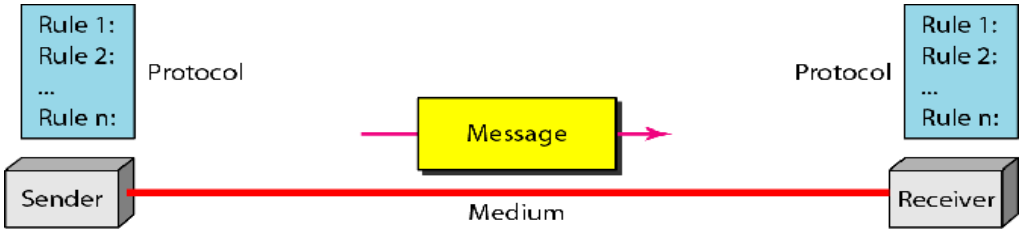
1.0 DATA COMMUNICATIONS AND NETWORKS

1.1 Introduction

In Data Communications, *data* generally are defined as information that is stored in digital form. *Data communications* is the process of transferring digital information between two or more points. *Information* is defined as the knowledge or intelligence. Data communications can be summarized as the transmission, reception, and processing of digital information. For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs). The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

1. **Delivery:** The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
2. **Accuracy:** The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.
3. **Timeliness:** The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.
4. **Jitter:** Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets. For example, let us assume that video packets are sent every 30ms. If some of the packets arrive with 30ms delay and others with 40ms delay, an uneven quality in the video is the result.

1.2 Components of a data communications system



A data communications system has five components:

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

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

Receiver: The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

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

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

1.3 NETWORK

A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

1.3.1 Network Criteria

A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security.

1. **Performance -** Performance can be measured in many ways, including transmit time and response time. Transmit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an inquiry and a response. The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software. Performance is often evaluated by two networking metrics: throughput and delay. We often need more throughputs and less delay.
2. **Reliability -** In addition to accuracy of delivery, network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure.
3. **Security -** Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

1.3.2 Network Models

Computer networks can be represented with two basic network models: peer-to-peer client/server and dedicated client/server. The client/server method specifies the way in which two computers can communicate with software over a network.

1. **Dedicated client/server network:** Here, one computer is designated as server and the rest of the computers are clients. Dedicated Server Architecture can improve the efficiency of client server systems by using one server for each application that exists within an organization.The designated servers store all the networks shared files and applications programs and function only as servers and are not used as a client or workstation. Client computers can access the servers and have shared files transferred to them over the transmission medium. In some client/server networks, client computers submit jobs to one of the servers and once they process the jobs, the results are sent back to the client computer.
2. **Peer-to-peer client/server network**: Here, all the computers share their resources, such as hard drives, printers and so on with all the other computers on the network. Individual resources like disk drives, CD-ROM drives, and even printers are transformed into shared, collective resources that are accessible from every PC. Unlike client-server networks, where network information is stored on a centralized file server PC and made available to tens, hundreds, or thousands client PCs, the information stored across peer-to-peer networks is uniquely decentralized. Because peer-to-peer PCs have their own hard disk drives that are accessible by all computers, each PC acts as both a client (information requestor) and a server (information provider). The peer-to-peer network is an appropriate choice when there are fewer than 10 users on the network, security is not an issue and all the users are located in the same general area.

In general, the dedicated client/server model is preferable to the peer-to-peer client/server model for general purpose data networks. However there some advantages of peer-to-peer over client-server this include:

- No need for a network administrator.
- Network is fast/inexpensive to setup & maintain.
- Each PC can make backup copies of its data to other PCs for security.
- Easiest type of network to build, peer-to-peer is perfect for both home and office use.

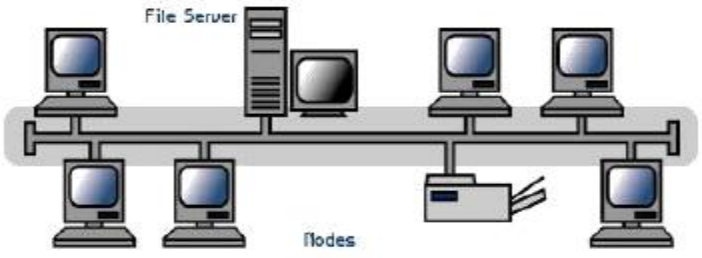
1.3.3 Network Topologies

In computer networking, *topology* refers to the layout of connected devices, i.e. how the computers, cables, and other components within a data communications network are interconnected, both physically and logically. The physical topology describes how the network is actually laid out, and the logical topology describes how the data actually flow through the network. There are four basic topologies possible:

- bus
- star
- ring
- mesh

a. Bus Topology

Bus networks use a common backbone to connect all devices. A single cable, (the backbone) functions as a shared communication medium that devices attach or tap into with an interface connector. A device wanting to communicate with another device on the network sends a broadcast message onto the wire that all other devices see, but only the intended recipient actually accepts and processes the message. The bus topology is the simplest and most common method of interconnecting computers. The two ends of the transmission line never touch to form a complete loop. A bus topology is also known as multidrop or linear bus or a horizontal bus.



Advantages

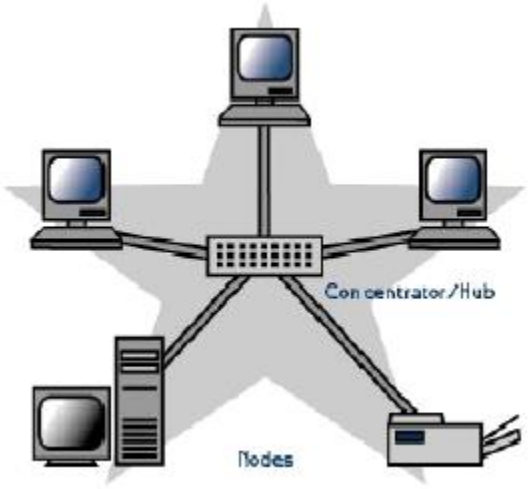
i. Bus topology includes ease of installation.
ii. A bus uses less cabling than mesh or star topologies.

Disadvantages

i. Difficult reconnection and fault isolation.
ii. A fault or break in the bus cable stops all transmission, even between devices on the same side of the problem.

b. Star Topology

A star topology is designed with each node (file server, workstations, and peripherals) connected directly to a central network hub or concentrator. Data on a star network passes through the hub or concentrator before continuing to its destination. The hub or concentrator manages and controls all functions of the network. It also acts as a repeater for the data flow.



Advantages

i. A star topology is less expensive than a mesh topology.
ii. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure.
iii. Far less cabling needs to be housed, and additions, moves, and deletions involve only one connection: between that device and the hub.
iv. Other advantages include robustness. If one link fails, only that link is affected. All other links remain active.

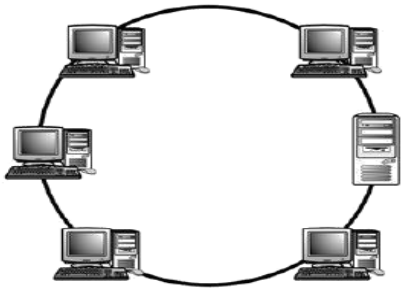
Disadvantages

i. The dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.

ii. Although a star requires far less cable than a mesh, each node must be linked to a central hub.

c. Ring Topology

In a ring network (sometimes called a loop), every device has exactly two neighbours for communication purposes. All messages travel through a ring in the same direction (either "clockwise" or "counter clockwise"). All the stations are interconnected in tandem (series) to form a closed loop or circle. Transmissions are unidirectional and must propagate through all the stations in the loop. Each computer acts like a repeater and the ring topology is similar to bus or star topologies.



Advantages

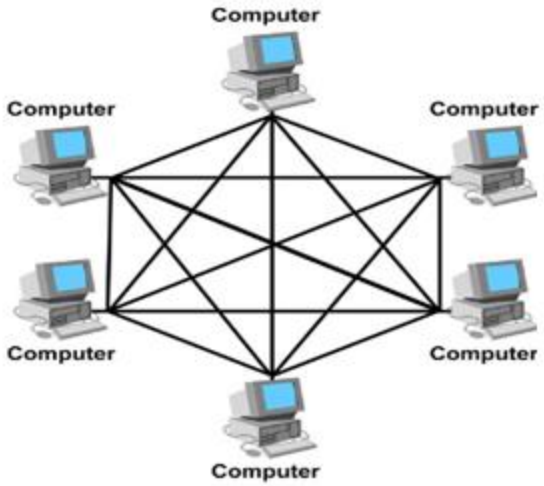
i. A ring is relatively easy to install and
ii. reconfigure. Fault isolation is simplified.

Disadvantages

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

d. Mesh Topology

The *mesh* topology incorporates a unique network design in which each computer on the network connects to every other, creating a point-to-point connection between every device on the network. Unlike each of the previous topologies, messages sent on a mesh network can take any of several possible paths from source to destination. A mesh network in which every device connects to every other is called a full mesh.



Advantages:

i. The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.

ii. A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.

iii. There is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages.

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

Disadvantages:

i. Disadvantage of a mesh are related to the amount of cabling because every device must be connected to every other device.

ii. Installation and reconnection are difficult.

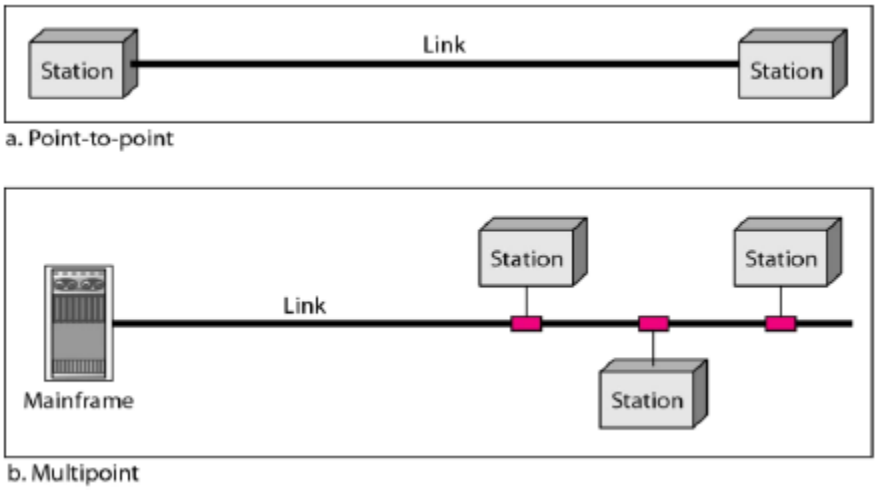
iii. The sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.

iv. The hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.

1.3.4 Line Configuration

Line configuration refers to the way two or more communication devices attach to a link. For communication to occur, two devices must be connected in some way to the same link at the same time. There are two possible line configurations: point to point or multipoint.

A *point to point* configuration involves only two locations or stations, whereas a *multipoint* configuration involves three or more stations.



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

A multi-point also called multidrop line configuration is one in which more than two specific devices share a link.

1.3.5 Types of Networks

Computer Networks are mostly classified on the basis of the geographical area that the network covers, the topology used, the transmission media used and the computing model used. Based on the geographical area covered the networks may be LAN,MAN or WAN.

a. Local area network(LAN)

A local area network (LAN) is a network that connects computers and devices in a limited geographical area such as home, school, computer laboratory, office building, or closely positioned group of buildings. LANs use a network operating system to provide two-way communications at bit rates in the range of 10 Mbps to 100 Mbps. In addition to operating in a limited space, LANs are also typically owned, controlled, and managed by a single person or

organization. They also tend to use certain connectivity technologies, primarily Ethernet and Token Ring.

b. Metropolitan area network(MAN)

A MAN is optimized for a larger geographical area than a LAN, ranging from several blocks of buildings to entire cities. Its geographic scope falls between a WAN and LAN. A MAN might be a single network like the cable television network or it usually interconnects a number of local area networks (LANs) using a high capacity backbone technology, such as fiber-optical links, and provides up-link services to wide area networks and the Internet. MANs typically operate at speeds of 1.5 Mbps to 10 Mbps and range from five miles to a few hundred miles in length. Examples of MANs are FDDI (fiber distributed data interface) and ATM (asynchronous transfer mode).

c. Wide area network(WAN)

Wide area networks are the oldest type of data communications network that provide relatively slow-speed, long-distance transmission of data, voice and video information over relatively large and widely dispersed geographical areas, such as country or entire continent. WANs interconnect routers in different locations. A WAN differs from a LAN in several important ways. Most WANs (like the Internet) are not owned by any one organization but rather exist under collective or distributed ownership and management. WANs tend to use technology like ATM, Frame Relay and X.25 for connectivity over the longer distances.

1.3.6 Advantages of Networks

Computers in a networked environment provide numerous advantages when compared to computers in a stand alone environment. The immense benefits that the computer networks provide are in the form of excellent sharing of computational resources, computational load, increased level of reliability, economy and efficient person-to-person communication. Following are some of the major advantages of using computer networks.

1. **Resource Sharing -** The main aim of a computer network is to make all programs, equipment, and data available to anyone on the network without regard to the physical location of the resource and the user. Users need to share resources other than files, as well. A common example being printers.Printers are utilised only a small percentage of the time;

therefore, companies don't want to invest in a printer for each computer. Networks can be used in this situation to allow all the users to have access to any of the available printers.

2. **High Reliability -** Computer networks provide high reliability by having alternative sources of supply. For example, all files could be replicated on two or three machines, so, if one of them is unavailable (due to hardware failure), the other copies could be used. In addition, the presence of multiple CPUs means that if one goes down, the others may be able to take over its work, although at reduced performance.
3. **Saving Money -** Small computers have a much better price/performance ratio than larger ones. Mainframes are roughly a factor of ton faster than personal computers but they cost much more. This imbalance has caused many systems designers to build systems consisting of personal computers, one per user, with data kept on one or more shared file server machines.In this model, the users are called clients, and the whole arrangement is called the client-server model.
4. **Scalability -** The ability to increase the system performance gradually as the workload grows just by adding more processors. With centralized mainframes, when a system is full, it must be replaced by a larger one, usually at great expense and even greater disruption to the users. With client-server model, new clients and new servers can be added when needed.
5. **Communication Medium -** A computer network can provide a powerful communication medium among widely separated users. Using a computer network it is easy for two or more people who are working on the same project and who live far apart to write a report together. When one worker, makes a change to an on-line document, the others can see the change immediately, instead of waiting several days for a letter. Such a speedup makes cooperation among far-flung groups of people easy whereas previously it was impossible.
6. **Increased Productivity -** Networks increase productivity as several people can enter data at the same time, but they can also evaluate and process the shared data. So, one person can handle accounts receivable, and someone else processes the profit-and-loss statements.

1.4 STANDARDS ORGANIZATIONS FOR DATA COMMUNICATIONS

An association of organizations, governments, manufacturers and users form the standards organizations and are responsible for developing, coordinating and maintaining the standards.

The intent is that all data communications equipment manufacturers and users comply with these standards. The primary standards organizations for data communication are:

1. International Standard Organization (ISO)

ISO is the international organization for standardization on a wide range of subjects. It is comprised mainly of members from the standards committee of various governments throughout the world. It is even responsible for developing models which provides high level of system compatibility, quality enhancement, improved productivity and reduced costs. The ISO is also responsible for endorsing and coordinating the work of the other standards organizations.

2. International Telecommunications Union-Telecommunication Sector (ITU-T)

ITU-T is one of the four permanent parts of the International Telecommunications Union based in Geneva, Switzerland. It has developed three sets of specifications: the *V series* for modem interfacing and data transmission over telephone lines, the *X series* for data transmission over public digital networks, email and directory services; the *I and Q series* for Integrated Services Digital Network (ISDN) and its extension Broadband ISDN. ITU-T membership consists of government authorities and representatives from many countries and it is the present standards organization for the United Nations.

3. Institute of Electrical and Electronics Engineers (IEEE)

IEEE is an international professional organization founded in United States and is compromised of electronics, computer and communications engineers. It is currently the world's largest professional society with over 200,000 members. It develops communication and information processing standards with the underlying goal of advancing theory, creativity, and product quality in any field related to electrical engineering.

4. American National Standards Institute (ANSI)

ANSI is the official standards agency for the United States and is the U.S voting representative for the ISO. ANSI is a completely private, non-profit organization comprised of equipment manufacturers and users of data processing equipment and services. ANSI membership is comprised of people form professional societies, industry associations, governmental and regulatory bodies, and consumer goods.

5. Electronics Industry Association (EIA)

EIA is a non-profit U.S. trade association that establishes and recommends industrial standards. EIA activities include standards development, increasing public awareness, and lobbying and it

is responsible for developing the RS (recommended standard) series of standards for data and communications.

6. Telecommunications Industry Association (TIA)

TIA is the leading trade association in the communications and information technology industry. It facilitates business development opportunities through market development, trade promotion, trade shows, and standards development. It represents manufacturers of communications and information technology products and also facilitates the convergence of new communications networks.

7. Internet Architecture Board (IAB)

IAB earlier known as Internet Activities Board is a committee created by ARPA (Advanced Research Projects Agency) so as to analyze the activities of ARPANET whose purpose is to accelerate the advancement of technologies useful for U.S military. IAB is a technical advisory group of the Internet Society and its responsibilities are:

i. Oversees the architecture protocols and procedures used by the Internet.
ii. Manages the processes used to create Internet Standards and also serves as an appeal board for complaints regarding improper execution of standardization process.
iii. Responsible for administration of the various Internet assigned numbers
iv. Acts as a representative for Internet Society interest in liaison relationships with other organizations.
v. Acts as a source of advice and guidance to the board of trustees and officers of Internet Society concerning various aspects of internet and its technologies.

8. Internet Engineering Task Force (IETF)

The IETF is a large international community of network designers, operators, vendors and researchers concerned with the evolution of the Internet architecture and smooth operation of the Internet.

