COMPUTER NETWORKS

UNIT-1

INTRODUCTION

When we communicate, we are sharing information. This sharing can be local or remote. Between individuals, Local communication usually occurs face to face, while remote communication takes over distances.

The term telecommunication, which includes telephony, telegraphy and television, means communication at a distance (tele is Greek for "far").

The word data refers to information presented in whatever form is agreed upon by the parties creating and using the data.

Data communication are the exchange of data between 2 devices via some form of transmission medium such as a wire cable. For data communication to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs). The effectiveness of a data communications system depends on four fundamental characteristics:

1) delivery 2) Accuracy 3) timeliness and jitter.

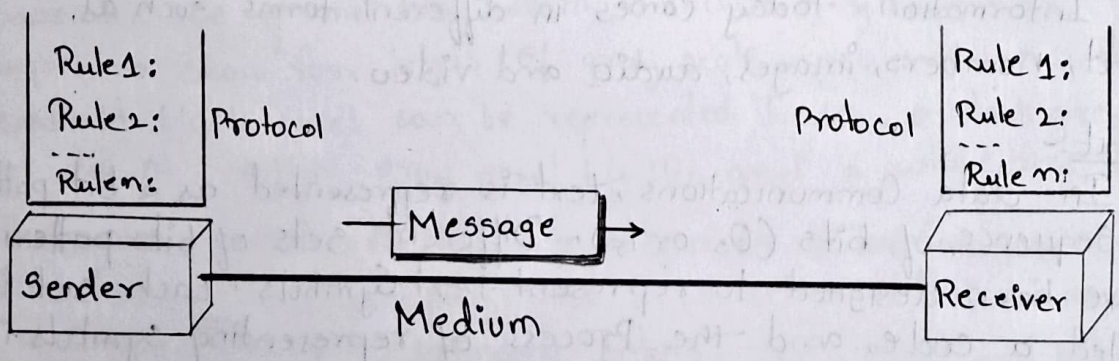


Fig 1.1

The data communication system has 5 components (see Fig 1.1)

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, 2 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.

Data Representation:

Information today comes in different forms such as text, numbers, images, audio and video

Text:-

In data communications, text is represented as a bit pattern, a sequence of bits (0s or 1s). Different sets of bits patterns have been designed to represent text symbols. Each set is called a code, and the process of representing symbols is called coding. Today, the prevalent coding system is called Unicode, which uses 32 bit to represent a symbol or character used in any language in the world. The American standard code for information Interchange (ASCII), developed some decades ago in the United States, now constitutes the first 127 character in Unicode and is also referred to as Basic Latin.

Numbers:-

Numbers are also represented by bit patterns. However, a code such as ASCII is not used to represent numbers; the numbers is directly converted to a binary number to simplify mathematical operations. Appendix B discusses several different numbering systems.

Images:

Images are also represented by bit patterns. In its simplest form, an image is composed of a matrix of pixels (picture elements), where each pixel is a small dot. The size of the pixel depends on the resolution. for example, an image can be divided into 1000 pixels or 10,000 pixels. In the second case, there is a better representation of image (better resolution), but more memory is needed is needed to store the image.

After an image is divided into pixels, each pixel is assigned a bit pattern. The size and the value of the pattern depend on the image. For an image made of only black and white dots (eg. chess board) a 1-bit pattern is enough to represent a pixel. If an image is not made of pure white and pure black pixels, you can increase the size of the bit pattern to include gray scale. For example, to show four levels of gray scale, you can use 2-bit patterns. A black pixel can be represented by 00, a dark grey pixel by 01, a light gray pixel by 10, and a white pixel by 11.

There are several methods to represent color images. One method is called RGB, so called because each color is made of a combination of 3 primary colors: red, green and blue. The intensity of each color is measured, and a bit pattern is assigned to it. Another method is called YCM, in which color is made of a combination of three other primary colors: yellow, cyan and magenta.

Audio:

Audio refers to the recording or broadcasting of sound or music. Audio is by nature different from text, numbers or images. It is continous, not discrete. Even when we use a microphone to

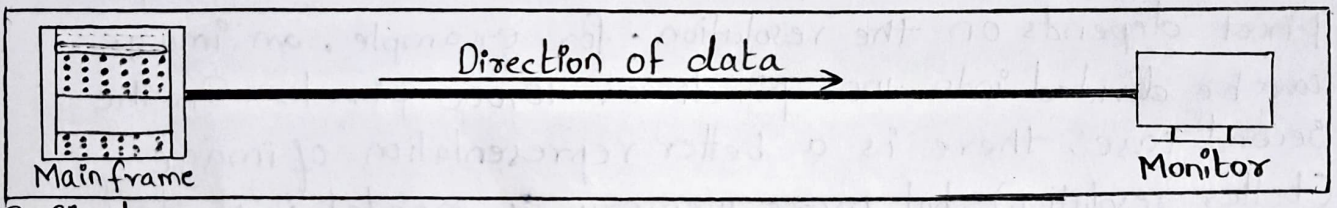
change voice or music to an electric signal, we create a continous signal.

Video

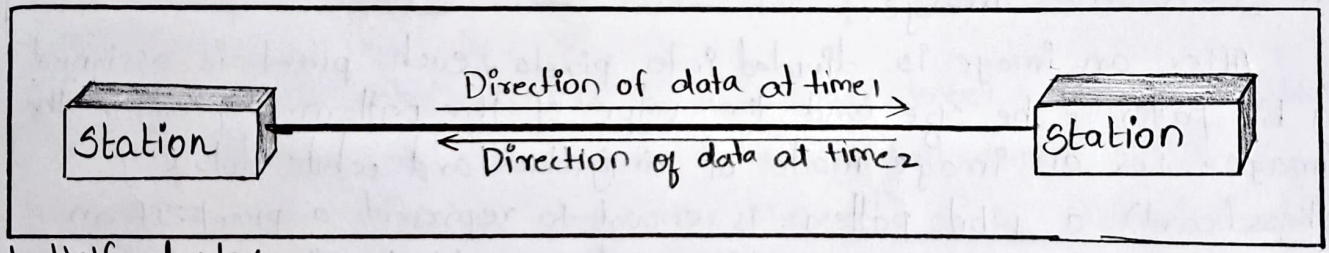
Video refers to the recording or broadcasting of a picture or movie. Video can either be produced as a continous entity (e.g by a TV camera) or it can be combination of images, each a discrete entity, arranged to convey the idea of motion.

Data Flow:

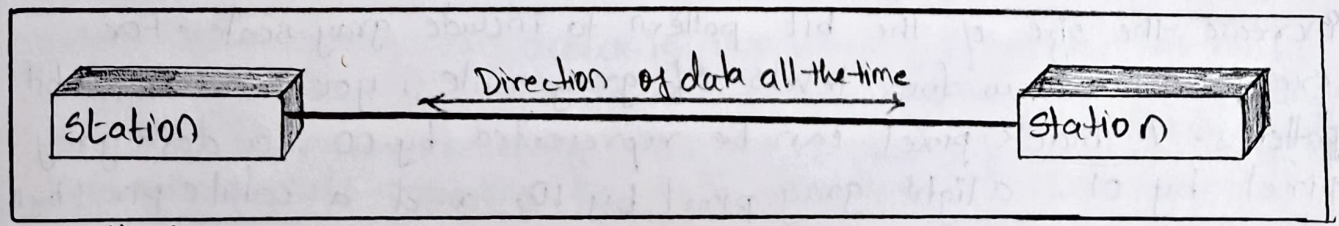
fig 1.2 Data flow (simplex, half-duplex & Full duplex)



a. Simplex



b. Half-duplex



c. Full-duplex

Simplex

In Simplex mode, the Communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive. Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction.

Half-Duplex

In half-duplex, each situation can both transmit and receive, but not at the same time. when one device is sending, the other can only receive and vice versa.

The half-duplex mode is like a one-lane road with traffic allowed in both directions. When cars are traveling in one direction, cars going the other way must wait.

In half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is tramsmitting at the time. Walkie-talkies and CB(citizen band) radio are both half-duplex systems. The half-duplex mode is used in cases where there is no need for communication in both directions at the same time; the entire capacity of channel can be utilized for each direction.

Full-Duplex

In full-duplex mode, both stations can transmit and receive simultaneously.

The full-duplex mode is like a two way street with traffic flowing in both direction at the same time. In full-duplex mode, signal going in one direction share the capacity of the channel is divided between signals traveling in both directions.

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.

One Common example of full-duplex communication is the telephone network. When two people are communicating by telephone line, both can talk and listen at the same time.

Network:

- A network is a set of devices (often referred to as nodes) connected by communication 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.

- Most networks use distributed processing in which a task is divided among multiple computers. Instead of one single large machine being responsible for all aspects of a process, separate computers (usually a personal computer or workstation) handle a subset
- A network must be able to meet a certain number of criteria. The most important of these are performance, reliability and security.

Performance

Performance can be measured in many ways, including transit time and response time. Transit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an inquiry and a response. The performance of a network depends on a number of factors, including the no. of users, the type of transmission medium, the capabilities of the connected hardware and the efficiency of software.

Reliability

In addition to accuracy of delivery, network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe

Security

Network security issues include protecting data from unauthorized access, protecting data from damage and development and implementing policies and procedures for recovery from breaches and data losses

Computer Network

A Computer Network is interconnection of several computers by communication links referred to as computer networks.

Advantages

Resource sharing
Ease of Accessibility
Less cost
Flexibility
Security

Types of Connection

A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. For visualization purposes, it is simplest to imagine any link as a line drawn between two points. For communication to occcur, two devices must be connected in some way to the same link at the same time.

There are two possible types of connection:

1. point-to-point Connection
2. Multipoint Connection

1) Point-to-Point

A point-to-point connection provides a dedicated link between link between two devices. The entire capacity of the link is reserved for transmission between those two devices.

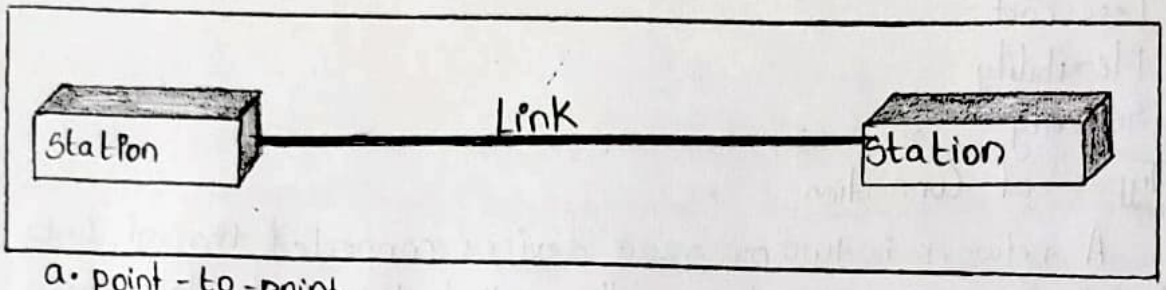
Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible.

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.

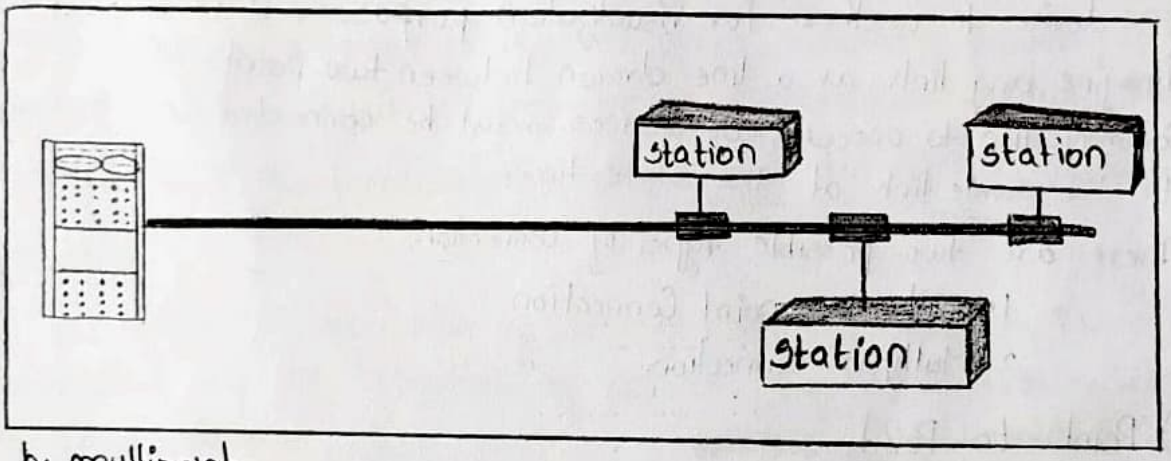
Multipoint

A multipoint (also called multi drop) connection is one in which 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.



a. point-to-point

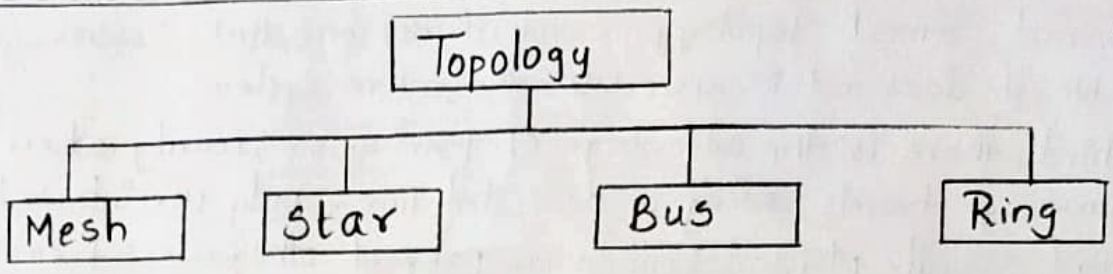


b. multipoint

Physical Topology:

The term physical topology refers to the way in which a network is laid out physically. Two or more devices connect to a link; and two or more links form a topology.

