UNIT-I

DATA COMMUNICATIONS AND NETWORKING

Introduction to Computer Networks

Modern world scenario is ever changing. Data Communication and network have changed the way business and other daily affair works. Now, they highly rely on computer networks and internetwork.

A set of devices often mentioned as nodes connected by media link is called a Network.

A node can be a device which is capable of sending or receiving data generated by other nodes on the network like a computer, printer etc. These links connecting the devices are called **Communication channels**.

Computer network is a telecommunication channel using which we can share data with other computers or devices, connected to the same network. It is also called Data Network. The best example of computer network is Internet.

Computer network does not mean a system with one Control Unit connected to multiple other systems as its slave. That is Distributed system, not Computer Network.

A network must be able to meet certain criteria's, these are mentioned below:

1. Performance
2. Reliability
3. Scalability

Computer Networks: Performance

It can be measured in the following ways:

- **Transit time :** It is the time taken to travel a message from one device to another.
- **Response time :** It is defined as the time elapsed between enquiry and response.

Other ways to measure performance are :

1. Efficiency of software
2. Number of users
3. Capability of connected hardware

Computer Networks: Reliability

It decides the frequency at which network failure take place. More the failures are, less is the network's reliability.

Computer Networks: Security

It refers to the protection of data from any unauthorized user or access. While travelling through network, data passes many layers of network, and data can be traced if attempted. Hence security is also a very important characteristic for Networks.

Properties of a Good Network

1. **Interpersonal Communication:** We can communicate with each other efficiently and easily. Example: emails, chat rooms, video conferencing etc, all of these are possible because of computer networks.
2. **Resources can be shared:** We can share physical resources by making them available on a network such as printers, scanners etc.
3. **Sharing files, data:** Authorized users are allowed to share the files on the network.

Basic Communication Model

A Communication model is used to exchange data between two parties. For example: communication between a computer, server and telephone (through modem).

Communication Model: Source

Data to be transmitted is generated by this device, example: telephones, personal computers etc.

Communication Model: Transmitter

The data generated by the source system is not directly transmitted in the form it's generated. The transmitter transforms and encodes the data in such a form to produce electromagnetic waves or signals.

Communication Model: Transmission System

A transmission system can be a single transmission line or a complex network connecting source and destination.

Communication Model: Receiver

Receiver accepts the signal from the transmission system and converts it into a form which is easily managed by the destination device.

Communication Model: Destination

Destination receives the incoming data from the receiver.

Data Communication

The exchange of data between two devices through a transmission medium is called **Data Communication**. The data is exchanged in the form of **0's** and **1's**. The transmission medium used is wire cable. For data communication to occur, the communication device must be a part of a communication system. Data Communication has two types - **Local** and **Remote** which are discussed below:

Data Communication: Local

Local communication takes place when the communicating devices are in the same geographical area, same building, or face-to-face etc.

Data Communication: Remote

Remote communication takes place over a distance i.e. the devices are farther. The effectiveness of a data communication can be measured through the following features :

1. **Delivery**: Delivery should be done to the correct destination.
2. **Timeliness**: Delivery should be on time.
3. **Accuracy**: Data delivered should be accurate.

Components of Data Communication

1. **Message:** It is the information to be delivered.
2. **Sender:** Sender is the person who is sending the message.
3. **Receiver:** Receiver is the person to whom the message is being sent to.
4. **Medium:** It is the medium through which the message is sent. For example: A Modem.
5. **Protocol:** These are some set of rules which govern data communication.

Uses of Computer Networks

Had it not been of high importance, nobody would have bothered connecting computers over a network. Let's start exploring the uses of Computer Networks with some traditional use cases at companies and for individuals and then move on to the recent developments in the area of mobile users and home networking.

Computer Networks: Business Applications

Following are some business applications of computer networks:

1. Resource Sharing:

The goal is to make all programs, equipments(like printers etc), and especially data, available to anyone on the network without regard to the physical location of the resource and the user.

2. Server-Client model:

One can imagine a company's information system as consisting of one or more databases and some employees who need to access it remotely. In this model, the data is stored on powerful computers called **Servers**. Often these are centrally housed and maintained by a system administrator. In contrast, the employees have simple machines, called **Clients**, on their desks, using which they access remote data.

3. Communication Medium:

A computer network can provide a powerful communication medium among employees. Virtually every company that has two or more computers now has e-mail (electronic mail), which employees generally use for a great deal of daily communication

4. eCommerce:

A goal that is starting to become more important in businesses is doing business with consumers over the Internet. Airlines, bookstores and music vendors have discovered that many customers like the convenience of shopping from home. This sector is expected to grow quickly in the future.

The most popular forms are listed in the below figure:

Tag and Full Name	Example
B2C - Business-to-Consumer	Ordering books on-line
B2B - Business-to-Business	Car manufacturer ordering tires from supplier
C2C - Consumer-to-Consumer	Auctioning second-hand products on line
G2C - Government-to-Consumer	Government distributing tax forms electronically
P2P - Peer-to-Peer	File sharing

Computer Networks: Home Applications

Some of the most important uses of the Internet for home users are as follows:

- **Access to remote information**
- **Person-to-person communication**
- **Interactive entertainment**
- **Electronic commerce**

Computer Networks: Mobile Users

Mobile computers, such as notebook computers and Mobile phones, are one of the fastest-growing segments of the entire computer industry. Although wireless networking and mobile computing are often related, they are not identical, as the below figure shows.

Wireless	Mlobile	Applications
No	No	Desktop computers in offices
No	Yes	A notebook computer used in a hotel room
Yes	No	Networks in older, unwired buildings
Yes	Yes	Portable office; PDA for store inventory

Line Configuration in Computer Networks

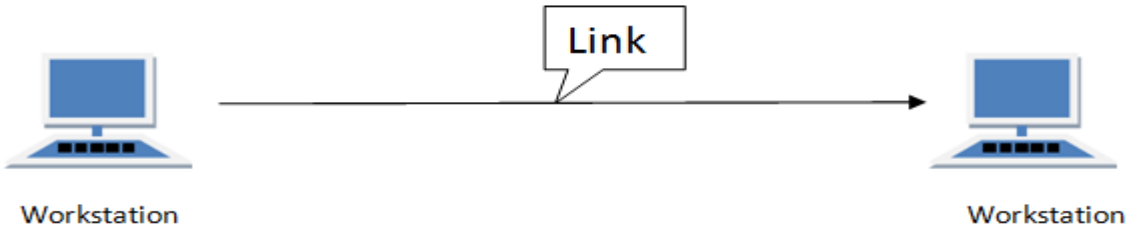
A Network is nothing but a connection made through connection links between two or more devices. Devices can be a computer, printer or any other device that is capable to send and receive data. There are two ways to connect the devices :

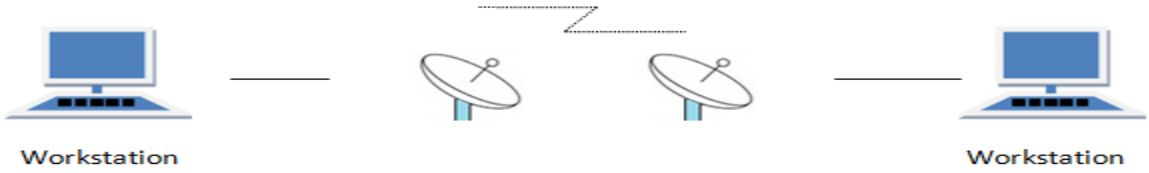
1. Point-to-Point connection
2. Multipoint connection

Point-To-Point Connection

It is a protocol which is used as a communication link between two devices. It is simple to establish. The most common example for Point-to-Point connection (PPP) is a computer connected by telephone line. We can connect the two devices by means of a pair of wires or using a microwave or satellite link.

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



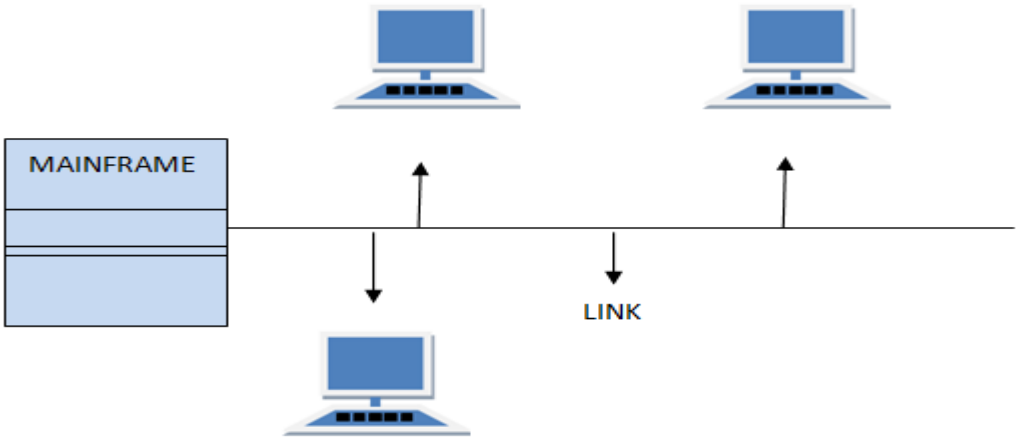


MultiPoint Connection

It is also called Multidrop configuration. In this connection two or more devices share a single link.

There are two kinds of Multipoint Connections :

- If the links are used simultaneously between many devices, then it is spatially shared line configuration.
- If user takes turns while using the link, then it is time shared (temporal) line configuration.

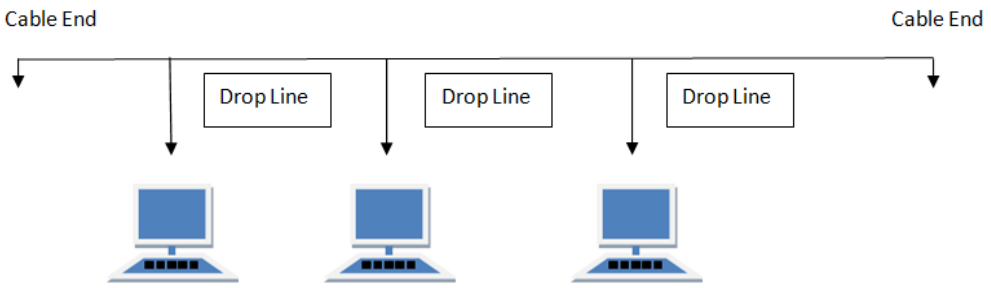


Types of Network Topology

Network Topology is the schematic description of a network arrangement, connecting various nodes(sender and receiver) through lines of connection.

BUS Topology

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called **Linear Bus topology**.



Features of Bus Topology

1. It transmits data only in one direction.
2. Every device is connected to a single cable

Advantages of Bus Topology

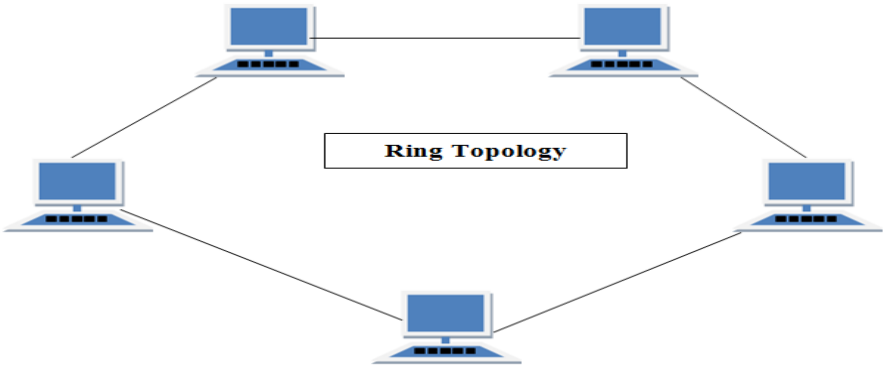
1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

Disadvantages of Bus Topology

1. Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance of the network decreases.
3. Cable has a limited length.
4. It is slower than the ring topology.

RING Topology

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbors for each device.



Features of Ring Topology

1. A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
2. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called **Dual Ring Topology**.
3. In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
4. Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

Advantages of Ring Topology

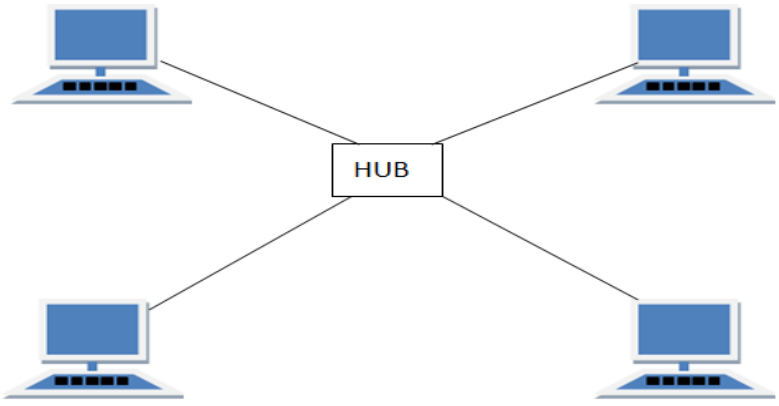
1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand

Disadvantages of Ring Topology

1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

STAR Topology

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.



Features of Star Topology

1. Every node has its own dedicated connection to the hub.
2. Hub acts as a repeater for data flow.
3. Can be used with twisted pair, Optical Fibre or coaxial cable.

Advantages of Star Topology

1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.
3. Easy to troubleshoot.
4. Easy to setup and modify.
5. Only that node is affected which has failed, rest of the nodes can work smoothly.

Disadvantages of Star Topology

1. Cost of installation is high.
2. Expensive to use.
3. If the hub fails then the whole network is stopped because all the nodes depend on the hub.
4. Performance is based on the hub that is it depends on its capacity

MESH Topology

It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has $n(n-1)/2$ physical channels to link n devices.

There are two techniques to transmit data over the Mesh topology, they are :

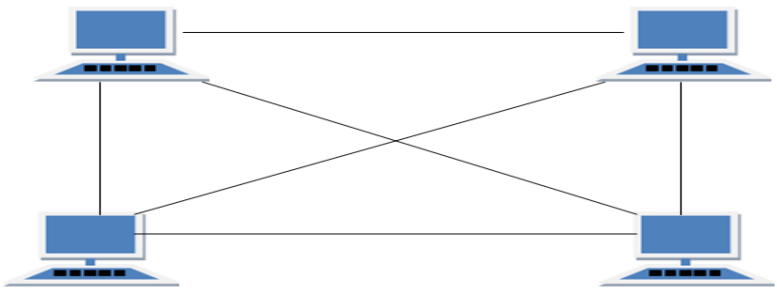
1. Routing
2. Flooding

MESH Topology: Routing

In routing, the nodes have a routing logic, as per the network requirements. Like routing logic to direct the data to reach the destination using the shortest distance. Or, routing logic which has information about the broken links, and it avoids those node etc. We can even have routing logic, to re-configure the failed nodes.

MESH Topology: Flooding

In flooding, the same data is transmitted to all the network nodes, hence no routing logic is required. The network is robust, and the its very unlikely to lose the data. But it leads to unwanted load over the network.



Types of Mesh Topology

1. **Partial Mesh Topology :** In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.
2. **Full Mesh Topology :** Each and every nodes or devices are connected to each other.

Features of Mesh Topology

1. Fully connected.
2. Robust.
3. Not flexible.

Advantages of Mesh Topology

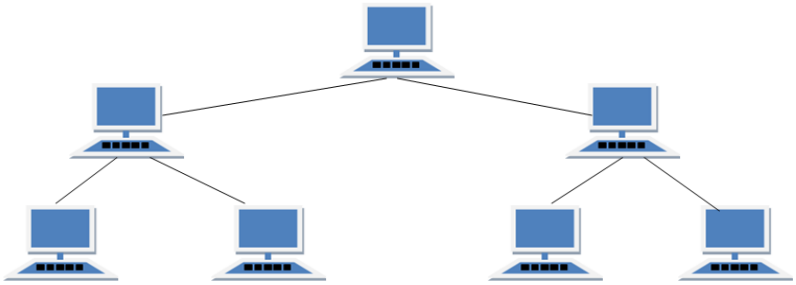
1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.

Disadvantages of Mesh Topology

1. Installation and configuration is difficult.
2. Cabling cost is more.
3. Bulk wiring is required.

TREE Topology

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.



Features of Tree Topology

1. Ideal if workstations are located in groups.
2. Used in Wide Area Network.

Advantages of Tree Topology

1. Extension of bus and star topologies.
2. Expansion of nodes is possible and easy.
3. Easily managed and maintained.
4. Error detection is easily done.

Disadvantages of Tree Topology

1. Heavily cabled.
2. Costly.
3. If more nodes are added maintenance is difficult.
4. Central hub fails, network fails.

HYBRID Topology

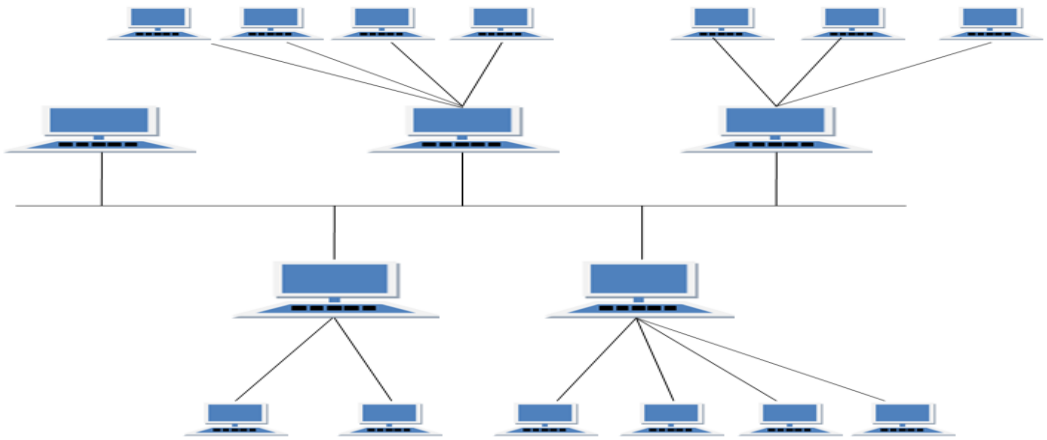
It is two different types of topologies which is a mixture of two or more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).

Features of Hybrid Topology

1. It is a combination of two or topologies
2. Inherits the advantages and disadvantages of the topologies included

Advantages of Hybrid Topology

1. Reliable as Error detecting and trouble shooting is easy.
2. Effective.
3. Scalable as size can be increased easily.
4. Flexible.