9. Internet Research Task Force (IRTF)

The IRTF promotes research of importance to the evolution of the future Internet by creating focused, long-term and small research groups working on topics related to Internet protocols, applications, architecture and technology.

2.0 DATA ENCODING TECHNIQUES

Encoding is the process of converting the data or a given sequence of characters, symbols, alphabets etc., into a specified format, for the secured transmission of data. **Decoding** is the reverse process of encoding which is to extract the information from the converted format. There are four possible combinations of encoding techniques:

1. Digital data, digital signal
2. Digital data, analog signal
3. Analog data, digital signal
4. Analog data, analog signal

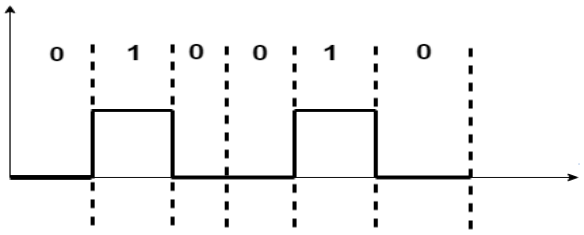
2.2 Digital Data, Digital Signals

Digital-to-digital encoding is the representation of digital information by a digital signal. When binary 1s and 0s generated by the computer are translated into a sequence of voltage pulses that can be propagated over a wire, this process is known as digital-to-digital encoding. There are basically following types of digital· to-digital encoding available:

- Unipolar
- Polar
- Bipolar.

2.2.1 Unipolar

Unipolar encoding uses only one level of value 1 as a positive value and 0 remains Idle. Since unipolar line encoding has one of its states at 0 Volts, it's also called Return to Zero (RTZ) . Unipolar encoding is simpler and inexpensive to implement.



2.2.2 Polar

Polar encoding uses two levels of voltages say positive and negative. For The signal does not return to *zero;* it is either a positive voltage or a negative voltage. Polar encoding may be classified as:

- non·return to zero (NRZ),
- return to zero (RZ) and
- biphase.

1. NRZ (Non-Return-to-Zero)

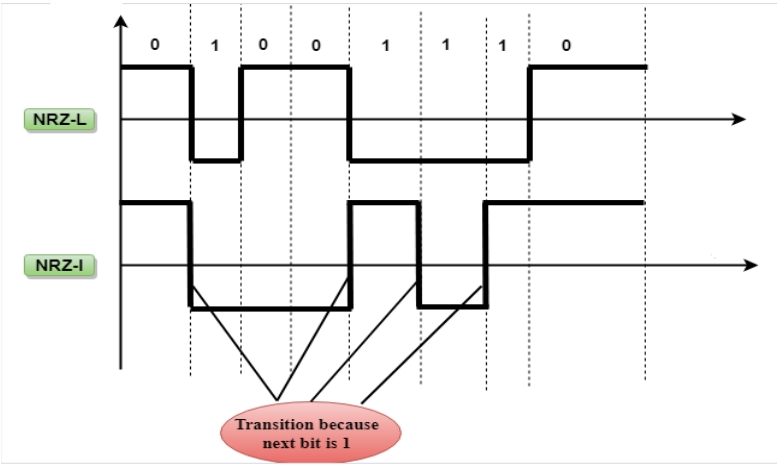
NRZ (Non-Return-to-Zero) Codes Data Encoding Uses two different voltage levels (one positive and one negative) as the signal elements for the two binary digits. NRZ may be further divided into NRZ·L and NRZ·I.

a. Non Return to Zero Level (NRZ – L)

There is a change in the polarity of the signal, only when the incoming signal changes from 1 to 0 or from 0 to 1. It is the same as NRZ, however, the first bit of the input signal should have a change of polarity.

b. Non Return to Zero Invertive (NRZ - I)

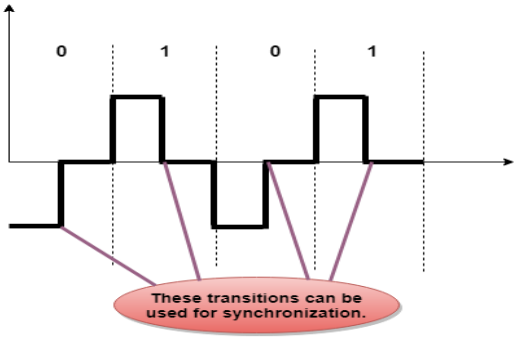
If a 1 occurs at the incoming signal, then there occurs a transition at the beginning of the bit interval. For a 0 at the incoming signal, there is no transition at the beginning of the bit interval.



NRZ codes has a disadvantage that the synchronization of the transmitter clock with the receiver clock gets completely disturbed, when there is a string of 1s and 0s. Hence, a separate clock line needs to be provided.

2. Return to Zero (RZ)

In the RZ scheme, halfway through each interval, the signal returns to zero. In RZ scheme, 1 bit is represented by positive-to-zero and 0 bit is represented by negative-to-zero.



3. Bi-phase Encoding

The signal level is checked twice for every bit time, both initially and in the middle. Hence, the clock rate is double the data transfer rate and thus the modulation rate is also doubled. The clock is taken from the signal itself. The bandwidth required for this coding is greater. There are two types of Bi-phase Encoding.

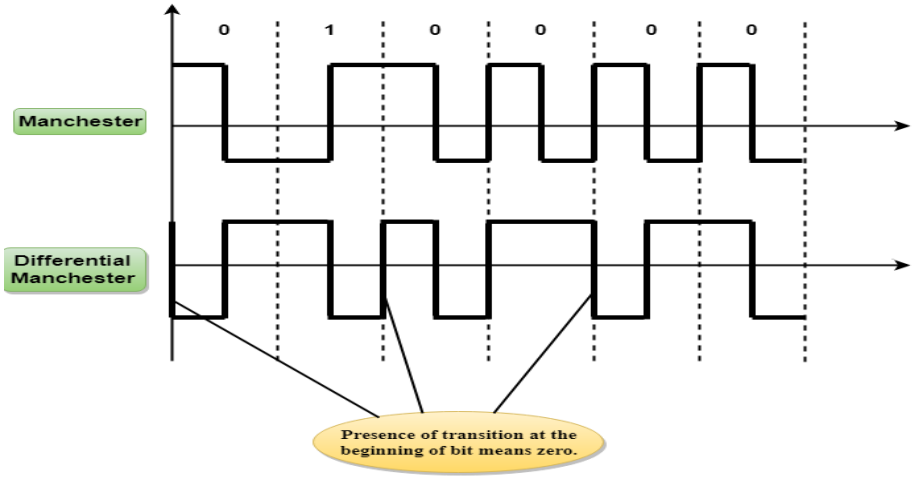
- Manchester
- Differential Manchester

a. Manchester

In this type of coding, the transition is done at the middle of the bit-interval. In Manchester encoding, a negative-to-positive transition represents binary 1, and positive-to-negative transition represents 0. Manchester has the same level of synchronization as RZ scheme except that it has two levels of amplitude.

b. Differential Manchester

In this type of coding, there always occurs a transition in the middle of the bit interval. If there occurs a transition at the beginning of the bit interval, then the input bit is **0**. If no transition occurs at the beginning of the bit interval, then the input bit is **1**.



2.2.3 Bipolar

Bipolar uses three voltage levels. These are positive, negative, and zero. In Bipolar encoding scheme, zero level represents binary 0, and binary 1 is represented by alternating positive and negative voltages. If the first 1 bit is represented by positive amplitude, then the second 1 bit is represented by negative voltage, third 1 bit is represented by the positive amplitude and so on. This alternation can also occur even when the 1bits are not consecutive. Bipolar can be classified as:

- Alternate Mark Inversion (AMI)
- Bipolar 8-Zero Substitution(B8ZS)
- High-Density Bipolar 3(HDB3)

a. Alternate Mark Inversion (AMI)

In Bipolar AMI encoding scheme, 0 bit is represented by zero level and 1 bit is represented by alternating positive and negative voltages.

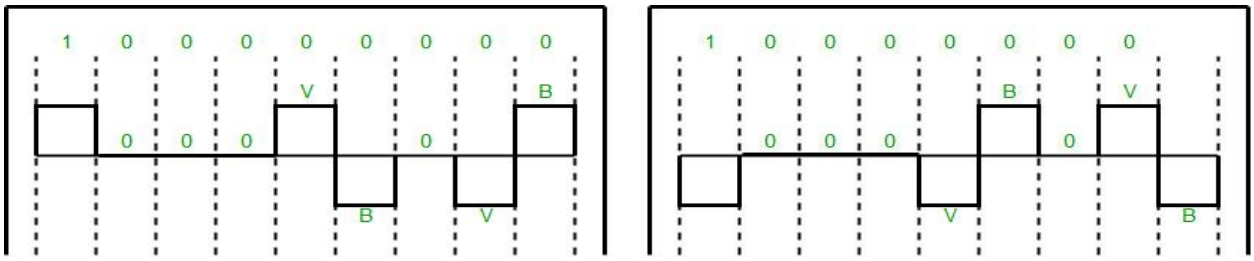
b. Bipolar 8-Zero Substitution(B8ZS)

B8ZS is similar to the bipolar AMI, but the only difference is that it provides the synchronization when a long sequence of 0s bits occur.B8ZS ensures synchronization of a long string of 0s by providing force artificial signal changes called violations, within 0 string pattern. when eight consecutive zero-level voltages are encountered they are replaced by the sequence, "000VB0VB".

V(Violation), is a non-zero voltage which means signal have same polarity as the previous non-zero voltage. Thus it is violation of general AMI technique. B(Bipolar), also non-zero voltage level which is in accordance with the AMI rule (i.e.,opposite polarity from the previous non-zero voltage).

Example:

Given Data = 100000000



Both figures (left and right one) are correct, depending upon last non-zero voltage signal of previous data sequence (i.e., sequence before current data sequence "100000000").

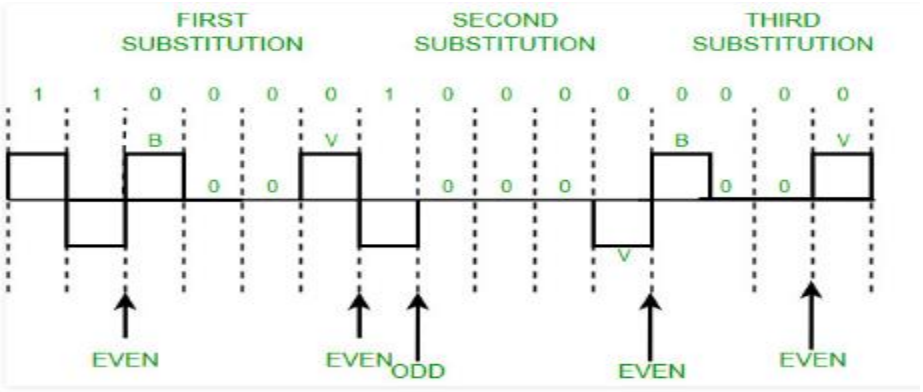
c. High-Density Bipolar 3(HDB3)

HDB3 technique is designed to provide the synchronization of a long sequence of 0s bits. In the HDB3 technique, the pattern of violation is based on the polarity of the previous bit. When four 0s occur, HDB3 looks at the number of 1s bits occurred since the last substitution. In this technique four consecutive zero-level voltages are replaced with a sequence "000V" or "B00V". Rules for using these sequences:

- If the number of nonzero pulses after the last substitution is odd, the substitution pattern will be “000V”, this helps maintaining total number of nonzero pulses even.
- If the number of nonzero pulses after the last substitution is even, the substitution pattern will be “B00V”. Hence even number of nonzero pulses is maintained again.

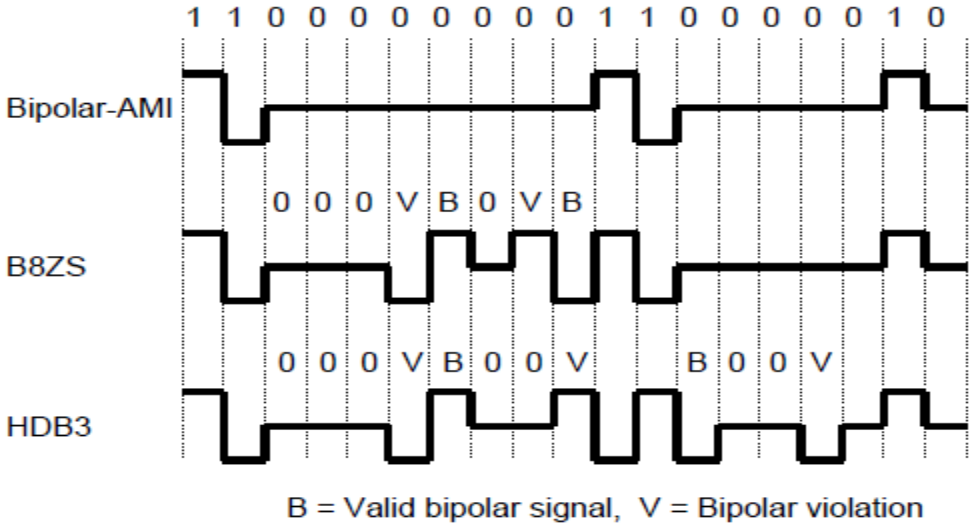
Example:

Given Data = 1100001000000000

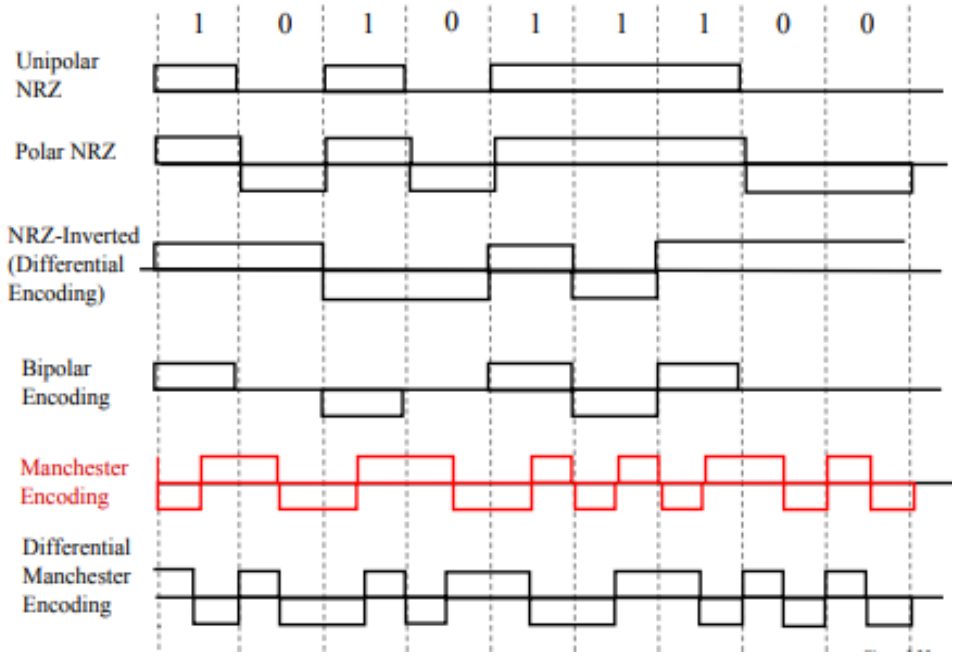


After representing first two 1’s of data we encounter four consecutive zeros. Since our last substitutions were two 1’s(thus number of non-zero pulses is even).So,we substitute four zeros with “B00V”.

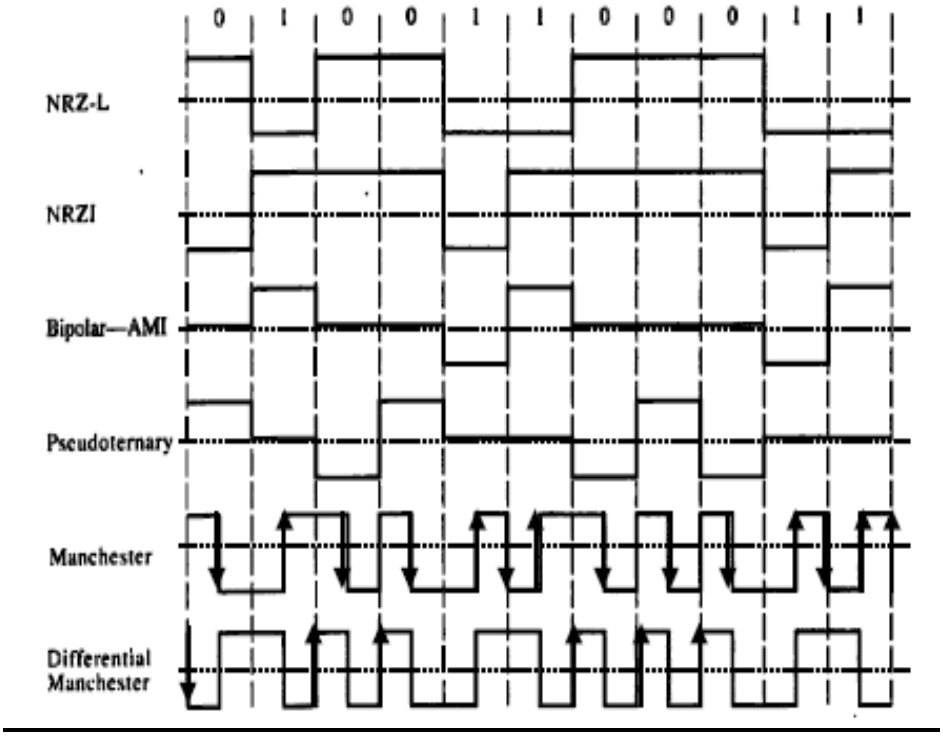
Example of Bipolar



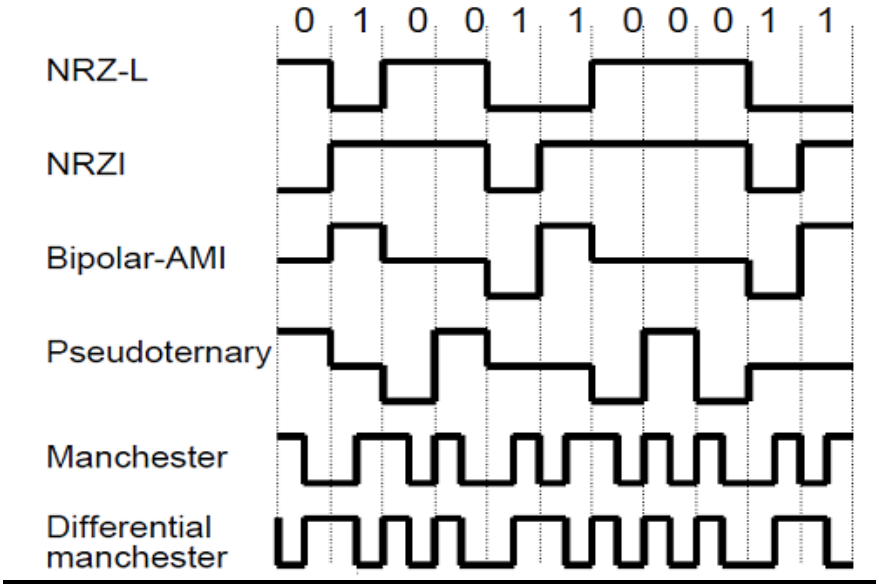
Example 1



Example 2



Example 3

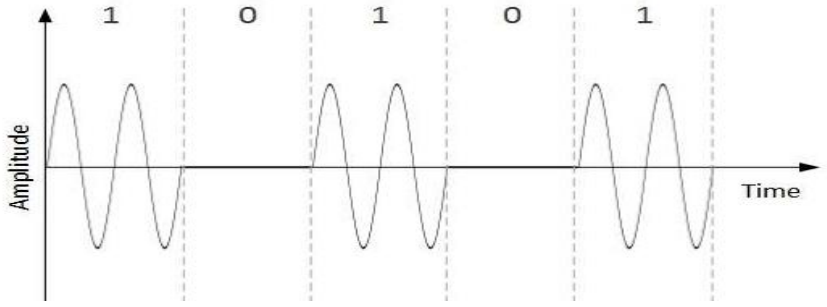


2.2 Digital Data, Analog Signals

Basis for analog signaling is a continuous, constant-frequency signal known as the carrier frequency.A modem (modulator-demodulator) converts digital data to analog signal. Digital data is encoded by modulating one of the three characteristics of the carrier: amplitude, frequency, or phase or some combination of these.