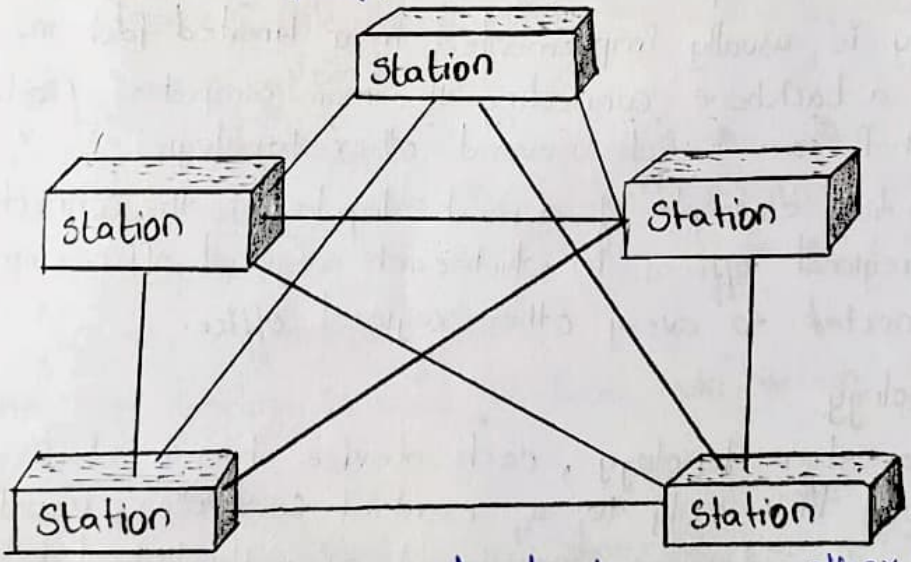
The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another. There are four basic topologies possible: mesh, star, bus and ring.



1. Mesh topology.

In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects. To find the number of physical links in a fully connected mesh network with n nodes, we first consider that each node must be connected to every other node.

Node 1 must be connected to n-1 nodes, node 2 must be connected to n-1 nodes, and finally node n must be connected to n-1 nodes. We need $n(n-1)$ physical links. However, if each (node must be connected to every other node)* physical links allows communication in both directions (duplex mode), we can divide the number of links by 2. In other words, we can say that in a mesh topology $n(n-1)/2$ links



A mesh offers several advantages over other network topologies. First, 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.

Second, a mesh topology is robust. If one links become unusable, it does not incapacitate the entire system.

Third, there is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it. physical boundaries prevent other users from gainining access to messages

Finally, point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location of the fault and aids in finding its cause and solution.

The main advantage of a mesh are related to the amount of cabling and the no. of I/o ports required. First, because every device must be connected to every other device, installation and reconnection are difficult. Second, the sheer bulk of the wiring can be greater than the available space (in walls. ceilings or floors) can accomodate.

Finally, the hardware required to connect each link (I/o ports and cable) can be prohibitively expensive. For these reason a mesh topology is usually implemented in a limited fashion, for example, as a backbone connecting the main computers of a hybrid network that can include several other topologies

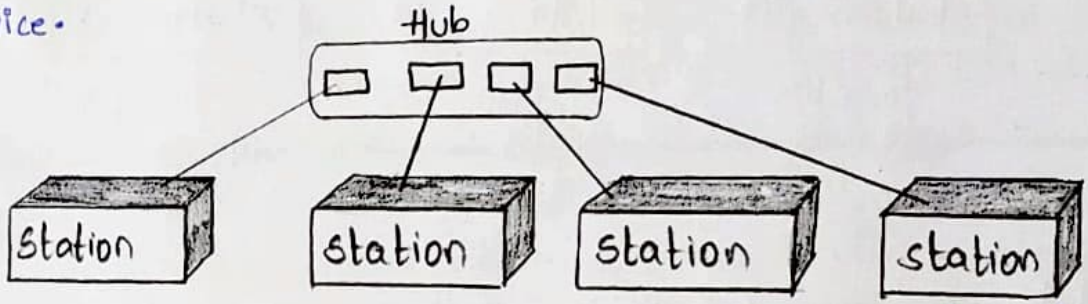
One practical example of a mesh topology is the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

2. Star Topology

In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, 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, which then relays the data to the other connected device.



The 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 reconfiguration. Far less cabling needs to be housed, and additions, moves and deletions involve only one connection : between that device and the hub.

Other advantages include robustness. If one link is affected, All other links remain active. This factor also lends itself to easy fault identification and fault isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.

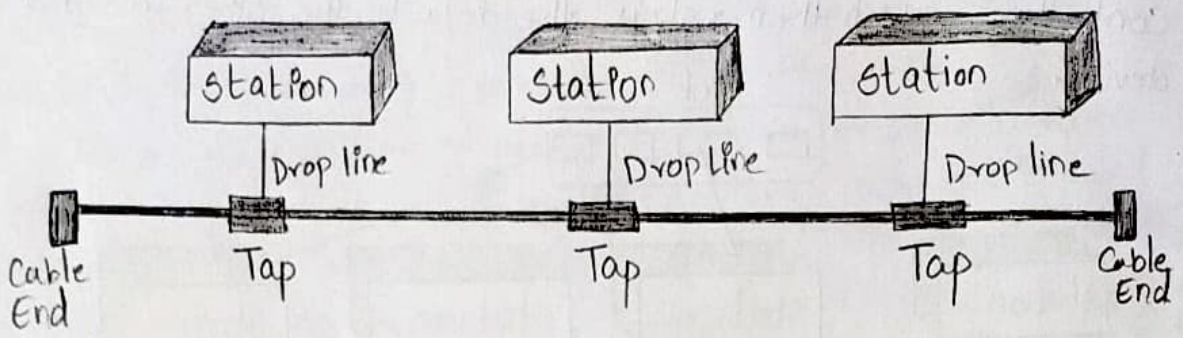
One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.

Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies (such as ring or bus).

The star topology is used in Local-area-network (LANs)

3. Bus Topology

The preceding examples all describe point-to-point connections A bus topology, on the other hand is multipoint. One long cable acts as a backbone to link all the devices in a network.



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 either splices into the signal travels along the backbone, some of its Energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the no. of taps a bus can support and on the distance between those taps.

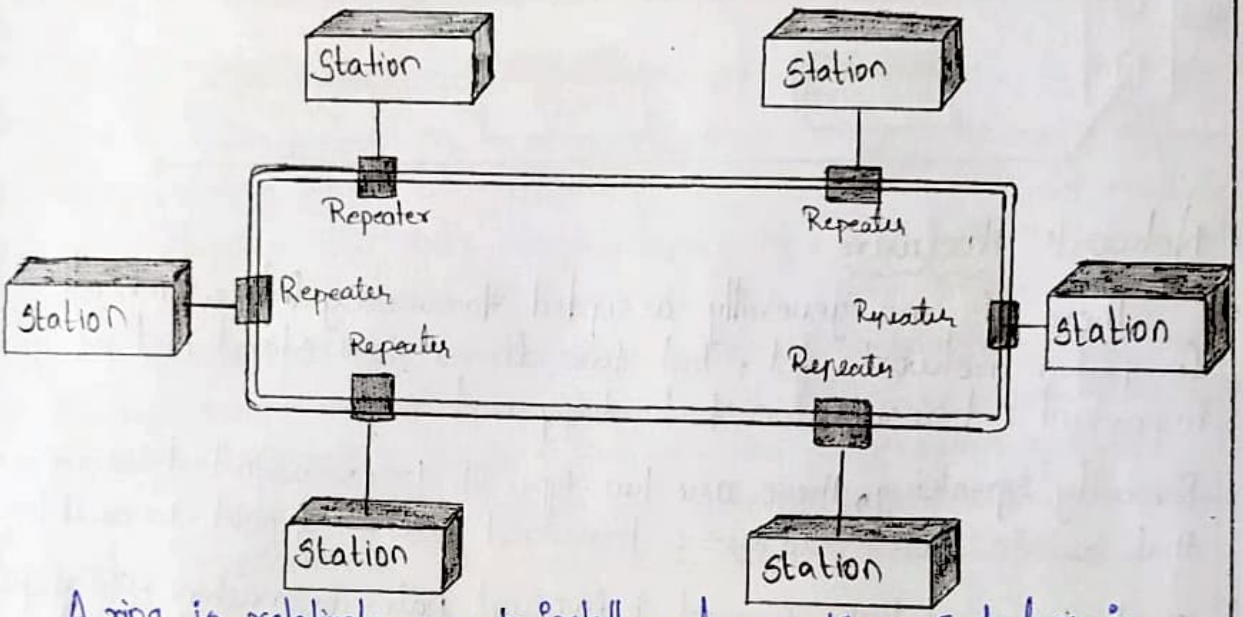
Advantages of a bus topology include ease of installation. Backbone cabel can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabling than mesh or star topologies. In a star, for Example, four network devices in the same room require four lengths of Cable reaching all the way to the hub. In a bus, this redundancy is eliminated. Only the backbone cable stretches through the entire facility. Each drop line has to reach only as far as the nearest point on backbone.

Disadvantages include difficult reconnection and fault isolation. A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices. Signal reflection at the taps can cause degradation in quality. This degradation can be controlled by limiting the number and spacing of devices connected to a given length of Cable. Adding new devices may therefore require modification or replacement of the backbone

Bus topology was the one of the first topologies used in the design of early Local area networks. Ethernet LANs can Use a bus topology, but they are less popular.

4. Ring Topology

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



A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors (either physically or logically). To add or delete a device require changing only two connections. The only constraints are media and traffic considerations (maximum ring length and no. of devices). In addition, fault isolation is simplified.

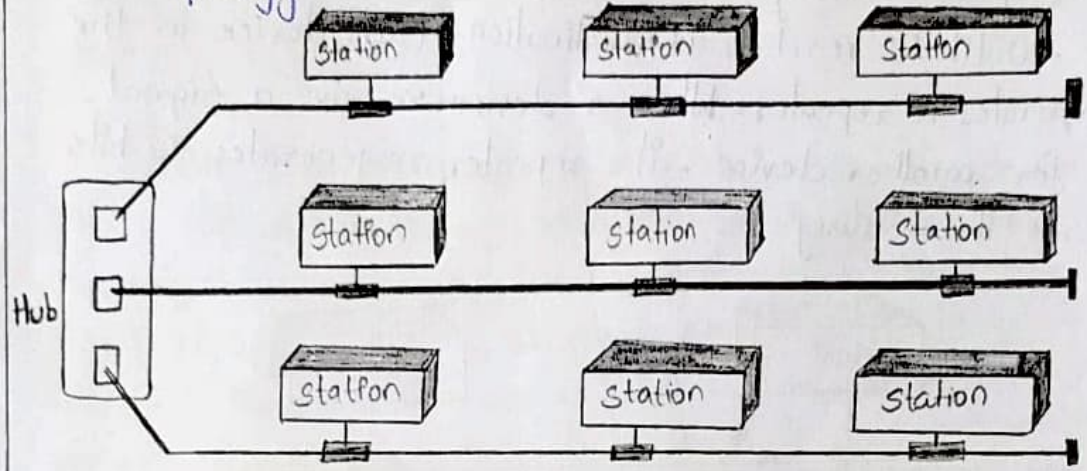
Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

However, unidirectional traffic can be a disadvantages. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.

Ring topology was prevalent when IBM introduced its local-area network Token Ring. Today, the need for higher speed LANs had made this topology less popular.

5. Hybrid Topology

A network can be hybrid. For Example, we can have a main star topology with each branch connecting several stations in a bus topology.



Network Hardware

There is no generally accepted taxonomy into which all Computer networks fit, but two dimensions stand out as important: transmission technology and scale.

Broadly speaking, there are two types of transmission technology that are in widespread use: broadcast links and point-to-point links.

Point-to-point links connect individual pairs of machine. To go from the Source to the destination on a network made up of point-to-point links, short messages, called Packets in certain contexts, may have to first visit one or more intermediate machines. Often multiple routes, of different lengths, are possible, so finding good ones is important in point-to-point network. Point-to-point transmission with exactly one sender and exactly one receiver is sometimes called unicasting.

In Constrast, on a broadcast network, the Communication channel is shared by all the machines on the network; Packets sent by any machine are received by all the others. An address field within each packet specifies the intended recipient. Upon receiving a packet specifies, a machine checks the address field. If the packet is intended for the receiving (a packet) machine, that machine processes the packet; if the packet is intended for some other machine, that machine prouses the packet; if the packet is

intended recipient. Upon zone other machine it is just ignored. A wireless network is a common example of a broadcast link, with Communication shared over a coverage region that depends on the wireless channel and the transmitting machine. Broadcast System usally also allow the possibility of addressing a packet to all destinations by using a special code in the address field. When a packet with this code is transmitted, it is recived and processed by every machine on the network. This mode of operation is called broadcasting. Some broadcast Systems also support transmission to a subset of machine which known as multicasting.

An alternative criterion for classifying networks is by scale. Distance is important as a classification metric because different technologies are used at different scales. We classify multiple processor System by their rough physical size. At the top are the personal area network, networks that are meant for one person. Beyond these come longer-range networks. These can be divided into local, metropolitian and wide area networks, each with increasing scale. Finally, the connection of two or more network is called an internetwork. The worldwide Internet is certainly the best known (but not the only) example of an internetwork.

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

Categories of Networks

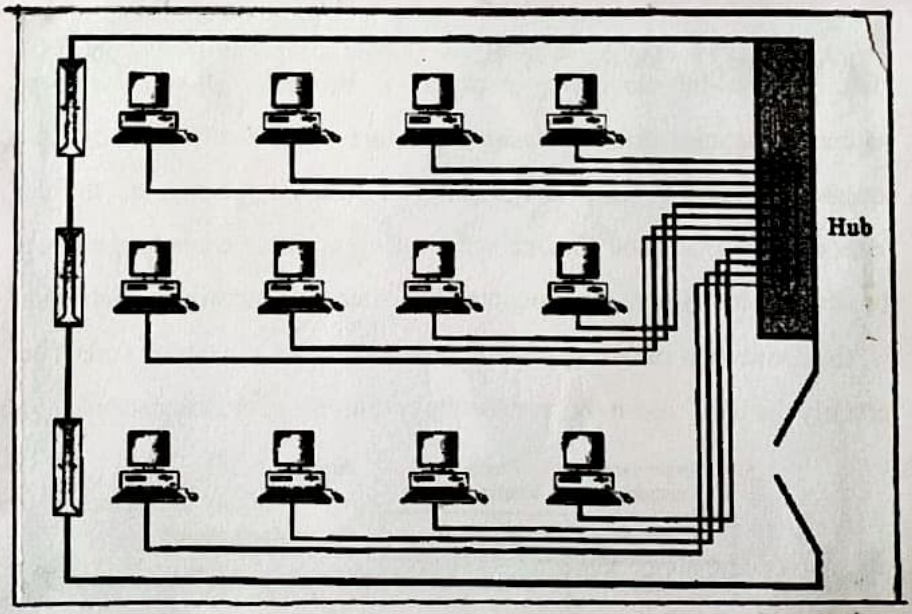
Today when we speak of networks, we are generally referring : Local-area network, Metropolitan area network and wide-area network

A LAN normally covers an area less than 1km. A WAN can be worldwide. Networks of a size in between are normally referred to as metropolitian area networks and span tens of miles.

i) Local-Area Network (LAN)

A Local area network (LAN) is usually privately owned and Links the devices in a single office, building or campus. Depending on the needs of an organization and the type of it can extend throughout a Company and include audio and video peripherals. Currently, LAN size is Limited to a few kilometers.

