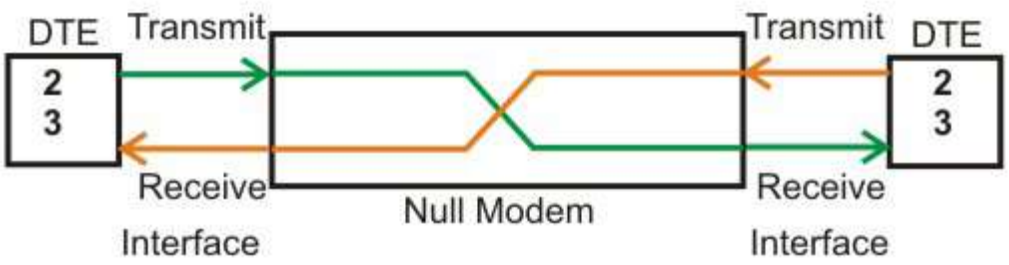
Pin No	Function
1	Protective ground
2	Transmit data to DCE
3	Receive data from DCE
4	Request to send to DCE
5	Clear to send from DCE
6	Data set ready from DCE
7	Signal ground
8	Data carrier detect from DCE
20	Data terminal ready to DCE

Null Modem

In many situations, the distance between two DTEs may be so close that use of modems (DCE), as shown in Fig. is unnecessary. In such a case the RS-232 C interface may still be used, but with out the DCEs. A scheme known as null modem is used, in which interconnection is done in such a way that both the DTEs are made to feel as if they have been connected through modems.

Essentially, null modem is a cable with two connectors at both ends for interfacing with the DTEs. The reason for this behavior is apparent from the swapping interconnection shown in Fig.





MODEMS

The DCE that is used to interface with the physical transmission media is known as MODEM, derived from MOdulator + DEModulator. The *modulator* converts digital data into an analog signal using ASK, FSK, PSK modulation techniques. A *demodulator* converts an analog signal back into a digital data. Important Parameters of the modems are the *transmission rate* and Bandwidth (Baud rate). The output of a modem has to match the bandwidth of the bandwidth of the medium, the telephone line.

TRANSMISSION IMPAIRMENTS

When a signal is transmitted over a communication channel, it is subjected to different types of impairments because of imperfect characteristics of the channel. As a consequence, the received and the transmitted signals are not the same. These impairments introduce modifications in analog signals leading to distortion. On the other hand, in case of digital signals, the impairments lead to error in the bit values. The impairment can be broadly categorised into the following three types:

- Attenuation
- Delay distortion
- Noise

Attenuation

Irrespective of whether a medium is guided or unguided, the strength of a signal falls off with distance. This is known as *attenuation.* If the strength of the signal is very low, the signal cannot be detected and interpreted properly at the receiving end. The signal strength should be sufficiently high so that the signal can be correctly detected by a receiver in presence of noise in the channel. An amplifier can be used to compensate the attenuation of the transmission line. So, attenuation decides how far a signal can be sent without amplification through a particular medium.

Delay distortion

The velocity of propagation of different frequency components of a signal are different in guided media. This leads to delay distortion in the signal. For any signal, the velocity of propagation has been found to be maximum near the center frequency and lower on both sides of the edges of the frequency band. In case of analog signals, the received signal is distorted because of variable delay of different components. In case of digital signals, the problem is much more severe. Some frequency components of one bit position spill over to other bit positions, because of delay distortion.

Noise

As signal is transmitted through a channel, undesired signal in the form of noise gets mixed up with the signal, along with the distortion introduced by the transmission media. Noise can be categorised into the following four types:

Thermal Noise
Induced Noise
Cross talk and Impulse Noise

The ***thermal noise*** is due to thermal agitation of electrons in a conductor. It is distributed across the entire spectrum and that is why it is also known as *white noise* (as the frequency encompass over a broad range of frequencies).