2.2.1 Amplitude shift keying (ASK):

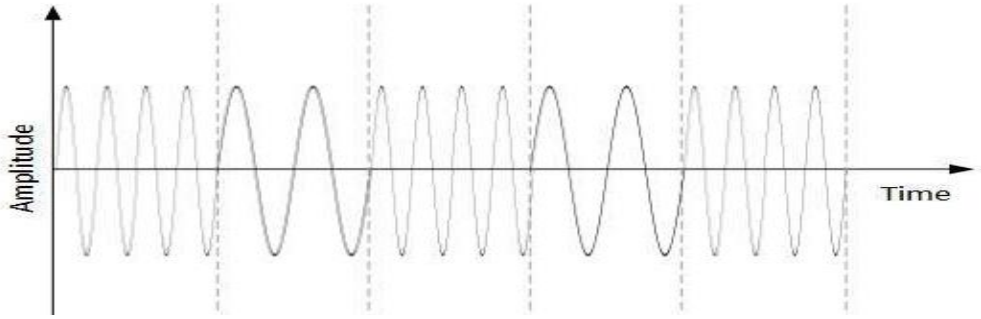
Amplitude shift keying is a form of modulation which represents digital data as variations in the amplitude of a carrier wave. 1 binary digit represented by presence of carrier, at constant amplitude while 0 binary digit represented by absence of carrier.



Relatively inexpensive to implement however Inefficient modulation technique since it is much more susceptible to noise.

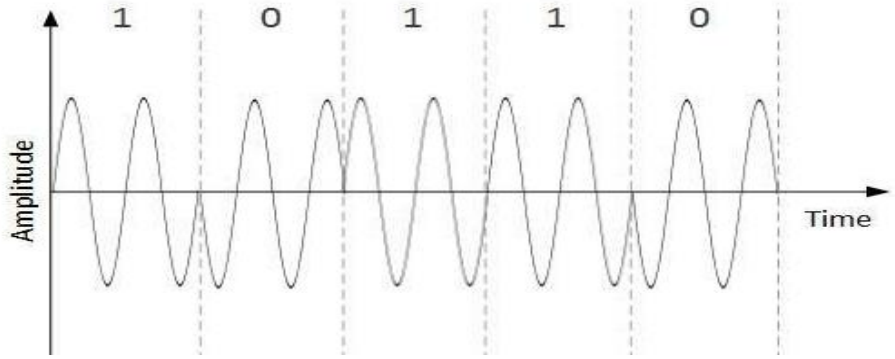
2.2.2 Frequency shift keying (FSK):

In Frequency Shift Keying, the change in frequency define different digits. Two different frequencies near carrier frequency represent '0' ,"1'.

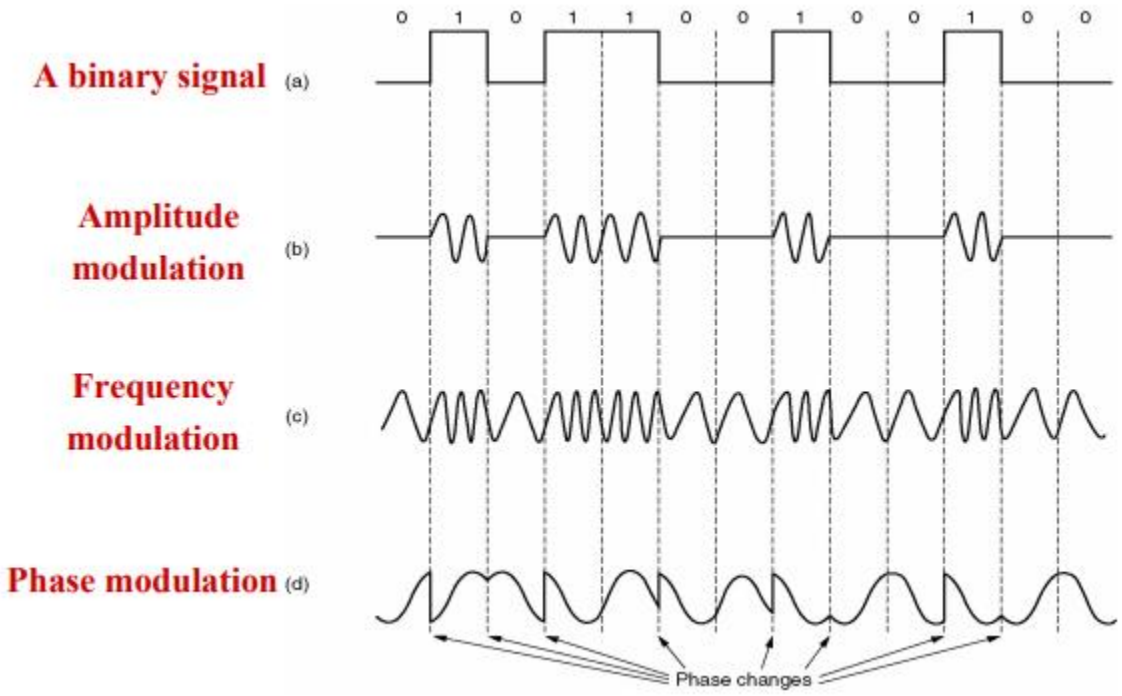


2.2.3 Phase shift keying (PSK):

The phase of the carrier is discretely varied in relation either to a reference phase or to the phase of the immediately preceding signal element, in accordance with data being transmitted. Phase of carrier signal is shifted to represent '0' , '1'.



Example of the three techniques



2.3 Analog data, digital signal

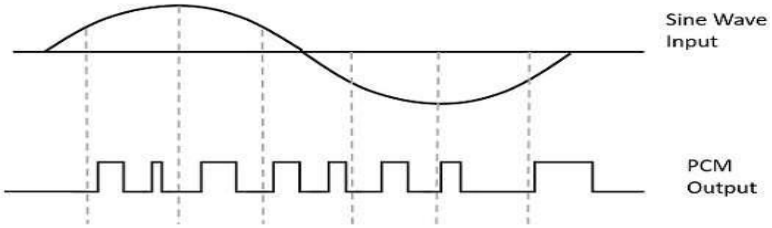
The process of transforming analog data into digital signal is called digitization. The device used for converting analog into digital form for transmission and subsequently recovering the original analog data from the digital is known as a codec(coder-decoder). There are two principal techniques used in codecs:

- Pulse code modulation
- Delta modulation

2.3.1 Pulse Code Modulation (PCM)

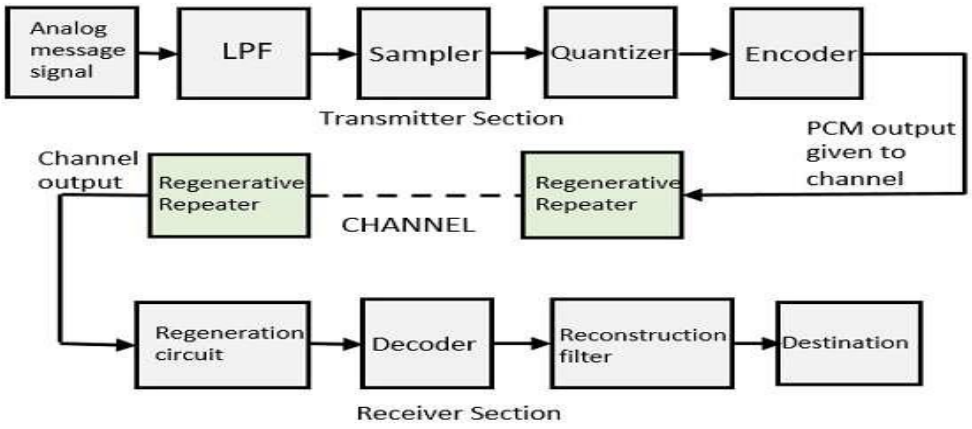
Pulse-code modulation (PCM) is a method used to digitally represent sampled analog signals. A PCM stream is a digital representation of an analog signal, in which the magnitude of the

analogue signal is sampled regularly at uniform intervals, with each sample being quantized to the nearest value within a range of digital steps. The following figure shows an example of PCM output with respect to instantaneous values of a given sine wave.



In Pulse Code Modulation, the message signal is represented by a sequence of coded pulses. This message signal is achieved by representing the signal in discrete form in both time and amplitude.

Basic Elements of PCM



The transmitter section of a Pulse Code Modulator circuit consists of **Sampling, Quantizing** and **Encoding**, which are performed in the analog-to-digital converter section. The low pass filter prior to sampling prevents aliasing of the message signal. The basic operations in the receiver section are:

- regeneration of impaired signals
- decoding, and
- reconstruction of the quantized pulse train.

Low Pass Filter

This filter eliminates the high frequency components present in the input analog signal which is greater than the highest frequency of the message signal, to avoid aliasing of the message signal.

Sampler

This is the technique which helps to collect the sample data at instantaneous values of message signal, so as to reconstruct the original signal. The sampling rate must be greater than twice the highest frequency component **W**of the message signal, in accordance with the sampling theorem.

Quantizer

Quantizing is a process of reducing the excessive bits and confining the data. The sampled output when given to Quantizer reduces the redundant bits and compresses the value.

Encoder

The digitization of analog signal is done by the encoder. It designates each quantized level by a binary code. The sampling done here is the sample-and-hold process. These three sections (LPF, Sampler, and Quantizer) will act as an analog to digital converter. Encoding minimizes the bandwidth used.

Regenerative Repeater

This section increases the signal strength. The output of the channel also has one regenerative repeater circuit, to compensate the signal loss and reconstruct the signal, and also to increase its strength.

Decoder

The decoder circuit decodes the pulse coded waveform to reproduce the original signal. This circuit acts as the demodulator.

Reconstruction Filter

After the digital-to-analog conversion is done by the regenerative circuit and the decoder, a low-pass filter is employed, called as the reconstruction filter to get back the original signal. Hence, the Pulse Code Modulator circuit digitizes the given analog signal, codes it and samples it, and then transmits it in an analog form. This whole process is repeated in a reverse pattern to obtain the original signal.

PCM Processes

A PCM encoder has the following three processes:

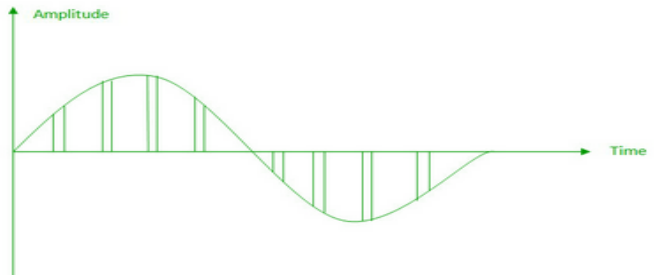
- Sampling
- Quantization
- Encoding

Sampling:

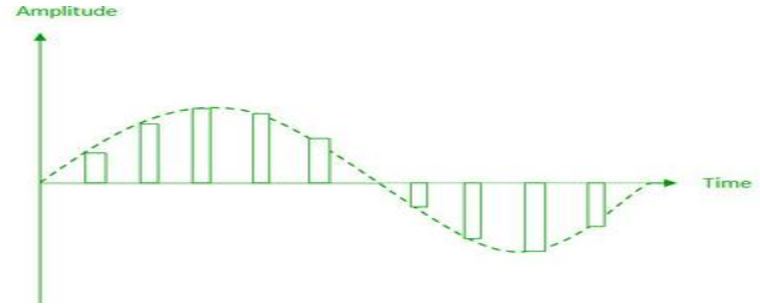
Sampling is the process of taking amplitude values of the continuous analog signal at discrete time intervals (sampling period Ts). There are three sampling methods:

(i) Ideal Sampling: In ideal Sampling also known as Instantaneous sampling pulses from the analog signal are sampled. This is an ideal sampling method and cannot be easily implemented.

(ii) Natural Sampling: Natural Sampling is a practical method of sampling in which pulse have finite width equal to T. The result is a sequence of samples that retain the shape of the analog signal.



(iii) Flat top sampling: In comparison to natural sampling flat top sampling can be easily obtained. In this sampling technique, the top of the samples remains constant by using a circuit. This is the most common sampling method used.



Quantization:

Quantization involves assigning a numerical value to each sampled amplitude value from a range of possible values covering the entire amplitude range (based on the number of bits).

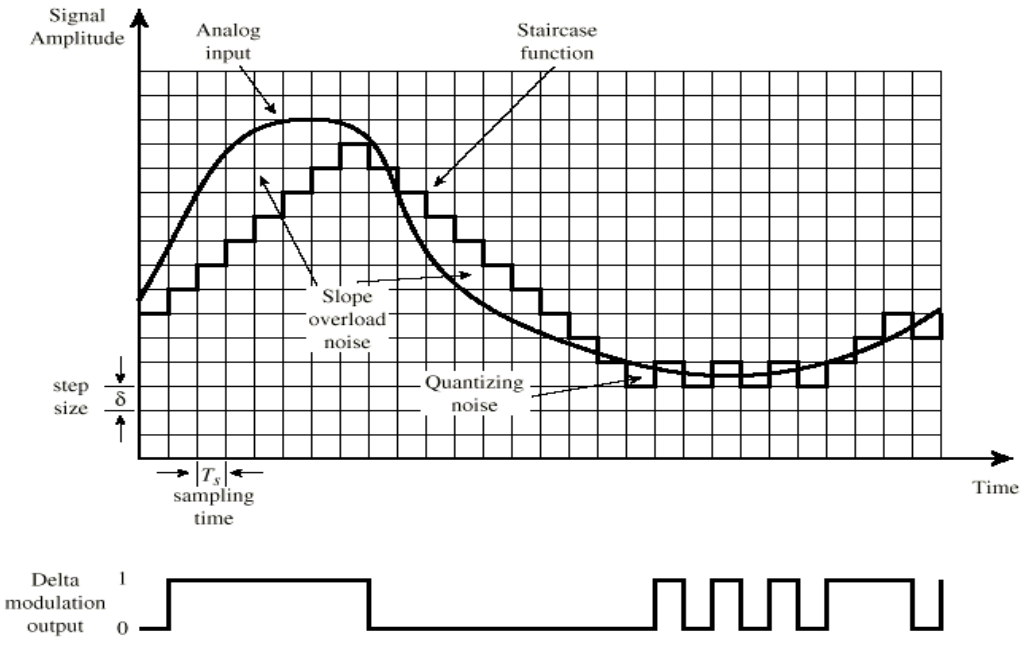
Coding:

Once the amplitude values have been quantized they are encoded into binary using an Encoder.

2.3.2 Delta Modulation

While the conversion of an analog signal into a binary signal, the PCM (pulse code modulation) technique is used. But this system has a disadvantage like it requires large bandwidth So these can be overcome by using Delta Modulation. It is one type of technique used for the conversion of an analog signal into a digital version.

In Delta modulation the analog signal is approximated with a series of segments. Each segment of the approximated signal is compared to the preceding bits and the successive bits are determined by this comparison. Only the change of information is sent, that is, only an increase or decrease of the signal amplitude from the previous sample is sent whereas a no-change condition causes the modulated signal to remain at the same 0 or 1 state of the previous sample. To achieve high signal-to-noise ratio, delta modulation must use oversampling techniques, that is, the analog signal is sampled at a rate several times higher than the Nyquist rate.