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 Common example of a LAN, found in many business environment, links a workgroup of task-related computers may be given a larger capacity disk drive and may become a server to clients. Software can be stored on this central server and used as needed by the whole group. In this example, the size of LAN may be determined by licensing restriction on the number of users per copy of software, or by restrictions on the number of users licensed to access the operating system.

In addition to size, LANs are distinguished from other types of networks by their transmission media and topology. In general, a given LAN will use only one type of transmission medium. The most Common LAN topologies are bus, ring and star.

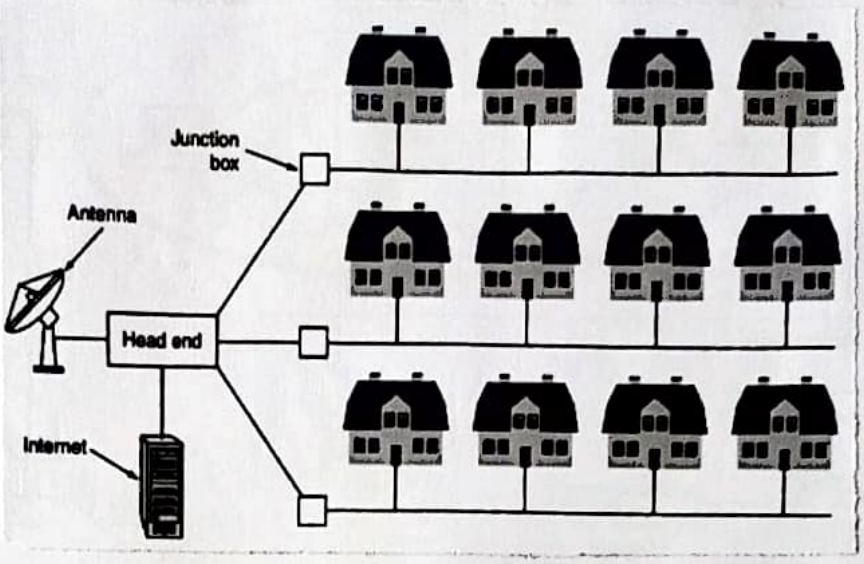
Early LANs had data rates in the 4 to 16 megabits per second (Mbps) range. Today, however, speeds are normally 100 or 1000 Mbps.

Wireless LANs are the most evolution in LAN technology.

ii) Metropolitian Area Network (MAN)

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, normally to the Internet, and have endpoints spread over a city or part of city. A good example of a MAN is the part of telephone company network that can provide a high-speed DSL Line to the customer.

Another example is the cable TV network that originally was designed for cable TV, but today can also be high-speed data connection to the Internet. We, discuss DSL lines and cable TV networks.



iii)

Wide Area Network (WAN)

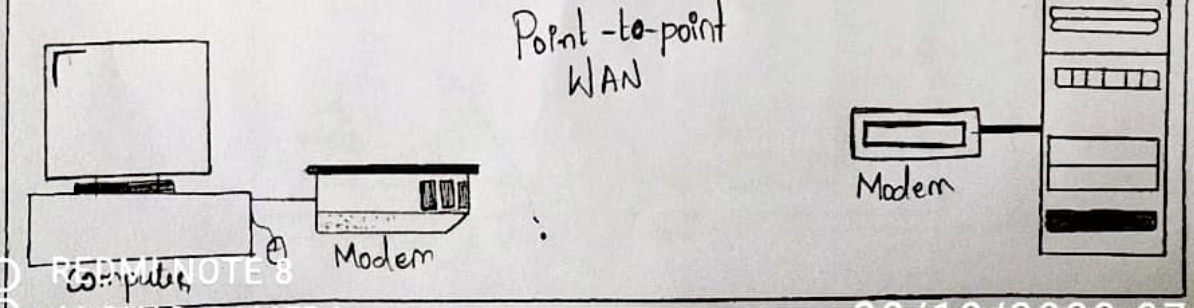
A wide area network (WAN) provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent or even the whole world. A WAN can be as complex as the backbones that connect the Internet or as simple as a dial-up line that connects a home computer to the Internet. We normally refer to the first as a switched WAN and to the second as a point-to-point WAN.

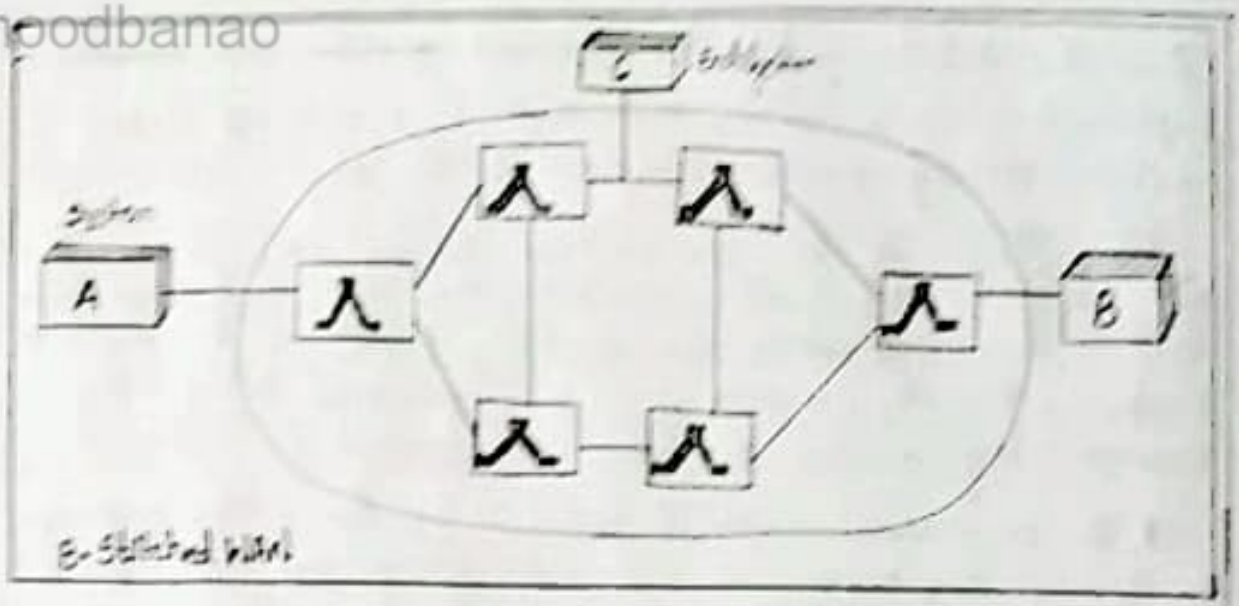
The switched WAN connects the end systems, which usually comprise a router (internetworking connecting device) that connects to another LAN or WAN.

The point-to-point WAN is normally a line leased from a telephone or cable TV provider that connects a home computer or a small LAN to an Internet service provider (ISP).

This type of WAN is often used to provide Internet access.

a. point-to-point WAN





Interconnection of Networks: Internetwork

Today, it is very rare to see a LAN, a MAN, or a LAN in isolation; they are connected to one another. When two or more networks are connected, they become an internetwork, or internet.

As an example, assume that an organization has two offices, one on the east coast and the other on the west coast. The established office on the west coast has a bus topology LAN; the newly opened office on the east coast has a star topology LAN.

To build a backbone WAN for connecting these three entities (two LANs and the president's computer), a switched WAN (operated by a service provider such as a telecom company) has been leased. To connect the LANs to this switched WAN, however, three point-to-point WANs are required. These point-to-point WANs can be high-speed DSL lines offered by a telephone company or a cable modem line offered by a cable TV provider.

Network Software:

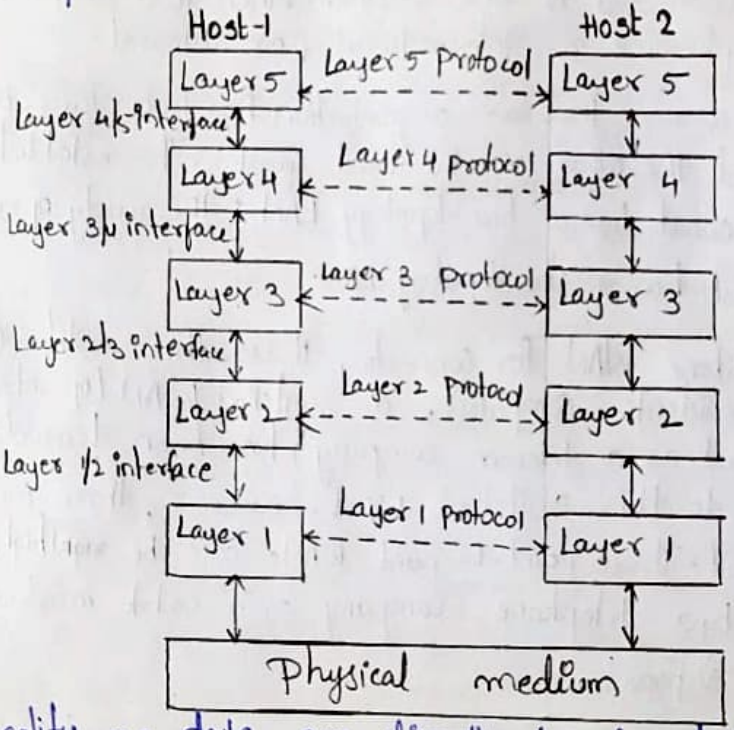
Protocol Hierarchies:

To reduce their design complexity, most networks are organized as a stack of layers or levels, each one built upon the one below it. The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network. The purpose of each layer is to offer certain services to the higher layers while shielding those layers

from the details of how the offered services are actually implemented. In a sense, each layer is a kind of virtual machine, offering certain services to the Layer above it.

When layer n on one machine carries on a conversation with layer n on another machine, the rules and conventions used in this conversation are collectively known as the layer n Protocol. Basically, a protocol is an agreement between the communicating parties on how communication is to proceed.

A five-layer network is illustrated in fig. The entities comprising the corresponding layers on different machine are called peers. The peers may be software processes, hardware devices, or even human beings. In other words, it is the peers that communicate by using the protocol to talk to each other.

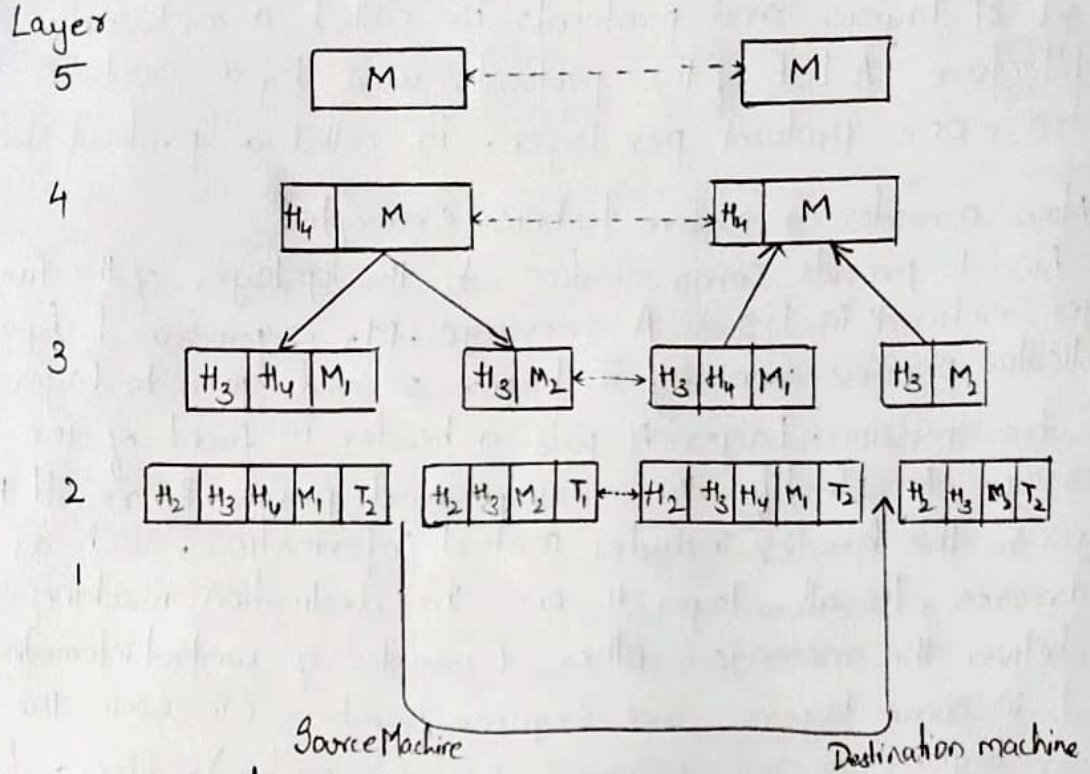


In reality, no data are directly transferred from Layer n on one machine to layer n on another machine. Instead, each Layer passes data and control information to the Layer immediately below it, until the lowest layer is reached. Below layer 1 is the physical medium through which actual communication occurs. Between each pair of adjacent Layers is an interface. The interface defines which primitive operations and services the lower layer makes available to the upper one.

A set of layers and protocols is called a network architecture. A list of the protocols used by a certain system, one protocol per layer, is called a protocol stack

Now consider a more technical example:

how to provide communication to the top layer of the five-layer network in fig. A message, M, is produced by an application process running in layer 5 and given to Layer 4 for transmission. Layer 4 puts a header in front of the message to identify the message and passes the result to Layer 3. The header includes control information, such as addresses, to allow layer 4 on the destination machine to deliver the message. other Examples of Control information used in some layers are sequence numbers (in case the lower layer does not preserve message order), sizes and times. In many networks, no limit is placed on the size of messages transmitted in the Layer 4 protocol but there is nearly always a Limit imposed by the Layer 3 protocol. Consequently, Layer 3 must break up the incoming messages into smaller units, packets, prepending a layer 3 header to each packet. In this example, M is split into two parts, M1 and M2, that will be transmitted Separately. Layer 3 decides which of the outgoing lines to use and passes the packets to Layer 2. Layer 2 adds to each piece not only a header but also a trailer and gives the resulting unit to Layer 1 for physical transmission. At the receiving machine the message moves upward, from layer to layer, with headers being stripped off as it progresses. None of the headers for layers below n are passed up to layer n



Design Issues for the Layers

Error Control
Flow Control
Multiplexing / Demultiplexing
Routing

Connection-oriented and Connectionless Services:

Connection-oriented service is modeled after the telephone system. To talk to someone, you pick up the phone, dial the number, talk, and then hang up. Similarly, to use a connection-oriented network service, the service user first establishes a connection, uses the connection, and then releases the connection.