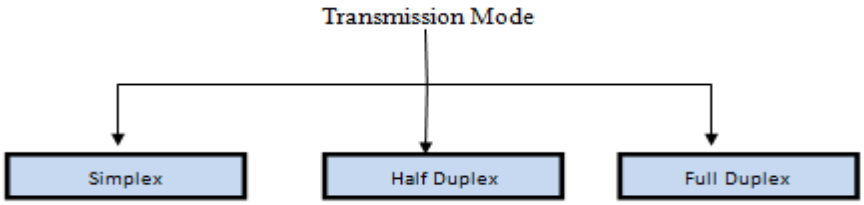
Disadvantages of Hybrid Topology

1. Complex in design.
2. Costly.

Transmission Modes in Computer Networks

Transmission mode refers to the mechanism of transferring of data between two devices connected over a network. It is also called **Communication Mode**. These modes direct the direction of flow of information. There are three types of transmission modes. They are:

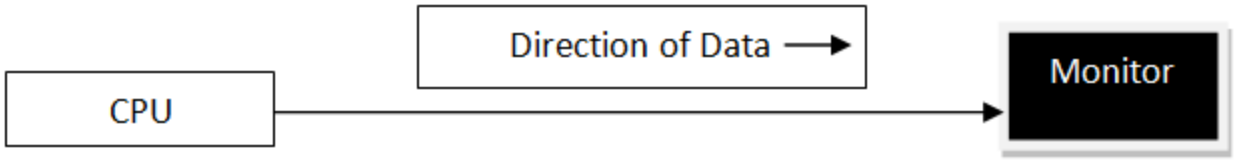
1. Simplex Mode
2. Half duplex Mode
3. Full duplex Mode



SIMPLEX Mode

In this type of transmission mode, data can be sent only in one direction i.e. communication is unidirectional. We cannot send a message back to the sender. Unidirectional communication is done in Simplex Systems where we just need to send a command/signal, and do not expect any response back.

Examples of simplex Mode are loudspeakers, television broadcasting, television and remote, keyboard and monitor etc.

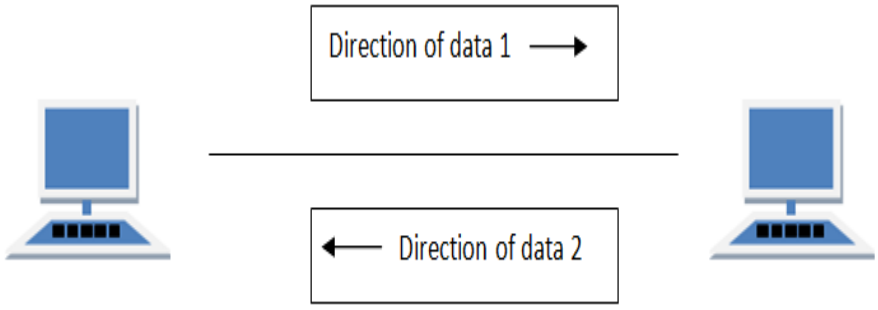


HALF DUPLEX Mode

Half-duplex data transmission means that data can be transmitted in both directions on a signal carrier, but not at the same time.

For example, on a local area network using a technology that has half-duplex transmission, one workstation can send data on the line and then immediately receive data on the line from the same direction in which data was just transmitted. Hence half-duplex transmission implies a bidirectional line (one that can carry data in both directions) but data can be sent in only one direction at a time.

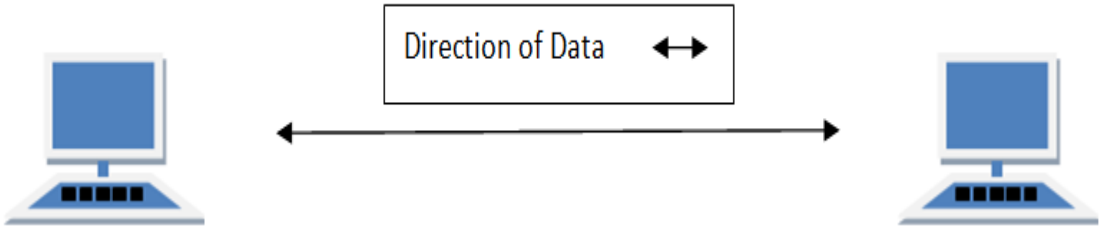
Example of half duplex is a walkie- talkie in which message is sent one at a time but messages are sent in both the directions.



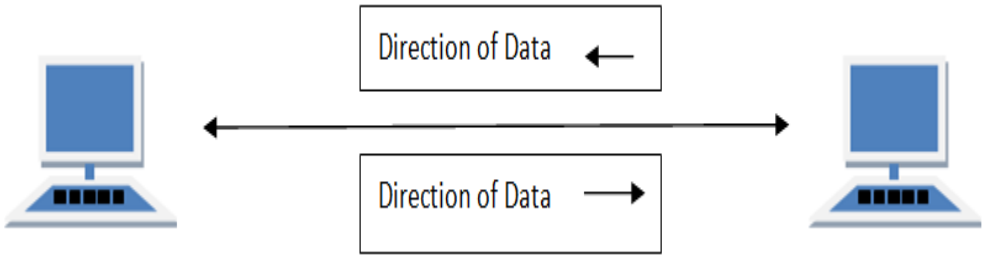
FULL DUPLEX Mode

In full duplex system we can send data in both the directions as it is bidirectional at the same time in other words, data can be sent in both directions simultaneously.

Example of Full Duplex is a Telephone Network in which there is communication between two persons by a telephone line, using which both can talk and listen at the same time.



In full duplex system there can be two lines one for sending the data and the other for receiving data.



Protocols:

In computer networks, communication occurs between entities in different systems. An **entity** is anything capable of sending or receiving information. However, two entities cannot simply send bit streams to each other and expect to be understood. For communication to occur, the entities must agree on a **protocol.**

A **protocol** is a set of rules that governs data communication. A protocol defines what is communicated, how it is communicated and what is communicated. The Key elements of a protocol are syntax, semantics and timing.

- **Syntax.** Syntax refers to the structure or format of the data, meaning the order in which they are presented. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to the address of the receiver, and the rest of the stream to the message itself.
- **Semantics**. Semantics refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation? For example, does an address identify the route to be taken or the final destination of the message?
- **Timing.** Timing refers to two characteristics: when data should be sent and how fast it can be sent. For example, if a sender produces data at 100 Megabits per second (Mbps) but the

receiver can process data at only 1 Mbps, the transmission will overload the receiver and data will be largely lost.

Standards

Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers and also in guaranteeing national and international interoperability of data and telecommunications technology and processes. They provide guidelines to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communication. Data communication standards fall into two categories: *de facto* (meaning "by fact" or "by convention") and *de jure* (meaning "by law" and "by regulation").

De facto. Standards that have not been approved by an organized body but have been adopted as standards through widespread use are **de facto standards.** De facto standards are often established originally by manufacturers that seek to define the functionality of a new product or technology.

- **De jure. De jure standards** are those that have been legislated by an officially recognized body.

Standards and Organizationsstandards are developed through cooperation of standards creation committees, forums and government regulatory agencies. Some of the standards establishment Organizations are:

- International Standards Organisation (ISO) http://www.iso.org/
- International Telecommunications Union-Telecommunication Standards Sector (ITU-T).
- American National Standard Institute (ANSI).
- Institute of Electrical and Electronics Engineers (IEEE). http://www.ieee.gov/
- Electronic Industries Association (EIA).

Forums

Telecommunications technology development is moving faster than the ability of standards committee to ratify standards. Standards committees are procedural bodies and by nature slow moving. To accommodate the need for working models and agreements and to facilitate the standardization process, many special-interest groups have developed *forums* made up of representatives from interested corporations. The forums work with universities and users to test,

evaluate and standardize new technologies. By concentrating their efforts on a particular technology, the forums are able to speed acceptance and use of those technologies in the telecommunications community. The forums present their conclusions to the standards bodies. Some important forums for the telecommunications industry include the following: **Regulatory Agencies**All communications technology is subject to regulation by government agencies such as Federal Communication Commission in the United States. The purpose of these agencies is to protect the public interest by regulating radio, television, and wire/cable communications.

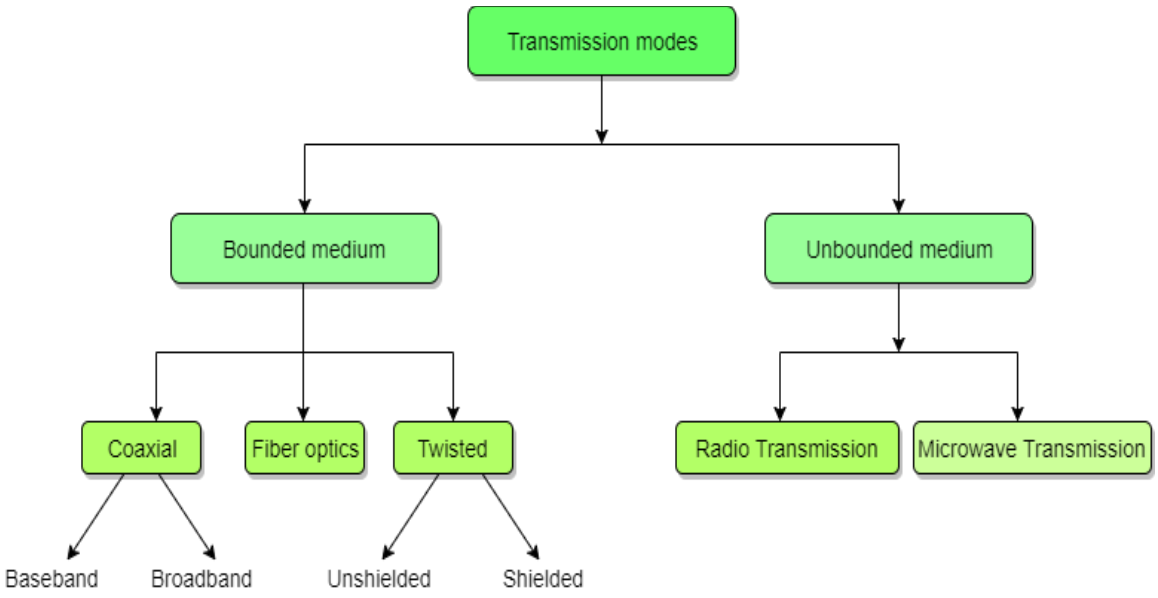
Federal Communications Commission (FCC). The Federal Communications Commission (FCC) has authority over interstate and international commerce as it relates to communications.

Transmission Mediums in Computer Networks

Data is represented by computers and other telecommunication devices using signals. Signals are transmitted in the form of electromagnetic energy from one device to another. Electromagnetic signals travel through vacuum, air or other transmission mediums to move from one point to another(from sender to receiver).

Electromagnetic energy (includes electrical and magnetic fields) consists of power, voice, visible light, radio waves, ultraviolet light, gamma rays etc.

Transmission medium is the means through which we send our data from one place to another. The first layer (physical layer) of Communication Networks OSI Seven layer model is dedicated to the transmission media.



Factors to be considered while selecting a Transmission Medium

1. Transmission Rate
2. Cost and Ease of Installation
3. Resistance to Environmental Conditions
4. Distances

Bounded or Guided Transmission Media

Guided media, which are those that provide a conduit from one device to another, include **Twisted-Pair Cable**, **Coaxial Cable**, and **Fibre-Optic Cable**.

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

Twisted Pair Cable

This cable is the most commonly used and is cheaper than others. It is lightweight, cheap, can be installed easily, and they support many different types of network. Some important points :

- Its frequency range is 0 to 3.5 kHz.
- Typical attenuation is 0.2 dB/Km @ 1kHz.
- Typical delay is 50 μs/km.
- Repeater spacing is 2km.

A twisted pair consists of two

conductors (normally copper), each with its own plastic insulation, twisted together. One of these wires is used to carry signals to the receiver, and the other is used only as ground reference. The receiver uses the difference between the two. In addition to the signal sent by the sender on one of the wires, interference(noise) and crosstalk may affect both wires and create 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 noise or crosstalk sources. This results in a difference at the receiver.

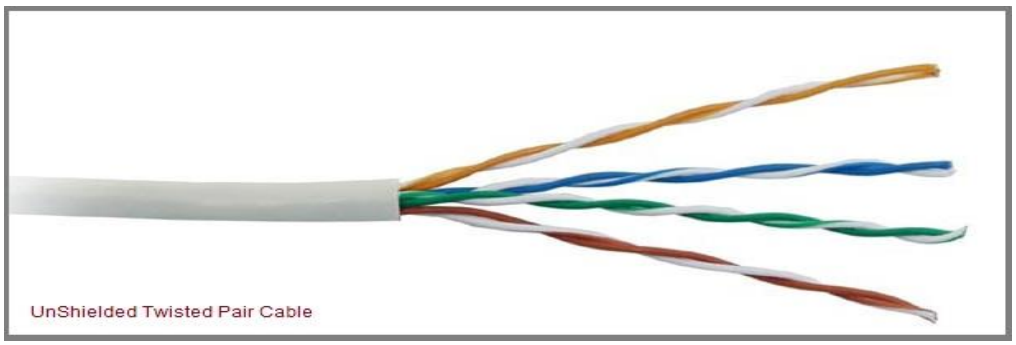
Twisted Pair is of two types:

- **Unshielded Twisted Pair (UTP)**
- **Shielded Twisted Pair (STP)**

Unshielded Twisted Pair Cable

It is the most common type of telecommunication when compared with Shielded Twisted Pair Cable which consists of two conductors usually copper, each with its own colour plastic insulator. Identification is the reason behind coloured plastic insulation.

UTP cables consist of 2 or 4 pairs of twisted cable. Cable with 2 pair use **RJ-11** connector and 4 pair cable use **RJ-45** connector.



Advantages of Unshielded Twisted Pair Cable

- Installation is easy
- Flexible
- Cheap
- It has high speed capacity,
- 100 meter limit
- Higher grades of UTP are used in LAN technologies like Ethernet.

It consists of two insulating copper wires (1mm thick). The wires are twisted together in a helical form to reduce electrical interference from similar pair.

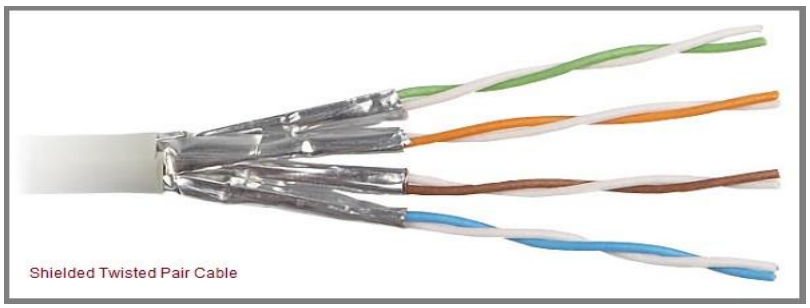
Disadvantages of Unshielded Twisted Pair Cable

- Bandwidth is low when compared with Coaxial Cable
- Provides less protection from interference.

Shielded Twisted Pair Cable

This cable has a metal foil or braided-mesh covering which encases each pair of insulated conductors. Electromagnetic noise penetration is prevented by metal casing. Shielding also eliminates crosstalk (explained in KEY TERMS Chapter).

It has same attenuation as unshielded twisted pair. It is faster the unshielded and coaxial cable. It is more expensive than coaxial and unshielded twisted pair.



Advantages of Shielded Twisted Pair Cable

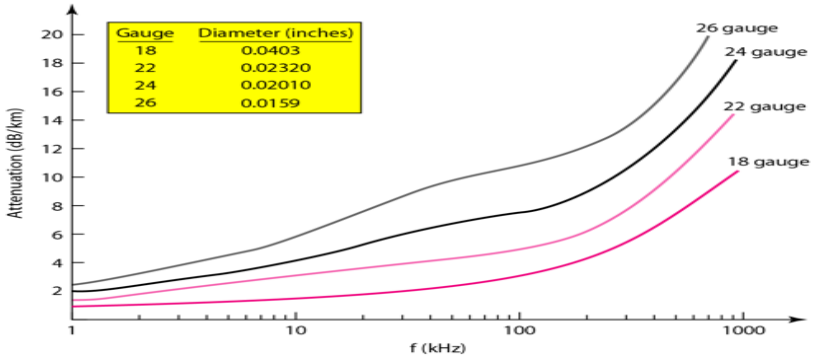
- Easy to install
- Performance is adequate
- Can be used for Analog or Digital transmission
- Increases the signalling rate
- Higher capacity than unshielded twisted pair
- Eliminates crosstalk

Disadvantages of Shielded Twisted Pair Cable

- Difficult to manufacture
- Heavy

Performance of Shielded Twisted Pair Cable

One way to measure the performance of twisted-pair cable is to compare attenuation versus frequency and distance. As shown in the below figure, a twisted-pair cable can pass a wide range of frequencies. However, with increasing frequency, the attenuation, measured in decibels per kilometre (dB/km), sharply increases with frequencies above 100kHz. Note that gauge is a measure of the thickness of the wire.



Applications of Shielded Twisted Pair Cable

- In telephone lines to provide voice and data channels. The DSL lines that are used by the telephone companies to provide high-data-rate connections also use the high-bandwidth capability of unshielded twisted-pair cables.
- Local Area Network, such as 10Base-T and 100Base-T, also use twisted-pair cables.

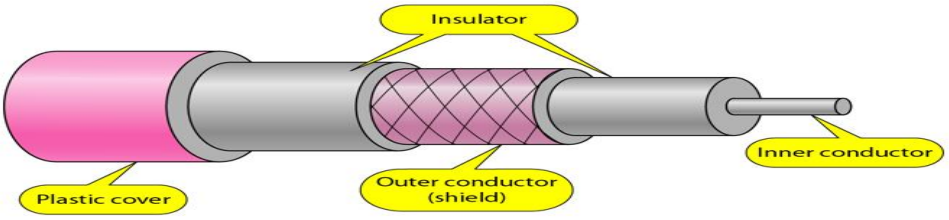
Coaxial Cable

Coaxial is called by this name because it contains two conductors that are parallel to each other. Copper is used in this as centre conductor which can be a solid wire or a standard one. It is surrounded by PVC installation, a sheath which is encased in an outer conductor of metal foil, braid or both.

Outer metallic wrapping is used as a shield against noise and as the second conductor which completes the circuit. The outer conductor is also encased in an insulating sheath. The outermost part is the plastic cover which protects the whole cable.

Here the most common coaxial standards.

- 50-Ohm RG-7 or RG-11 : used with thick Ethernet.
- 50-Ohm RG-58 : used with thin Ethernet
- 75-Ohm RG-59 : used with cable television
- 93-Ohm RG-62 : used with ARCNET.



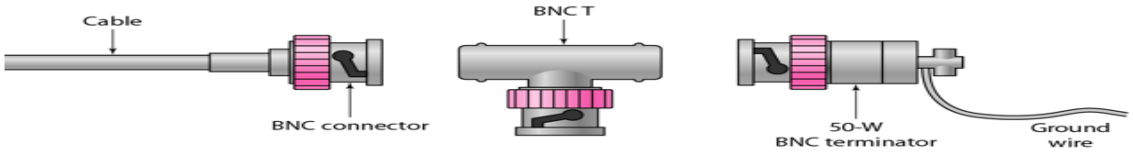
Coaxial Cable Standards

Coaxial cables are categorized by their Radio Government(RG) ratings. Each RG number denotes a unique set of physical specifications, including the wire gauge of the inner conductor, the thickness and the type of the inner insulator, the construction of the shield, and the size and type of the outer casing. Each cable defined by an RG rating is adapted for a specialized function, as shown in the table below:

Category	*Impedance*	*Use*
RG-59	75 Ω	Cable TV
RG-58	50 Ω	Thin Ethernet
RG-11	50 Ω	Thick Ethernet

Coaxial Cable Connectors

To connect coaxial cable to devices, we need coaxial connectors. The most common type of connector used today is the Bayonet Neill-Concelman (BNC) connector. The below figure shows 3 popular types of these connectors: the BNC Connector, the BNC T connector and the BNC terminator.



The BNC connector is used to connect the end of the cable to the device, such as a TV set. The BNC T connector is used in Ethernet networks to branch out to a connection to a computer or other device. The BNC terminator is used at the end of the cable to prevent the reflection of the signal.