1 = Signal up one step, 0 = Signal down one step

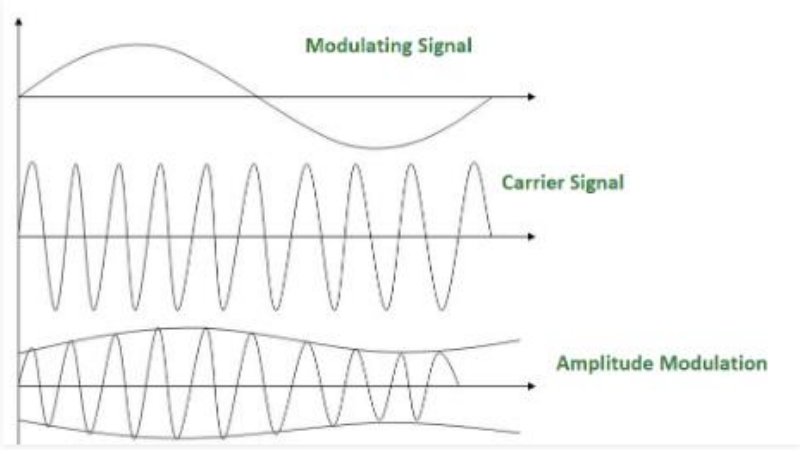
2.4 Analog data, analog signal

Analog-to-analog conversion, or modulation, is the representation of analog information by an analog signal. It is a process by virtue of which a characteristic of carrier wave is varied according to the instantaneous amplitude of the modulating signal. This modulation is generally needed when a *bandpass channel* is required. Bandpass is a range of frequencies which are transmitted through a bandpass filter which is a filter allowing specific frequencies to pass preventing signals at unwanted frequencies. Analog to Analog conversion can be done in three ways:

- Amplitude Modulation
- Frequency Modulation
- Phase Modulation

2.4.1 Amplitude Modulation

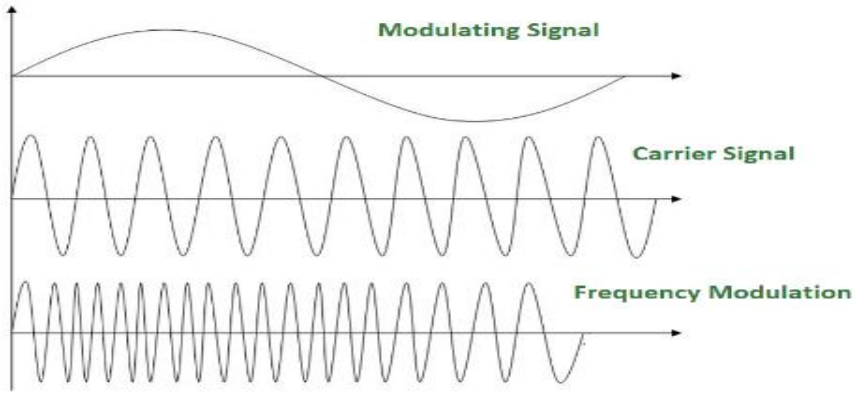
In this modulation, the amplitude of the carrier signal is modified to reflect the analog data keeping phase and frequency constant.



AM is normally implemented by using a simple multiplier because the amplitude of the carrier signal needs to be changed according to the amplitude of the modulating signal.

2.4.2 Frequency Modulation

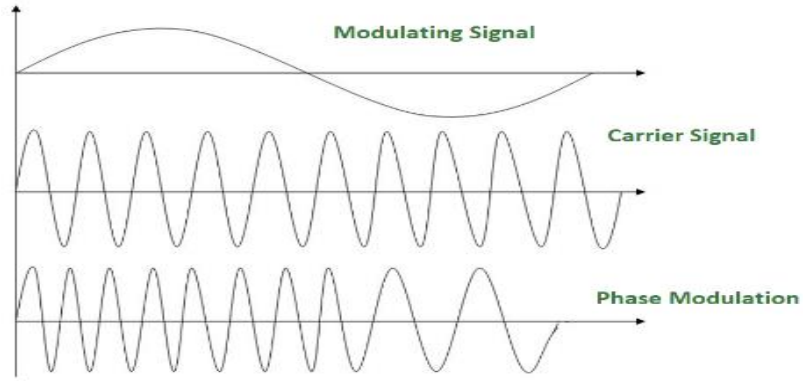
The modulation in which the frequency of the carrier wave is varied according to the instantaneous amplitude of the modulating signal keeping phase and amplitude as constant.



FM is normally implemented by using a voltage-controlled oscillator as with FSK. The frequency of the oscillator changes according to the input voltage which is the amplitude of the modulating signal.

2.4.3 Phase Modulation

The modulation in which the phase of the carrier wave is varied according to the instantaneous amplitude of the modulating signal keeping amplitude and frequency as constant.



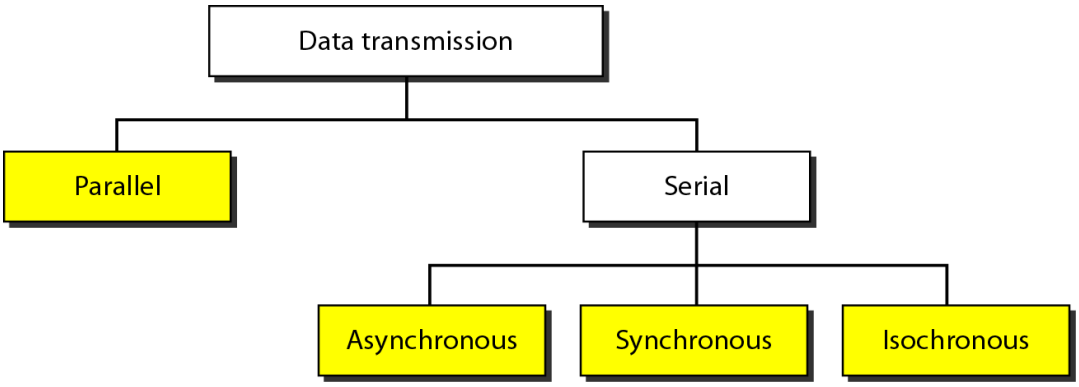
Phase modulation is practically similar to Frequency Modulation, but in Phase modulation frequency of the carrier signal is not increased. Frequency of carrier is signal is changed (made dense and sparse) to reflect voltage change in the amplitude of modulating signal.

It is normally implemented by using a voltage-controlled oscillator along with a derivative. The frequency of the oscillator changes according to the derivative of the input voltage which is the amplitude of the modulating signal.

3.0 MODES OF DATA TRANSMISSION

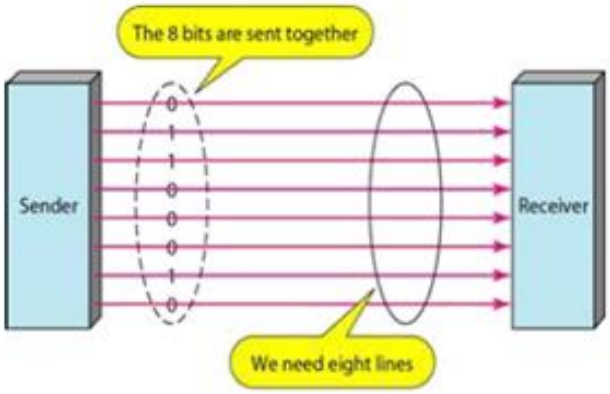
Data transmission refers to the process of transferring data between two or more digital devices. Data is transmitted from one device to another in analog or digital format. Basically, data transmission enables devices or components within devices to speak to each other. Data is transferred in the form of bits between two or more digital devices. There are two methods used to transmit data between digital devices:

- serial transmission
- parallel transmission.



Serial transmission has three classifications: asynchronous , synchronous and Isochronous.

3.1 Parallel data transmission

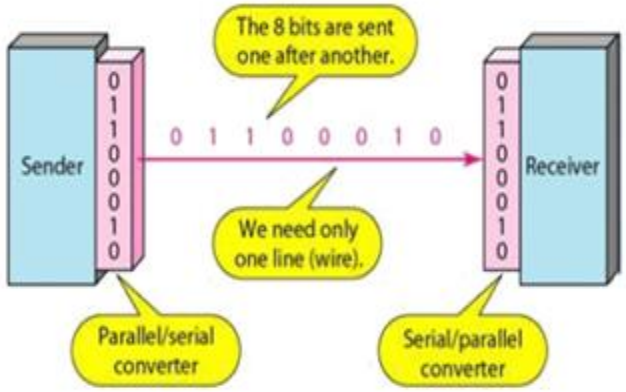


In parallel data transmission, all bits of the binary data are transmitted simultaneously. For example, to transmit an 8-bit binary number in parallel from one unit to another, eight

transmission lines are required. Each bit requires its own separate data path. All bits of a word are transmitted at the same time.

This method of transmission can move a significant amount of data in a given period of time. Its disadvantage is the large number of interconnecting cables between the two units. For large binary words, cabling becomes complex and expensive. This is particularly true if the distance between the two units is great. Long multiwire cables are not only expensive, but also require special interfacing to minimize noise and distortion problems.

3.2 Serial data transmission



In Serial data transmission, bits are transmitted serially, one after the other. The least significant bit (LSB) is usually transmitted first. While sending data serially, characters or bytes have to be separated and sent bit by bit. Thus, some hardware is required to convert the data from parallel to serial. At the destination, all the bits are collected, measured and put together as bytes in the memory of the destination. This requires conversion from serial to parallel.

One of the major difficulties in data transmission is that of synchronising the receiver (destination) with the sender (source). This is the main problem with serial communication. The receiver must be able to detect the beginning of each new character in the bit stream that is being presented to it and if it is not able to achieve this, it will not be able to interpret the incoming bit stream correctly. The three mechanisms used for synchronisation are:

- Asynchronous Communication
- Synchronous Communication
- Isochronous Communication

3.2.1. Asynchronous Communication

Asynchronous communication sends individual characters one at a time framed by a start bit and I or 2 stop bits. Each frame begins with a start bit that enables the receiving device to adjust to the timing of the transmitted signal. The message can begin at any time. Here, messages are kept as short as possible because, the sending and receiving devices should not draft out of synchronisation, when the message is being transferred. Asynchronous communication is most frequently used to transmit character data and is ideally suited for characters that are transmitted at irregular intervals, such as, when users are typing in character data from the keyboard.

A typical frame used to transmit a character data has four components:

- **A start bit**: Signals the starting a frame and enables the receiving device to synchronise itself with the message.
- **Data Bits**: Consists of 7 or 8 bits when character data is being transmitted.
- **Parity Bits**: Optionally used as a crude method for detecting transmission errors.
- **A stop bit or bits:** Signals the end of the data frame.

Error detection in asynchronous transmission makes use of the parity bit. Parity techniques can detect errors that affect only one bit and if two or more bits are affected by errors, the parity techniques may not be able to detect them.

Advantages of Asynchronous Communication

i. Asynchronous transmission is simple, inexpensive and is ideally suited for transmitting small frames at irregular intervals (e.g.,Data entry from a keyboard).
ii. As each individual character is complete in itself, if a character is corrupted during transmission, its successor and predecessor will not be affected.

Disadvantages of Asynchronous Communication

i. As start, stop and parity bits must be added to each character that is to be transmitted, this adds a high overhead to transmission. This wastes the bandwidth; as a result, asynchronous transmission is undesirable for transmitting large amounts of data.
ii. Successful transmission inevitably depends on the recognition of the start bits, hence, as these bits can be easily missed or occasionally spurious, as start bits can be generated by line interference, the transmission may be unsuccessful.
iii. Due to the effects of distortion the speed of asynchronous transmission is limited.

3.2.2 Synchronous Communication

In synchronous communication the whole block of data bits is transferred at once, instead of one character at a time. Here, transmission begins at a predetermined regular time instant. A sync signal is used to tell the receiving station that a new frame is arriving and to synchronise the receiving station.Sync signals, generally utilise a bit pattern that cannot appear elsewhere in the messages, ensuring that they will always be distinct and easy for the receiver to recognise.

As the transmitter and receiver remain in synchronisation for the duration of the transmission, frames can be of longer length. As frames are longer the parity method of error detection is not suitable because, if multiple bits are affected, then, the parity technique will not report error accurately. Hence, the technique used with synchronous transmission is the Cyclic Redundancy Check (CRC).

The transmitter uses an algorithm to calculate a CRC value that summarises the entire value of data bits. This CRC value is appended to the data frame. The receiver uses the same algorithm, recalculates the CRC and compares the CRC in the frame to the value that it has calculated. If these values match then, it is sure that the frame was transmitted without error.

An end bit pattern indicates the end of the frame. Like sync the bit pattern for end is such that, it will not appear elsewhere in the messages, ensuring that they will always be distinct and easy for the receiver to recognise at the end of the frame. Serial synchronous transmission is used for high-speed communication between computers. It is used when high volumes of data are to be transmitted.

Advantages of Synchronous Communication

i. Synchronous transmission is more efficient because, only 4 additional bytes (for start and end frames).are required to transmit up to 64 k bits.
ii. Synchronous transmission is not really prone to distortion, as a result, it can be used at high- speeds.

Disadvantages of Synchronous Communication

i. Synchronous transmission is expensive as complex circuitry is required and it is difficult to implement.
ii. If an error occurs during transmission, rather than just a single character the whole block of data is lost.

iii. The sender cannot transmit characters simply, as they occur, but has to store them until it has built up a block. Thus, this is not suitable where characters are generated at irregular intervals.

3.2.3 Isochronous Communication

This method combines the approaches of asynchronous and synchronous cornunications. As in the asynchronous method, each character has both the start and stop bits. The idle period (where no transmission takes place) between the two characters is not random but an exact multiple of one character time interval. If, the time to transmit a character (Including its parity, start, stop bits) is t, the time interval between characters cannot be random as in the asynchronous method. It is also not 0 as in the synchronous method. It has to be t, 2t, 3t…….nt where n is any positive integer. Here, the signal is expected to be received within certain delay bounds say Tmin to Tmax.

Advantages of Isochronous Communication

i. Isochronous transmission guarantees transmission rates, and it is almost deterministic.
ii. It has low overheads.
iii. It has high speed.

Disadvantages of Isochronous Communication

i. In isochronous transmission its necessary to ensure that the clocking device is fault tolerant.

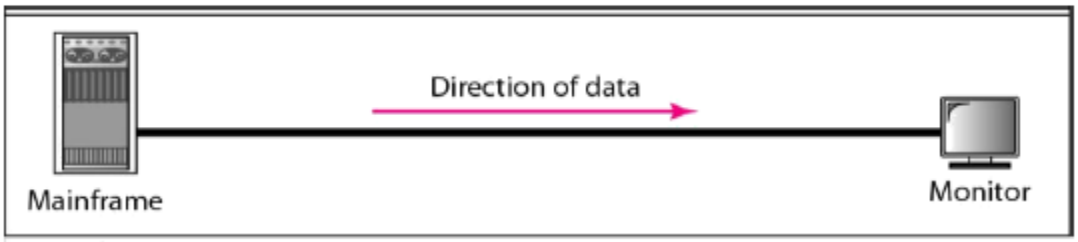
3.3 DUPLEXITY

The term duplexity defines the direction of signal flow between two linked devices. The three basic ways in which this can be done are:

- Simplex.
- Half Duplex
- Full Duplex, sometimes called Duplex.

3.3.1 simplex mode(SX)

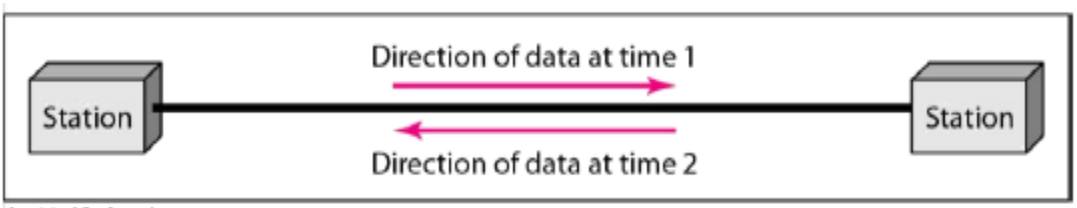
In ***simplex mode,*** the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive. Commercial radio broadcasting is an example. Simplex lines are also called receive-only, transmit-only or one-way-only lines.



a. Simplex

3.3.2 half-duplex(HDX) mode

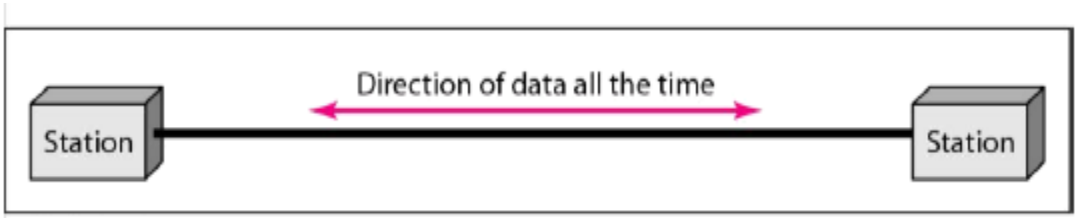
In ***half-duplex*** mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. The half-duplex mode is used in cases where there is no need for communication in both directions at the same time; the entire capacity of the channel can be utilized for each direction. Citizens band (CB) radio is an example where push to talk (PTT) is to be pressed or depressed while sending and transmitting.



b. Half-duplex

3.3.3 full-duplex mode(FDX)

In ***full-duplex mode*** (called duplex), both stations can transmit and receive simultaneously. One common example of full-duplex communication is the telephone network. The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel must be divided between the two directions.



c. Full-duplex

3.3.4 full/full duplex (F/FDX) mode

In ***full/full duplex (F/FDX)*** mode, transmission is possible in both directions at the same time but not between the same two stations (i.e. station 1 transmitting to station 2, while receiving from station 3). F/FDX is possible only on multipoint circuits. Postal system can be given as a person can be sending a letter to one address and receive a letter from another address at the same time.