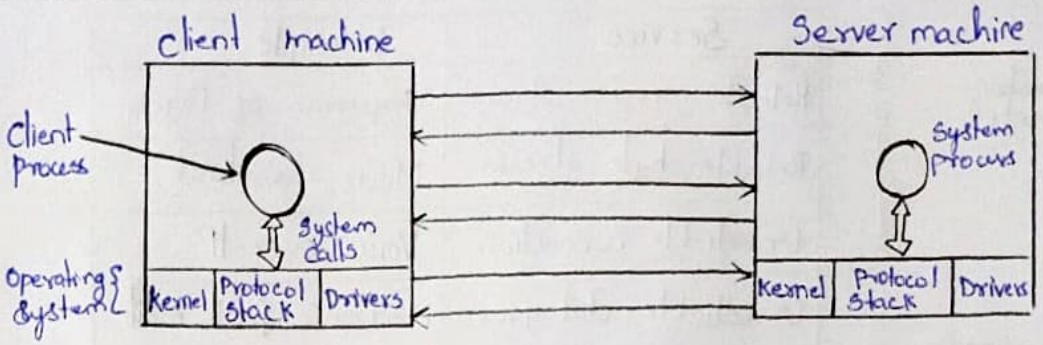
In contrast to connection-oriented service, connectionless service is modeled after the postal system. Each message (letter) carries the full destination address, and each one is routed through the intermediate nodes inside the system independent of all subsequent messages.

	Service	Example
Connection-oriented	Reliable message stream	Sequence of Pages
	Reliable byte stream	Movie download
	Unreliable connection	Voice over IP
Connectionless	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Text messaging
	Request-reply	Database query

Service Primitives:

A service is formally specified by a set of primitives (operations) available to user processes to access the service. These primitives tell the service to perform some action or report on an action taken by a peer entity. If the protocol stack is located in the operating system, as it often is, the primitives are normally system calls. These calls cause a trap to kernel mode, which then turns control of the machine over to the operating system to send the necessary packets. The set of primitives available depends on the nature of service being provided. The primitives for connection-oriented service are different from those of connectionless services. As a minimal example of the service primitives that might provide a reliable byte stream, consider the primitives listed.

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



Reference Models:

THE OSI MODEL:

The ISO Model has established in 1947, the international Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standards that Covers all aspects of network communication is the Open Systems Interconnection model. It was first introduced in the late 1970s. 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 framwork for the design of network system that allows communication between all types of Computer systems. It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network.

The Layers are:
1. Physical Layer
2. Data Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer

6. Presentation Layer
7. Application Layer

Layered Architecture:

The OSI model is composed of seven ordered layer: physical (Layer 1), data link (layer 2), network (Layer 3), transport (Layer 4), session (layer 5), presentation (Layer 6) and application (Layer 7). Figure 2.3 shows the Layers involved when a message is sent from device A to device B. As the message travels from A to B, it may pass through many intermediate nodes. These intermediate nodes usually involve only the first three layers of the OSI model.

In developing the model, the designers distilled the process of transmitting data to its most fundamental elements. They identified which networking functions had related uses and collected those functions into discrete groups that became the Layers. Each Layer defines a family of functions distinct from those of the other Layer. By defining and localizing functionality in this fashion, the designer created an architecture that is both comprehensive and flexible. Most importantly, the OSI model allows complete interoperability between otherwise incompatible systems.

Within a single machine, each Layer calls upon the services of the layer just below it. Layer 3, for example, uses the services provided by layer 2 and provides services for Layer 4. Between machines, Layer x on one machine communicates with Layer x on another machine. This communication is governed by an agreed-upon series of rules and conventions called protocols. The process on each machine that communicate at a given Layer are called peer-to-peer process. Communication between machines is therefore a peer-to-peer process using the protocols appropriate to given Layer

Peer-to-Peer Process

At the physical layer, communication is direct: In figure, device A sends a stream of bits to device B (through intermediate nodes). At the higher layers, however, communication must move down through the layers on device A, over to device B and then back up through the layers. 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.

At layer 1 the entire package is converted to a form that can be transmitted to the receiving device. At the receiving machine, the message is unwrapped layer by layer, with each process receiving and removing the data meant for it. For example, layer 2 removes the data meant for it, then passes the rest to layer 3. Layer 3 then removes the data meant for it and passes the rest to layer 4 and so on.

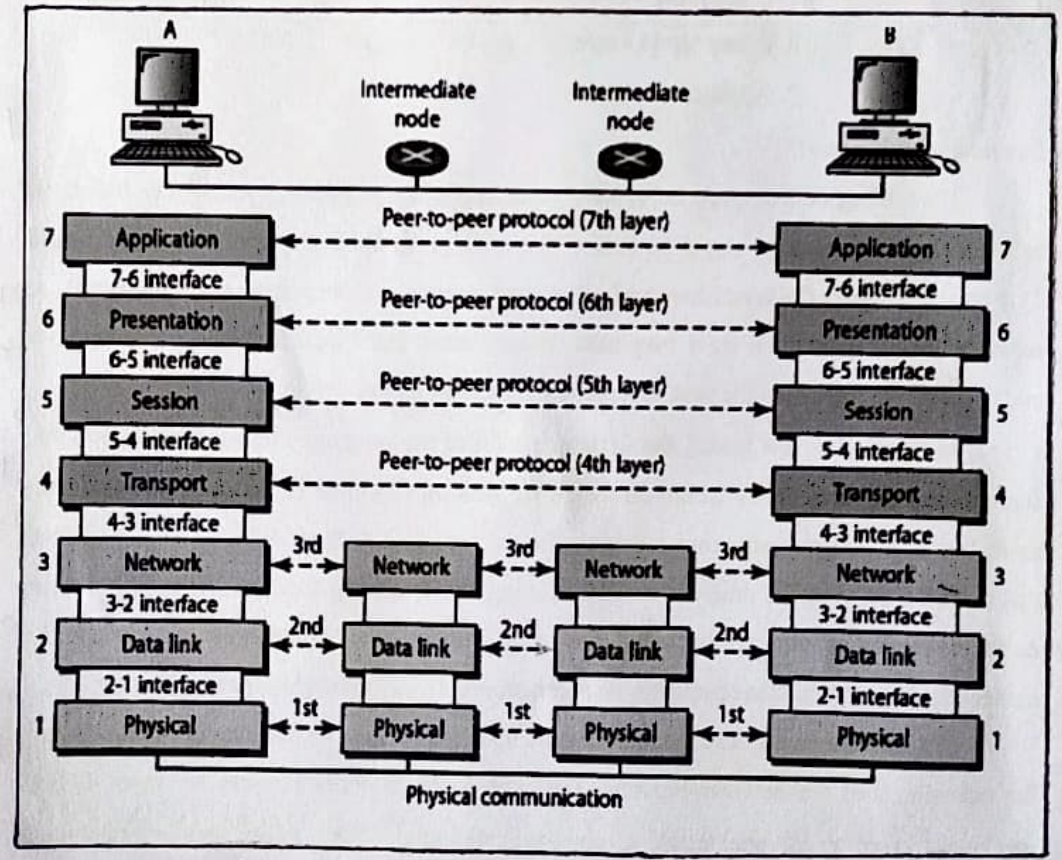


Figure 2.3

Interfaces between Layers

The passing of the data and network information down through the Layers of the sending device and back up through the Layers of the receiving device is made possible by an interface between each pair of adjacent Layer

Each interface defines the information and services a Layer must provide for the Layer above it. Well-defined interfaces and Layer factors provide modularity to a network. As long as a layer provides the expected services to the Layer above it, the specific implementation of its functions can be modified or replaced without requiring changes to the surrounding Layers.

Organization of the Layers

The seven layers can be thought of as belonging to three subgroups. Layers 1, 2 and 3 - physical, data link and network are the network support Layers; they deal with the physical aspects of moving data from one device to another (such as electrical specifications, physical connections, physical addressing and transport timing and reliability).

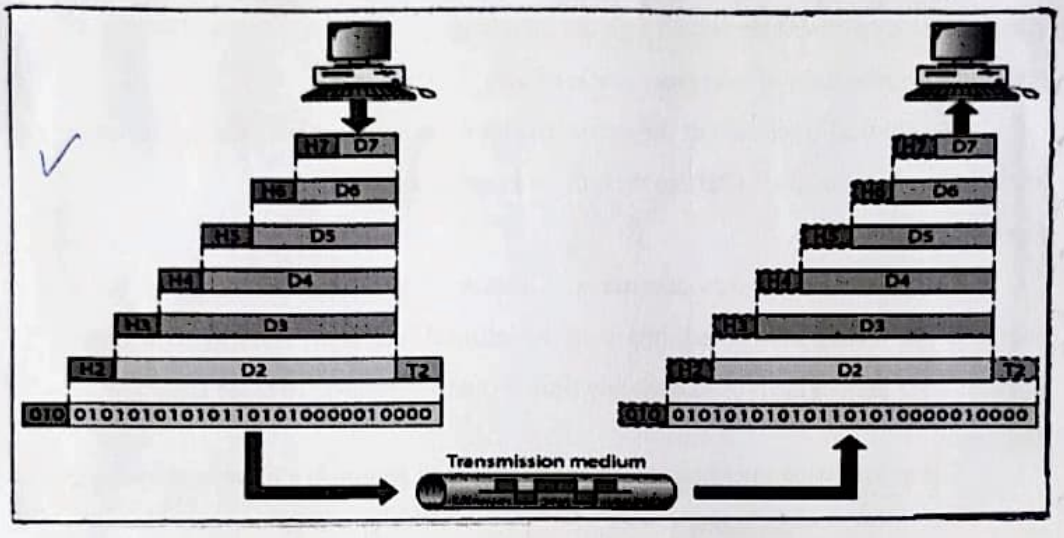
Layers 5, 6 and 7 - session, presentation and application - can be thought of as the user support layers; they allow interoperability among unrelated software systems. Layer 4, the transport Layer, links the two subgroups and ensures that what the lower layers have transmitted is in a form that the upper layer can use.

The upper OSI Layers are almost always implemented in software; Lower Layers are a combination of hardware and software, except for the physical layer, which is mostly hardware.

In fig 2.4 which gives an overall view of the OSI Layers, D7 means the data unit at Layer 7, D6 means data unit at Layer 6 and so on. The process starts at Layer 7 (the application Layer), then moves from Layer to layer in descending, sequential

order. At each Layer, a header, or possibly a trailer, can be added to the data unit.

Commonly, the trailer is added only at layer 2. When the formatted data unit passes through the physical layer (layer 1) it is changed into an electromagnetic signal and transported along a physical link.

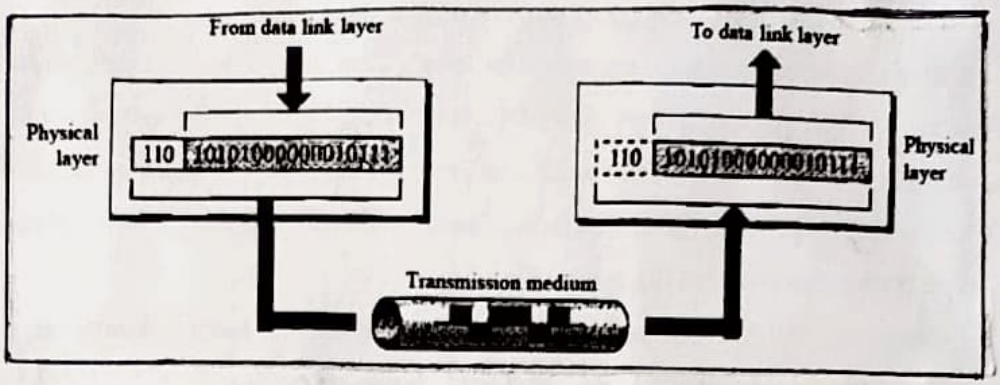


Upon reaching its destination, the signal passes into layer 1 and is transformed back into digital form. The data units then move back up through the OSI layers. As each block of data reaches the next higher layer, the header and trailers attached to it at the corresponding sending layer are removed, and actions appropriate to that layer are taken. By the time it reaches Layer 7, the message is again in a form appropriate to the application and is made available to the recipient.

LAYERS IN THE OSI MODEL:

1. Physical Layer

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



The physical layer is responsible for movements of individual bits from one hop (node) to the next.

The physical Layer is also concerned with following:

Physical charecterstics of interfaces and medium.

The physical layer defines the charecterstics of the interface between the device 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 0s and 1s) with no interpretation. To be transmitted, bits must be encoded into signals - electrical or optical. The physical layer defines the type of encoding (how 0s and 1s are changed to signals).

Data rate

The transmission rate - the no. of bits sent each second - is also defined by the physical layer. In other words, the physical layer. In other words, the physical layer defines the durations 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.