There are two types of Coaxial cables:

1. BaseBand

This is a 50 ohm (Ω) coaxial cable which is used for digital transmission. It is mostly used for LAN's. Baseband transmits a single signal at a time with very high speed. The major drawback is that it needs amplification after every 1000 feet.

2. BroadBand

This uses analog transmission on standard cable television cabling. It transmits several simultaneous signal using different frequencies. It covers large area when compared with Baseband Coaxial Cable.

Advantages of Coaxial Cable

- Bandwidth is high
- Used in long distance telephone lines.

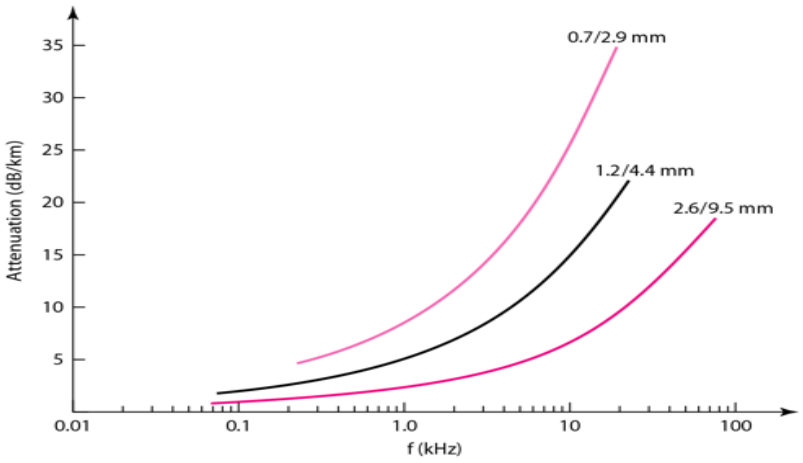
- Transmits digital signals at a very high rate of 10Mbps.
- Much higher noise immunity
- Data transmission without distortion.
- The can span to longer distance at higher speeds as they have better shielding when compared to twisted pair cable

Disadvantages of Coaxial Cable

- Single cable failure can fail the entire network.
- Difficult to install and expensive when compared with twisted pair.
- If the shield is imperfect, it can lead to grounded loop.

Performance of Coaxial Cable

We can measure the performance of a coaxial cable in same way as that of Twisted Pair Cables. From the below figure, it can be seen that the attenuation is much higher in coaxial cable than in twisted-pair cable. In other words, although coaxial cable has a much higher bandwidth, the signal weakens rapidly and requires the frequent use of repeaters.



Applications of Coaxial Cable

- Coaxial cable was widely used in analog telephone networks, where a single coaxial network could carry 10,000 voice signals.
- Cable TV networks also use coaxial cables. In the traditional cable TV network, the entire network used coaxial cable. Cable TV uses RG-59 coaxial cable.
- In traditional Ethernet LANs. Because of it high bandwidth, and consequence high data rate, coaxial cable was chosen for digital transmission in early Ethernet LANs. The 10Base-2, or

Thin Ethernet, uses RG-58 coaxial cable with BNC connectors to transmit data at 10Mbps with a range of 185 m.

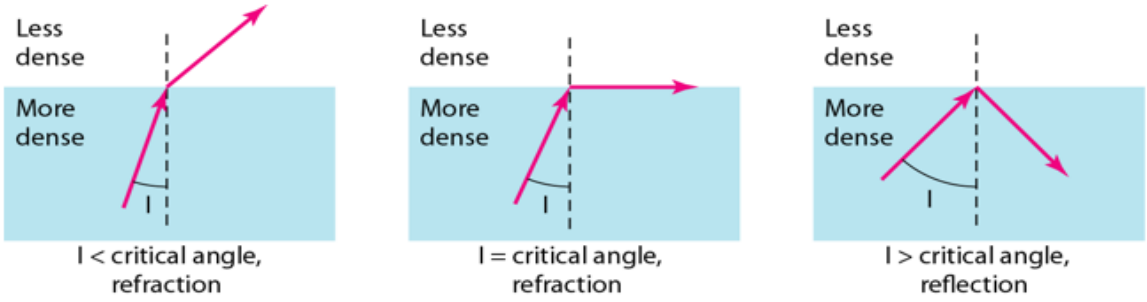
Fiber Optic Cable

A fibre-optic cable is made of glass or plastic and transmits signals in the form of light.

For better understanding we first need to explore several aspects of the **nature of light**.

Light travels in a straight line as long as it is mobbing through a single uniform substance. If ray of light travelling through one substance suddenly enters another substance (of a different density), the ray changes direction.

The below figure shows how a ray of light changes direction when going from a more dense to a less dense substance.



Bending of a light ray

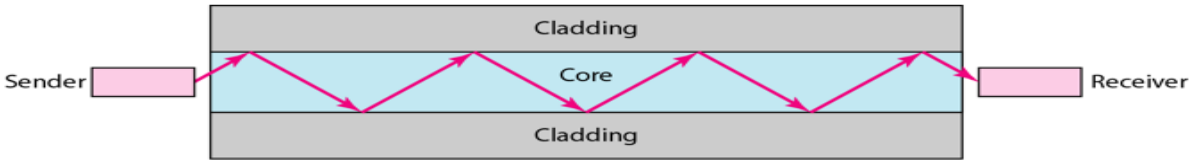
As the figure shows:

- If the **angle of incidence I**(the angle the ray makes with the line perpendicular to the interface between the two substances) is **less** than the **critical angle**, the ray **refracts** and moves closer to the surface.
- If the angle of incidence is **greater** than the critical angle, the ray **reflects**(makes a turn) and travels again in the denser substance.
- If the angle of incidence is **equal** to the critical angle, the ray refracts and **moves parallel** to the surface as shown.

Note: *The critical angle is a property of the substance, and its value differs from one substance to another.*

Optical fibres use reflection to guide light through a channel. A glass or plastic core is surrounded by a cladding of less dense glass or plastic. The difference in density of the two

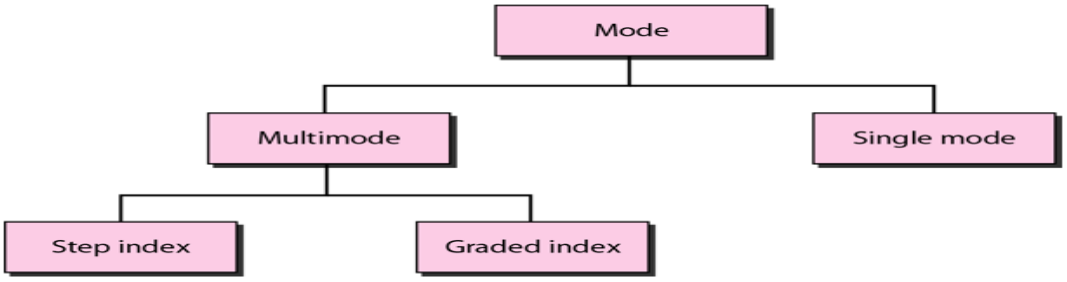
materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it.



Internal view of an Optical fibre

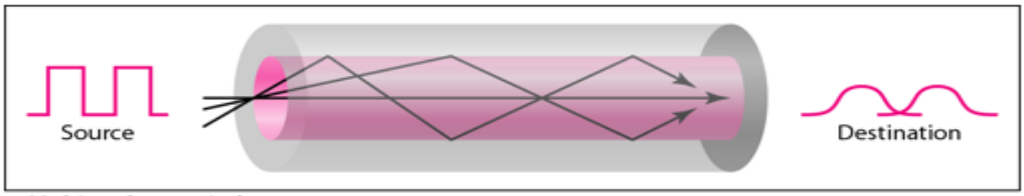
Propagation Modes of Fiber Optic Cable

Current technology supports two modes(**Multimode** and **Single mode**) for propagating light along optical channels, each requiring fibre with different physical characteristics. Multimode can be implemented in two forms: **Step-index** and **Graded-index**.

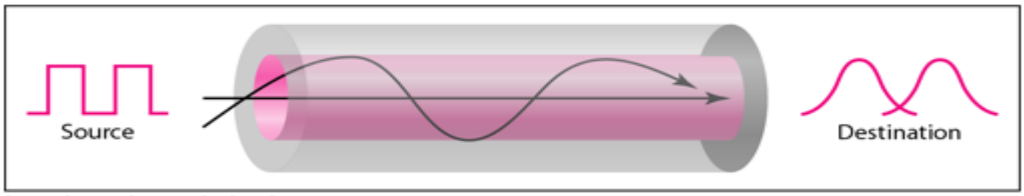


Multimode Propagation Mode

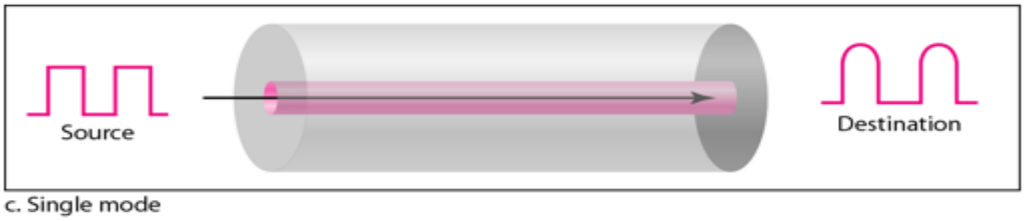
Multimode is so named because multiple beams from a light source move through the core in different paths. How these beams move within the cable depends on the structure of the core as shown in the below figure.



a. Multimode, step index



b. Multimode, graded index



c. Single mode

- In **multimode step-index fibre**, the density of the core remains constant from the centre to the edges. A beam of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding. The term step-index refers to the suddenness of this change, which contributes to the distortion of the signal as it passes through the fibre.
- In **multimode graded-index fibre**, this distortion gets decreases through the cable. The word index here refers to the index of refraction. This index of refraction is related to the density. A graded-index fibre, therefore, is one with varying densities. Density is highest at the centre of the core and decreases gradually to its lowest at the edge.

Single Mode

Single mode uses step-index fibre and a highly focused source of light that limits beams to a small range of angles, all close to the horizontal. The single-mode fibre itself is manufactured with a much smaller diameter than that of multimode fibre, and with substantially lower density. The decrease in density results in a critical angle that is close enough to 90 degree to make the propagation of beams almost horizontal.

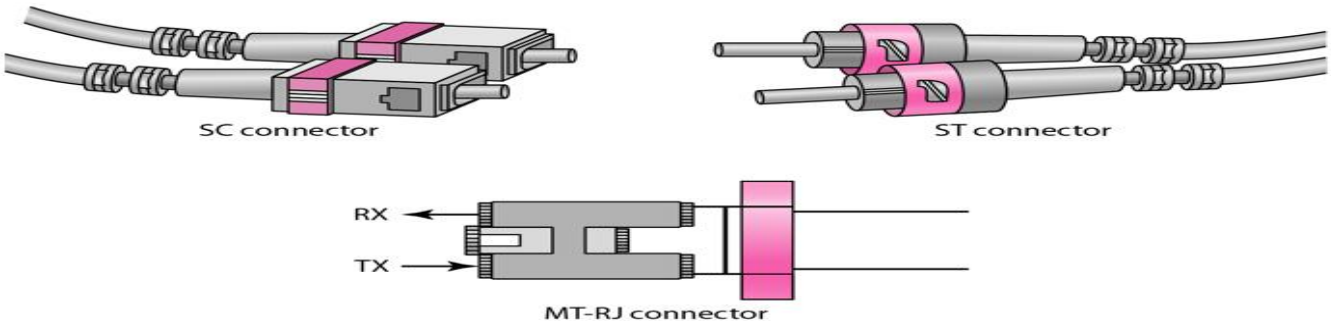
Fibre Sizes for Fiber Optic Cable

Optical fibres are defined by the ratio of the diameter or their core to the diameter of their cladding, both expressed in micrometers. The common sizes are shown in the figure below:

Type	*Core (µm)*	*Cladding (µm)*	*Mode*
50/125	50.0	125	Multimode, graded index
62.5/125	62.5	125	Multimode, graded index
100/125	100.0	125	Multimode, graded index
7/125	7.0	125	Single mode

Fibre Optic Cable Connectors

There are three types of connectors for fibre-optic cables, as shown in the figure below.



The **Subscriber Channel(SC)** connector is used for cable TV. It uses push/pull locking system. The **Straight-Tip(ST)** connector is used for connecting cable to the networking devices. MT-RJ is a connector that is the same size as RJ45.

Advantages of Fibre Optic Cable

Fibre optic has several advantages over metallic cable:

- Higher bandwidth
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials
- Light weight
- Greater immunity to tapping

Disadvantages of Fibre Optic Cable

There are some disadvantages in the use of optical fibre:

- Installation and maintenance
- Unidirectional light propagation
- High Cost

Performance of Fibre Optic Cable

Attenuation is flatter than in the case of twisted-pair cable and coaxial cable. The performance is such that we need fewer(actually one tenth as many) repeaters when we use the fibre-optic cable.

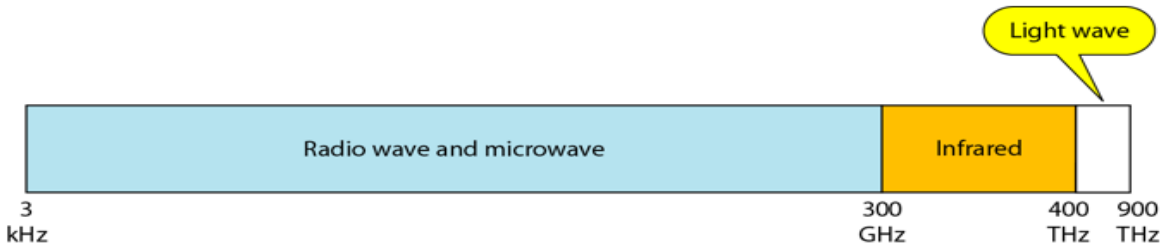
Applications of Fibre Optic Cable

- Often found in backbone networks because its wide bandwidth is cost-effective.
- Some cable TV companies use a combination of optical fibre and coaxial cable thus creating a hybrid network.
- Local-area Networks such as 100Base-FX network and 1000Base-X also use fibre-optic cable.

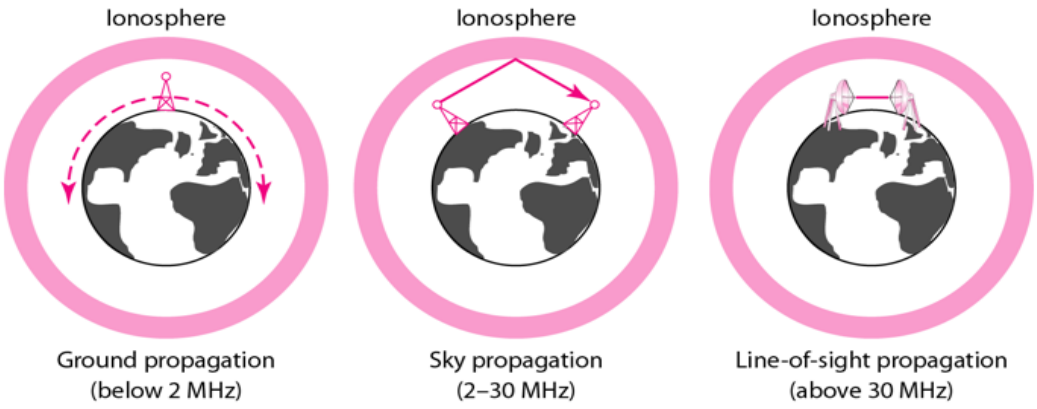
UnBounded or UnGuided Transmission Media

Unguided medium transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication. Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.

The below figure shows the part of the electromagnetic spectrum, ranging from 3 kHz to 900 THz, used for wireless communication.



Unguided signals can travel from the source to the destination in several ways: **Ground propagation**, **Sky propagation** and **Line-of-sight propagation** as shown in below figure.



Propagation Modes

- **Ground Propagation:** In this, radio waves travel through the lowest portion of the atmosphere, hugging the Earth. These low-frequency signals emanate in all directions from the transmitting antenna and follow the curvature of the planet.
- **Sky Propagation:** In this, higher-frequency radio waves radiate upward into the ionosphere where they are reflected back to Earth. This type of transmission allows for greater distances with lower output power.
- **Line-of-sight Propagation:** in this type, very high-frequency signals are transmitted in straight lines directly from antenna to antenna.

We can divide wireless transmission into three broad groups:

1. Radio waves
2. Micro waves
3. Infrared waves

Radio Waves

Electromagnetic waves ranging in frequencies between 3 KHz and 1 GHz are normally called radio waves.

Radio waves are omnidirectional. When an antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned. A sending antenna send waves that can be received by any receiving antenna. The omnidirectional property has disadvantage, too. The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signal suing the same frequency or band.

Radio waves, particularly with those of low and medium frequencies, can penetrate walls. This characteristic can be both an advantage and a disadvantage. It is an advantage because, an AM

radio can receive signals inside a building. It is a disadvantage because we cannot isolate a communication to just inside or outside a building.

Omnidirectional Antenna for Radio Waves

Radio waves use omnidirectional antennas that send out signals in all directions.

Applications of Radio Waves

- The omnidirectional characteristics of radio waves make them useful for multicasting in which there is one sender but many receivers.
- AM and FM radio, television, maritime radio, cordless phones, and paging are examples of multicasting.

Micro Waves

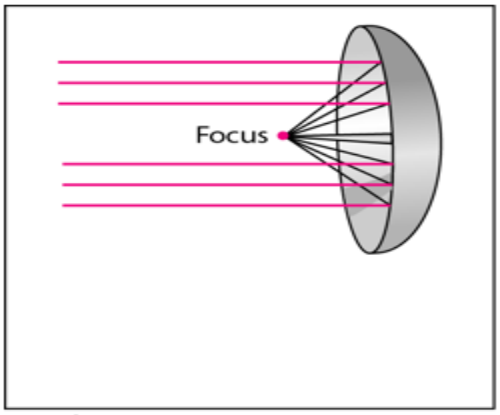
Electromagnetic waves having frequencies between 1 and 300 GHz are called micro waves. Micro waves are unidirectional. When an antenna transmits microwaves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned. The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas.

The following describes some characteristics of microwaves propagation:

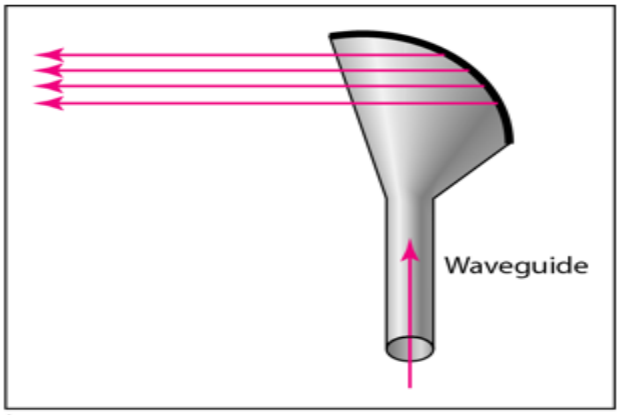
- Microwave propagation is line-of-sight. Since the towers with the mounted antennas need to be in direct sight of each other, towers that are far apart need to be very tall.
- Very high-frequency microwaves cannot penetrate walls. This characteristic can be a disadvantage if receivers are inside the buildings.
- The microwave band is relatively wide, almost 299 GHz. Therefore, wider sub-bands can be assigned and a high date rate is possible.
- Use of certain portions of the band requires permission from authorities.