4.0 MULTIPLEXING

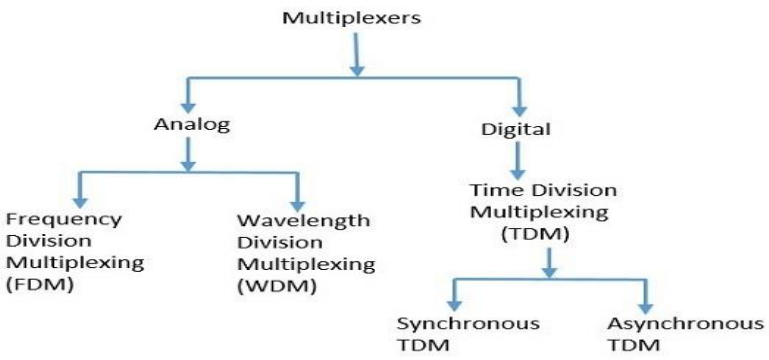
multiplexing or muxing is a method by which multiple analog or digital signals are combined into one signal over a shared medium. The aim is to share a scarce resource. The multiplexed signal is transmitted over a communication channel such as a cable. The multiplexing divides the capacity of the communication channel into several logical channels, one for each message signal or data stream to be transferred. A reverse process, known as demultiplexing, extracts the original channels on the receiver end.

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

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

4.1 Types of Multiplexers

There are mainly two types of multiplexers, namely analog and digital. They are further divided into Frequency Division Multiplexing (FDM), Wavelength Division Multiplexing (WDM), and Time Division Multiplexing (TDM).



4.1.1 Analog Multiplexing

The signals used in analog multiplexing techniques are analog in nature. The analog signals are multiplexed according to their frequency (FDM) or wavelength (WDM).

a. Frequency division multiplexing (FDM)

Frequency Division Multiplexing (FDM) is primarily used with analogue signals rather than digital data streams.

It works by dividing the entire bandwidth which is available in a data source, into sub-channels that each have a different frequency; hence the name 'frequency division'. Each sub-channel then carries separate signals through a transmission line or an aggregated channel (a combination of channels with higher bandwidth). The sub-channels can travel independently through a transmission line or they can travel simultaneously besides one another. These sub-channels are then separated by the strips of unused bandwidth called guard bands. These guard bands prevent the signals from overlapping.

A demultiplexer applies a set of filters that each extract a small range of frequencies near one of the carrier frequencies.

Advantage of FDM:

i. The senders can send signals continuously.
ii. FDM support full duplex information flow.
iii. FDM is used for analog signals.
iv. Noise problem for analog communication has lesser effect.
v. FDM process is very simple and easy modulation and demodulation.
vi. It does not require any synchronization between sender and receiver.

Disadvantage of FDM:

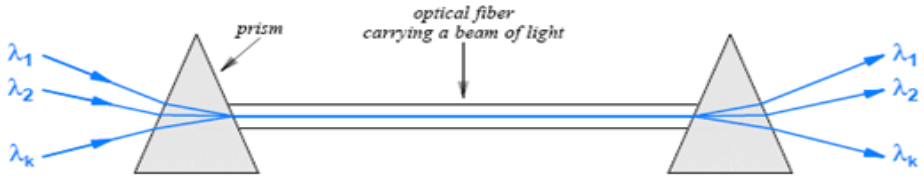
i. Each user requires a precise carrier frequency.
ii. FDM technique is used only when low-speed channels are required.
iii. It requires a high bandwidth channel.
iv. Inflexible, one channel idle and other one busy
v. It suffers the problem of crosstalk.
vi. Large number of modulators and filters are required.
vii. All the FDM channels get affected due to wideband fading.

Applications of FDM:

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

b. Wavelength Division Multiplexing(WDM)

Wavelength Division multiplexing (WDM) also called Dense WDM (DWDM) is an analog technique, in which many data streams of different wavelengths are transmitted in the light spectrum. If the wavelength increases, the frequency of the signal decreases. A prism, which can turn different wavelengths into a single line, can be used at the output of MUX and input of DEMUX. Optical fiber communications use WDM technique, to merge different wavelengths into a single light for communication. The inputs and outputs of such multiplexing are wavelengths of light denoted by the Greek letter λ, and informally called colors.



Advantages of WDM

i. ***Speed:*** Works with low speed equipment
ii. ***Transparency:*** WDM is transparent. It does not depend on the protocol that has to be

transmitted.

iii. ***Scalable:*** It is scalable. Instead of switching to a new technology, a new channel can easily be added to existing channels.

iv. ***Capacity Increment:*** It is easy for network providers to add additional capacity in a few days if customers need it.

Disadvantages of WDM

i. ***Complexity:*** Complex transmitters and receivers.

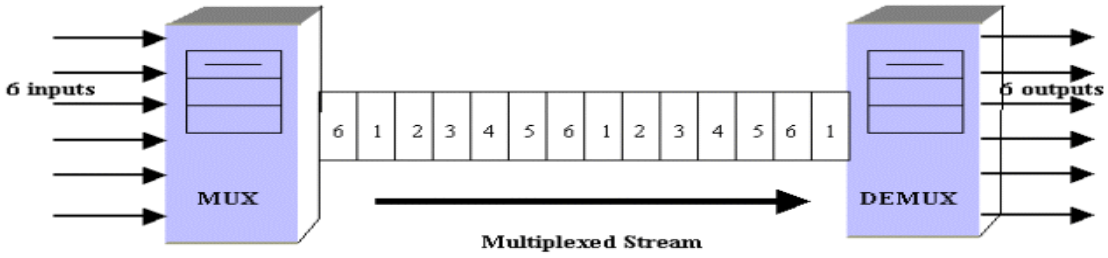
ii. ***Reliability and Cost:*** They must be wide-band, which means they are more expensive and possibly less reliable.

4.1.2 Digital Multiplexing

The term digital represents the discrete bits of information. Hence, the available data is in the form of frames or packets, which are discrete.

a. Time division multiplexing

Time-division multiplexing (TDM) is a digital process that allows several connections to share the high bandwidth of a line. Instead of sharing a portion of the bandwidth as in FDM, time is shared. Time Division Multiplexing is the process of dividing up one communication time slot into smaller time slots.



Time Division Multiplexing (TDM) system, a single path and carrier frequency is used. Each user is assigned a unique time slot for their operation. A central switch or multiplexer goes from one user to the next in a specific predictable sequence and time. TDM system can be applied when the data rate capacity of the transmission medium is greater than the data rate required by the sending and receiving devices. TDM is more efficient than FDM, in that it does not require

guard bands and it operates directly in digital form. In TDM, the transmission between the multiplexers is provided by a single high speed digital transmission line. Types of Time Division Multiplexing It can be categories into two types:

- Synchronous TDM
- Asynchronous TDM

1. Synchronous TDM

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

The most popular Synchronous TDM are T-1 multiplexing, ISDN multiplexing, and SONET multiplexing.

Disadvantages of Synchronous TDM:

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

ii. The speed of the transmission medium should be greater than the total speed of the input lines. An alternative approach to the Synchronous TDM is Asynchronous Time Division Multiplexing.

2. Asynchronous TDM

An asynchronous TDM is also known as Statistical TDM. An asynchronous TDM is a technique in which time slots are not fixed as in the case of Synchronous TDM. Time slots are allocated to

only those devices which have the data to send. Therefore, we can say that Asynchronous Time Division multiplexor transmits only the data from active workstations.

An asynchronous TDM technique dynamically allocates the time slots to the devices. In Asynchronous TDM, total speed of the input lines can be greater than the capacity of the channel. Asynchronous Time Division multiplexor accepts the incoming data streams and creates a frame that contains only data with no empty slots. In Asynchronous TDM, each slot contains an address part that identifies the source of the data.

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

Advantages of TDM

i. The user gets full bandwidth of the channel in a particular time slot.
ii. For bursty signals such as voice or speech TDMA gives maximum utilization of the channel.
iii. Most suitable technique for digital transmission.
iv. It does not require precise carrier matching at both end of the links.
v. Can expand the number of users on a system at a low cost.

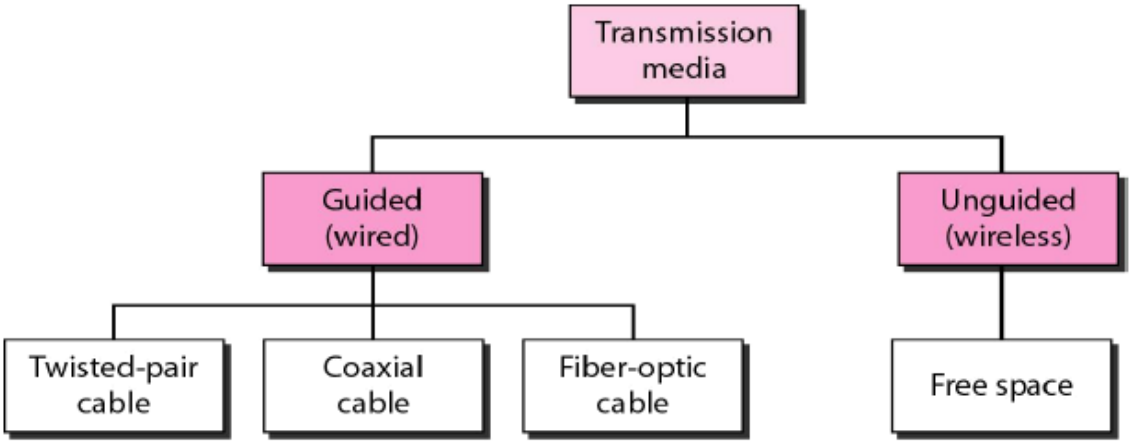
Disadvantages of TDM

i. It is not much suitable for continues signals.
ii. Initial cost is high.
iii. The noise problem for analog communication has greater effect.
iv. Extra guard times are necessary.
v. Synchronization is necessary.

5.0 TRANSMISSION MEDIA

Introduction

The ***transmission medium*** is the physical path between transmitter and receiver in a data transmission system. The information is usually a signal that is the result of a conversion of data from another form. Transmission media can be generally categorized as either *unguided or guided.*



5.1 Guided Transmission Media

Guided Transmission Media uses a "cabling" system (or some sort of conductor) that guides the data signals along a specific path. The data signals are bound by the "cabling" system. Guided Media is also known as Bound Media. The conductor directs the signal propagating down it. Only devices physically connected to the medium can receive signals propagating down a guided transmission medium. Examples of guided transmission media are copper wire and optical fiber.

5.1.1 Twisted-Pair (TP)

A twisted-pair (TP) transmission line is formed by twisting two insulated conductors around each other. Usually, a number of pairs of these wires are put together into a cable. The cable may contain more than a hundred pairs of wires for long-distance communications. Twisted-pair wires are the most common media in a telephone network. These wires support both analog and digital signals and can transmit the signal at a speed of 10 Mbps over a short distance. The

twisting of wires with different twisting lengths reduces the effect of cross talk and low-frequency interference.

Twisted-pair cable

Twisted-pair transmission lines are also the transmission medium of choice for most local area networks because twisted-pair cable is simple to install and relatively independent when compared to coaxial and optical fiber cables. The two basic types of twisted-pair transmission lines specified are unshielded twisted pair (UTP) and shielded twisted pair (STP).

a. Unshielded twisted-pair:

UTP cable consist of four twisted pairs of copper wires, enclosed in a protective plastic cover, with the greater number of pairs corresponding to more bandwidth. Bandwidth can be improved by controlling the number of twists per foot and also the manner in which multiple pairs are twisted around each other. The minimum number of twists for UTP cable is two per foot. The two individual wires in a single pair are twisted around each other, and then the pairs are twisted around each other, as well. This is done to reduce crosstalk and electromagnetic interference, each of which can degrade network performance.

Twisted pairs are color-coded to make it easy to identify each pair. One wire in a pair is identified by one of five colors: blue, orange, green, brown or slate (gray). This wire is paired with a wire from a different color group: white, red, black, yellow or violet. Typically, one wire in a pair is solid-colored, and the second is striped with the color of its mate -- e.g., a solid blue wire would be paired with a white-and-blue striped wire -- so they can be easily identified and matched.

UTP Categories

The Electronic Industries Association (EIA) has developed standard to grade UTP cable by quality; Category 1 as the lowest quality and category 6 as the highest quality.

1. **Category 1:** The basic twisted-pair cabling used in telephone systems. This level of quality is fine for voice but inadequate for data transmission.
2. **Category 2:** This category is suitable for voice and data transmission of up to 2Mbps.
3. **Category 3:** This category is suitable for data transmission of up to 10 Mbps. It is now the standard cable for most telephone systems. At least three twist per feet
4. **Category 4:** This category is suitable for data transmission of up to 20 Mbps.
5. **Category 5:** This category is suitable for data transmission of up to 100 Mbps.
6. **Category 6:** CAT- 6 is recently proposed cable type comprised of four pairs of wire capable of operating at transmission rates of up to 400Mbps.

Advantages Of Unshielded Twisted Pair:

i. It is smaller in size. Hence installation is easier as it does not fill up wiring ducts.
ii. It is less expensive compare to other networking media types.
iii. It is thin and flexible which further makes installation easier.
iv. UTP cables are used in most of the networking architecture.

Disadvantage:

i. It is more susceptible to interference compare to most of the other cable types. Twisting of pair helps to certain extent but it does not make cable impervious to electrical noise completely.
ii. It can be used up to cable segment lengths of about 100 meters only.
iii. UTP cable should follow specifications for number of twists or braids permitted per meter of cable to reduce crosstalk.

b. Shielded Twisted Pair (STP) Cable:

STP is also the type of twisted pair which stands for Shielded twisted pair. Shielded twisted-pair cable encases the signal-carrying wires in a conducting shield as a means of reducing the

potential for electromagnetic interference. How effective the shielding is depends on the material used for the shield,its thickness and frequency, the type of electromagnetic noise field, the distance from the noise source to the shield, any shield discontinuity and the grounding practices. Also, crosstalk and signal noise can increase if the effects of the shield are not compensated for.

Some STP cables, use a thick braided shield that makes a cable heavier, thicker and more difficult to install than its UTP counterpart. Other STP cables use only a thin outer foil shield. These cables, known as screened twisted-pair cables or foil twisted-pair cables, are thinner and less expensive than braided STP cable.

Shielded Twisted Pair (STP)

Shielding Types

Common shield construction types include:

1. **Individual shield**

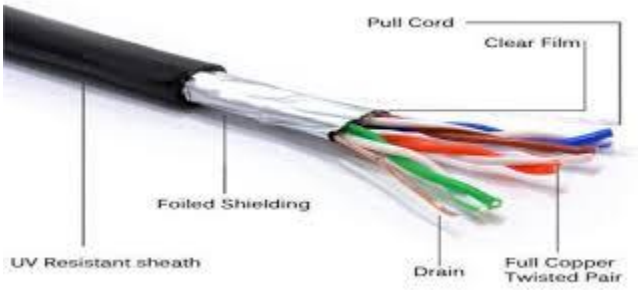
Individual shielding with aluminum foil for each twisted pair or quad. Common names: pair in metal foil, shielded twisted pair, screened twisted pair. There only one type under this category:

- **U/FTP –Unshielded with Foiled Twisted Pairs -** This type of cable has no overall shielding but individual twisted pairs are wrapped in a foil screen, offering some protection from EMI and crosstalk from adjacent pairs and other cables.

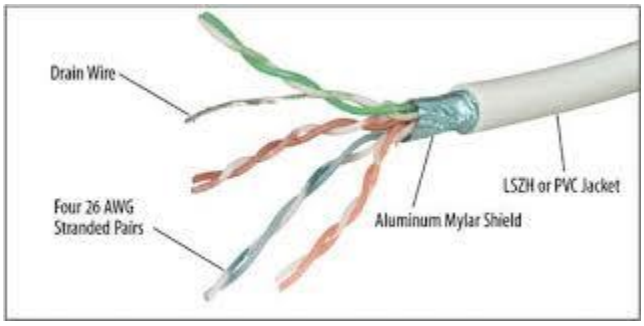
2. Overall shield

Overall foil, braided shield or braiding with foil across all of the pairs within the 100 ohm twisted pair cable. Common names: foiled twisted pair, shielded twisted pair, screened twisted pair. This type of shielding helps prevent EMI from entering or exiting the cable. There three categories here this include **F/UTP, S/UTP, and SF/UTP.**

- **F/UTP Foiled with Unshielded Twisted Pair** - An overall foil shield (F) with unscreened twisted pairs (UTP) and a drain wire. When the drain wire is correctly connected, unwanted noise is redirected to ground, offering extra protection against EMI/RFI. This cable is very much like common UTP cables, with the addition of foil underneath the main cable jacket. Another common name for this cable is FTP. F/UTP cables are common in 10GBaseT applications.



- **S/UTP: Shielded with Unshielded Twisted Pairs.** –This cable construction has an overall braid screen with unshielded twisted pair. This cable is often referred to as an STP, however this term should be used with caution due to other shielded cables also using this term.



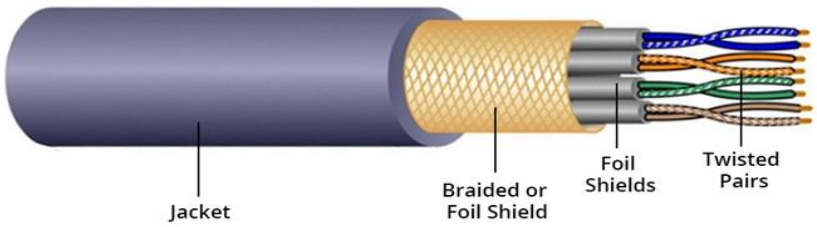
- **SF/UTP: Shielded and Foiled with unshielded twisted pairs -** This cable has both an overall braid shield and foil shield with unshielded twisted pairs. This cable offers effective protection from EMI both from the cable and into the cable as well as much better grounding due to the additional braid.