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 shared among several devices

Physical topology

The physical topology defines how devices are connected to make a network. Devices can be connected by using a mesh topology (every device is connected to every other device), a star topology (devices are connected through a central device), a ring topology (each device is connected to next, forming a ring), a bus topology (every device is on a common link) or a hybrid topology (this is a combination of 2 or more topogies

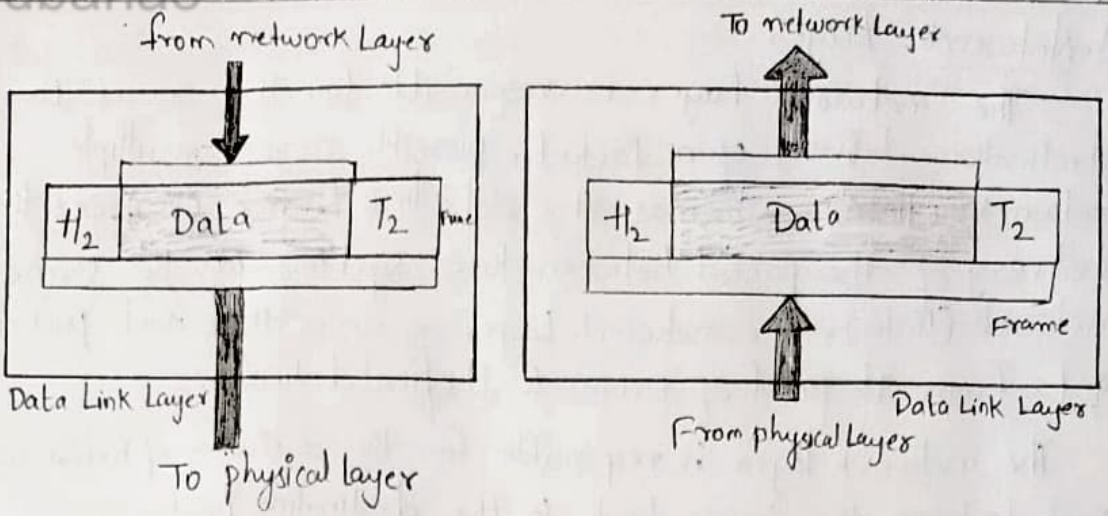
Transmission mode

The physical layer also defines the direction of transmission between two devices: simplex, half duplex or full duplex. In simplex mode, only one devices can send; the other can only receive. The simplex mode is a one-way communication. In the half-duplex mode, two devices can send and receive, but not at the same time. In a full-duplex (or simply duplex) mode, two devices can send and receive at the same time.

2. Data Link Layer

The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error-free to the upper layer (network layer).

The data link Layer is responsible for moving frames from one hop (node) to the next



Framing

To 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/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address of the device that connects the network to next one

Flow Control

If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link Layer imposes a flow control mechanism to avoid overwhelming the reciver.

Error Control

The data link Layer adds reliability to the physical Layer by adding mechanism 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 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.

3. Network Layer

The network Layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). whereas the data link Layer oversees the delivery of the packet between two systems on the same network (links), the network Layer ensures that each packet gets from its point of origin to its final destination.

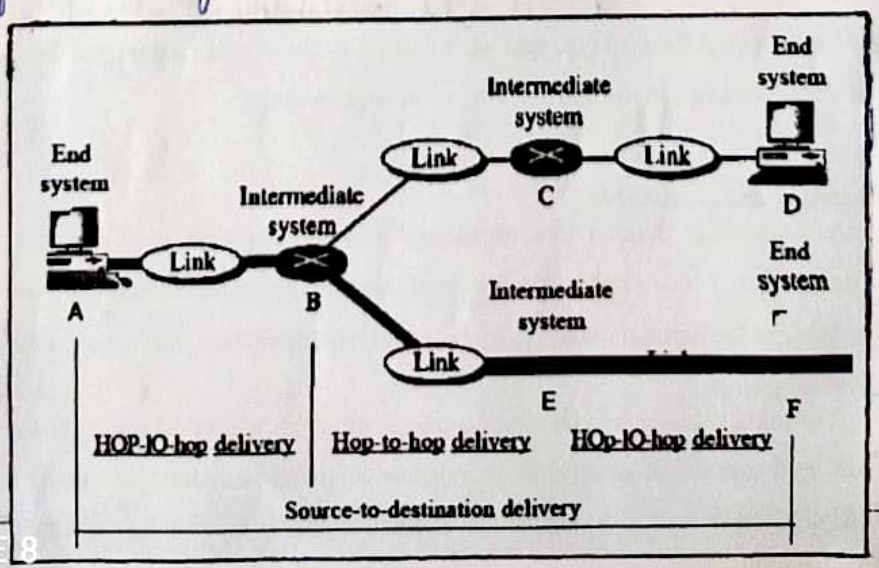
The network layer is responsible for the delivery of individual packets from the source host to the destination host.

Logical addressing

The physical addressing implemented by the data link Layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper Layer that, among other things, includes the logical addresses of sender and receiver.

Routing

when independent networks or links are connected to create internetworks (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 network Layer is to provides this mechanisms.



The network layer at A sends the packet to the network layer at B. when the packet arrives at router B, the router makes a decision based on the final destination (F.) of the packet. The router B uses its routing table to find that the next hop is router E. The network layer at B, therefore, sends the packet to the network layer at E. The network layer at E, in turn, sends the packet to the network layer at F.

4. 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. whereas the network layer oversees source-to-destination delivery of individual packet, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message, whether or not it does. The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at source-to-destination level.

The transport layer is responsible for the delivery of a message from one process to another.

Service-point addressing

Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The transport layer header must therefore include a type of address called a service-point address (or port address). The network layer gets each packet to the correct computer; the transport layer gets the the entire message to the correct process on that computer.

Segmentation and reassembly

A message is divided into transmittable segements, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the distination and to identify and replace packet that were lost in transmission.

Connection Control

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

Flow Control

Like the data link Layer, the transport Layer is responbile for flow control. However, flow control at this Layer is performed end to end rather than across a single link.

Error Control

Like the data link Layer, the transport Layer is responsible for error control. However, error control at this Layer is performed prouss-to prouss rather than across a single link. The sending transport Layer makes sure that the entire message arrives at the receiving transport Layer without error (damage, loss or duplications). Error Correction is usually achieved through retransmission.

5. Session Layer

The services provided by the first three Layers (physical, data link and network) are not sufficient for some processes. The session layer is the network dialog Controller. It establishes, maintains and synchronizes the interaction among communication systems.

The session layer is responsible for dialog control & synchronization.

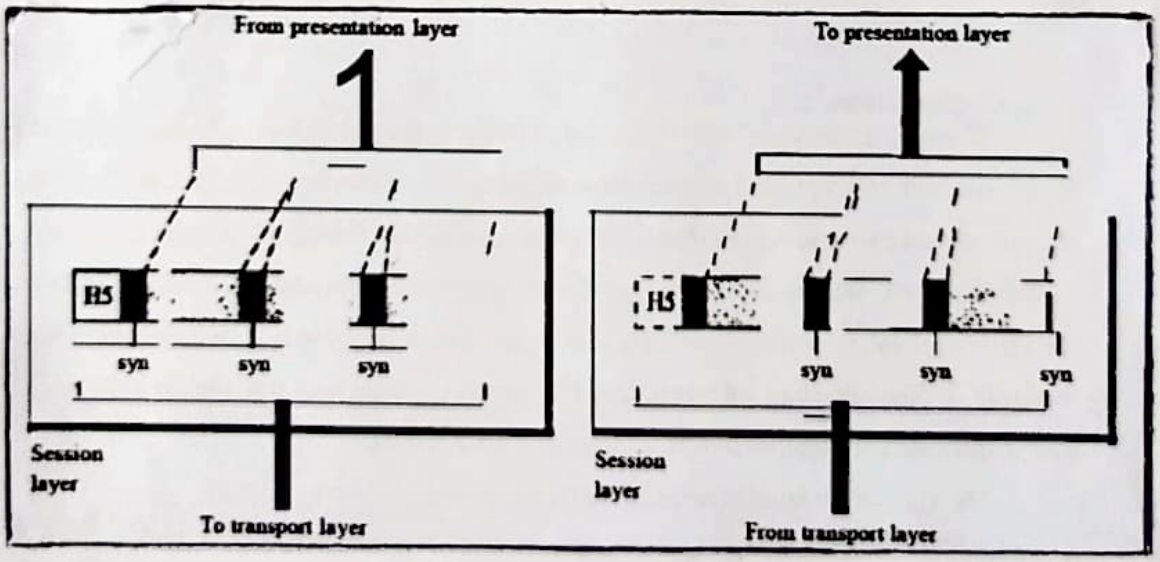
Dialog Control

The session layer allow two systems to enter into a dialog. It allows the communication between two process to taken 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 checkpoint or Synchronization point, to a stream of data. For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pges to ensure that each 100 page unit is received and acknowledged independently.

In this case, if a crash happens during the transmission of Page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent.



6. 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 process (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. 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

To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.

Compression

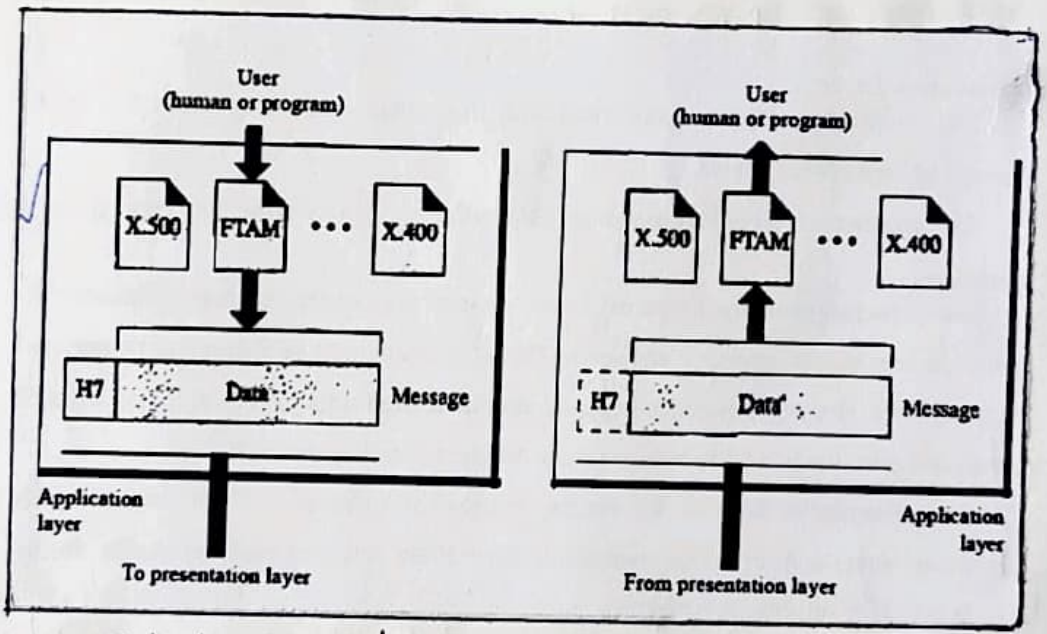
Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio and video.

7. Application Layer

The application Layer enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database managment and other types of distributed information services.

Figure shows the relationship of the application layer to the user and the presentation Layer. Of the many application service available, the figure shows only three: X.400 (message-handling Service, X.500 (directory service), and file transfer, access and managment (FTAM). The user in this example employs X.400 to send an e-mail message.

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



Network virtual terminal

A network virtual terminal is a software version of a physical terminal and it allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host.

The user's computer talks to the software terminal which, in turn, talks to the host, and vice versa. The remote host believes it is communicating with one of its own terminals and allows the user to log on.

File transfer, access and managment

This application allows a user to access file in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the Local computer, and to manage or control files in a remote computer locally.

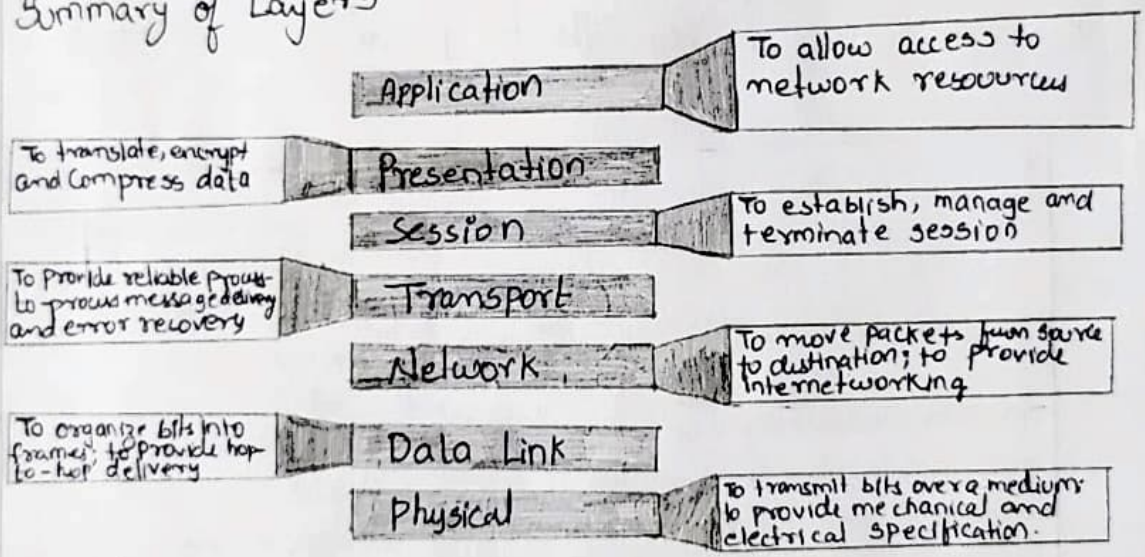
Mail services

This application provides the basis for e-mail forwarding and storage.

Directory service

This application provides distributed database sources and access for global information about various object and services.

Summary of Layers



TCP/IP REFERENCE MODEL (PROTOCOL SUITE):

The TCP/IP protocol suite was developed prior to the OSI model. Therefore, the layers in the TCP/IP protocol suite do not exactly match those in the OSI Model. The original TCP/IP protocol suite was defined as having four Layers: host-to-network, Internet, transport and application. However, when TCP/IP is compared to OSI, we can say that the host-to-network Layer is equivalent to the combination of physical and data link Layers.

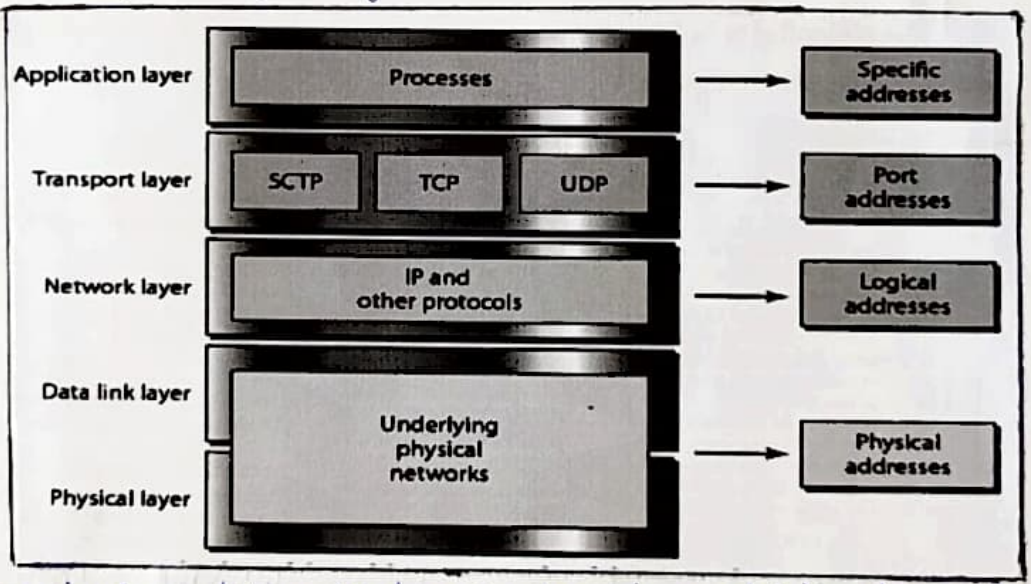
The internet Layer is equivalent to the network layer, and the application layer is roughly doing the job of the session, presentation

and application Layers with the transport layer in TCP/IP taking care of part of the duties of session Layer.