Unidirectional Antenna for Micro Waves

Microwaves need unidirectional antennas that send out signals in one direction. Two types of antennas are used for microwave communications: **Parabolic Dish** and **Horn**.



a. Dish antenna



b. Horn antenna

A parabolic antenna works as a funnel, catching a wide range of waves and directing them to a common point. In this way, more of the signal is recovered than would be possible with a single-point receiver.

A horn antenna looks like a gigantic scoop. Outgoing transmissions are broadcast up a stem and deflected outward in a series of narrow parallel beams by the curved head. Received transmissions are collected by the scooped shape of the horn, in a manner similar to the parabolic dish, and are deflected down into the stem.

Applications of Micro Waves

Microwaves, due to their unidirectional properties, are very useful when unicast(one-to-one) communication is needed between the sender and the receiver. They are used in cellular phones, satellite networks and wireless LANs.

There are 2 types of Microwave Transmission:

1. Terrestrial Microwave
2. Satellite Microwave

Advantages of Microwave Transmission

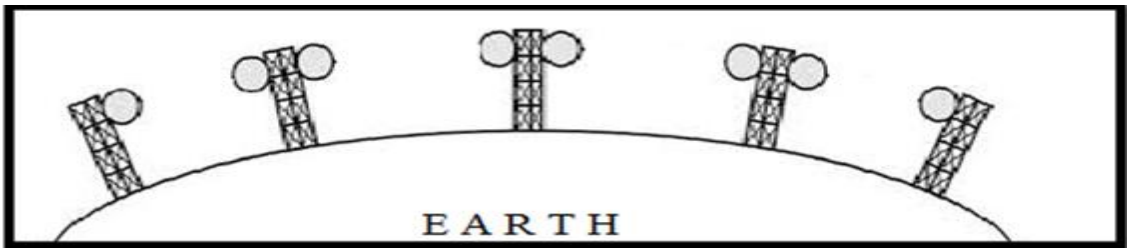
- Used for long distance telephone communication
- Carries 1000's of voice channels at the same time

Disadvantages of Microwave Transmission

- It is very costly

Terrestrial Microwave

For increasing the distance served by terrestrial microwave, repeaters can be installed with each antenna .The signal received by an antenna can be converted into transmittable form and relayed to next antenna as shown in below figure. It is an example of telephone systems all over the world



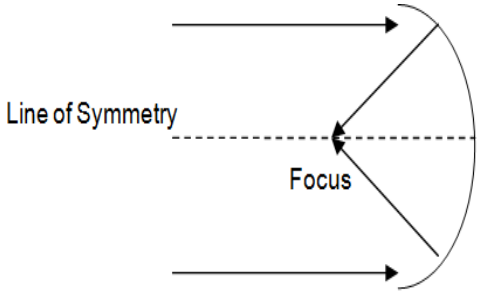
There are **two types of antennas** used for terrestrial microwave communication :

1. Parabolic Dish Antenna

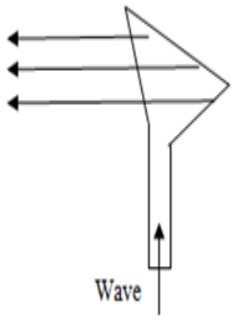
In this every line parallel to the line of symmetry reflects off the curve at angles in a way that they intersect at a common point called focus. This antenna is based on geometry of parabola.

2. Horn Antenna

It is a like gigantic scoop. The outgoing transmissions are broadcast up a stem and deflected outward in a series of narrow parallel beams by curved head.



Parabolic dish antenna

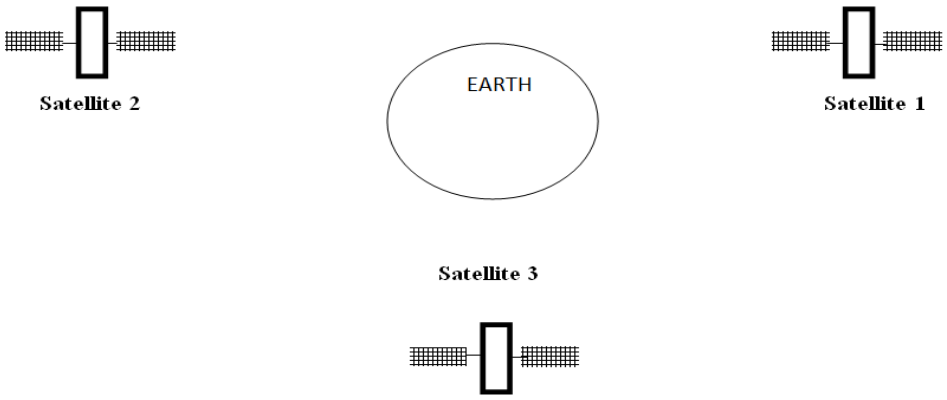


Horn Antenna

Satellite Microwave

This is a microwave relay station which is placed in outer space. The satellites are launched either by rockets or space shuttles carry them.

These are positioned 36000 Km above the equator with an orbit speed that exactly matches the rotation speed of the earth. As the satellite is positioned in a geo-synchronous orbit, it is stationery relative to earth and always stays over the same point on the ground. This is usually done to allow ground stations to aim antenna at a fixed point in the sky.



Features of Satellite Microwave

- Bandwidth capacity depends on the frequency used.
- Satellite microwave deployment for orbiting satellite is difficult.

Advantages of Satellite Microwave

- Transmitting station can receive back its own transmission and check whether the satellite has transmitted information correctly.
- A single microwave relay station which is visible from any point.

Disadvantages of Satellite Microwave

- Satellite manufacturing cost is very high
- Cost of launching satellite is very expensive
- Transmission highly depends on whether conditions, it can go down in bad weather

Infrared Waves

Infrared waves, with frequencies from 300 GHz to 400 THz, can be used for short-range communication. Infrared waves, having high frequencies, cannot penetrate walls. This advantageous characteristic prevents interference between one system and another, a short-range communication system in on room cannot be affected by another system in the next room.

When we use infrared remote control, we do not interfere with the use of the remote by our neighbours. However, this same characteristic makes infrared signals useless for long-range communication. In addition, we cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.

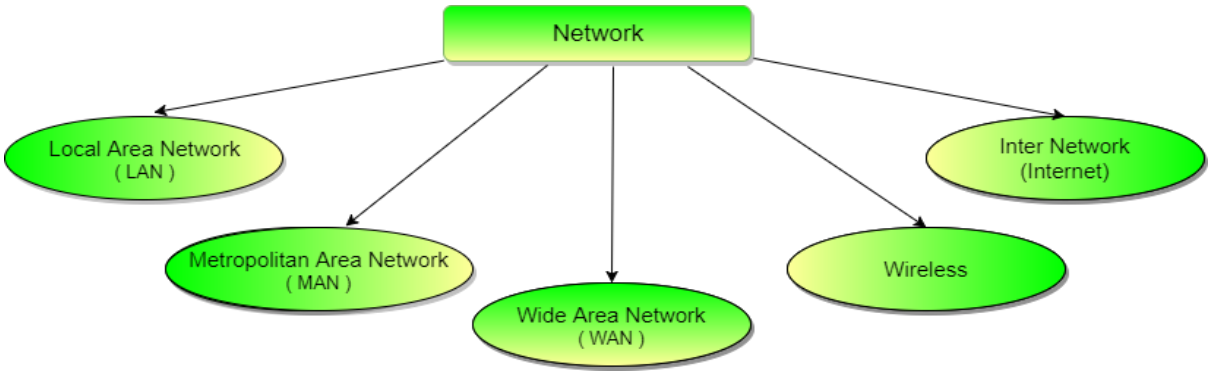
Applications of Infrared Waves

- The infrared band, almost 400 THz, has an excellent potential for data transmission. Such a wide bandwidth can be used to transmit digital data with a very high data rate.
- The Infrared Data Association(IrDA), an association for sponsoring the use of infrared waves, has established standards for using these signals for communication between devices such as keyboards, mouse, PCs and printers.
- Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation.

Types of Communication Networks

Communication Networks can be of following 5 types:

1. Local Area Network (LAN)
2. Metropolitan Area Network (MAN)
3. Wide Area Network (WAN)
4. Wireless
5. Inter Network (Internet)

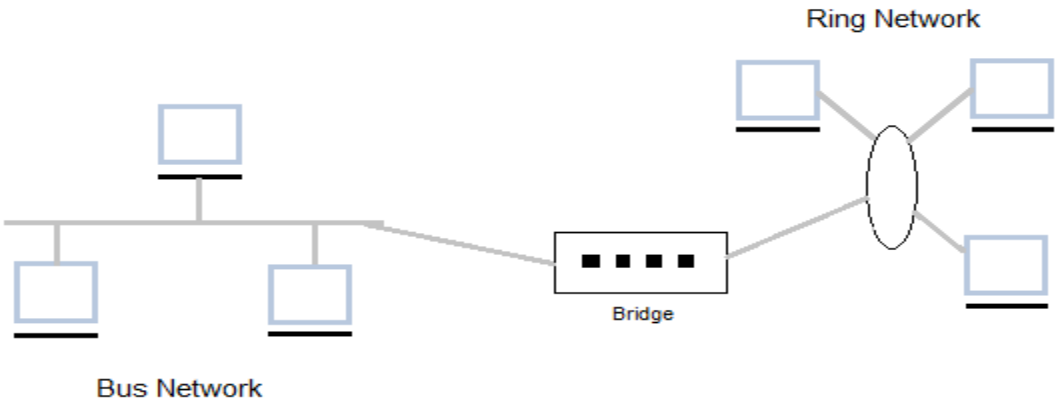


Local Area Network (LAN)

It is also called LAN and designed for small physical areas such as an office, group of buildings or a factory. LANs are used widely as it is easy to design and to troubleshoot. Personal computers and workstations are connected to each other through LANs. We can use different types of topologies through LAN, these are Star, Ring, Bus, Tree etc.

LAN can be a simple network like connecting two computers, to share files and network among each other while it can also be as complex as interconnecting an entire building.

LAN networks are also widely used to share resources like printers, shared hard-drive etc.



(Different Topologies interconnected in a Local Area Network)

Characteristics of LAN

- LAN's are private networks, not subject to tariffs or other regulatory controls.
- LAN's operate at relatively high speed when compared to the typical WAN.
- There are different types of Media Access Control methods in a LAN, the prominent ones are Ethernet, Token ring.
- It connects computers in a single building, block or campus, i.e. they work in a restricted geographical area.

Applications of LAN

- One of the computers in a network can become a server serving all the remaining computers called clients. Software can be stored on the server and it can be used by the remaining clients.
- Connecting locally all the workstations in a building to let them communicate with each other locally without any internet access.
- Sharing common resources like printers etc are some common applications of LAN.

Advantages of LAN

- **Resource Sharing:** Computer resources like printers, modems, DVD-ROM drives and hard disks can be shared with the help of local area networks. This reduces cost and hardware purchases.

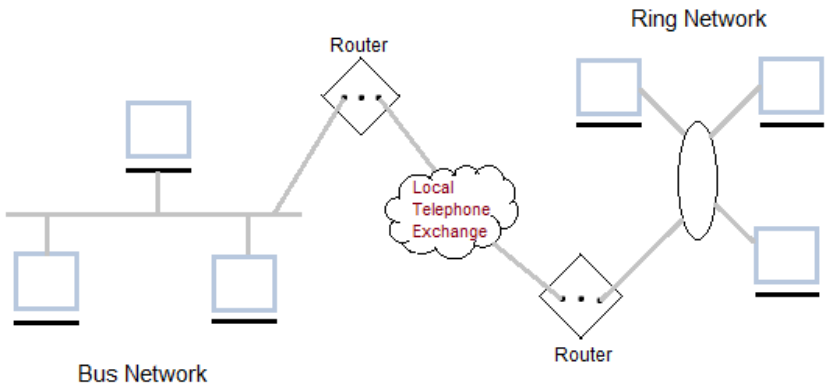
- **Software Applications Sharing:** It is cheaper to use same software over network instead of purchasing separate licensed software for each client a network.
- **Easy and Cheap Communication:** Data and messages can easily be transferred over networked computers.
- **Centralized Data:** The data of all network users can be saved on hard disk of the server computer. This will help users to use any workstation in a network to access their data. Because data is not stored on workstations locally.
- **Data Security:** Since, data is stored on server computer centrally, it will be easy to manage data at only one place and the data will be more secure too.
- **Internet Sharing:** Local Area Network provides the facility to share a single internet connection among all the LAN users. In Net Cafes, single internet connection sharing system keeps the internet expenses cheaper.

Disadvantages of LAN

- **High Setup Cost:** Although the LAN will save cost over time due to shared computer resources, but the initial setup costs of installing Local Area Networks is high.
- **Privacy Violations:** The LAN administrator has the rights to check personal data files of each and every LAN user. Moreover he can check the internet history and computer use history of the LAN user.
- **Data Security Threat:** Unauthorized users can access important data of an organization if centralized data repository is not secured properly by the LAN administrator.
- **LAN Maintenance Job:** Local Area Network requires a LAN Administrator because, there are problems of software installations or hardware failures or cable disturbances in Local Area Network. A LAN Administrator is needed at this full time job.
- **Covers Limited Area:** Local Area Network covers a small area like one office, one building or a group of nearby buildings.

Metropolitan Area Network (MAN)

It was developed in 1980s.It is basically a bigger version of LAN. It is also called MAN and uses the similar technology as LAN. It is designed to extend over the entire city. It can be means to connecting a number of LANs into a larger network or it can be a single cable. It is mainly hold and operated by single private company or a public company.



Characteristics of MAN

- It generally covers towns and cities (50 km)
- Communication medium used for MAN are optical fibers, cables etc.
- Data rates adequate for distributed computing applications.

Advantages of MAN

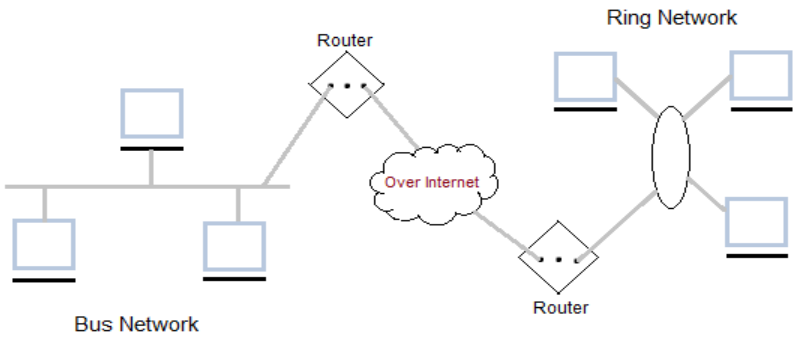
- Extremely efficient and provide fast communication via high-speed carriers, such as fibre optic cables.
- It provides a good back bone for large network and provides greater access to WANs.
- The dual bus used in MAN helps the transmission of data in both directions simultaneously.
- A MAN usually encompasses several blocks of a city or an entire city.

Disadvantages of MAN

- More cable required for a MAN connection from one place to another.
- It is difficult to make the system secure from hackers and industrial espionage(spying) graphical regions.

Wide Area Network (WAN)

It is also called WAN. WAN can be private or it can be public leased network. It is used for the network that covers large distance such as cover states of a country. It is not easy to design and maintain. Communication medium used by WAN are PSTN or Satellite links. WAN operates on low data rates.



Characteristics of WAN

- It generally covers large distances(states, countries, continents).
- Communication medium used are satellite, public telephone networks which are connected by routers.

Advantages of WAN

- Covers a large geographical area so long distance business can connect on the one network.
- Shares software and resources with connecting workstations.
- Messages can be sent very quickly to anyone else on the network. These messages can have picture, sounds or data included with them(called attachments).
- Expensive things(such as printers or phone lines to the internet) can be shared by all the computers on the network without having to buy a different peripheral for each computer.
- Everyone on the network can use the same data. This avoids problems where some users may have older information than others.

Disadvantages of WAN

- Need a good firewall to restrict outsiders from entering and disrupting the network.
- Setting up a network can be an expensive, slow and complicated. The bigger the network the more expensive it is.
- Once set up, maintaining a network is a full-time job which requires network supervisors and technicians to be employed.
- Security is a real issue when many different people have the ability to use information from other computers. Protection against hackers and viruses adds more complexity and expense.

Wireless Network

Digital wireless communication is not a new idea. Earlier, **Morse code** was used to implement wireless networks. Modern digital wireless systems have better performance, but the basic idea is the same.

Wireless Networks can be divided into three main categories:

1. **System interconnection**
2. **Wireless LANs**
3. **Wireless WANs**

System Interconnection

System interconnection is all about interconnecting the components of a computer using **short-range radio**. Some companies got together to design a short-range wireless network called **Bluetooth** to connect various components such as monitor, keyboard, mouse and printer, to the main unit, without wires. Bluetooth also allows digital cameras, headsets, scanners and other devices to connect to a computer by merely being brought within range.

In simplest form, system interconnection networks use the master-slave concept. The system unit is normally the **master**, talking to the mouse, keyboard, etc. as **slaves**.

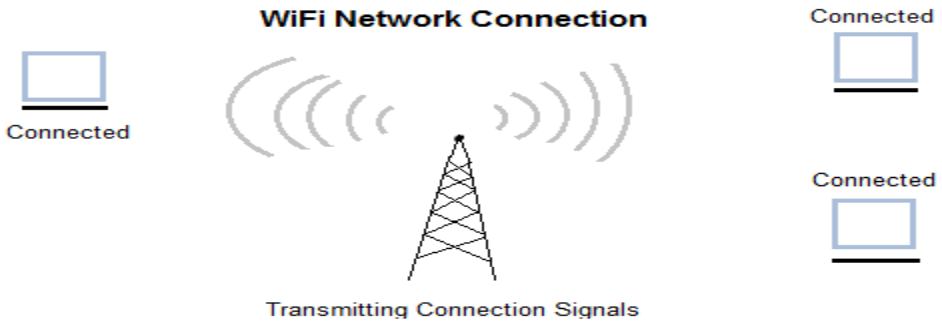
Wireless LANs

These are the systems in which every computer has a **radio modem** and **antenna** with which it can communicate with other systems. Wireless LANs are becoming increasingly common in small offices and homes, where installing **Ethernet** is considered too much trouble. There is a standard for wireless LANs called **IEEE 802.11**, which most systems implement and which is becoming very widespread.

Wireless WANs

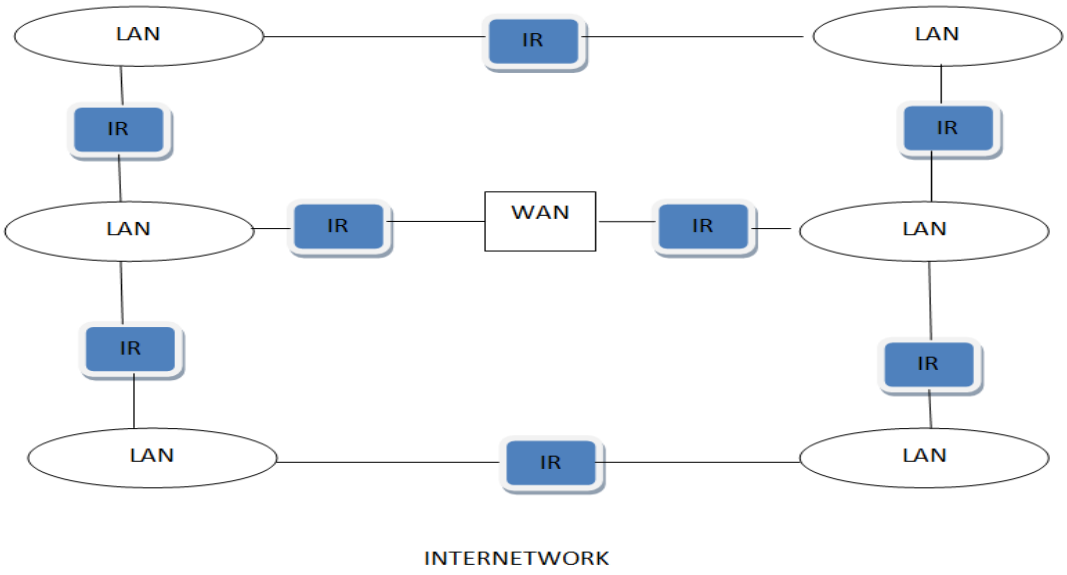
The radio network used for cellular telephones is an example of a low-bandwidth wireless WAN. This system has already gone through three generations.