3. Individual and overall shield

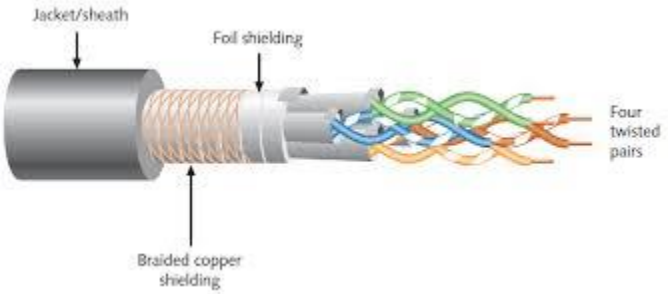
Individual shielding using foil between the twisted pair sets, and also an outer foil or braided shielding. Common names: fully shielded twisted pair, screened foiled twisted pair, shielded foiled twisted pair, screened shielded twisted pair, shielded screened twisted pair. This type of shielding helps prevent EMI from entering or exiting the cable and also protects neighboring pairs from crosstalk. There three categories here they include: **F/FTP, S/FTP, and SF/FTP.**

- **F/FTP Foiled with foiled Twisted Pairs -** This type of cable features an overall foil shield with individually foil tape shielded twisted pairs. These are similar to F/UTP cables, with the addition of a foil shield around each twisted pair. The cable construction is designed to provide the assembly with greater protection from crosstalk from adjacent pairs and other cables, RFI and EMI.

- **S/FTP Shielded with Foiled Twisted Pairs** – In S/FTP each individual pairs are wrapped in a foil tape before being wrapped in an overall flexible yet mechanically strong brain screen. The additional foil on the twisted pair helps reduce crosstalk from adjacent pairs and other cables . The braid provides better grounding



- **SF/FTP:Shielded and Foiled With Foiled Twisted Pairs -**This cable has both an overall braid shield and foil shield with individually foil tape screened twisted pairs. This type of cable provides the best level of protection from interference and better grounding due to the braid.



Advantages Shielded Twisted Pair:

i. Shielding reduces chance of crosstalk and provide protection from interference.
ii. It has higher capacity as compared to unshielded twisted pair cable.
iii. It offers better electrical characteristics than unshielded cables.

Disadvantages

i. Shielding increases overall diameter and weight of the cable. Hence it is more difficult to install compare to UTP cables. The larger thickness make them unfit for narrow cable ducts.
ii. Shield of STP cables must be grounded properly otherwise it acts like an antenna and picks up unwanted signals.
iii. It is more expensive as compared to UTP and coaxial cable.

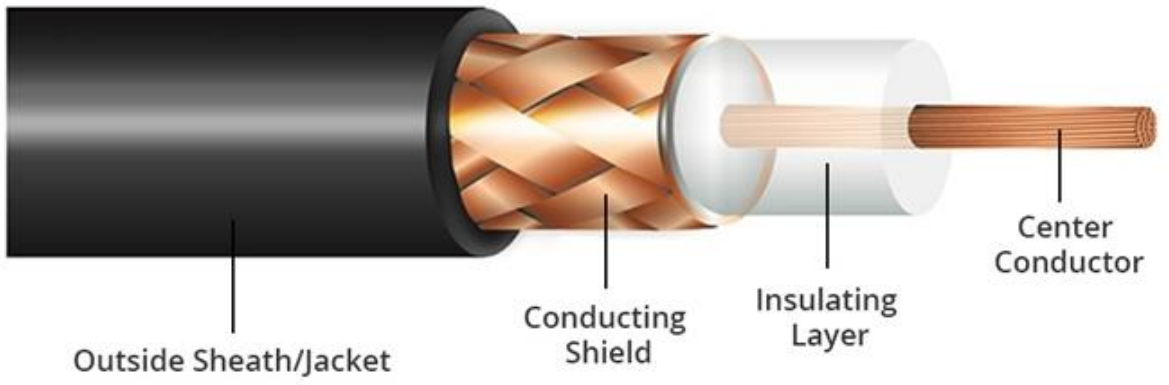
Unshielded Twisted Pair (UTP) VS Shielded Twisted Pair (STP) cables:

UTP	STP
In UTP grounding cable is not necessary.	STP grounding cable is required.
Data rate in UTP is slow compared to STP.	Data rate in STP is high.
The cost of UTP is less.	STP is costlier than UTP.

In UTP much more maintenance are not needed.	STP much more maintenance are needed.
In UTP noise is high compared to STP.	STP noise is less.
In UTP the generation of crosstalk is also high compared to STP.	STP generation of crosstalk is also less.

5.1.2 Coaxial Cable

Coaxial cable is named after the two conductors that run parallel to each other. The center conductor in the cable is usually copper, which is usually either a solid wire or stranded, twisted copper. Outside this central conductor is a non-conductive material called a dielectric insulator. It is usually a white, plastic material used to separate the inner conductor from the outer conductor. The other conductor is a fine mesh made from braided copper. It is used to help shield the cable from electromagnetic interference, or EMI. Wrapped outside the copper mesh is the final non-conductive protective cover. The actual data travels through the center conductor in the cable. EMI is "caught", or redirected, by the outer copper mesh.



There are different types of coaxial cable that vary by gauge and impedance. "Gauge" is the thickness of a given cable. It is measured by the radio guide measurement or RG number. The higher the RG number, the thinner the central core conductor. The lower the RG number, the thicker the core conductor. The following are the most common coaxial standards:

- **50-Ohm RG-7 or RG-11:** Used for thick Ethernet or "thicknet".
- **50-Ohm RG-58:** Used for thin Ethernet, or "cheapernet".

- **75-Ohm RG-59:** Used for cable television.
- **93-Ohm RG-62:** Used for ARCNET.

Advantages of Coaxial cable:

i. It is less susceptible to noise or interference (EMI or RFI) compare to twisted pair cable.
ii. It supports high bandwidth signal transmission compare to twisted pair.
iii. It is easy to wire and easy to expand due to flexibility.
iv. It allows high transfer rates with coaxial cable having better shielding materials.
v. The outer conductor in coaxial cable is used to improve attenuation and shield effectiveness.

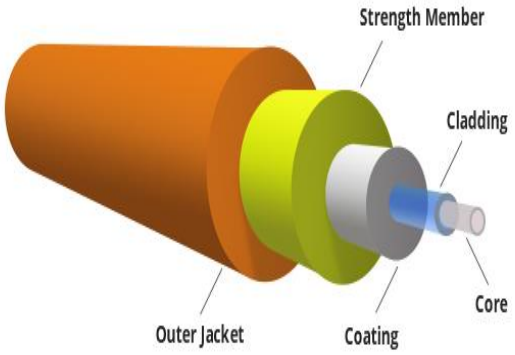
Disadvantages of Coaxial cable:

i. It is bulky.
ii. It is expensive to install for longer distances due to its thickness and stiffness.
iii. The security is a great concern as it is easy to tap the coaxial cable by breaking it and inserting T-joint (of BNC type) in between.
iv. It must be grounded to prevent interference.

5.1.3 Fiber Optic Cable

Fiber optics, or optical fiber, refers to the medium and the technology associated with the transmission of information as light pulses along a glass or plastic strand or fiber. Optical fiber is a very thin strand of pure glass which acts as a waveguide for light over long distances. It uses a principle known as total internal reflection. Fiber optic cable is actually composed of two layers of glass: The core, which carries the actual light signal, and the cladding, which is a layer of glass surrounding the core. The glass fiber core and the cladding each have a different refractive index that bends incoming light at a certain angle. The cladding has a lower refractive index than the core. When light signals are sent through the fiber optic cable, they reflect off the core and cladding in a series of zig-zag bounces, adhering to a process called total internal reflection.

Basic elements of Fiber optic cable:



- **Core:** The optical fibre consists of a narrow strand of glass or plastic known as a core. A core is a light transmission area of the fibre. The more the area of the core, the more light will be transmitted into the fibre.
- **Cladding:** The concentric layer of glass is known as cladding. The main functionality of the cladding is to provide the lower refractive index at the core interface as to cause the reflection within the core so that the light waves are transmitted through the fibre.
- **Primary Coating**: The primary coating comes after the cladding, and is also known as the primary buffer. It is designed to absorb shocks, provide protection against excessive cable bends, and reinforce the fiber core. This primary coating is basically a layer of plastic which does not interfere with the cladding or the light transmission of the core.
- **Strength Members**: Also known as strengthening fibers, these are strands of Kevlar (Aramid yarn) which have been specifically placed to protect the core against excessive tension during installation and other crushing forces.
- **Cable Jacket**: The outer layer of any cable is known as the cable jacket. The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fibre strength, absorb shock and extra fibre protection.

  Depending on the application, some fiber-optic cables have yellow, black, aqua, and other colored jackets. However, fiber-optic cables typically have an orange jacket. Different applications can be designated within a network by using different colors.

Types of Fiber optics:

Generally optical fiber is classified into two categories based on:

- The number of modes, and
- The refractive index. T

1. On the basis of the Number of Modes:

It is classified into 2 types single and multi-mode.

a) Single-mode fiber (SMF):

Single mode means the fiber enables one type of light mode to be propagated at a time. This type of fiber has a small core diameter (5um) and high cladding diameter (70um) and the difference between the refractive index of core and cladding is very small. There is no dispersion i.e. no degradation of the signal during traveling through the fiber.

Single-mode fiber gives a higher transmission rate and up to 50 times more distance than multimode, but it also costs more. Single-mode fiber has a much smaller core than multimode. The small core and single light-wave virtually eliminate any distortion that could result from overlapping light pulses, providing the least signal attenuation and the highest transmission speeds of any fiber cable type.

b) Multi-mode fiber (MMF):

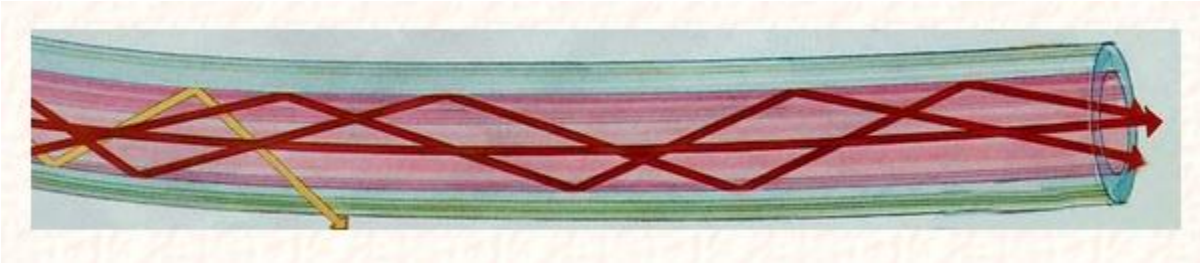
Multimode fiber allows a large number of modes for the light ray traveling through it. The core diameter is generally (40um) and that of cladding is (70um). The larger diametrical core permits multiple modes of light to pass through at a given time. This characteristic allows the number of light reflections created as the light passes through the core to increase, creating the ability for more data to pass through at any given time. The attenuation rate and high dispersion of this fiber reduce the signal quality over long distances. Multimode optical fiber is commonly used short distances, audio/video applications, and Local Area Networks (LANs).

2. On the basis of Refractive Index:

It is also classified into 2 types:

a) Step-index optical fiber:

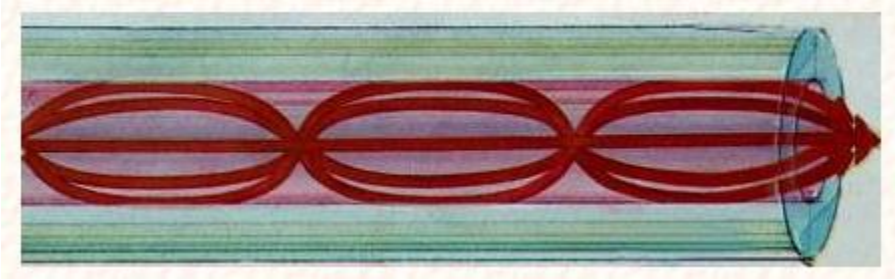
The refractive index of core is constant. The refractive index of the cladding is also constant. The rays of light propagate through it in the form of meridional rays which cross the fiber axis during every reflection at the core-cladding boundary.



A ray that exceeds a certain "critical" angle escapes from the fiber (yellow line).

b) Graded index optical fiber:

In this type of fiber, the core has a non-uniform refractive index that gradually decreases from the center towards the core-cladding interface. The cladding has a uniform refractive index. The light rays propagate through it in the form of skew rays or helical rays. it is not cross the fiber axis at any time.



Advantages of Fiber optic

i. **Wider bandwidth and greater information capacity:** The light wave occupies the frequency range between 2×10^{12}Hz to 37×10^{12} Hz. This makes the information carrying capability of fiber opticcables is much higher.

ii. **Immunity to crosstalk:** Since fiber optic cables use glass and plastic fibers, which are nonconductors of electrical current, no magnetic field is present. No magnetic induction means no crosstalk.

iii. **Immunity to static interference:** As optical fiber cables are non-conductors, they are immune to electromagnetic interference (EMI) caused by lightning, electric motors, relays,fluorescent lights and other electrical noise sources.

iv. **Environmental immunity:** Optical fibers are more immune to environmental extremes. They can operate over large temperature variations and are also not affected by corrosive liquids and gases.

v. **Safety and convenience:** As only glass and plastic fibers are present, no electrical currents or voltages are associated with them. Also they can be used around any volatile liquids and gasses without worrying about their causing explosions or fires.

vi. **Lower transmission loss:** Fiber optic cables offers less signal attenuation over long distances. Typically, it is less than 1 dB/km

vii. **Security:** Optical fibers are more secure as they are almost impossible to tap into because they do not radiate signals. No ground loops exist between optical fibers hence they are more secure.

viii. **Durability and reliability:** Optical cables last longer and are more reliable than metallic facilities because fiber cables have a higher tolerance to changes in environmental conditions and are immune to corrosive materials.

ix. **Economics:** Cost of optical fiber cables is same as metallic cables. Fiber cables have less loss and require fewer repeaters, which in turn needs lower installation and overall system costs.

Disadvantages of Fiber optic

i. **Interfacing costs:** As optical cables need to be connected standard electronic facilities requiring expensive interfaces.

ii. **Strength:** Optical cables have lower tensile strength than coaxial cable. They need an extra coating of Kevlar and also a protective jacket of PVC. Glass fiber is also fragile making them less attractive in case of hardware portability is required

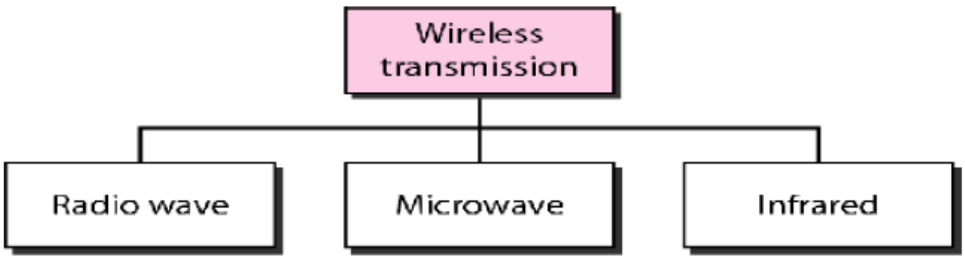
iii. **Remote electrical power:** Occasionally, electrical power needs to be provided to remote interfaces,which cannot be accomplished using optical cables

iv. **Losses through bending:** Bending the cable causes irregularities in the cable dimensions, resulting in loss of signal power. Also, optical cables are prone to manufacture defects causing an excessive loss of signal power.

v. **Specialized tools, equipment and training:** Special tools are required to splice and repair cables and special test equipment are needed to make routine measurements. Technicians working on optical cables need special skills and training.

5.2 Unguided Transmission Media

Unguided Transmission Media consists of a means for the data signals to travel but nothing to guide them along a specific path. The data signals are not bound to a cabling media and as such are often called Unbound Media. Unguided transmission media are wireless systems. Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them. Unguided signals can travel from the source to destination in several ways: ground propagation, sky propagation, and line-of-sight propagation



5.2.1 Radio Waves:

Although there is no clear-cut demarcation between radio waves and microwaves, electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves; waves ranging in frequencies between 1 and 300 GHz are called microwaves. However, the behavior of the waves, rather than the frequencies, is a better criterion for classification.

Radio waves use omni-directional antennas that send out signals in all directions. The omni-directional characteristics of radio waves make them useful for multicasting, in which there is one sender but many receivers. AM and FM radio, television, cordless phones, and paging are examples of multicasting.

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

Advantages of Radio transmission:

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

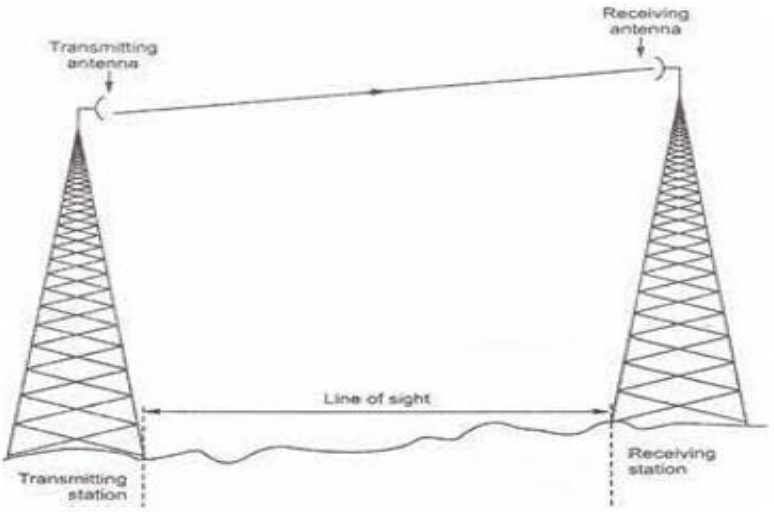
5.2.2 Microwaves

Microwaves are electromagnetic waves having frequencies between 1 and 300 GHz. Microwaves are unidirectional. When an antenna transmits microwave waves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned. The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas. Microwaves, due to their unidirectional properties, are very useful when unicast (one-to-one) communication is needed between the sender and the receiver. Microwaves are of two types:

- Terrestrial microwave
- Satellite microwave communication.

a) Terrestrial Microwave Transmission

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



Advantages of Microwave:

i. Microwave transmission is cheaper than using cables.

ii. It is free from land acquisition as it does not require any land for the installation of cables.

iii. Microwave transmission provides an easy communication in terrains as the installation of cable in terrain is quite a difficult task.

iv. Communication over oceans can be achieved by using microwave transmission.