The TCP/IP protocol suite is made of five Layer

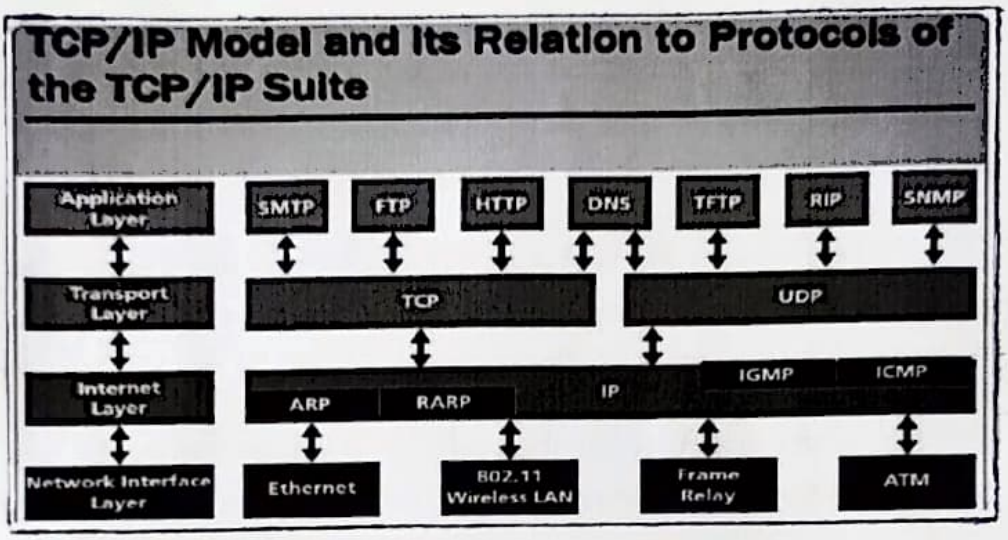
1. physical Layer
2. Data link Layer
3. Network Layer
4. Transport Layer
5. Application Layer

The first four Layers provide physical standards, network interfaces, internetworking and transport functions that correspond to the first four layers of the OSI model. The three topmost layers in the OSI model, however, are represented in TCP/IP by a single Layer called the application layer



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. whereas the 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 system. The term hierarchical means that each upper-level protocol is supported by one or more lower-level protocol.

At the transport layer, TCP/IP defines three protocols: Transmission control protocol (TCP), User Datagram Protocol (UDP) and stream Control Transmission Protocol (SCTP). At the network Layer, the main protocol defined by TCP/IP is the Internetworking Protocol (IP); there are also some other protocols the support data movement in this Layer.



1. Physical and Data Link Layers (HOST-to-Network Layers)

At the physical and data Link Layers, 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.

2. Network Layer (Internet Layer)

At the network Layer (or, more accurately, the Internetwork layer), TCP/IP supports the Internetworking Protocol. 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. IP assumes the unreliability of the underlying Layers and does it best to get a transmission through to its destination but with no guarantees.

IP transports data in packets called datagrams, each of which is transported separately.

Datagram's can travel along different routes and can arrive out of sequence or be duplicated. IP does not keep track of the routes and has no facility for reordering datagrams once they arrive at their destination

Address Resolution Protocol

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

Reverse Address Resolution Protocol

The Reverse Address Resolution Protocol (RARP) allows a host to discover its Internet address when it known only its 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

The Internet Control Message Protocol (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 message.

Internet Group Message Protocol

The Internet Group Message Protocol (IGMP) is used to facilitate the simultaneous transmission of a message to a group of recipients.

3. Transport Layer

Traditionally the transport Layer was represented in TCP/IP by two protocols: TCP and UDP. IP is a host-to-host protocol meaning that it can deliver a packet from one physical device to another. UDP and TCP are transport level protocol responsible for delivery of a message from a process (running program) to another process. A new transport Layer protocol, SCTP has been devised to meet the needs of some newer applications.

User Datagram Protocol

The User Datagram Protocol (UDP) is the simpler of the two standard TCP/IP transport protocol. It is a process-to-process protocol that adds only port addresses, checksum error control and length information to data from the upper layer.

Transmission Control protocol

The Transmission Control Protocol (TCP) provides full transport-layer services to applications. TCP is a reliable stream transport protocol. The term stream, in this context, means connection-oriented: A connection must be established between both ends of a transmission before either can transmit data.

At the sending end of each transmission, TCP divides a stream of data into smaller units called Segements. Each segement includes a sequence number for reordering after receipt, together with an acknowledgment number for the segments received. Segements are carried across the internet inside of IP datagram's. At the receiving end, TCP collects each datagram as it comes in and reorders the transmission based on sequence numbers.

Stream Control Transmission Protocol

The stream Control transmission protocol (SCTP) provides support for newer applications such as voice over internet. It is a transport layer protocol that combines the best features of UDP and TCP.

4. Application Layer

The application Layer in TCP/IP is equivalent to the combined session, presentation and application layer in the OSI model many protocols are defined at this layer.

Comparision of OSI and TCP/IP Reference model

The OSI and TCP/IP reference models have much in common. Both are based on the concept of a stack of independent protocols

The following differences show the important of OSI and TCP/IP reference model.

OSI Model	TCP/IP Reference model
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the n/w and end user	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol which allows connection of host overall n/w.
2. In OSI model the transport Layer guarantees the delivery of packets	2. In TCP/IP model the transport Layer does not gaurantees delivery of packets. It is more reliable
3. It follows vertical approach	3. Follows horizontal approach
4. OSI has a separate presentation layer and session layer	4. It does not have a presentation and layer.
5. OSI is a reference model around which the n/w's are built	5. TCP/IP model is in a way implementation of model
6. Network Layer of OSI model provides both connection oriented and Connection less services	6. the n/w Layer in TCP/IP model provides Connection less services
7. OSI model has a problem of fitting the protocol into model	7. TCP/IP model does not fit any protocol
8. protocol are hidden in OSI model and easily replaced as the technology	8. In TCP/IP replacing protocol is not easy
9. OSI model defines services interface and protocol very clearly and makes clear distinction between them	9. In TCP/IP, service, interface and protocols are not clearly separated
10. It is protocol independent	10. It is protocol dependent
11. It has 7 layers	11. It has 4 Layers
12. The layers are i) physical ii) Datalink iii) Network iv) Transport v) session vi) Presentation vii) Application	i) Link ii) Internet iii) Transport iv) Application.

Example Network:

Internet:

The Internet has revolutionized many aspects of our daily lives. It has affected the way we do business as well as the way we spend our leisure time. Count the ways you've used the Internet recently. Perhaps you've sent electronic mail (e-mail) to a business associate, paid a utility bill, read a newspaper from a distant city or looked up a local movie schedule - all by using the Internet

Brief History

A network is a group of Connected Communicating devices such as Computers and printers. An Internet (note the lowercase letter i) is two or more networks that can Communicate with each other. The most notable Internet is called the Internet (uppercase letter I), a collaboration of more than hundreds of thousands of interconnected networks.

Private individuals as well as various organization such as government agencies, schools, research facilities, corporations and libraries in more than 100 countries use the Internet. Millions of people are users. Yet this extraordinary Communication System only came into being in 1969.

In the mid-1960s mainframe Computer in research organization were standalone devices. Computers from different manufactures were unable to Communicate with one another. The Advanced Research Projects Agency (ARPA) in the department of Defense (DoD) was intrested in finding a way to connect computer so that the researches they funded could share their finding, thereby reducing costs and eliminating duplication of effort.

In 1967, at an Association for Computing Machinery (ACM) meeting, ARPA presented its idea for ARPANET, a small network of Connected Computers. The idea was that each host computer (not necessarily from the same manufacturer) would be attached to

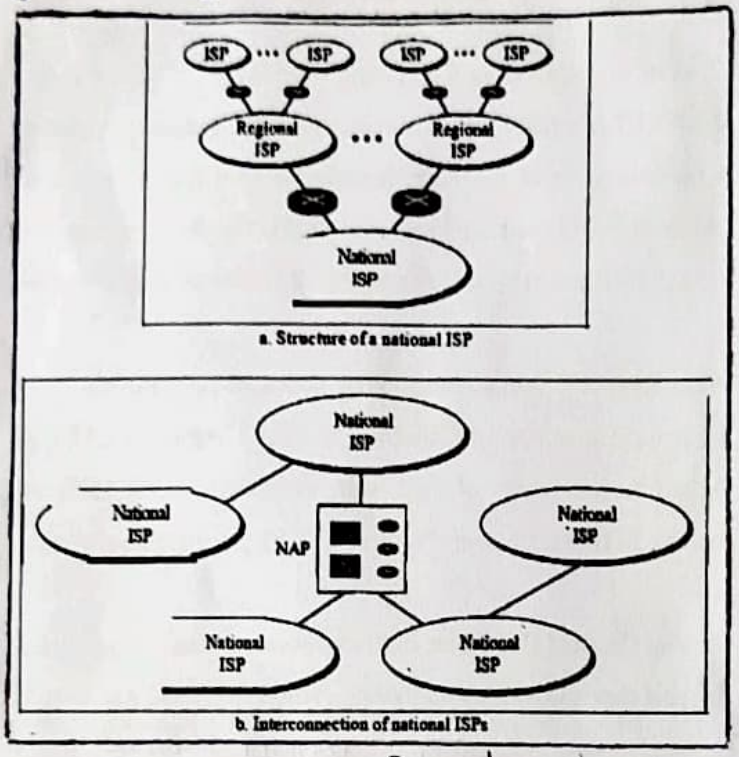
a specialized computer, called an interface message processor (IMP). The IMPs, in turn, would be attached to a specialized Computer called an Interface message processor (IMP). The IMPs, in turn, would be connected to another. Each IMP had to be able to Communicate with other IMPs as well as with its own attached host.

By 1969, ARPANET was a reality. Four nodes, at the University of California at Los Angeles (UCLA), the University of California at Santa Barbara (UCSB), Standford Research Institute (SRI), and the University of utah, were connected via the IMPs to form a network. Software called the Network Control Protocol (NCP) provided Communication between the hosts.

In 1972, Vint Cerf and Bob Kahn, both of whom were part of the core ARPANET group, collaborated on what they called the Internetting Project. Cerf and Kahn's Landmark 1973 paper Outlined the protocols to achieve end-to-end delivery of packet. This paper on Transmission Control Protocol (TCP) included Concepts such as encapsulation, the datagram, and the functions of a gateway. Shortly thereafter, authorities made a decision to split TCP into two protocols:
Transmission Control Protocol (TCP) and Internetworking Protocol (IP). IP would handle datagram routing while TCP would be responsible for higher-level function such as segementation, reassembly and error detection. The internetworking protocol become known as TCP/IP

The Internet has come a long way since the 1960. The Internet today is not a simple hierarchical structure. It is made up of many wide- and local- area networks joined by Connecting devices and switching stations. It is difficult to give an accurate representation of Internet because it is Continually changing new networks are beingadded, existing network are adding addresses and networks of difund Companies are being removed.

Today most end users who want Internet Connection use the services of Internet service providers (ISPs). There are International service providers, national service providers, regional service providers, and local service providers. The Internet today is run by private companies, not the government.



International Internet Service Providers

At the top of the hierarchy are the International service providers that connect nations together.

Nation Internet Service Providers

The national Internet service providers are backbone network created and maintained by specialized companies. There are many national ISPs operating in North america; some of the most well known are SprintLink, PSINet, UUNet Technology, AGIS and Internet Mel. To provide connectivity between the end users, these backbone network are connected by complex switching stations (normally run by a third party) called network access points (NAPs). Some national ISP networks also connected to one another by private switching stations called peering points. They normaly operate at high data rate (upto 600 Mbps).

Regional Internet Service Providers

Regional Internet Service providers or regional ISPs are smaller ISPs that are connected to one or more national ISPs. They are at the third level of the hierarchy with smaller data rate.

Local Internet Service Providers

Local Internet service providers provide direct service to the end users. The local ISPs can be connected to regional ISPs or directly to national ISPs. Most end users are connected to the local ISPs. Note that in this sense, a local ISP can be a company that just provides Internet services, a corporation with a network that supplies services to its own employees, or a nonprofit organization, such as a college or a university, that runs its own network. Each of these local ISPs can be connected to a regional or national service providers.

Physical Layer

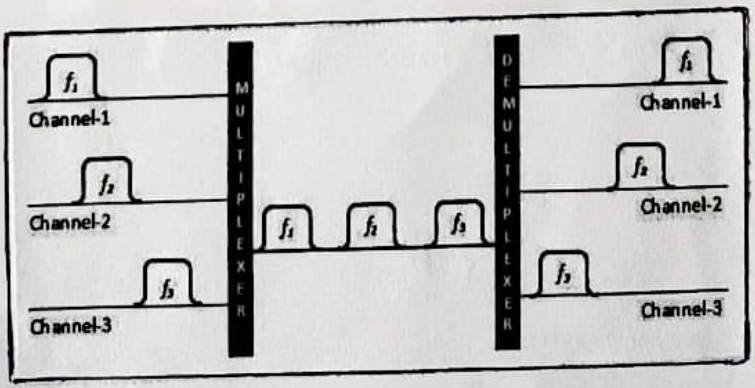
Multiplexing

Multiplexing is a technique by which different analog and digital streams of transmission can be simultaneously processed over a shared link. Multiplexing divides the high capacity medium into low capacity logical medium which is then shared by different streams. Communication is possible over the air (radio frequency) using a physical media (cable) and light (optical fibre). All medium are capable of multiplexing

When multiple senders try to send over a single medium, a device called Multiplexer divides the physical channel and allocates one to each. On the other end of communication, a De-multiplexer receives data from a single medium, identifies each and sends to different receivers.