- The first generation was analog and for voice only.
- The second generation was digital and for voice only.
- The third generation is digital and is for both voice and data.



Inter Network

Inter Network or Internet is a combination of two or more networks. Inter network can be formed by joining two or more individual networks by means of various devices such as routers, gateways and bridges.



THEINTERNET: An internet (*note the lowercase i*)istwoor morenetworks thatcan communicatewith eachother. Themostnotableinternetiscalledthe **Internet**(*uppercaseI*), andis composed**of t**housands ofinterconnected networks.

Internet containsseveral backbones, providernetworks,and customer networks.

Atthetoplevel, the*backbones*arelargenetworksownedbysome communicationcompaniessuchasSprint,Verizon(MCI),AT&T,and NTT. The backbonenetworksareconnectedthrough somecomplexswitchingsystems,called *peering points*.

Atthesecondlevel,therearesmallernetworks,called*providernetworks* thatusethe servicesofthebackbonesforafee.Theprovidernetworksare connectedto backbones andsometimes to other provider networks.

The*customernetworks*arenetworksattheedgeofthe Internet thatactually usetheservicesprovided by theInternet.They pay feestoprovidernetworksfor receivingservices.

Backbones and provider networksarealsocalledInternet**ServiceProviders(ISPs).** Thebackbonesareoftenreferredto as*internationalISPs;*the provider networks areoften referred to as *national*or *regionalISPs*.

INTERNET HISTORY:

EarlyHistory: There weresomecommunicationnetworks, suchastelegraphand telephone networks, before1960. Thesenetworksweresuitableforconstant-rate communication at that time, which means that after a connection was made betweentwousers,theencodedmessage(telegraphy)orvoice(telephony)could be exchanged.

Acomputernetwork,ontheotherhand,shouldbeabletohandle*bursty*data, whichmeans data receivedatvariableratesatdifferent times. Theworld neededto wait for the packet-switched networkto be invented.

BirthofPacket-SwitchedNetworks:Thetheory ofpacketswitchingfor bursty trafficwasfirstpresentedbyLeonardKleinrockin 1961at MIT.Atthesame time,twootherresearchers,Paul BaranatRandInstituteandDonaldDaviesat National Physical LaboratoryinEngland,publishedsomepapersaboutpacket- switched networks.

ARPANET: In the m i d -1960s, mainframe computers in research organizationswerestand-alonedevices. Computersfromdifferent manufacturers were unable to communicate with one another.

The**Advanced ResearchProjectsAgency(ARPA)**intheDepartmentof Defense(DOD)was interestedinfindingawaytoconnectcomputerssothatthe researcherstheyfundedcouldsharetheir findings, thereby reducing costsand eliminating duplicationofeffort.

In 1967, at an Associationfor ComputingMachinery (ACM)meeting, ARPA presented itsideasfor the**AdvancedResearchProjectsAgency Network (ARPANET),**asmallnetwork**of** connectedcomputers.

The idea was that each hostcomputer(not necessarilyfromthe samemanufacturer)wouldbeattachedto aspecializedcomputer,calledan*interface messageprocessor*(IMP).TheIMPs,inturn,wouldbeconnectedtoeachother. EachIMPhadto

beabletocommunicatewithotherIMPsaswell aswithitsown attachedhost.By1969,ARPANET was a reality.

BIRTH OF THE INTERNET:

In1972,VintCerfandBobKahn,both ofwhomwerepartofthecore ARPANETgroup, collaboratedonwhattheycalledthe*InternettingProject*. They wanted to link dissimilar networks so that a host on one network could communicatewith ahostonanother. Therewere many problemstoovercome: diversepacketsizes,diverseinterfaces,anddiversetransmissionrates,aswell as differingreliabilityrequirements.CerfandKahndevisedtheideaofadevicecalled a*gateway*toserveas theintermediary hardwaretotransferdata fromonenetwork to another.

TCP/IP: Cerf and Kahn's landmark 1973paper outlined theprotocols toachieveend-to-enddeliveryofdata.ThiswasanewversionofNCP(Network Control Protocol).Thispaperontransmissioncontrolprotocol (TCP)included concepts such asencapsulation, the datagram, andthe functionsofa gateway.

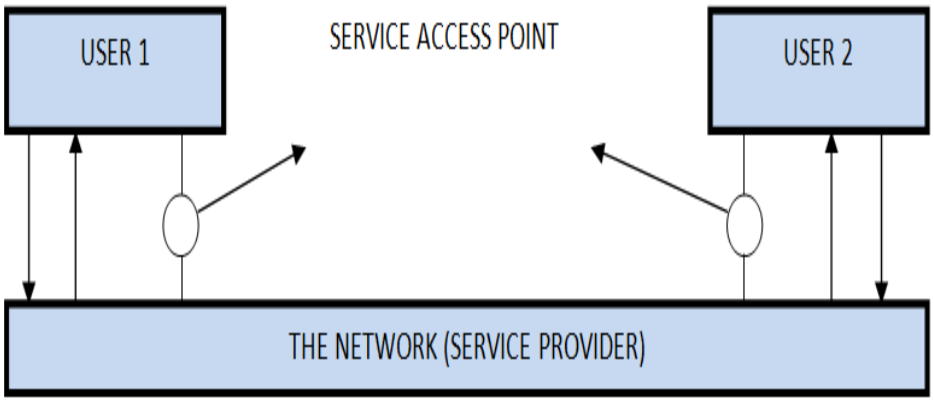
Aradical idea wasthetransferof responsibility for error correction from the IMP tothehostmachine. ThisARPAInternetnowbecame thefocusofthe communicationeffort.Around this time,responsibility fortheARPANETwashanded over to the Defense Communication Agency(DCA).

In October 1977, an internet consisting of three different networks (ARPANET, packet radio, and packet satellite) was successfully demonstrated. Communication betweennetworks was now possible.TCPsplitsinto two protocols: **TransmissionControlProtocol(TCP)**and**Internet Protocol(IP).**

IPwouldhandledatagramroutingwhileTCP wouldberesponsiblefor higher level functionssuchassegmentation,reassembly,anderrordetection.Thenew combination becameknown as TCP/IP.

What are Services?

These are the operations that a layer can provide to the layer above it in the OSI Reference model. It defines the operation and states a layer is ready to perform but it does not specify anything about the implementation of these operations.



What are Protocols?

These are set of rules that govern the format and meaning of frames, messages or packets that are exchanged between the server and client.

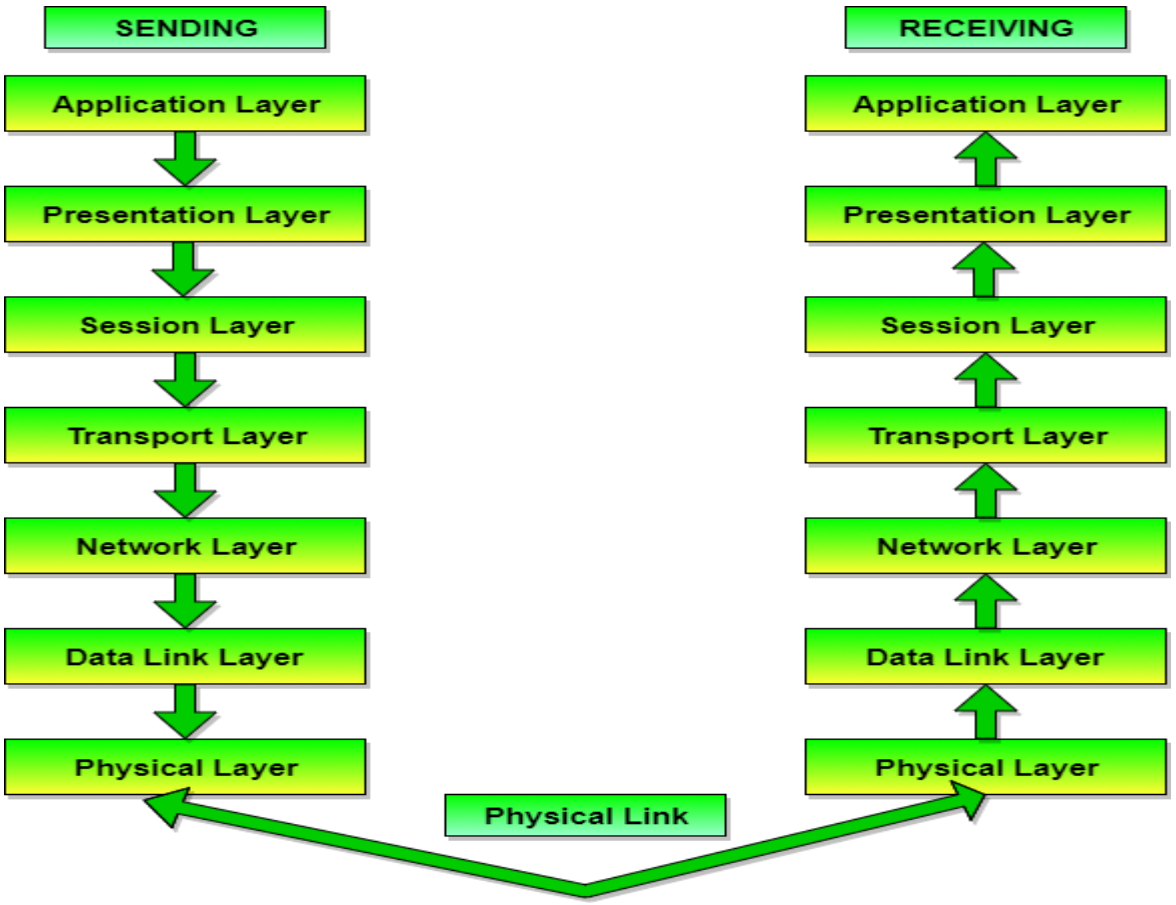
Reference Models in Communication Networks

The most important reference models are :

1. OSI reference model.
2. TCP/IP reference model.

Introduction to ISO-OSI Model

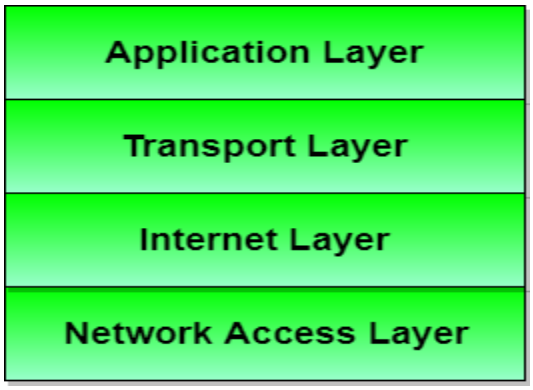
There are many users who use computer network and are located all over the world. To ensure national and worldwide data communication ISO (ISO stands for International Organization of Standardization.) developed this model. This is called a model for open system interconnection (OSI) and is normally called as OSI model.OSI model architecture consists of seven layers. It defines seven layers or levels in a complete communication system. OSI Reference model is explained in other chapter.



Introduction to TCP/IP Reference Model

TCP/IP is transmission control protocol and internet protocol. Protocols are set of rules which govern every possible communication over the internet. These protocols describe the movement of data between the host computers or internet and offers simple naming and addressing schemes.

TCP/IP Reference model is explained in details other chapter.



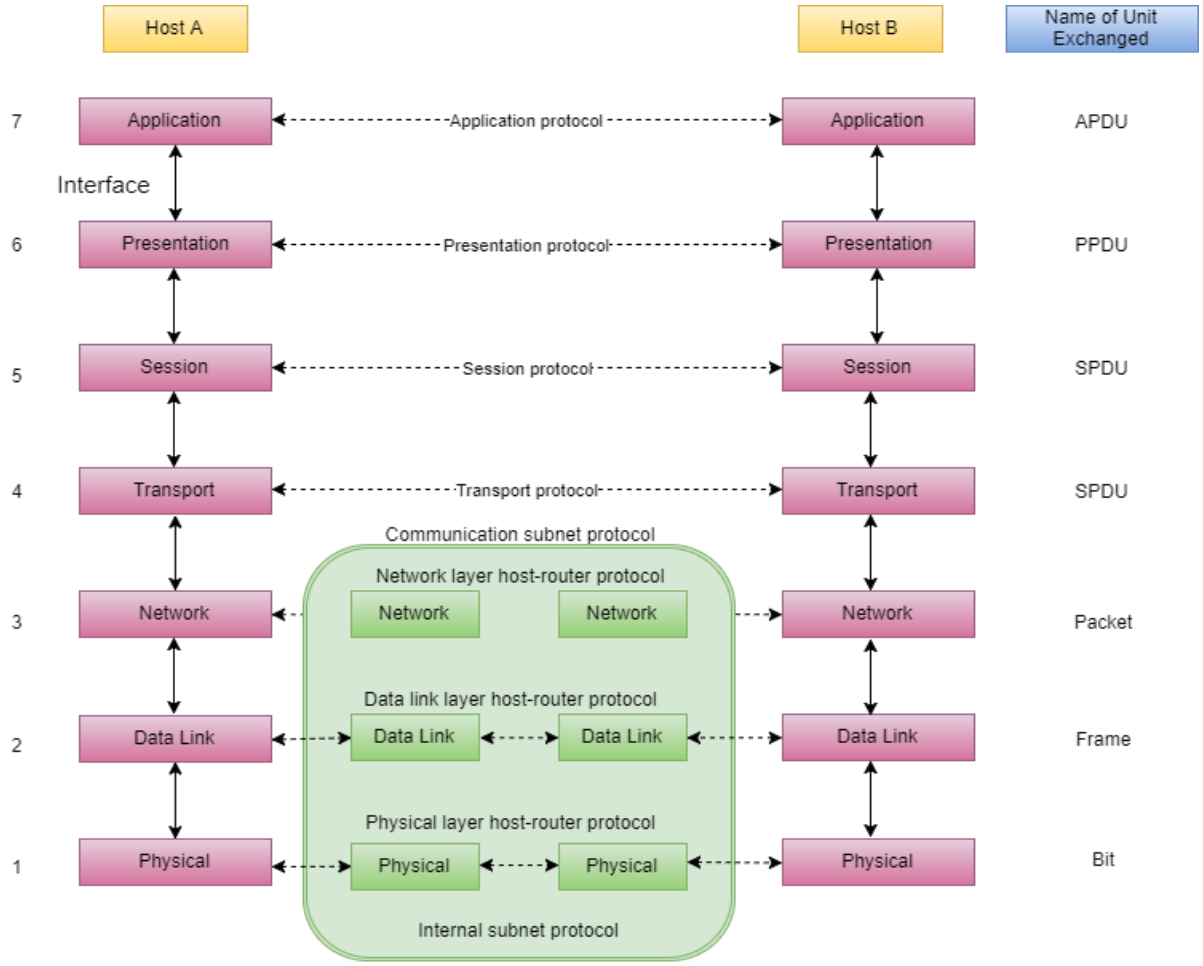
The OSI Model - Features, Principles and Layers

There are n numbers of users who use computer network and are located over the world. So to ensure, national and worldwide data communication, systems must be developed which are compatible to communicate with each other ISO has developed a standard. ISO stands for **International organization of Standardization**. This is called a model for **Open System Interconnection** (OSI) and is commonly known as OSI model.

The ISO-OSI model is a seven layer architecture. It defines seven layers or levels in a complete communication system. They are:

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

Below we have the complete representation of the OSI model, showcasing all the layers and how they communicate with each other.



In the table below, we have specified the **protocols** used and the **data unit** exchanged by each layer of the OSI Model.

Layer	Name of Protocol	Name of Unit exchanged
Application	Application Protocol	APDU - Application Protocol Data Unit
Presentation	Presentation Protocol	PPDU - Presentation Protocol Data Unit
Session	Session Protocol	SPDU - Session Protocol Data Unit
Transport	Transport Protocol	TPDU - Transport Protocol Data Unit
Network	Network layer host-router Protocol	Packet
Data Link	Data link layer host-router Protocol	Frame
Physical	Physical layer host-router Protocol	Bit

Feature of OSI Model

1. Big picture of communication over network is understandable through this OSI model.
2. We see how hardware and software work together.
3. We can understand new technologies as they are developed.
4. Troubleshooting is easier by separate networks.
5. Can be used to compare basic functional relationships on different networks.

Principles of OSI Reference Model

The OSI reference model has 7 layers. The principles that were applied to arrive at the seven layers can be briefly summarized as follows:

1. A layer should be created where a different abstraction is needed.
2. Each layer should perform a well-defined function.
3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
4. The layer boundaries should be chosen to minimize the information flow across the interfaces.
5. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that architecture does not become unwieldly.

Merits of OSI reference model

1. OSI model distinguishes well between the services, interfaces and protocols.
2. Protocols of OSI model are very well hidden.
3. Protocols can be replaced by new protocols as technology changes.
4. Supports connection oriented services as well as connectionless service.

Demerits of OSI reference model

1. Model was devised before the invention of protocols.
2. Fitting of protocols is tedious task.
3. It is just used as a reference model.

Functions of Different Layers

Following are the functions performed by each layer of the OSI model.

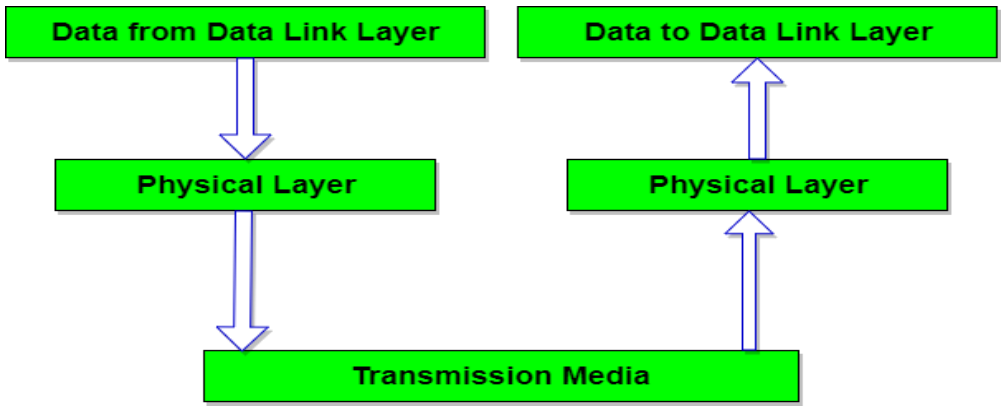
Physical Layer - OSI Reference Model

Physical layer is the lowest layer of the OSI reference model. It is responsible for sending bits from one computer to another. This layer is not concerned with the meaning of the bits and deals with the setup of physical connection to the network and with transmission and reception of signals.

Functions of Physical Layer

Following are the various functions performed by the Physical layer of the OSI model.