Disadvantages of Microwave transmission:

i. **Eavesdropping:** An eavesdropping creates insecure communication. Any malicious user can catch the signal in the air by using its own antenna.

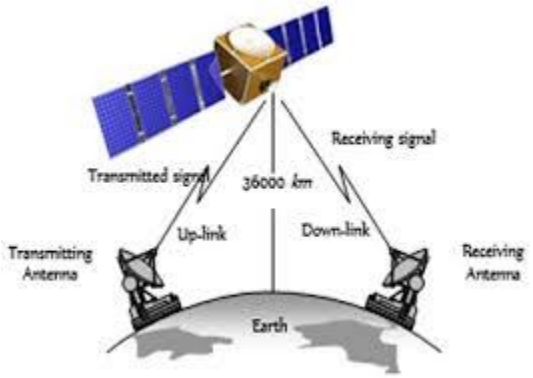
ii. **Out of phase signal:** A signal can be moved out of phase by using microwave transmission.

iii. **Susceptible to weather condition:** A microwave transmission is susceptible to weather condition. This means that any environmental change such as rain, wind can distort the signal.

iv. **Bandwidth limited:** Allocation of bandwidth is limited in the case of microwave transmission.

b) Satellite Microwave Communication

A satellite is a physical object that revolves around the earth at a known height. Satellite communication is more reliable nowadays as it offers more flexibility than cable and fibre optic systems. We can communicate with any point on the globe by using satellite communication. The satellite accepts the signal that is transmitted from the earth station, and it amplifies the signal. The amplified signal is retransmitted to another earth station.



Advantages of Satellite Microwave Communication:

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

Disadvantages of Satellite Microwave Communication:

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

5.2.3 Infrared

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

Characteristics of Infrared:

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

6.0 MEDIA ACCESS CONTROL

Introduction

A media access control is a network data transfer policy that determines how data is transmitted between two computer terminals through a network cable. The media access control policy involves sub-layers of the data link layer 2 in the OSI reference model.

The essence of the MAC protocol is to ensure non-collision and eases the transfer of data packets between two computer terminals. A collision takes place when two or more terminals transmit data/information simultaneously. This leads to a breakdown of communication, which can prove costly for organizations that lean heavily on data transmission.

6.1 Types of Media access control

There are three forms of media access control this include:

- Contention
- Token Passing
- Polling

6.1.1 Contention

Contention-based media access describes a way of getting data on to the network whereby systems 'contend for' or share the media. On a contention-based network, systems can only transmit when the media is free and clear of signals. In this way, devices listen to the media, and if no other system is transmitting, they can go ahead and send data. In cases where more than one system finds the network free and attempts to transmit, a data collision will occur, and systems will need to retransmit. On busy networks, the number of collisions can quickly get very high, adversely affecting performance. Remember that in this scenario, only a single system truly has access to the media at any given time, even though multiple systems may have data to send. There two methods of contention this includes:

- Carrier Sense Multiple Access with Collision Detection (CSMA/CD).
- Carrier sense multiple access with collision avoidance (CSMA/CA)

a. Carrier Sense Multiple Access with Collision Detection(CSMA/CD)

Carrier Sense Multiple Access with Collision Detection – To send a frame, listens to the medium to see if it is busy. – If the medium is busy, waits per the persistent CSMA. – If the station is able to transmit a frame, it listens to the medium for collision while transmitting the frame. – If it detects a collision, it immediately stops the transmission and sends a short jamming signal.

If it receives a jamming signal, it stops the transmission immediately. – After a collision, it waits a random amount of time according to the Binary Exponential Backoff algorithm and then repeats the above steps.

b. Carrier sense multiple access with collision avoidance (CSMA/CA)

In Carrier sense multiple access with collision avoidance (CSMA/CA) the station ready to transmit, senses the line by using one of the persistent strategies. As soon as it find the line to be idle, the station waits for an IFG (Interframe gap) amount of time. If then waits for some random time and sends the frame. After sending the frame, it sets a timer and waits for the acknowledgement from the receiver. If the acknowledgement is received before expiry of the timer, then the transmission is successful. But if the transmitting station does not receive the expected acknowledgement before the timer expiry then it increments the back off parameter, waits for the back off time and resenses the line.

Advantages of Contention

i. Contention is a very simple simple access method that has low administrative overhead requirements. No network traffic is necessary to manage the access scheme.
ii. Actual user data throughout is rather high at low traffic levels in comparison to total amount of utilized network bandwidth.

Disadvantages of Contention

i. At high traffic levels, data collisions and resulting retransmission diminish performance dramatically. It is theoretically possible that collisions can be so frequent at higher traffic levels that no station has a clear chance to transmit.
ii. Channel access is probabilistic rather than deterministic. Because of retransmissions and the time it takes to sense collisions, automated equipment that cannot tolerate delays cannot use this type of access.
iii. Contention offers no means of establishing the frequency of a stations opportunities to transmit.

6.1.2 Token Passing

In token passing scheme, all stations are logically connected in the form of a ring and control of the access to the medium is performed using a token. A token is a special bit pattern or a small packet, usually several bits in length, which circulate from node to node. Token passing can be used with both broadcast (token bus) and sequentially connected (token ring) type of networks.

In case of token ring, token is passed from a node to the physically adjacent node. On the other hand, in the token bus, token is passed with the help of the address of the nodes, which form a logical ring. In either case a node currently holding the token has the 'right to transmit'. When it has got data to send, it removes the token and transmits the data and then forwards the token to the next logical or physical node in the ring.

If a node currently holding the token has no data to send, it simply forwards the token to the next node. The token passing scheme is efficient compared to the polling technique, but it relies on the correct and reliable operation of all the nodes. There exists a number of potential problems, such as lost token, duplicate token, and insertion of a node, removal of a node, which must be tackled for correct and reliable operation of this scheme.

Advantages of Token Passing

i. Token Passing offers the highest data throughput possible under high traffic conditions. Only one transmission can occur at a time, and collisions cannot occur(non-contention). Therefore, token passing experiences less performance degradation at higher traffic levels than contention.
ii. Token passing is deterministic. Each station is guaranteed an opportunity to transmit each time the token travels around the ring.
iii. Some token passing systems enable you to set priorities for devices that need controlled access to the token
iv. As the traffic increases, data throughput also increases to a certain level and then stabilizes.

Disadvantages of Token Passing

i. Token passing involves complicated protocols for managing the network and recovering from errors. The traffic associated with these protocols has higher band width overhead than is required for CSMA
ii. All devices require complicated software that needs to be modified whenever a station is added or removed.
iii. Some systems require an additional central controller that adds to the overhead and reduces throughput. Cabling and network hardware can be more expensive for token passing networks than for CSMA networks.

6.1.3 Polling

Polling is a deterministic way of allowing systems access to the network while also avoiding collisions. Polling is most closely associated with mainframe (point-to-point) computer networks. By using polling, one device such as a mainframe *front-end processor*, is designated as the primary device. Primaries also are known as the *channel access administrators*, *controllers*, or *masters*. All access to the network is controlled by the primary. The primary queries (polls) each of the secondary devices, also known as *slaves*. As each secondary is polled,

the primary inquires if the secondary has information to be transmitted. Only when it is polled does the secondary have access to the communication channel. Each system has rules pertaining to how long each secondary can transmit data. In this way, polling is similar to token passing, except that the central device controls the order in which systems are contacted.

Advantages of Polling

i. Many characteristics of polling can be determined centrally, including the polling order and node priorities.
ii. Polling ensures that channel access is *predictable* and fixed. Because the time delays between the primary and secondary devices can be calculated, this access method is called deterministic. Deterministic access methods are suitable for controlling some automated equipment because each piece of equipment is guaranteed access to the network at predetermined intervals.
iii. Polled channels cannot be *over saturated* with traffic. As demand increases, traffic increases up to a maximum level. The polling mechanism ensures that maximum traffic level cannot be exceeded. Nor can excess traffic reduce the performance of the network.

Disadvantages of Polling

i. Some applications cannot function with the time delays required for polling other devices.
ii. The process of polling involves large numbers of messages that take up available bandwidth. Traffic is required to poll each node, even nodes that are idle.
iii. Some polled networks use half-duplex transmission line. This means that the primary and secondary devices must " turn around " the line requiring some band width.
iv. Polling required a sophisticated central control mechanism that required extensive configuration.

7.0 TRANSMISSION IMPAIRMENTS

With any communications system, the signal that is received may differ from the signal that is transmitted, due to various transmission impairments. For analog signals, these impairments introduce various random modifications that degrade the signal quality. For digital signals, bit errors may be introduced, such that a binary 1 is transformed into a binary 0 or vice versa.

1. Attenuation

Attenuation means a loss of energy. When a signal, simple or composite, travels through a medium, it loses some of its energy in overcoming the resistance of the medium. That is why a wire carrying electric signals gets warm, if not hot, after a while. Some of the electrical energy in the signal is converted to heat. To compensate for this loss, amplifiers are used to amplify the signal.

2. Distortion

Distortion means that the signal changes its form or shape. Distortion can occur in a composite signal made of different frequencies. Each signal component has its own propagation speed (see the next section) through a medium and, therefore, its own delay in arriving at the final destination. Differences in delay may create a difference in phase if the delay is not exactly the same as the period duration. In other words, signal components at the receiver have phases different from what they had at the sender. The shape of the composite signal is therefore not the same.

3. Noise

Noise is unwanted signals that are inserted somewhere between transmission and reception. Noise is the major limiting factor in communications system performance. Noise may be divided into four categories:

- Thermal noise

- Intermodulation noise
- Crosstalk
- Impulse noise

a) Thermal noise :

Thermal noise is due to thermal agitation of electrons. It is present in all electronic devices and transmission media and is a function of temperature. Thermal noise is uniformly distributed across the bandwidths typically used in communications systems and hence is often referred to as white noise. Thermal noise is particularly significant for satellite communication.

b) Intermodulation noise :

When signals at different frequencies share the same transmission medium, the result may be intermodulation noise. The effect of intermodulation noise is to produce signals at a frequency that is the sum or difference of the two original frequencies or multiples of those frequencies. For example, the mixing of signals at frequencies f1 and f2 might produce energy at the frequency f1+f2.

c) Crosstalk:

Crosstalk has been experienced by anyone who, while using the telephone, has been able to hear another conversation; it is an unwanted coupling between signal paths. It can occur by electrical coupling between nearby twisted pairs or, rarely coax cable lines carrying multiple signals. Crosstalk can also occur when microwave antennas pick up unwanted signals.

d) **Impulse noise:**

Impulse noise is noncontinuous, consisting of irregular pulses or noise spikes of short duration and of relatively high amplitude. It is generated from a variety of causes, including external electromagnetic disturbances, such as lightning, and faults and flaws in the communications system

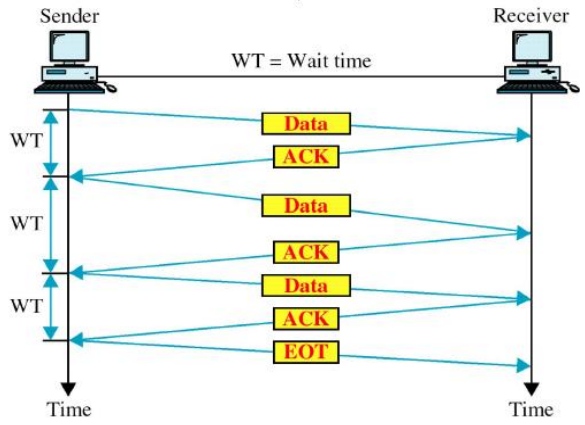
7.1 FLOW CONTROL

The most important responsibilities of the data link layer are flow control and error control. Collectively, these functions are known as data link control. Flow Control is a technique for assuring that a transmitting entity does not overwhelm a receiving entity with data. The receiving entity typically allocates a data buffer of some maximum length for a transfer. When data are received, the receiver must do a certain amount of processing before passing the data to the higher level software. In absence of flow control the receivers buffer may fill up and over flow while it is processing old data. Error control in the data link layer is based on automatic repeat request (ARQ) , which is the retransmission of data. Two types of mechanisms can be deployed to control the flow:

- Stop and wait
- Sliding window

7.1.1 Stop and Wait

This flow control mechanism forces the sender after transmitting a data frame to stop and wait until the acknowledgement of the data-frame sent is received.



Advantages of Stop and Wait

i. It is very simple to implement.

ii. The main advantage of this protocol is the accuracy. The next frame is sent only when the first frame is acknowledged. So, there is no chance of any frame being lost.

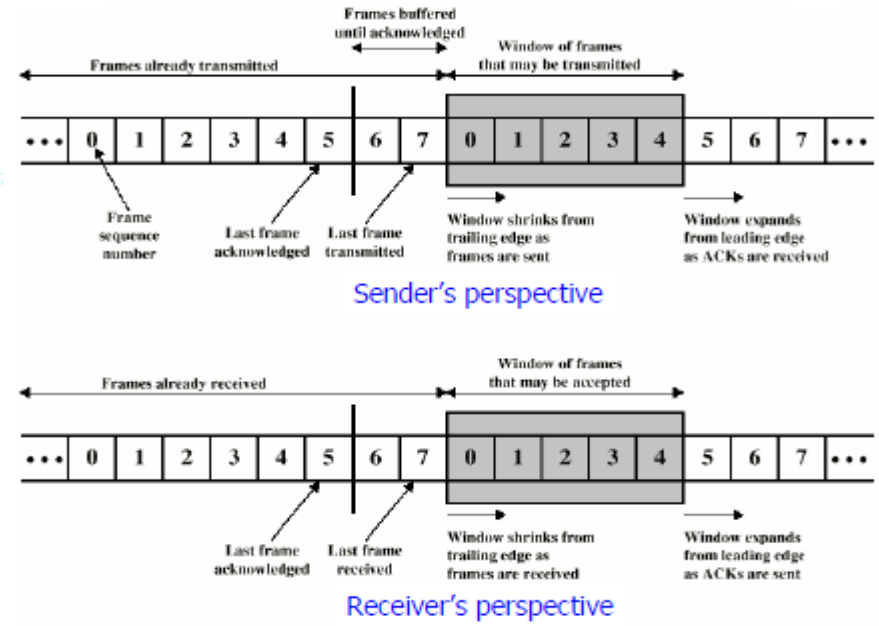
Disadvantages of Stop and Wait

i. We can send only one packet at a time.
ii. If the distance between the sender and the receiver is large then the propagation delay would be more than the transmission delay. Hence, efficiency would become very low.
iii. After every transmission, the sender has to wait for the acknowledgment and this time will increase the total transmission time. This makes the transmission process **slow**.

7.1.2 Sliding Window

In this flow control mechanism, both sender and receiver agree on the number of data-frames after which the acknowledgement should be sent. Stop and wait flow control mechanism wastes resources, this protocol tries to make use of underlying resources as much as possible.

In sliding window the Receiver allocates buffer space for W-frames and the Transmitter can send up to W frames without waiting for any ACK. Each frame is numbered to keep track of which frames have been Acknowledged and ACK includes number of next frame expected.



Shaded rectangle shows frames that may be sent. Sender transmits 5 frames starting with frame 0 when a frame is sent, shaded window shrinks. When a ACK is received, the shaded window grows . Frames between vertical bar and shaded window have been sent but not yet ACKed.

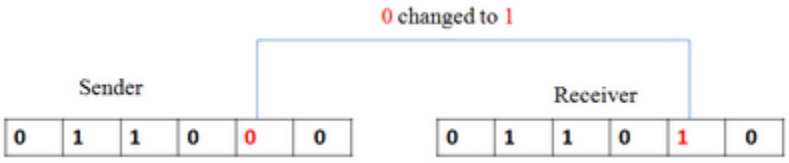
7.2 ERROR CONTROL

Error Control in the data link layer is a process of detecting and retransmitting the data which has been lost or corrupted during the transmission of data. Any reliable system must have a mechanism for detecting and correcting such errors. Error detection and correction occur at both the transport layer and the data link layer.

7.2.1 Types of error

a. Single bit Error:

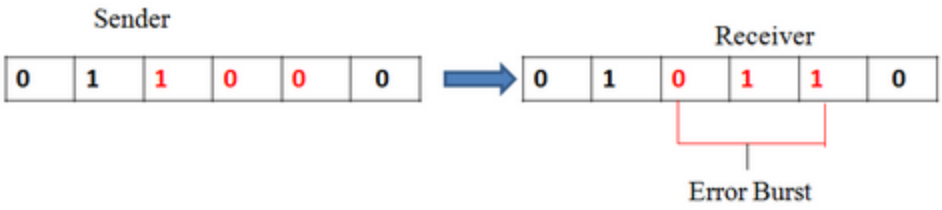
Whenever bits flow from one point to another, they are subject to unpredictable changes because of interference. This interference can change the shape of the signal. In a single-bit error, a 0 is changed to a 1 or a 1 to a 0. The term single-bit error means that only 1 bit of a given data unit (such as a byte, character, or packet) is changed from 1 to 0 or from 0 to 1.