Frequency Division Multiplexing

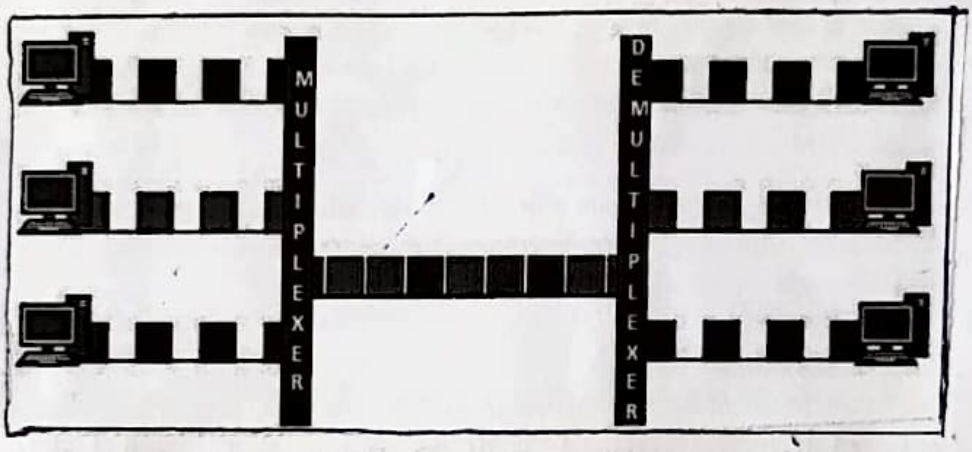
When the carrier is frequency, FDM is used. FDM is an analog technology. FDM divides the spectrum or carrier bandwidth in logical channels and allocate one user to each channel. Each user can use the channel frequency independently and has exclusive access of it. All channels are divided in such a way that they do not overlap with each other. Channels are separated by gaurd bands. Gaurd band is a frequency which is not used by either channel



Time Division Multiplexing

TDM is applied primarily on digital signals but can be applied on analog signals as well. In TDM the shared channel is divided among its user by means of time slot. Each user can transmit data within the provided time slot only. Digital signals are divided in frames, equivalent to time slot i.e. frame of an optimal size which can be transmitted in given time slot.

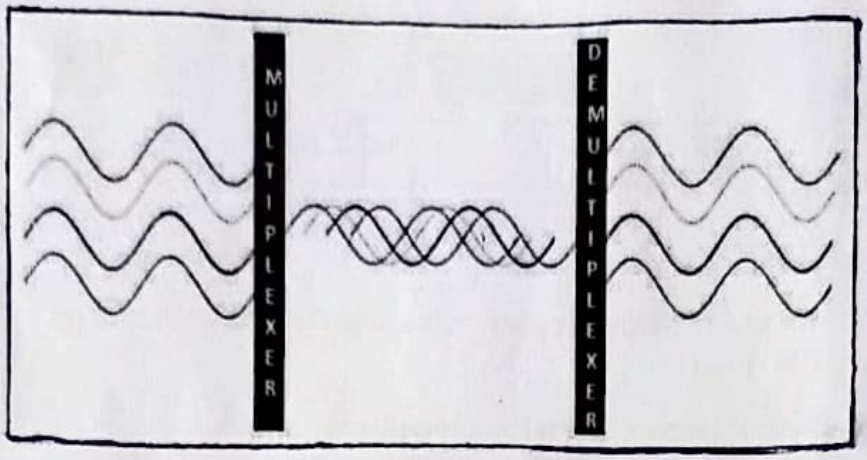
TDM works in Synchronized mode. Both ends, i.e Multiplexer and De-multiplexer are timely Synchronized and both switch to next channel simultaneously.



When channel A transmits its frame at one end, the De-multiplexer provides media to channel A on the other end. As soon as the channel A's time slot expires, this side switches to channel B. On the other end, the De-multiplexer works in a Synchronized manner and provides media to channel B. Signals from different channels travel the path in interleaved manner.

Wavelength Division Multiplexing

Light has different wavelength (colors). In fiber optics mode, multiple optical carrier signals are multiplexed into an optical fiber by using different wavelengths. This is an analog multiplexing technique and is done conceptually in the same manner as FDM but uses light as signals



Further, on each wavelength time division multiplexing can be incorporated to accommodate more data signals.

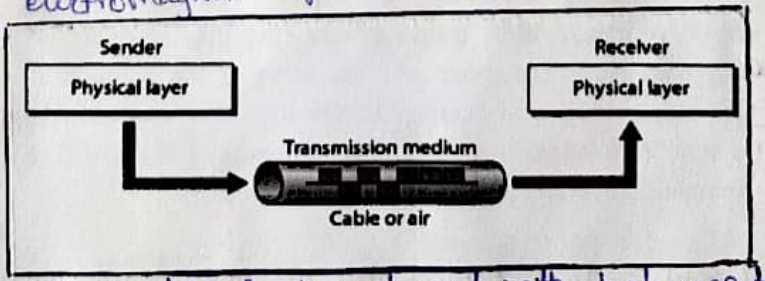
Code Division Multiplexing

Multiple data signals can be transmitted over a single frequency by using code Division Multiplexing. FDM divides the frequency in smaller channels but CDM allows its users to full bandwidth and transmit signals all the time using a unique code. CDM uses orthogonal codes to spread signals.

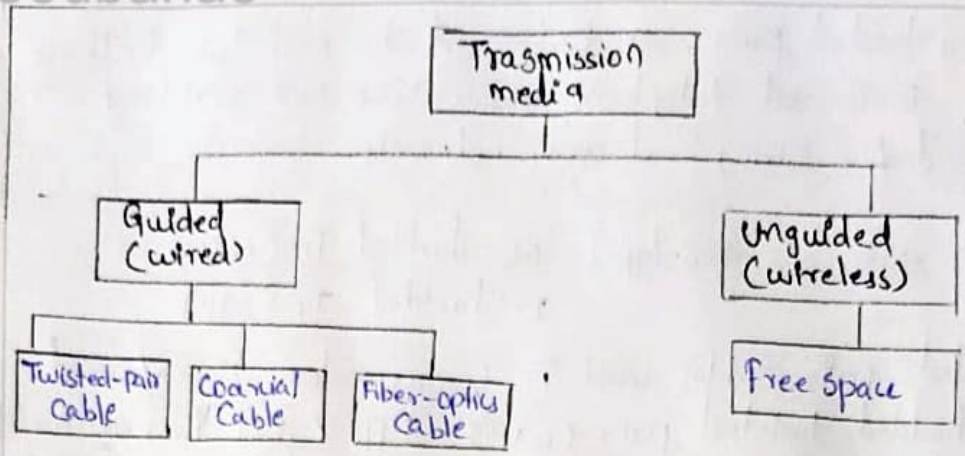
Each station is assigned with a unique code, called chip. Signals travel with these codes independently, inside the whole bandwidth. The receiver knows in advance the chip code signal it has to receive.

Transmission media:

The main objective of the physical layer is to move data in the form of electromagnetic signal across a transmission medium.



The transmission medium is the physical path between transmitter and receiver in a data transmission system.



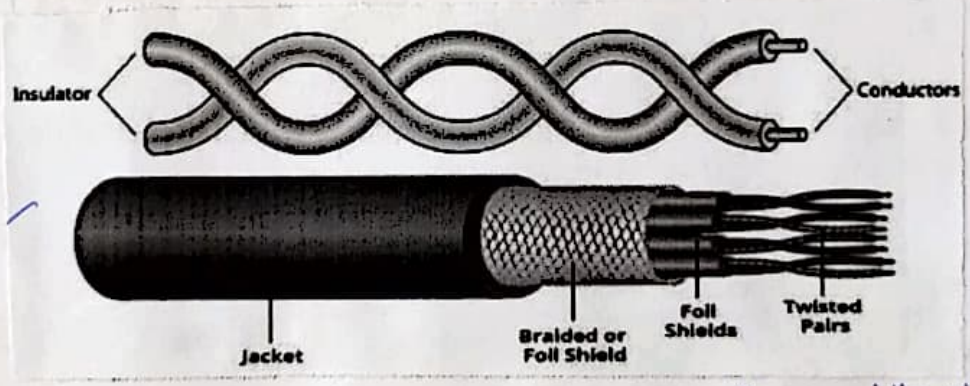
The Signal travelling along any of these media is directed and contained by the physical limits of medium.

Guided transmission medium can be used by following

1. Twisted pair cable
2. Co-axial Cable
3. Optical fiber Cable

1. Twisted Pair Cable

Two insulated wires are twisted around each other and combined with others into a cable



One of the wire is used to carry signals to the receiver and the other is used to only as a ground reference. In addition signal sent by the sender on one of wires, Interference (noise) and cross talk may affect both wires and created unwanted signals.

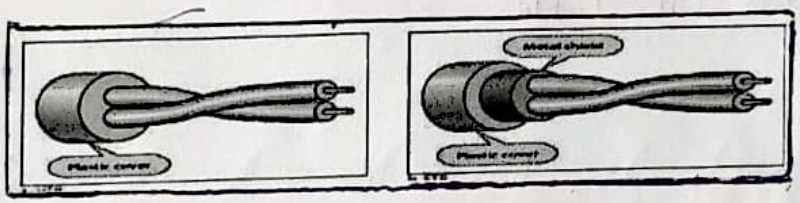
If the two wires are parallel, the effect of these unwanted signals is not the same in both wires because they are at different Locations relative to the noised or cross talk source, which may result in a difference at the receiver.

By using twisted pair, a balanced is maintained. These are used to Conned telephone subscribers two switching Centers and for wiring local area networks.

Twisted pair cables are two types 1. Unshielded TP (UTP)
2. Shielded TP (STP)

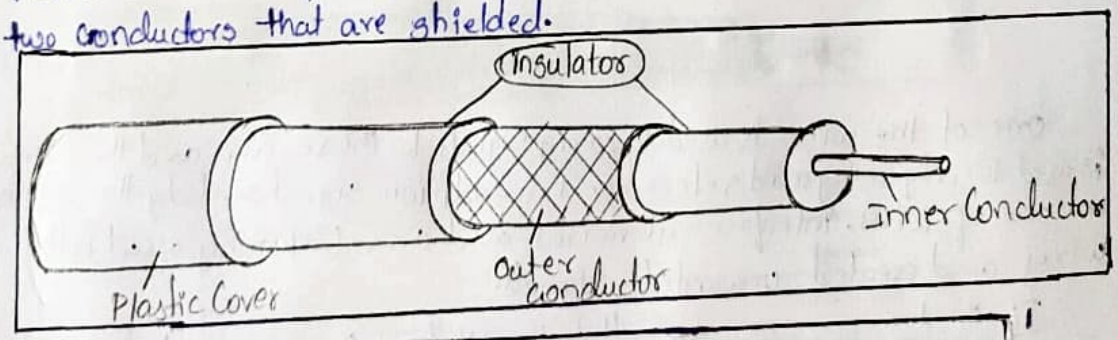
Most twisted pair cables used in Communication is referred to as unshielded twisted pair (UTP). STP Cabel has a metal foil or braided mesh covering that encases each pair of insulated conductors. The metal casing improves the quality of cable by preventing the penetration of noise or cross talk.

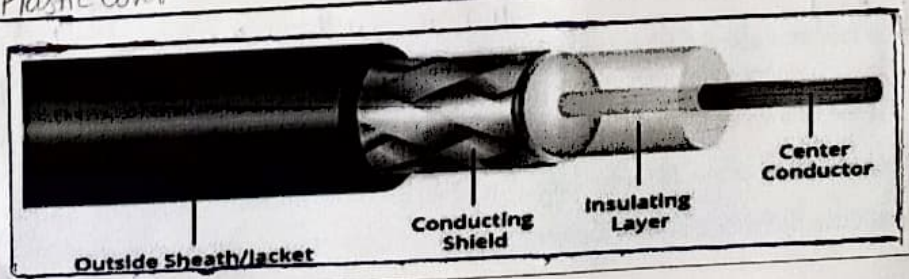
STPs are bulker more expensive
The most common UTP connector is RJ-45.
It is key connector inserted in only one way.



2. Co-Axial Cable:

Co-Axial cable carries signals of higher fequency ranges than those in twisted pair cable. It is like a twisted pair, it has two conductors that are shielded.





The outer metallic wrapping serves both as a shield against noise and is the second conductor, which completes the circuit. The outer conductor is also enclosed in an insulating sheath and whole cable is protected by plastic cover.

Co-axial cable uses for TV supports a spectrum of 50-750 MHz

RG-59-75Ω of impedance - cable TV

RG-58-50Ω - thin Ethernet.

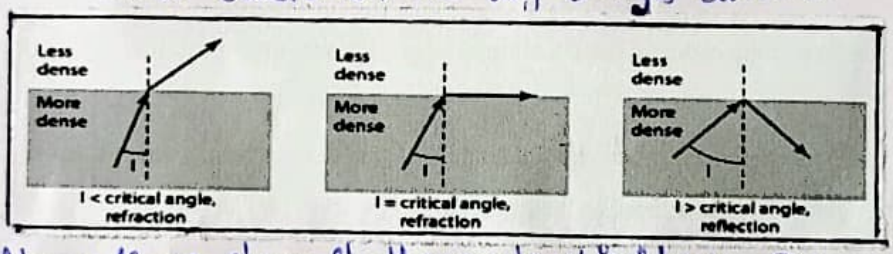
RG-11-50Ω - thick Ethernet

Co-axial cable could carry digital data upto 600mbps.

3. Fiber Optic Cable

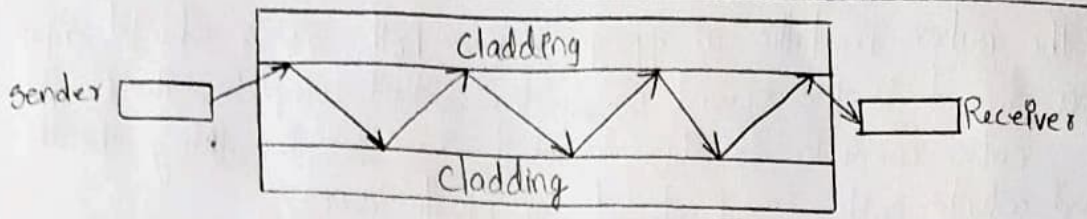
A fiber optic cable is made of glass or plastic and transmits signals in form of light. The light travels in a stright line as long as it is moving through a single uniform substance.