1. **Representation of Bits:** Data in this layer consists of stream of bits. The bits must be encoded into signals for transmission. It defines the type of encoding i.e. how 0's and 1's are changed to signal.
2. **Data Rate:** This layer defines the rate of transmission which is the number of bits per second.
3. **Synchronization:** It deals with the synchronization of the transmitter and receiver. The sender and receiver are synchronized at bit level.
4. **Interface:** The physical layer defines the transmission interface between devices and transmission medium.
5. **Line Configuration:** This layer connects devices with the medium: Point to Point configuration and Multipoint configuration.
6. **Topologies:** Devices must be connected using the following topologies: Mesh, Star, Ring and Bus.
7. **Transmission Modes:** Physical Layer defines the direction of transmission between two devices: Simplex, Half Duplex, Full Duplex.
8. Deals with baseband and broadband transmission.



Design Issues with Physical Layer

- The Physical Layer is concerned with transmitting raw bits over a communication channel.
- The design issue has to do with making sure that when one side sends a 1 bit, it is received by the other side as a 1 bit and not as a 0 bit.
- **Typical questions here are:**
  - How many volts should be used to represent a 1 bit and how many for a 0?
  - How many nanoseconds a bit lasts?
  - Whether transmission may proceed simultaneously in both directions?
  - Whether transmission may proceed simultaneously in both directions?
  - How many pins the network connector has and what each pin is used for?
- The design issues here largely deal with mechanical, electrical and timing interfaces, and the physical transmission medium, which lies below the physical layer.

Data Link Layer - OSI Model

Data link layer performs the most reliable node to node delivery of data. It forms frames from the packets that are received from network layer and gives it to physical layer. It also synchronizes the information which is to be transmitted over the data. Error controlling is easily done. The encoded data are then passed to physical.

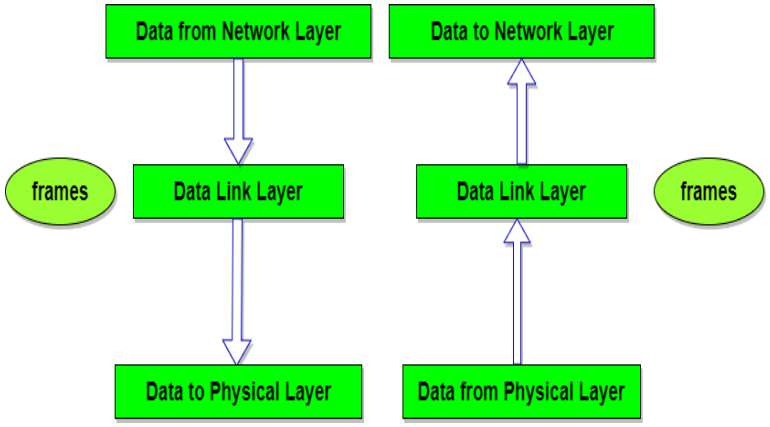
Error detection bits are used by the data link layer. It also corrects the errors. Outgoing messages are assembled into frames. Then the system waits for the acknowledgements to be received after the transmission. It is reliable to send message.

The main task of the **data link layer** is to transform a raw transmission facility into a line that appears free of undetected transmission errors to the network layer. It accomplishes this task by having the sender break up the input data into **data frames**(typically a few hundred or few thousand bytes) and transmit the frames sequentially. If the service is reliable, the receiver confirms correct receipt of each frame by send back an **acknowledgement frame**.

Functions of Data Link Layer

1. **Framing:** Frames are the streams of bits received from the network layer into manageable data units. This division of stream of bits is done by Data Link Layer.
2. **Physical Addressing:** The Data Link layer adds a header to the frame in order to define physical address of the sender or receiver of the frame, if the frames are to be distributed to different systems on the network.

3. **Flow Control:** A flow control mechanism to avoid a fast transmitter from running a slow receiver by buffering the extra bit is provided by flow control. This prevents traffic jam at the receiver side.
4. **Error Control:** Error control is achieved by adding a trailer at the end of the frame. Duplication of frames are also prevented by using this mechanism. Data Link Layers adds mechanism to prevent duplication of frames.
5. **Access Control:** Protocols of this layer determine which of the devices has control over the link at any given time, when two or more devices are connected to the same link.



Design Issues with Data Link Layer

- The issue that arises in the data link layer(and most of the higher layers as well) is how to keep a fast transmitter from drowning a slow receiver in data. Some traffic regulation mechanism is often needed to let the transmitter know how much buffer space the receiver has at the moment. Frequently, the flow regulation and the error handling are integrated.
- Broadcast networks have an additional issue in the data link layer: How to control access to the shared channel. A special sublayer of the data link layer, the Medium Access Control(MAC) sublayer, deals with this problem.

Network Layer - OSI Model

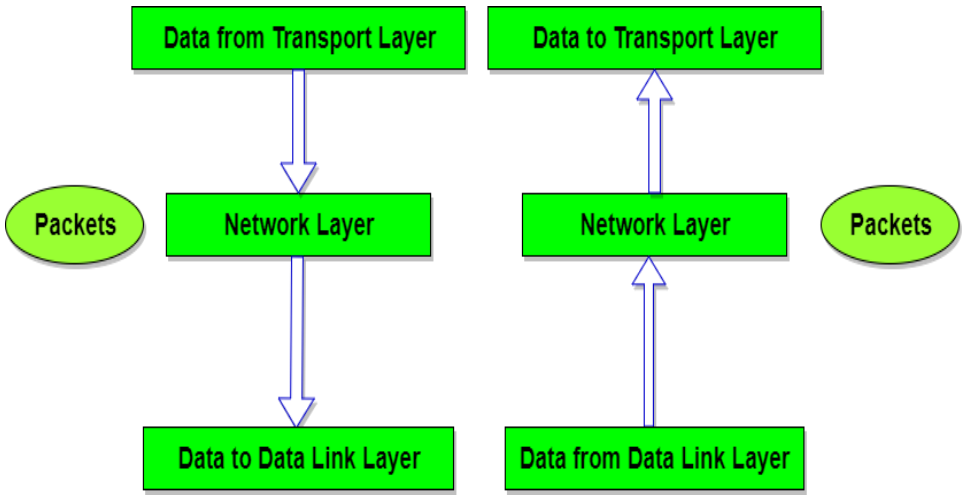
The network Layer controls the operation of the subnet. The main aim of this layer is to deliver packets from source to destination across multiple links (networks). If two computers (system) are connected on the same link, then there is no need for a network layer. It routes the signal through different channels to the other end and acts as a network controller.

It also divides the outgoing messages into packets and to assemble incoming packets into messages for higher levels.

In broadcast networks, the routing problem is simple, so the network layer is often thin or even non-existent.

Functions of Network Layer

1. It translates logical network address into physical address. Concerned with circuit, message or packet switching.
2. Routers and gateways operate in the network layer. Mechanism is provided by Network Layer for routing the packets to final destination.
3. Connection services are provided including network layer flow control, network layer error control and packet sequence control.
4. Breaks larger packets into small packets.



Design Issues with Network Layer

- A key design issue is **determining how packets are routed from source to destination**. Routes can be based on static tables that are wired into the network and rarely changed. They can also be highly dynamic, being determined anew for each packet, to reflect the current network load.
- If **too many packets** are present in the subnet at the same time, they will get into one another's way, forming **bottlenecks**. The **control of such congestion** also belongs to the network layer.

- Moreover, the **quality of service** provided(delay, transmit time, jitter, etc) is also a network layer issue.
- When a packet has to **travel from one network to another to get to its destination**, many problems can arise such as:
  - The addressing used by the second network may be different from the first one.
  - The second one may not accept the packet at all because it is too large.
  - The protocols may differ, and so on.
- It is up to the network layer to overcome all these problems to allow heterogeneous networks to be interconnected.

Transport Layer - OSI Model

The basic function of the Transport layer is to accept data from the layer above, split it up into smaller units, pass these data units to the Network layer, and ensure that all the pieces arrive correctly at the other end.

Furthermore, all this must be done efficiently and in a way that isolates the upper layers from the inevitable changes in the hardware technology.

The Transport layer also determines what type of service to provide to the Session layer, and, ultimately, to the users of the network. The most popular type of transport connection is an **error-free point-to-point channel** that delivers messages or bytes in the order in which they were sent.

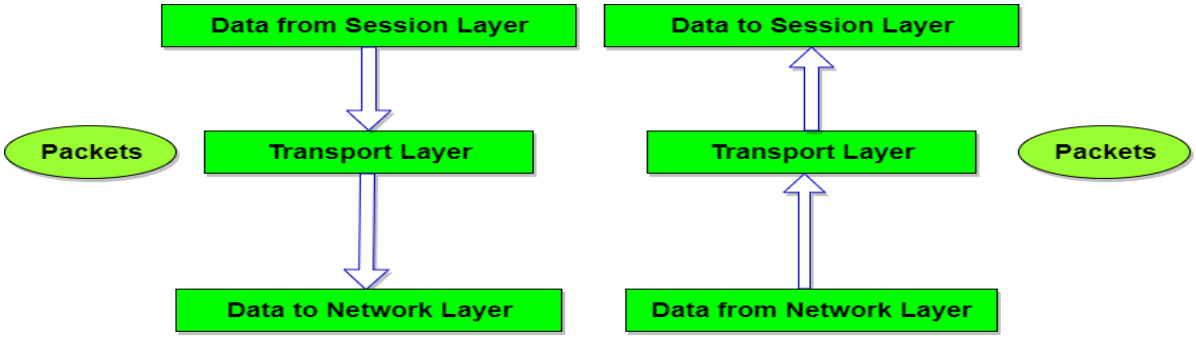
The Transport layer is a true end-to-end layer, all the way from the source to the destination. In other words, a program on the source machine carries on a conversation with a similar program on the destination machine, using the message headers and control messages.

Functions of Transport Layer

1. **Service Point Addressing:** Transport Layer header includes service point address which is port address. This layer gets the message to the correct process on the computer unlike Network Layer, which gets each packet to the correct computer.
2. **Segmentation and Reassembling:** A message is divided into segments; each segment contains sequence number, which enables this layer in reassembling the message. Message is reassembled correctly upon arrival at the destination and replaces packets which were lost in transmission.
3. **Connection Control:** It includes 2 types:

- Connectionless Transport Layer : Each segment is considered as an independent packet and delivered to the transport layer at the destination machine.
- Connection Oriented Transport Layer : Before delivering packets, connection is made with transport layer at the destination machine.

4. **Flow Control:** In this layer, flow control is performed end to end.
5. **Error Control:** Error Control is performed end to end in this layer to ensure that the complete message arrives at the receiving transport layer without any error. Error Correction is done through retransmission.



Design Issues with Transport Layer

- Accepting data from Session layer, split it into segments and send to the network layer.
- Ensure correct delivery of data with efficiency.
- Isolate upper layers from the technological changes.
- Error control and flow control.

Session Layer - OSI Model

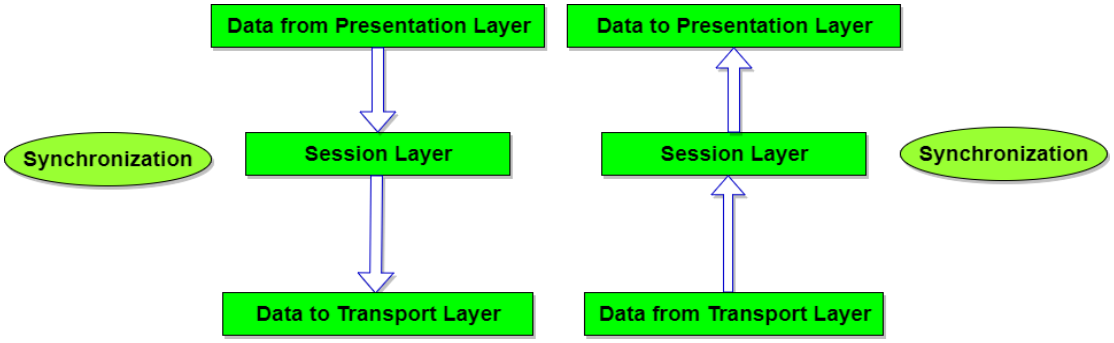
The Session Layer allows users on different machines to establish active communication sessions between them.

It's main aim is to establish, maintain and synchronize the interaction between communicating systems. Session layer manages and synchronize the conversation between two different applications. In Session layer, streams of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely and data loss is avoided.

Functions of Session Layer

1. **Dialog Control :** This layer allows two systems to start communication with each other in half-duplex or full-duplex.

2. **Token Management:** This layer prevents two parties from attempting the same critical operation at the same time.
3. **Synchronization :** This layer allows a process to add checkpoints which are considered as synchronization points into stream of data. Example: If a system is sending a file of 800 pages, adding checkpoints after every 50 pages is recommended. This ensures that 50 page unit is successfully received and acknowledged. This is beneficial at the time of crash as if a crash happens at page number 110; there is no need to retransmit 1 to100 pages.



Design Issues with Session Layer

- To allow machines to establish sessions between them in a seamless fashion.
- Provide enhanced services to the user.
- To manage dialog control.
- To provide services such as **Token management** and **Synchronization**.

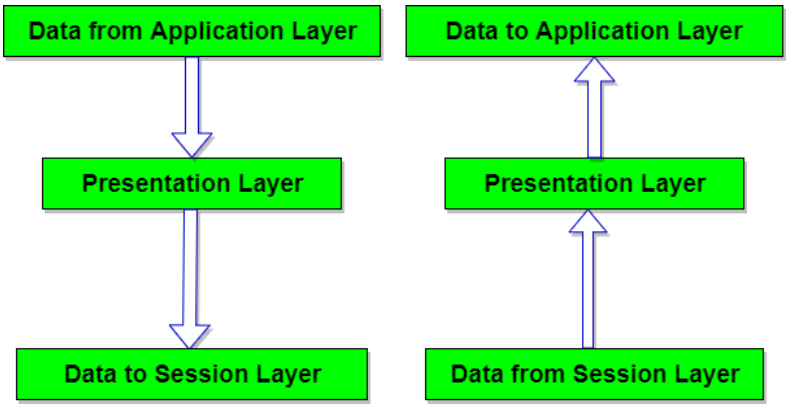
Presentation Layer - OSI Model

The primary goal of this layer is to take care of the **syntax** and **semantics** of the information exchanged between two communicating systems. Presentation layer takes care that the data is sent in such a way that the receiver will understand the information(data) and will be able to use the data. Languages(syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role translator.

In order to make it possible for computers with different data representations to communicate, the data structures to be exchanged can be defined in an **abstract** way. The presentation layer manages these **abstract data structures** and allows higher-level data structures(eg: banking records), to be defined and exchanged.

Functions of Presentation Layer

1. **Translation:** Before being transmitted, information in the form of characters and numbers should be changed to bit streams. The presentation layer is responsible for interoperability between encoding methods as different computers use different encoding methods. It translates data between the formats the network requires and the format the computer.
2. **Encryption:** It carries out encryption at the transmitter and decryption at the receiver.
3. **Compression:** It carries out data compression to reduce the bandwidth of the data to be transmitted. The primary role of Data compression is to reduce the number of bits to be 0transmitted. It is important in transmitting multimedia such as audio, video, text etc.



Design Issues with Presentation Layer

- To manage and maintain the **Syntax** and **Semantics** of the information transmitted.
- **Encoding data** in a standard agreed upon way. Eg: String, double, date, etc.
- Perform **Standard Encoding** on wire.

Application Layer - OSI Model

It is the top most layer of OSI Model. Manipulation of data(information) in various ways is done in this layer which enables user or software to get access to the network. Some services provided by this layer includes: E-Mail, transferring files, distributing the results to user, directory services, network resources, etc.

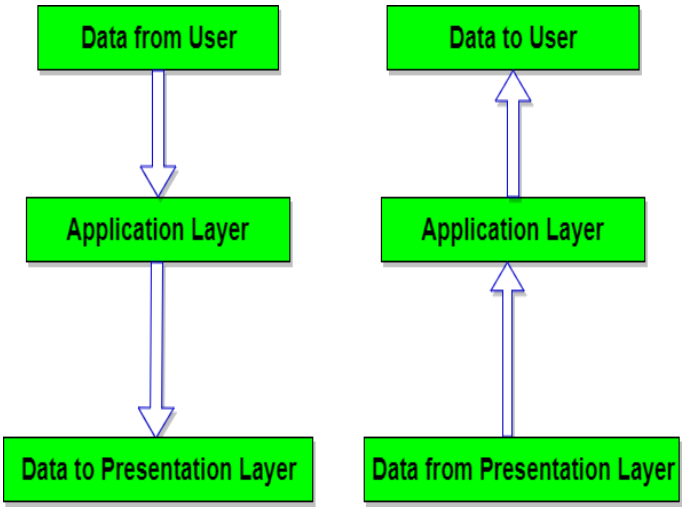
The Application Layer contains a variety of protocols that are commonly needed by users. One widely-used application protocol is **HTTP(Hypertext Transfer Protocol)**, which is the basis for

the World Wide Web. When a browser wants a web page, it sends the name of the page it wants to the server using HTTP. The server then sends the page back.

Other Application protocols that are used are: **File Transfer Protocol (FTP)**, **Trivial File Transfer Protocol (TFTP)**, **Simple Mail Transfer Protocol (SMTP)**, **TELNET**, **Domain Name System (DNS)**etc.

Functions of Application Layer

1. **Mail Services:** This layer provides the basis for E-mail forwarding and storage.
2. **Network Virtual Terminal:** It allows a user to log on to a remote host. The application creates software emulation of a terminal at the remote host. User's computer talks to the software terminal which in turn talks to the host and vice versa. Then the remote host believes it is communicating with one of its own terminals and allows user to log on.
3. **Directory Services:** This layer provides access for global information about various services.
4. **File Transfer, Access and Management (FTAM):** It is a standard mechanism to access files and manages it. Users can access files in a remote computer and manage it. They can also retrieve files from a remote computer.