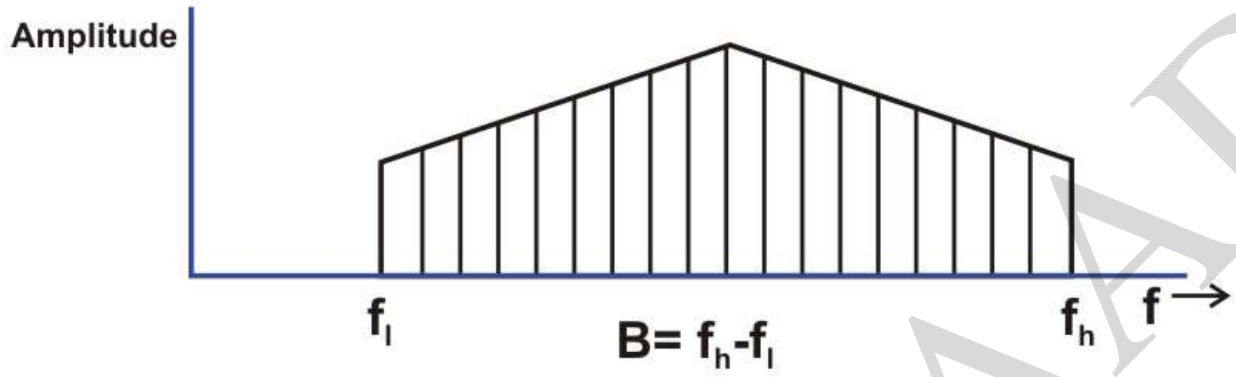
Cross talk is a result of bunching several conductors together in a single cable. Signal carrying wires generate electromagnetic radiation, which is induced on other conductors because of close proximity of the conductors. While using telephone, it is a common experience to hear conversation of other people in the background. This is known as *cross talk.*

Impulse noise is irregular pulses or noise spikes of short duration generated by phenomena like lightning, spark due to loose contact in electric circuits, etc. Impulse noise is a primary source of bit-errors in digital data communication. This kind of noise introduces burst errors.

Induced noise *is* the noise that comes from sources such as other devices.

Bandwidth and Channel Capacity

Bandwidth refers to the range of frequencies that a medium can pass. The below figure shows the bandwidth of a channel.



Shannon Capacity (Noisy Channel)

Shannon-Hartley theorem gives the maximum data rate capacity

C = B log2 (1 + S/N), where B = bandwidth of the channel and S/N is the signal to noise ratio.

Note: Do numerical from book.

PERFORMANCE OF SIGNALS: Measured by Throughput, Latency

Throughput : It is the number of bits passed through a point in the medium in a second.

Latency **(Delay)**: is the amount of time a message takes to traverse a system.

In a computer network, it is an expression of how much time it takes for a packet of data to get from one designated point to another.

Latency depends on the speed of the transmission medium (e.g., copper wire, optical fiber or radio waves) and the delays in the transmission by devices along the way (e.g., routers and modems). A low latency indicates a high network efficiency.

Latency and *throughput* are the two most fundamental measures of network performance. They are closely related, but whereas latency measures the amount of time between the start of an action and its completion, throughput is the total number of such actions that occur in a given amount of time.

Propagation speed - speed at which a bit travels though the medium from source to destination.

Wavelength

Definition: Wavelength can be defined as the distance between two successive crests or troughs of a wave. It is measured in the direction of the wave.

Description: Wavelength is the distance from one crest to another, or from one trough to another, of a wave (which may be an electromagnetic wave, a sound wave, or any other wave). Crest is the highest point of the wave whereas the trough is the lowest. Since wavelength is distance/length, it is measured in units of lengths such as metres, centimetres, milimetres, nanometres, etc.

The following equation is known as the wavelength formula or the wavelength equation:

? = V/f (where ' V' is the speed of the wave and 'f' is the frequency of the wave)

Thus, Wavelength of the wave = Speed of the wave/ Frequency

Example: If the speed of a wave is 600m per second and the frequency of the waves is 30 waves per sec, then the wavelength will be equal to:

? = 600/30

? = 20 m