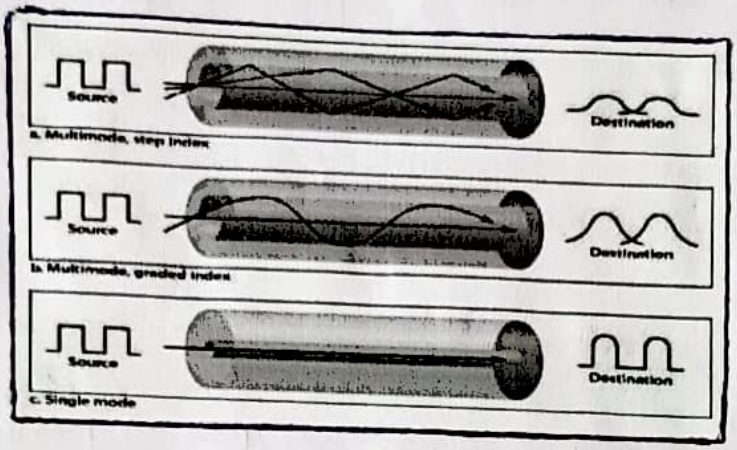
If a ray of light travelling through one substance suddenly enters another substance, the ray changes direction.



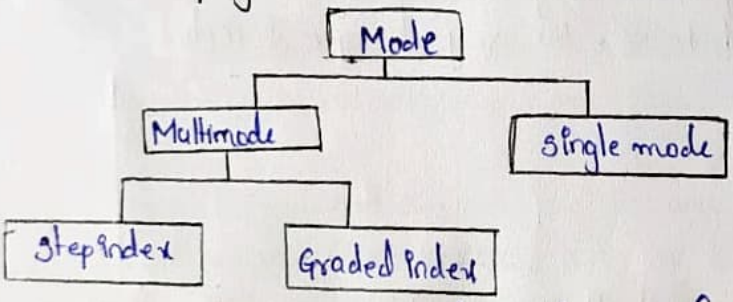
Above figure shows if the angle of incidence I is < the critical angle, the ray refracts and moves closer to the surface. If angle of incidence I is equal the critical angle, the light bends along the interface. If angle of incidence I is > the critical angle, the ray reflects and travels again in the denser substance.

Optical fibers use reflection to guide light through a channel. A glass or plastic core is surrounded by a cladding of less denser 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.





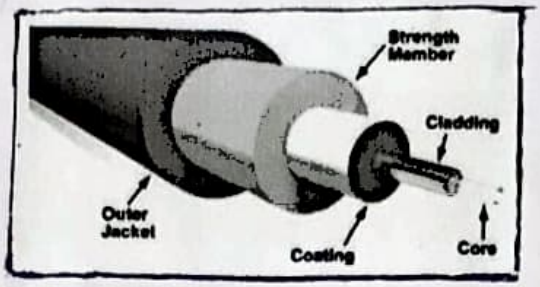
Modes of Propogation:



In multimode, the multiple beams from a light source move through the core in different patterns. In multi-mode step index, the density of the core remains constant from the center of the edges. The 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 abrupt changes due to a lower density.

In multimode step index fiber, the suddenness of this changes, which contributes to the distortion of the signal as it passes through the fiber.

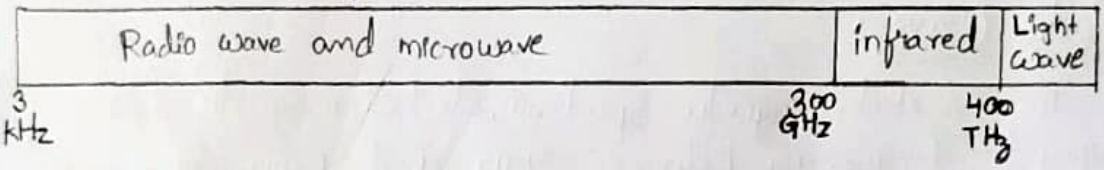
In multimode graded index fiber, decreases the distortion of the signal through the cable. A graded index fiber is one with varying densities. Density is highest at the center of the core and decreases gradually to its lowest at edge.



Wireless Transmission Media:

Unguided media transport electromagnetic waves without using physical conductor. This type of communication is called as wireless communications.

Signals are normally broad cast through free space and thus are available to anyone who has device capable of receiving them.



Unguided signals can travel from the source to distination in several ways.

i) Ground wave propogation
ii) Sky wave propogation
iii) Line-of-Sight propogation.

i) Ground Wave Propogation

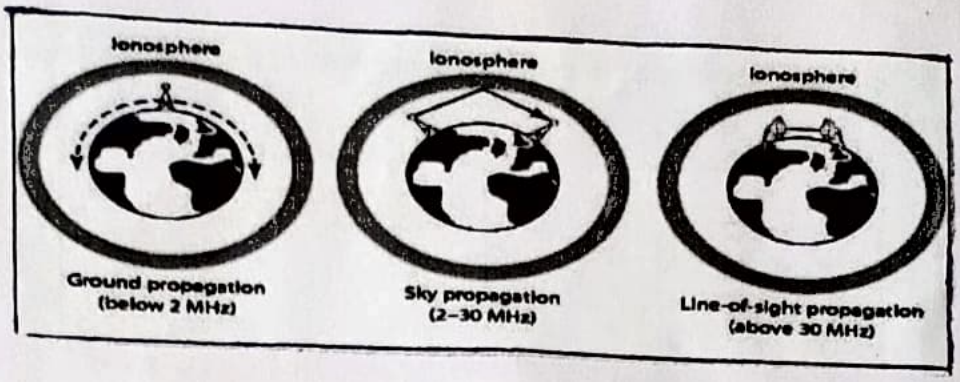
In ground wave propogation, radio wave travels through the lowest portion of the atmosphere, touchs the earth.

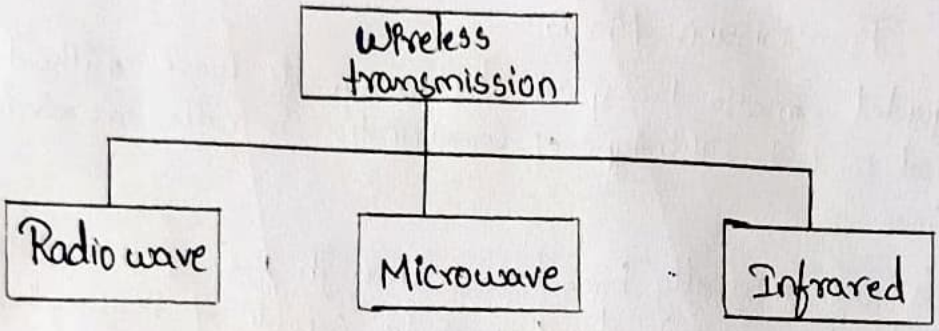
These low frequency signals propogate in all directions from the transmitting antenna and follow the curvature of planet.

ii) Sky wave Propogation

In line-of-sight propogation, very high fequency signals are trasmitted in straight line directly from antenna to antenna.

Antenna must be directional, facing each other and either tall enough or close enough together not to be affected by curvature of earth.





1. Radio Waves:

In an electromagnetic spectrum, electron magnetic waves ranging in frequencies between 3KHz and 1 GHz are normally called radio waves.

Radio waves are Omni directional, when an antenna transmits radio waves; they are propogated in all directions.

Radio wave particularly propogate in the sky mode and can travel long distances and it is good for broad casting.

Radio wave use Omni directional antennas that send out signals in all directions.

Radio waves are used for multicast Communications, such as radio and television and paging systems.

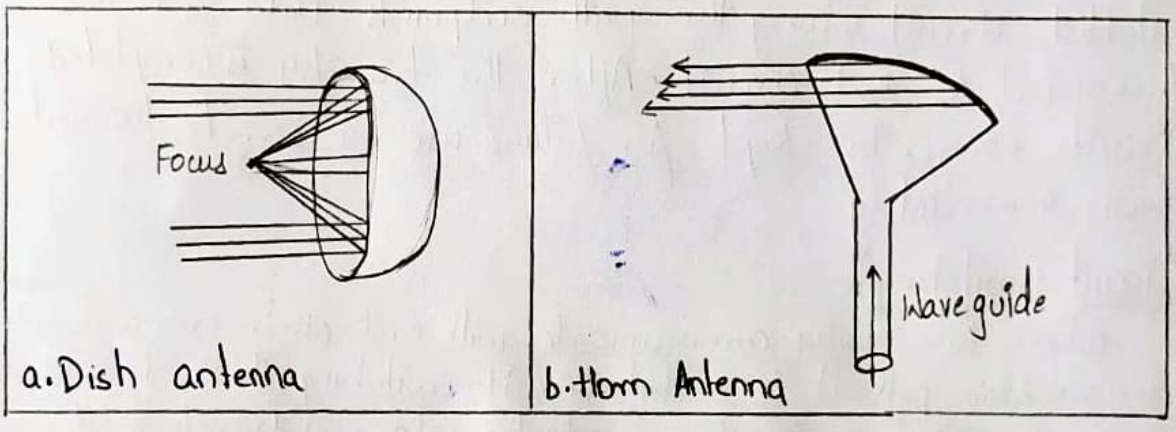
2. Micro Waves :-

Electromagnetic waves of frequencies between 1 and 300 GHz are called microwaves.

Microwaves are Uni-directional, when an antenna transmits microwaves, they can be narrowly focused.

Micro wave propagation is line-of-sight.
Repeaters are often needed for long distance Communication
Very light frequency microwaves cannot penetrate walls.

Two types antennas used in microwave Communication
Parabolic dish antenna horn antenna



a. Dish antenna b. Horn Antenna

Microwaves are used for Unicast Communication such as Cellular telephones, satellite networks, and wireless LANs

3. Infrared :-

Infrared waves are electromagnetic waves with frequencies from 300 GHz to 400 GHz (wavelength from 1mm to 770nm) can be used for short-range Communication.

Infrared waves, having high frequency, cannot penetrate

Infrared signals can be used for short-range Communication in a closed area using line-of-sight propogation.

Switching:

Switching is process to forward packets coming in from one port to a port leading towards the destination. when data comes on a port it is called ingress, and when data leaves a port or goes out it is called egress. A Communication system may include number of switches and nodes. At broad level, Switching can be divided into two major categories:

- Connectionless (Packet Switching): The data is forwarded on behalf of forwarding tables. No previous handshaking is required and acknowledgments are option
- Connection Oriented (Circuit Switching): Before switching data to be forwarded to distination, there is a need to pre-establish circuit along the path endpoints. Data is then forwarded on that circuit. After the transfer is completed, circuits can be kept for future use or can be turned down immediately.

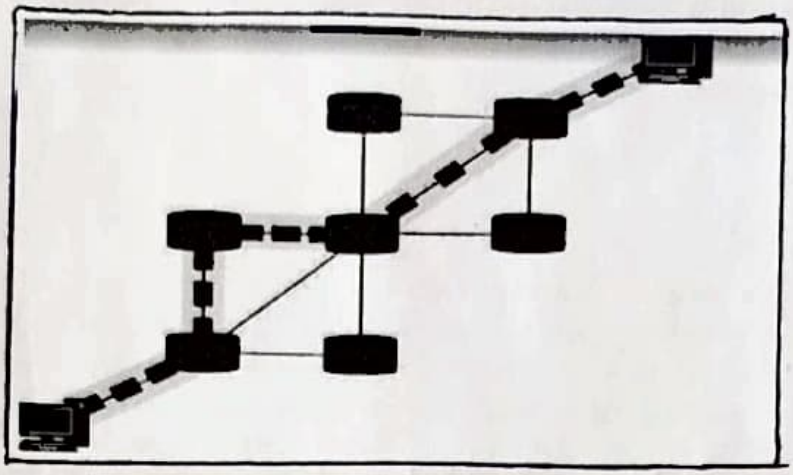
Circuit Switching:

when two nodes communicate with each other over a decade communication path, it is called Circuit switching. There is a need of pre-specified route from which data will travels and no other data is permitted. In Circuit switching, to transfer the data, Circuit must be established so that the data transfer can take place.

Circuit can be permanent or temporary. Applications which use Circuit switching may have to go through three phases:

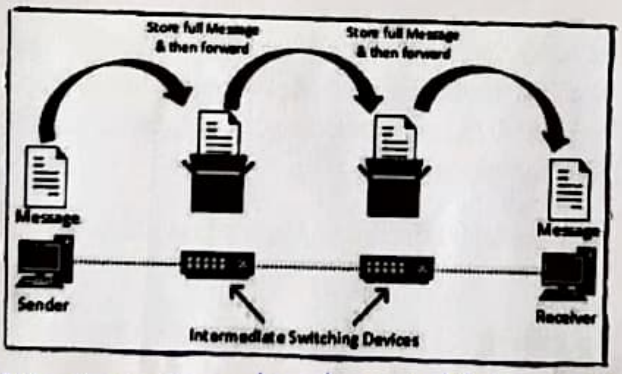
- Establish a Circuit
- Transfer the data
- Disconnect the Circuit

Circuit switching was designed for voice applications. Telephone is the best suitable Example of Circuit switching. Before a user can make a call, a virtual path between caller and callee is established over the network.



Message Switching:-

This technique was somewhere in middle of Circuit switching and packet switching. In message switching, the whole message is treated as a data unit and is switching / transferred in its entirety. A switch working on message switching, first recieves the whole message and buffers it until these are resources available to transfer it to the next hop. If the next hop is not having enough resource to accomadate large size message, the message is stored and switch waits.



This technique was considered substitute to circuit switching. As in circuit switching the whole path is blocked for two entities only. Message switching is replaced by packet switching. Message switching has following Drawbacks:

- Every switch in transit path needs enough storage to accommodate entire message.
- Because of store-and-forward technique and waits included until resources are available, message switching is very slow.
- Message switching was not a solution for streaming media and real-time applications.

Packet Switching:-

Shortcomings of message switching gave birth to an idea of packet switching. The entire message is broken down into smaller chunks called Packets. The switching information is added in the header of each packet and transmitted independently. It is easier for intermediate networking devices to store small size packets and they do not take much resources either on carrier path or in internal memory of switches.

Packet switching enhances line efficiency as packets from multiple applications can be multiplexed over the carrier. The internet uses packet switching technique. Packet switching enables the user to differentiate data streams based on priorities. Packet switching enables the user to differentiate data streams based on Priorities. Packets are stored and forwarded according to their priority to provide quality of service.