Design Issues with Application Layer

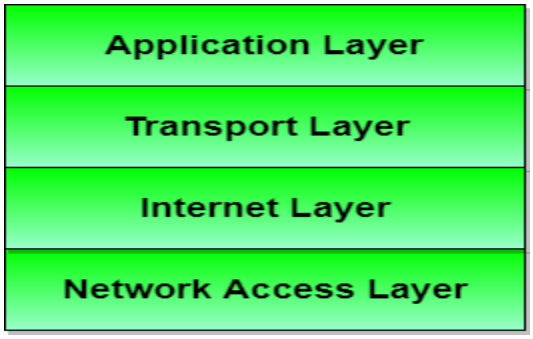
There are commonly reoccurring problems that occur in the design and implementation of Application Layer protocols and can be addressed by patterns from several different pattern languages:

- Pattern Language for Application-level Communication Protocols

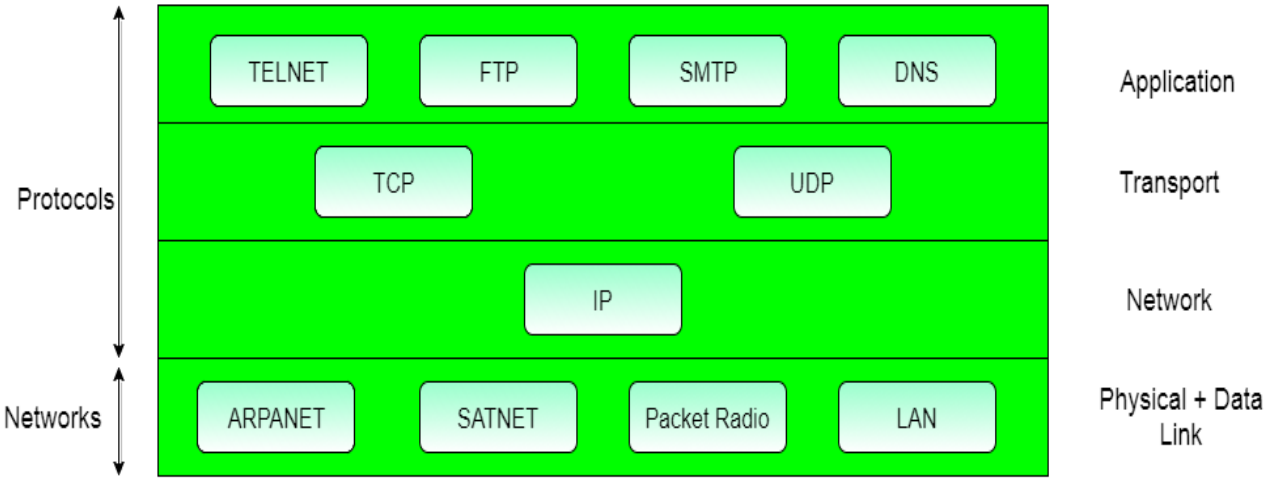
- Service Design Patterns
- Patterns of Enterprise Application Architecture
- Pattern-Oriented Software Architecture

The TCP/IP Reference Model

TCP/IP means Transmission Control Protocol and Internet Protocol. It is the network model used in the current Internet architecture as well. **Protocols** are set of rules which govern every possible communication over a network. These protocols describe the movement of data between the source and destination or the internet. They also offer simple naming and addressing schemes.



Protocols and networks in the TCP/IP model:



Overview of TCP/IP reference model

TCP/IP that is Transmission Control Protocol and Internet Protocol was developed by Department of **Defence's Project Research Agency** (ARPA, later DARPA) as a part of a research project of network interconnection to connect remote machines.

The features that stood out during the research, which led to making the TCP/IP reference model were:

- Support for a flexible architecture. Adding more machines to a network was easy.
- The network was robust, and connections remained intact untill the source and destination machines were functioning.

The overall idea was to allow one application on one computer to talk to(send data packets) another application running on different computer.

Different Layers of TCP/IP Reference Model

Below we have discussed the 4 layers that form the TCP/IP reference model:

Layer 1: Host-to-network Layer

1. Lowest layer of the all.
2. Protocol is used to connect to the host, so that the packets can be sent over it.
3. Varies from host to host and network to network.

Layer 2: Internet layer

1. Selection of a packet switching network which is based on a connectionless internetwork layer is called a internet layer.
2. It is the layer which holds the whole architecture together.
3. It helps the packet to travel independently to the destination.
4. Order in which packets are received is different from the way they are sent.
5. IP (Internet Protocol) is used in this layer.
6. The various functions performed by the Internet Layer are:
    - Delivering IP packets
    - Performing routing
    - Avoiding congestion

Layer 3: Transport Layer

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.
3. The applications can read and write to the transport layer.
4. Transport layer adds header information to the data.

5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
6. Transport layer also arrange the packets to be sent, in sequence.

Layer 4: Application Layer

The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.

1. **TELNET** is a two-way communication protocol which allows connecting to a remote machine and run applications on it.
2. **FTP**(File Transfer Protocol) is a protocol, that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.
3. **SMTP**(Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.
4. **DNS**(Domain Name Server) resolves an IP address into a textual address for Hosts connected over a network.
5. It allows peer entities to carry conversation.
6. It defines two end-to-end protocols: TCP and UDP
    - **TCP(Transmission Control Protocol):** It is a reliable connection-oriented protocol which handles byte-stream from source to destination without error and flow control.
    - **UDP(User-Datagram Protocol):** It is an unreliable connection-less protocol that do not want TCPs, sequencing and flow control. Eg: One-shot request-reply kind of service.

Merits of TCP/IP model

1. It operated independently.
2. It is scalable.
3. Client/server architecture.
4. Supports a number of routing protocols.
5. Can be used to establish a connection between two computers.

Demerits of TCP/IP

1. In this, the transport layer does not guarantee delivery of packets.
2. The model cannot be used in any other application.
3. Replacing protocol is not easy.
4. It has not clearly separated its services, interfaces and protocols.

Comparison of OSI and TCP/IP Reference Model

Now it's time to compare both the reference model that we have learned till now. Let's start by addressing the similarities that both of these models have.

Following are some **similarities** between OSI Reference Model and TCP/IP Reference Model.

- Both have layered architecture.
- Layers provide similar functionalities.
- Both are protocol stack.
- Both are reference models.

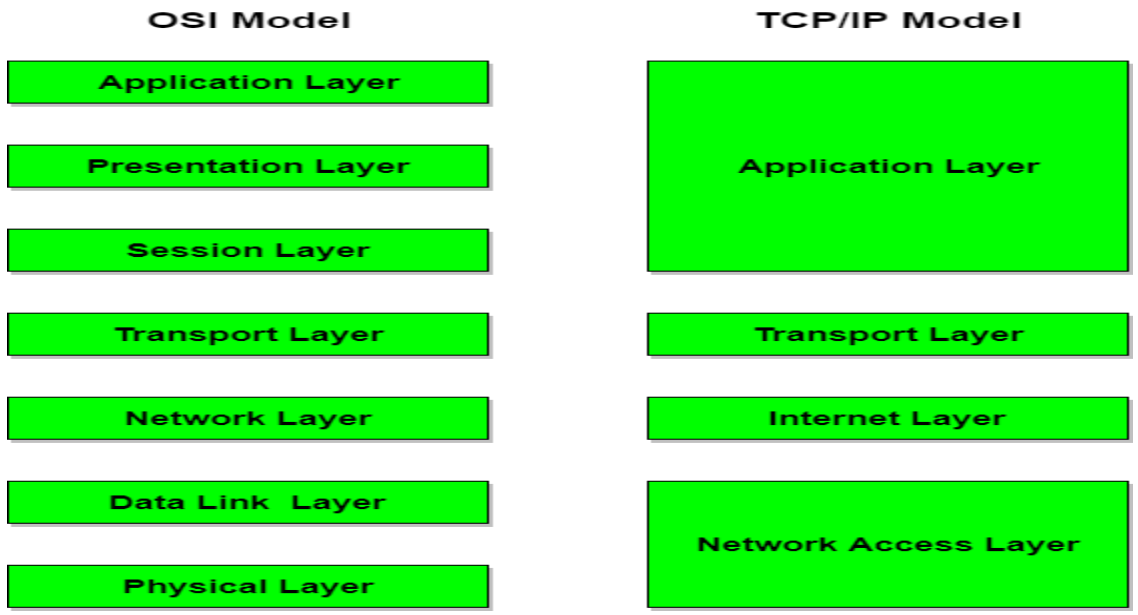
Difference between OSI and TCP/IP Reference Model

Following are some major differences between OSI Reference Model and TCP/IP Reference Model, with diagrammatic comparison below.

OSI(Open System Interconnection)	**TCP/IP(Transmission Control Protocol / Internet Protocol)**
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network 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 hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. Transport Layer is Connection Oriented.	5. Transport Layer is both Connection Oriented and Connection less.

6. Network Layer is both Connection Oriented and Connection less.	6. Network Layer is Connection less.
7. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	7. TCP/IP model is, in a way implementation of the OSI model.
8. Network layer of OSI model provides both connection oriented and connectionless service.	8. The Network layer in TCP/IP model provides connectionless service.
9. OSI model has a problem of fitting the protocols into the model.	9. TCP/IP model does not fit any protocol
10. Protocols are hidden in OSI model and are easily replaced as the technology changes.	10. In TCP/IP replacing protocol is not easy.
11. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	11. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
12. It has 7 layers	12. It has 4 layers

Diagrammatic Comparison between OSI Reference Model and TCP/IP Reference Model



KEY TERMS in Computer Networks

Following are some important terms, which are frequently used in context of Computer Networks.

Terms	**Definition**
1. ISO	The OSI model is a product of the Open Systems Interconnection project at the International Organization for Standardization. ISO is a voluntary organization.
2. OSI Model	Open System Interconnection is a model consisting of seven logical layers.
3. TCP/IP Model	Transmission Control Protocol and Internet Protocol Model is based on four layer model which is based on Protocols.
4. UTP	Unshielded Twisted Pair cable is a Wired/Guided media which consists of two conductors usually copper, each with its own colour plastic insulator

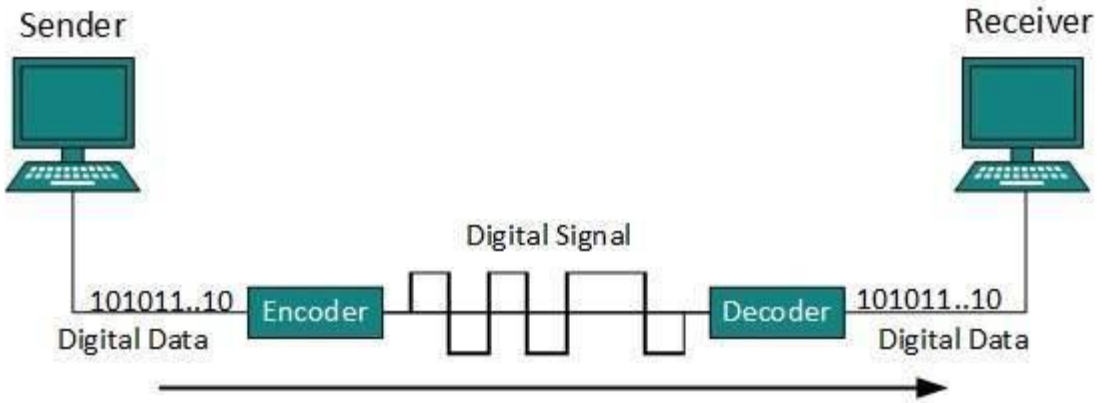
5. STP	Shielded Twisted Pair cable is a Wired/Guided media has a metal foil or braided-mesh covering which encases each pair of insulated conductors. Shielding also eliminates crosstalk
6. PPP	Point-to-Point connection is a protocol which is used as a communication link between two devices.
7. LAN	Local Area Network is designed for small areas such as an office, group of building or a factory.
8. WAN	Wide Area Network is used for the network that covers large distance such as cover states of a country
9. MAN	Metropolitan Area Network uses the similar technology as LAN. It is designed to extend over the entire city.
10. Crosstalk	Undesired effect of one circuit on another circuit. It can occur when one line picks up some signals travelling down another line. Example: telephone conversation when one can hear background conversations. It can be eliminated by shielding each pair of twisted pair cable.
11. PSTN	Public Switched Telephone Network consists of telephone lines, cellular networks, satellites for communication, fiber optic cables etc. It is the combination of world's (national, local and regional) circuit switched telephone network.
12. File Transfer, Access and Management (FTAM)	Standard mechanism to access files and manages it. Users can access files in a remote computer and manage it.
13. Analog Transmission	The signal is continuously variable in amplitude and

	frequency. Power requirement is high when compared with Digital Transmission.
14. Digital Transmission	It is a sequence of voltage pulses. It is basically a series of discrete pulses. Security is better than Analog Transmission.
15. Asymmetric digital subscriber line(ADSL)	A data communications technology that enables faster data transmission over copper telephone lines than a conventional voice band modem can provide.
16. Access Point	Alternatively referred to as a base station and wireless router, an access point is a wireless receiver which enables a user to connect wirelessly to a network or the Internet. This term can refer to both Wi-Fi and Bluetooth devices.
17. Acknowledgement (ACK)	Short for acknowledgement, ACK is an answer given by another computer or network device indicating to another computer that it acknowledged the SYN/ACK or other request sent to it. **Note:** If the signal is not properly received an NAK is sent.
18. Active Topology	The term active topology describes a network topology in which the signal is amplified at each step as it passes from one computer to the next.
19. Aloha	Protocol for satellite and terrestrial radio transmissions. In pure Aloha, a user can communicate at any time, but risks collisions with other users' messages. Slotted Aloha reduces the chance of collisions by dividing the channel into time slots and requiring that the user send only at the beginning of a time slot.

20. Address Resolution Protocol(ARP)	ARP is a used with the IP for mapping a 32-bit Internet Protocol address to a MAC address that is recognized in the local network specified in RFC 826.

Line Coding

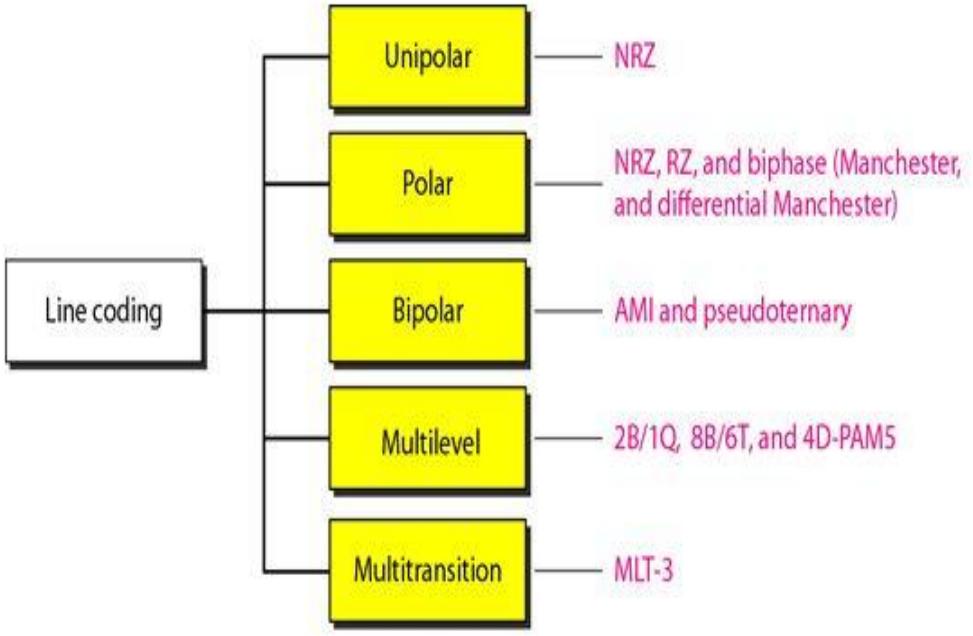
The process for converting digital data into digital signal is said to be Line Coding. Digital data is found in binary format.It is represented (stored) internally as series of 1s and 0s.



Digital signal is denoted by discreet signal, which represents digital data.There are fivetypes of line coding schemes available:

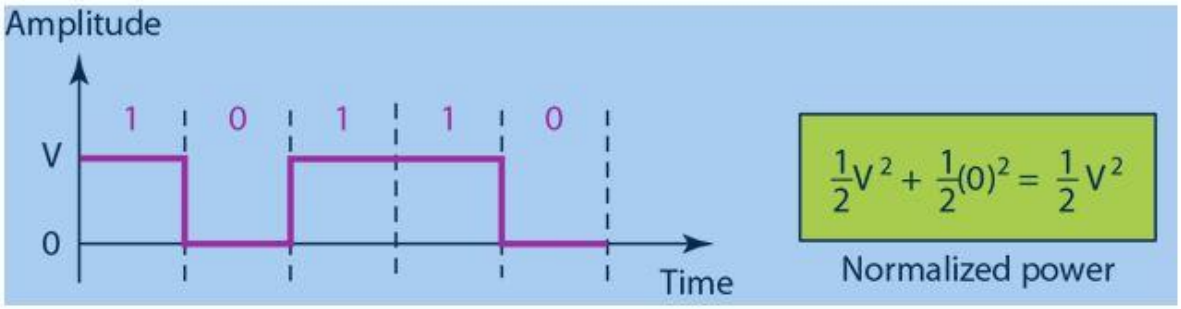
LINE CODING SCHEMES

The Line Coding schemes are categorized as shown in the following figure:



I. Unipolar Scheme:

In a unipolar scheme, all the signal levels are on one side of the time axis, either above or below. NRZ (Non-Return-to-Zero): Traditionally, a unipolar scheme was designed as a non-return-to-zero (NRZ) scheme in which the positive voltage defines bit 1 and the zero voltage defines bit O. It is called NRZ because the signal does not return to zero at the middle of the bit. The following figure shows a unipolar NRZ scheme.



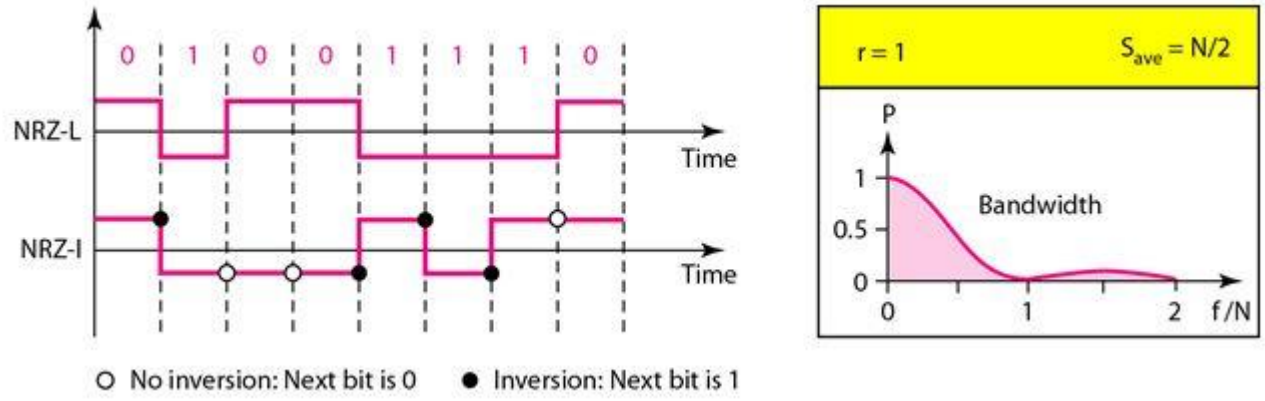
Compared with its polar counterpart, the normalized power (power needed to send 1 bit per unit line resistance) is double that for polar NRZ. For this reason, this scheme is normally not used in data communications today.

II. Polar Schemes

In polar schemes, the voltages are on the both sides of the time axis. For example, the voltage level for 0 can be positive and the voltage level for I can be negative.

a). Non-Return-to-Zero (NRZ):

In polar NRZ encoding, we use two levels of voltage amplitude. We can have two versions of polar NRZ: NRZ-Land NRZ-I, as shown in the following Figure. The figure also shows the value of r, the average baud rate, and the bandwidth.



In the first variation, NRZ-L (NRZ-Level), the level of the voltage determines the value of the bit. In the second variation, NRZ-I (NRZ-Invert), the change or lack of change in the level of the voltage determines the value of the bit. If there is no change, the bit is 0; if there is a change, the bit is 1.

Drawbacks:

1. Baseline wandering is a problem for both variations; it is twice as severe in NRZ-L. If there is a long sequence of Os or Is in NRZ-L, the average signal power becomes skewed. The receiver might have difficulty discerning the bit value.

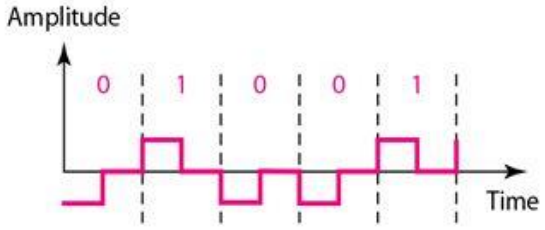
In NRZ-I this problem occurs only for a long sequence of O s. If we eliminate the long sequence of Os, we can avoid baseline wandering.

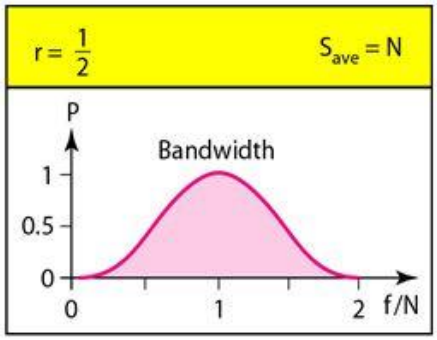
2. The synchronization problem (sender and receiver clocks are not synchronized) also exists in both schemes. Again, this problem is more serious in NRZ-L than in NRZ-I. While a long sequence of as can cause a problem in both schemes, a long sequence of 1s affects only NRZ-L.

3. Another problem with NRZ-L occurs when there is a sudden change of polarity in the system. For example, if twisted-pair cable is the medium, a change in the polarity of the wire results in all Os interpreted as I s and all I s interpreted as Os. NRZ-I does not have this problem. Both schemes have an average signal rate of N/2.

b). Return to Zero (RZ):

The main problem with NRZ encoding occurs when the sender and receiver clocks are not synchronized. The receiver does not know when one bit has ended and the next bit is starting. One solution is the return-to-zero (RZ) scheme, which uses three values: positive, negative, and zero. In RZ, the signal changes not between bits but during the bit. In the following figure, we see that the signal goes to 0 in the middle of each bit. It remains there until the beginning of the next bit.





Drawbacks:

1. The main disadvantage of RZ encoding is that it requires two signal changes to encode a bit and therefore occupies greater bandwidth.

2. Sudden change of polarity resulting in all Os interpreted as 1s and all 1s interpreted as Os, still exist here, but there is no DC component problem.

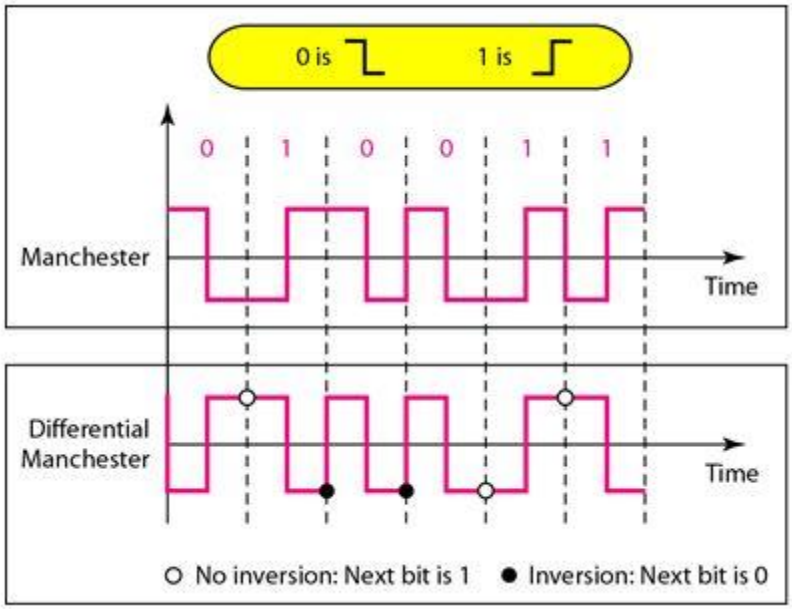
3. Another problem is the complexity: RZ uses three levels of voltage, which is more complex to create and discern. As a result of all these deficiencies, the scheme is not used today.

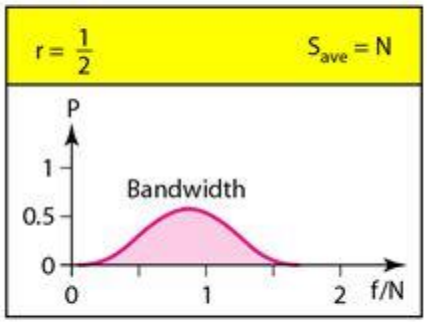
c).Biphase Manchester and Differential Manchester:

The idea of RZ (transition at the middle of the bit) and the idea of NRZ-L are combined into the Manchester scheme.

In Manchester encoding, the duration of the bit is divided into two halves. The voltage remains at one level during the first half and moves to the other level in the second half. The transition at the middle of the bit provides synchronization.

Differential Manchester, on the other hand, combines the ideas of RZ and NRZ-I. There is always a transition at the middle of the bit, but the bit values are determined at the beginning of the bit. If the next bit is 0, there is a transition; if the next bit is 1, there is none. The following figure shows both Manchester and differential Manchester encoding.



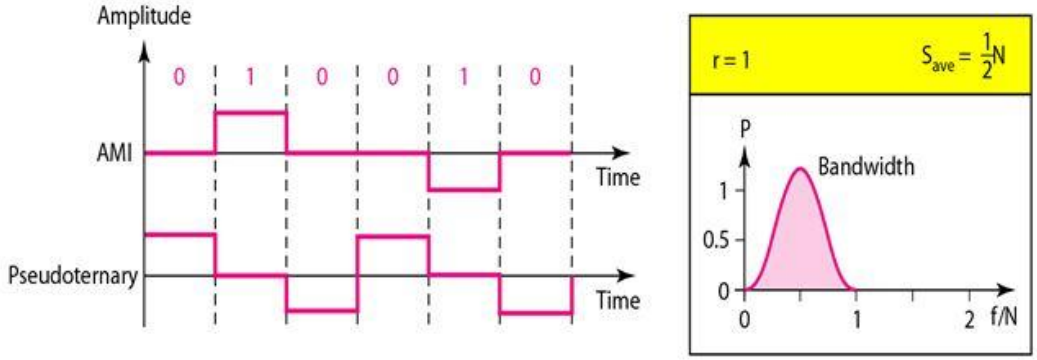


The Manchester scheme overcomes several problems associated with NRZ-L, and differential Manchester overcomes several problems associated with NRZ-I. First, there is no baseline wandering. There is no DC component because each bit has a positive and negative voltage contribution. The only drawback is the signal rate. The signal rate for Manchester and differential Manchester is double that for NRZ. The reason is that there is always one transition at the middle of the bit and maybe one transition at the end of each bit.

III. Bipolar Schemes

In bipolar encoding (sometimes called multilevel binary), there are three voltage levels, positive, negative, and zero. The voltage level for one data element is at zero, while the voltage level for the other element alternates between positive and negative.

AMI and Pseudoternary: The following figure shows two variations of bipolar encoding: AMI and pseudo ternary.



A common bipolar encoding scheme is called bipolar alternate mark inversion (AMI). In alternate mark inversion, a neutral zero voltage represents binary O. Binary 1s are represented by alternating positive and negative voltages.

A variation of AMI encoding is called Pseudoternary in which the 1 bit is encoded as a zero voltage and the 0 bit is encoded as alternating positive and negative voltages.

The bipolar scheme was developed as an alternative to NRZ. The bipolar scheme has the same signal rate as NRZ, but there is no DC component. The NRZ scheme has most of its energy concentrated near zero frequency, which makes it unsuitable for transmission over channels with poor performance around this frequency. The concentration of the energy in bipolar encoding is around frequency N/2.

IV. Multilevel Schemes:

The desire to increase the data speed or decrease the required bandwidth has resulted in the creation of many schemes. The goal is to increase the number of bits per baud by encoding a pattern of m data elements into a pattern of n signal elements. We only have two types of data elements(Os and 1s), which means that a group of m data elements can produce a combination of 2m data patterns.

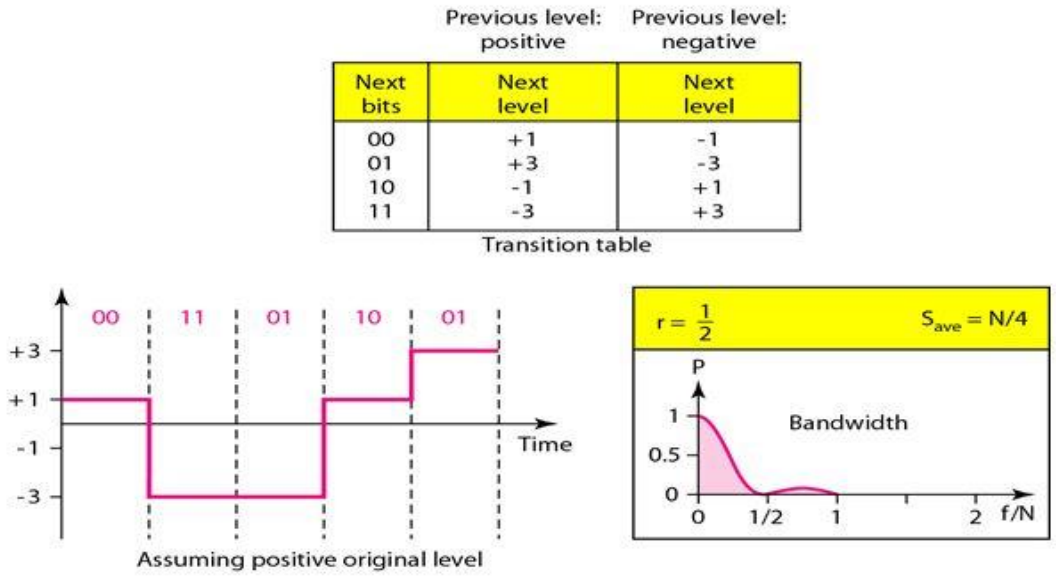
We can have different types of signal elements by allowing different signal levels. If we have L different levels, then we can produce Ln combinations of signal patterns.

If 2m =Ln, then each data pattern is encoded into one signal pattern. If 2m<Ln, data patterns occupy only a subset of signal patterns. The subset can be carefully designed to prevent baseline wandering, to provide synchronization, and to detect errors that occurred during data transmission. Data encoding is not possible if 2m > Ln because some of the data patterns cannot be encoded.

The code designers have classified these types of coding as mBnL, where m is the length of the binary pattern, B means binary data, n is the length of the signal pattern, and L is the number of levels in the signaling. A letter is often used in place of L: B(binary)for L=2, T (ternary) for L =3, and Q (quaternary) for L =4. Note that the first two letters define the data pattern, and the second two define the signal pattern.

a). 2BIQ:

The first mBnL scheme we discuss, two binary, one quaternary (2BIQ), uses data patterns of size 2 and encodes the 2-bit patterns as one signal element belonging to a four-level signal. In this type of encoding m =2, n =1, and L =4 (quaternary). The following figure shows an example of a 2B1Q signal.



Next bits	Previous level: positive — Next level	Previous level: negative — Next level
00	+1	-1
01	+3	-3
10	-1	+1
11	-3	+3

Transition table

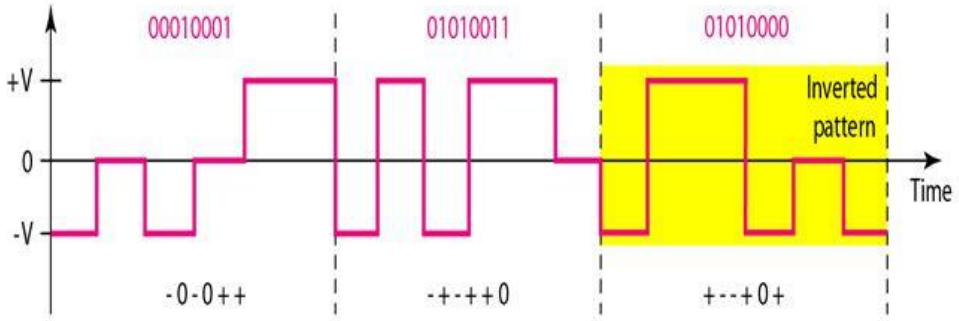
The average signal rate of 2BlQ is S =N/4. This means that using 2BIQ, we can send data 2 times faster than by using NRZ-L. However, 2B lQ uses four different signal levels, which means the receiver has to discern four different thresholds. The reduced bandwidth comes with a price. There are no redundant signal patterns in this scheme because 22=41.

b). 8B6T:

A very interesting scheme is eight binary, six ternary (8B6T). The idea is to encode a pattern of 8 bits as a pattern of 6 signal elements, where the signal has three levels (ternary). In this type of scheme, we can have 28=256 different data patterns and data patterns and 36=729 different signal patterns.

There are 729 – 256= 473 redundant signal elements that provide synchronization and error detection. Part of the redundancy is also used to provide DC balance. Each signal pattern has a weight of 0 or +1 DC values. This means that there is no pattern with the weight -1. To make the whole stream Dc-balanced, the sender keeps track of the weight. If two groups of weight 1 are encountered one after another, the first one is sent as is, while the next one is totally inverted to give a weight of -1. The following figure shows an example of three data patterns encoded as three signal patterns.

The three possible signal levels are represented as -,0, and +. The first 8-bit pattern 00010001 is encoded as the signal pattern -0-0++ with weight 0; the second 8-bit pattern 010 10011 is encoded as - + - + + 0 with weight +1. The third bit pattern should be encoded as + - - + 0 + with weight +1. To create DC balance, the sender inverts the actual signal. The receiver can easily recognize that this is an inverted pattern because the weight is -1. The pattern is inverted before decoding.



C).4D-PAM5:

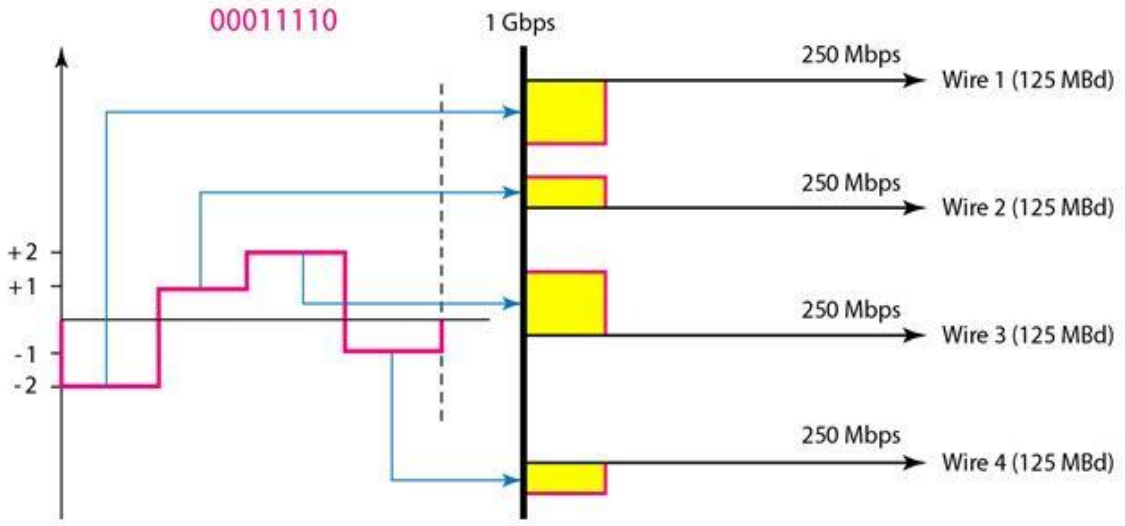
The last signaling scheme we discuss in this category is called four dimensional five-level pulse amplitude modulation (4D-PAM5). The 4D means that data is sent over four wires at the same time. It uses five voltage levels, such as -2, -1, 0, 1, and 2.

However, one level, level 0, is used only for forward error detection. If we assume that the code is just one-dimensional, the four levels create something similar to 8B4Q. In other words, an 8-

bit word is translated to a signal element of four different levels. The worst signal rate for this imaginary one-dimensional version is N X 4/8, or N12.

The technique is designed to send data over four channels (four wires). This means the signal rate can be reduced to N/8, a significant achievement. All 8 bits can be fed into a wire simultaneously and sent by using one signal element. The point here is that the four signal elements comprising one signal group are sent simultaneously in a four-dimensional setting.

The following figure shows the imaginary one-dimensional and the actual four-dimensional implementation. Gigabit LANs use this technique to send 1-Gbps data over four copper cables that can handle 125 Mbaud. This scheme has a lot of redundancy in the signal pattern because 28 data patterns are matched to 44= 256 signal patterns. The extra signal patterns can be used for other purposes such as error detection.



V. Multiline Transmission: MLT-3:

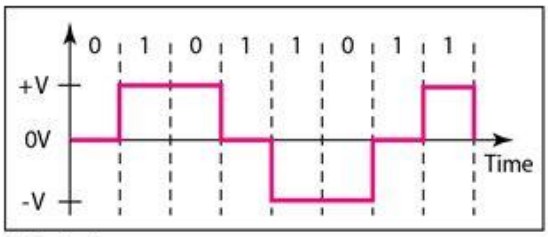
NRZ-I and differential Manchester are classified as differential encoding but use two transition rules to encode binary data (no inversion, inversion). If we have a signal with more than two levels, we can design a differential encoding scheme with more than two transition rules. MLT-3 is one of them. The multiline transmission, three level (MLT-3) scheme uses three levels (+V, 0 and -V) and three transition rules to move between the levels.

1. If the next bit is 0, there is no transition.

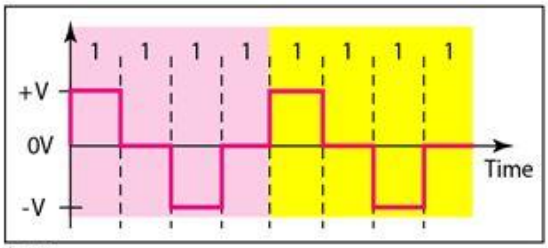
2. If the next bit is 1 and the current level is not 0, the next level is 0.
3. If the next bit is 1 and the current level is 0, the next level is the opposite of the last nonzero level.

The behavior ofMLT-3 can best be described by the state diagram shown in the following figure.

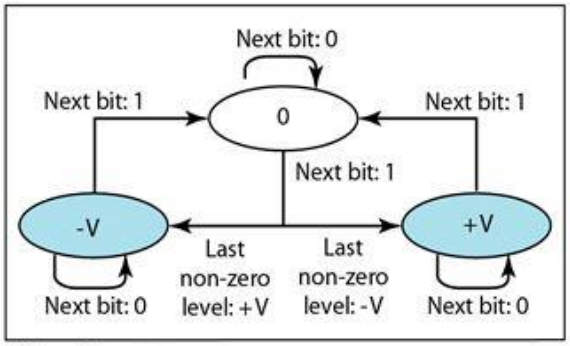
The three voltage levels (-V, 0, and +V) are shown by three states (ovals). The transition from one state (level) to another is shown by the connecting lines. The following figure also shows two examples of an MLT-3 signal.



a. Typical case



b. Worse case



c. Transition states

The signal rate is the same as that for NRZ-I, but with greater complexity (three levels and complex transition rules). It turns out that the shape of the signal in this scheme helps to reduce the required bandwidth. Let us look at the worst-case scenario, a sequence of Is. In this case, the signal element pattern +VO - VO is repeated every 4 bits.

A non-periodic signal has changed to a periodic signal with the period equal to 4 times the bit duration. This worst-case situation can be simulated as an analog signal with a frequency one-fourth of the bit rate. In other words, the signal rate for MLT-3 is one-fourth the bit rate. This makes MLT-3 a suitable choice when we need to send 100 Mbps on a copper wire that cannot support more than 32 MHz (frequencies above this level create electromagnetic emissions).