Single bit errors are very rare in the communication system because the noise must not a short duration that it can only disturb only one bit. So these errors in the communication system are less however this type of errors can happen in parallel communication where the noise will distribute in all the communication lines.

b. Burst Error

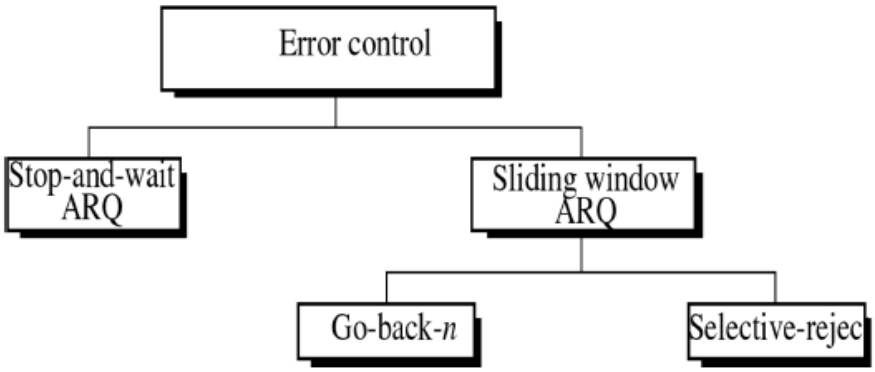
The term burst error means that 2 or more bits in the data unit have changed from 1 to 0 or from 0 to 1.



These errors are most common in serial communication where the noise can interfere the some amount of bits in sequence or in multiple bits. The number of corrupted bits depends on the data rate and noise duration. The error correction of this type is difficult which leads to incorporation of complex detecting and correcting algorithms.

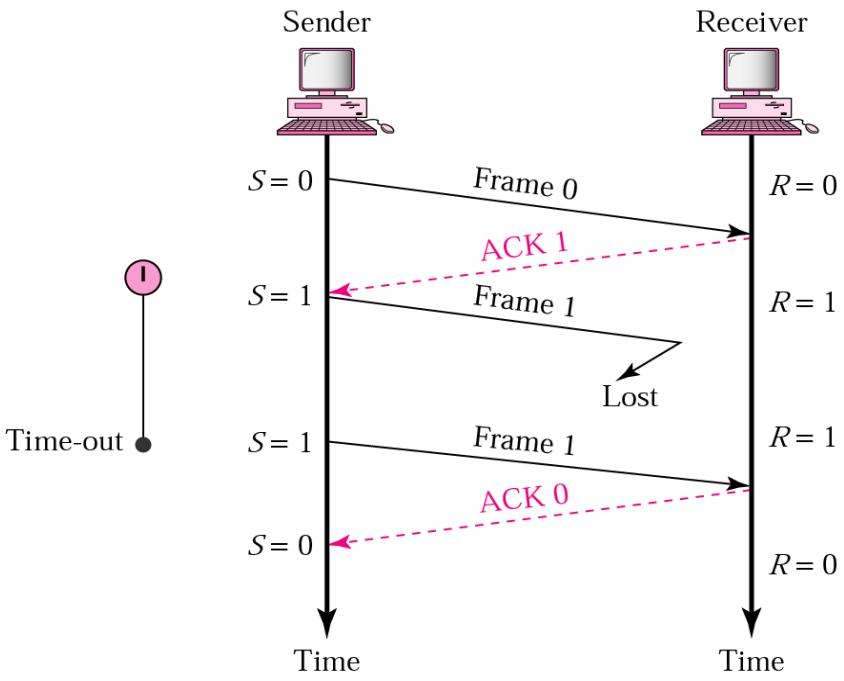
7.2.2 Types of techniques of error control

There are three types of techniques available which Data-link layer may deploy to control the errors by Automatic Repeat Requests (ARQ):



a) Stop-and-wait ARQ

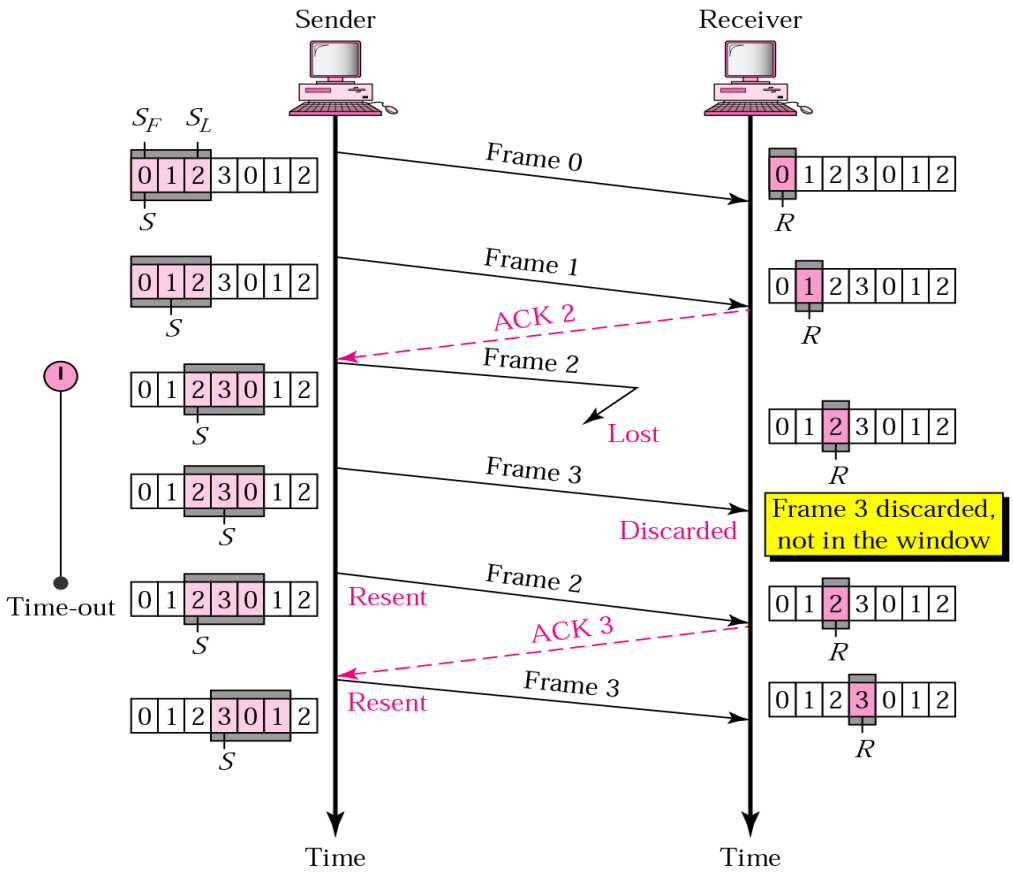
In Stop-and-wait ARQ the source station transmits a single frame and then must await an acknowledgement (ACK). No other data frames can be sent until the destination stations reply arrives at the source station. The sending device keeps a copy of the last frame until it receives an acknowledgement for that frame. Keeping a copy allows the sender to retransmits lost or damaged frames until they are received correctly.



b) Go-Back-N ARQ

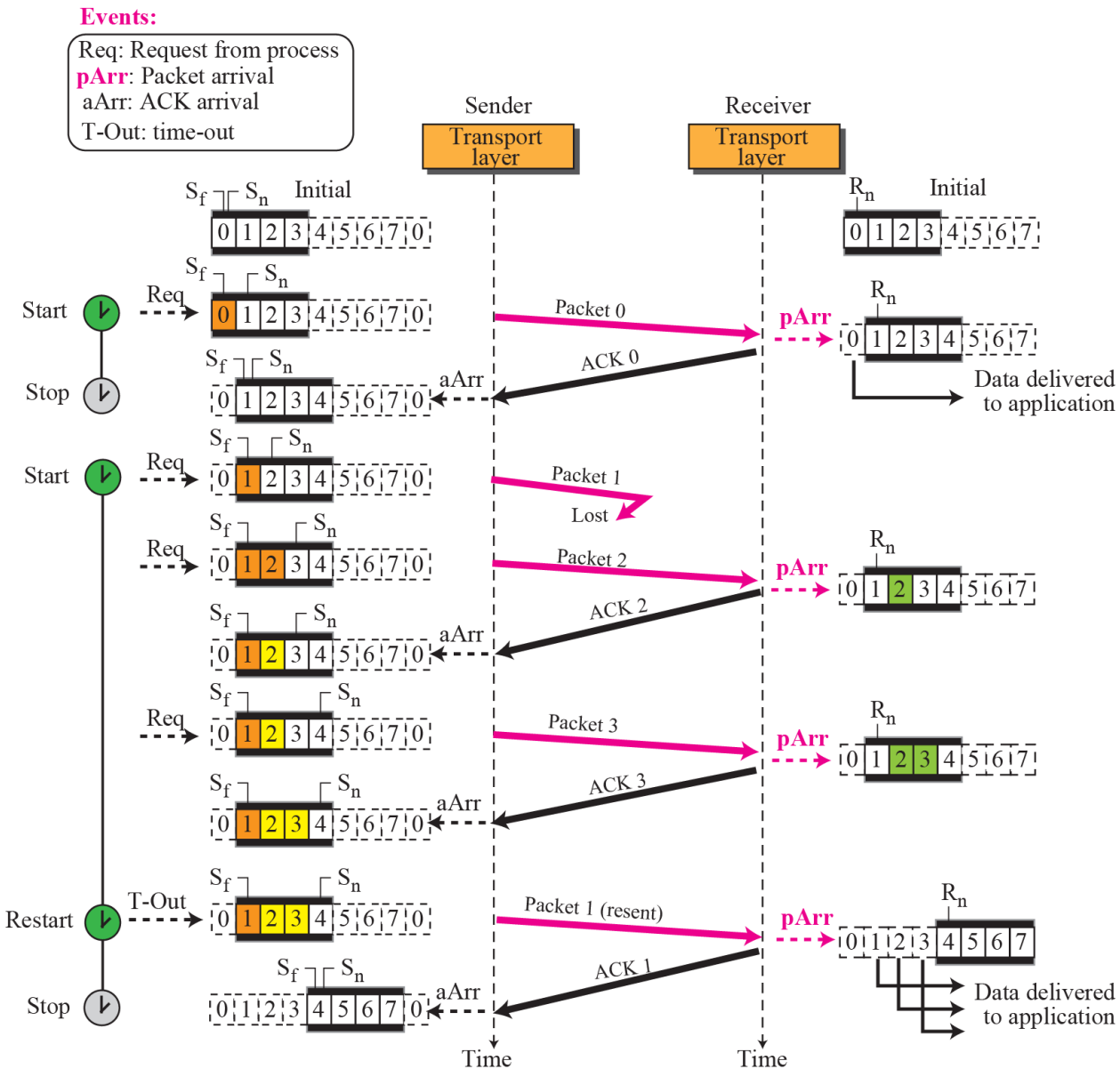
Stop and wait ARQ mechanism does not utilize the resources at their best.When the acknowledgement is received, the sender sits idle and does nothing. In Go-Back-N ARQ method, both sender and receiver maintain a window. The sending-window size enables the sender to send multiple frames without receiving the acknowledgement of the previous ones. The receiving-window enables the receiver to receive multiple frames and acknowledge them. The receiver keeps track of incoming frame's sequence number.

When the sender sends all the frames in window, it checks up to what sequence number it has received positive acknowledgement. If all frames are positively acknowledged, the sender sends next set of frames. If sender finds that it has received NACK or has not receive any ACK for a particular frame, it retransmits all the frames after which it does not receive any positive ACK.



c) Selective Repeat ARQ

In Go-back-N ARQ, it is assumed that the receiver does not have any buffer space for its window size and has to process each frame as it comes. This enforces the sender to retransmit all the frames which are not acknowledged. In Selective-Repeat ARQ, the receiver while keeping track of sequence numbers, buffers the frames in memory and sends NACK for only frame which is missing or damaged. The sender in this case, sends only packet for which NACK is received



7.3 ERROR DETECTION:

Error detection is the process of verifying the received information whether it is correct or not at the receiver end without having any information of sent original message. In sender side some redundant bits are added to the original message based some property of message signal (i.e. parity bits) and in the receiver side by scanning this redundant bits, the error in the message will be predicted.

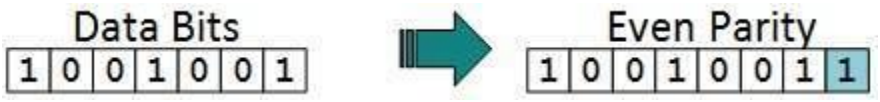
7.3.1 Types of Error detection Checks

- Parity Checking
- Check Sum
- Cyclic Redundancy Check (CRC)

1. Parity Check

One extra bit is sent along with the original bits to make number of 1s either even in case of even parity, or odd in case of odd parity.

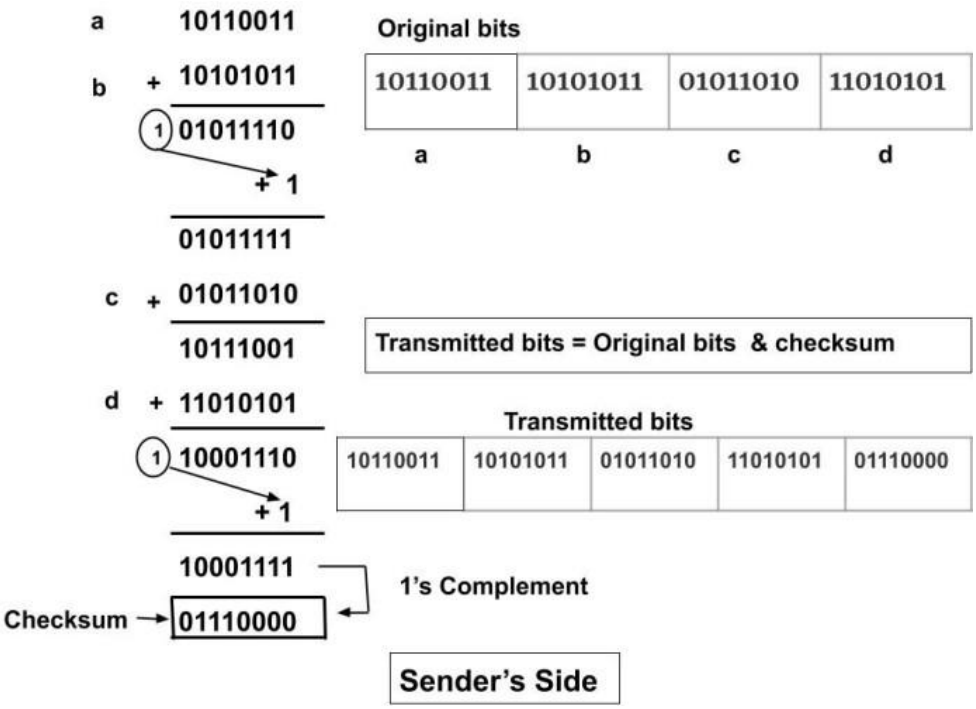
The sender while creating a frame counts the number of 1s in it. For example, if even parity is used and number of 1s is even then one bit with value 0 is added. This way number of 1s remains even.If the number of 1s is odd, to make it even a bit with value 1 is added.

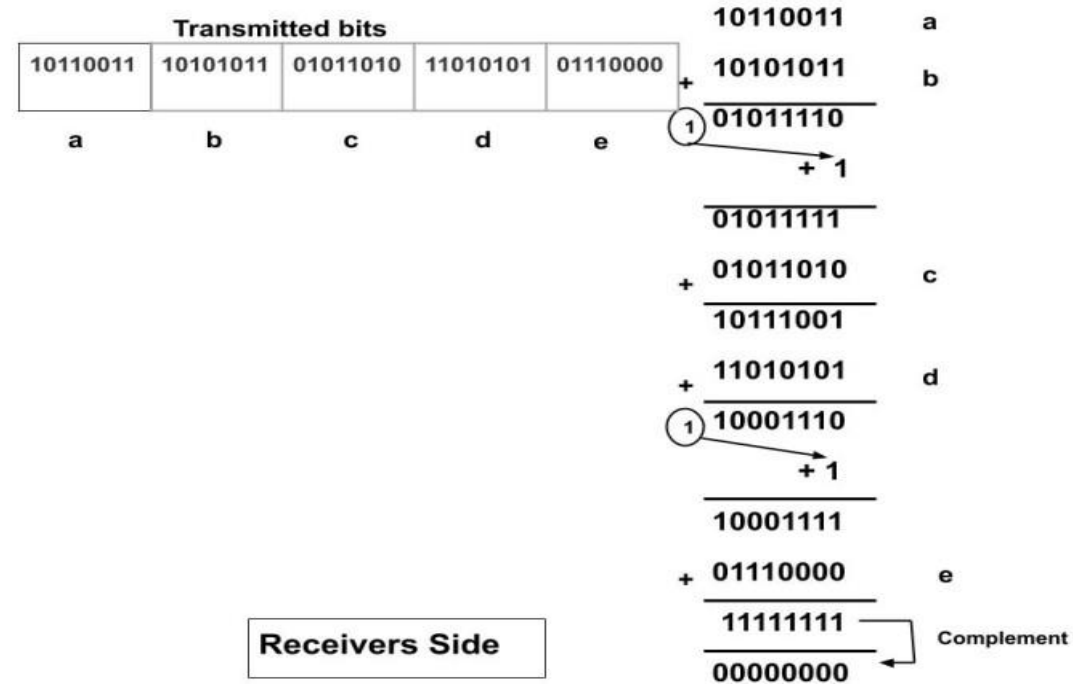


The receiver simply counts the number of 1s in a frame. If the count of 1s is even and even parity is used, the frame is considered to be not-corrupted and is accepted. If the count of 1s is odd and odd parity is used, the frame is still not corrupted. If a single bit flips in transit, the receiver can detect it by counting the number of 1s. But when more than one bits are erroneous, then it is very hard for the receiver to detect the error.

2. Checksum

In checksum error detection scheme, the data is divided into k segments each of m bits. In the sender's end the segments are added using 1's complement arithmetic to get the sum. The sum is complemented to get the checksum.The checksum segment is sent along with the data segments. At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum. The sum is complemented. If the result is zero, the received data is accepted; otherwise discarded.

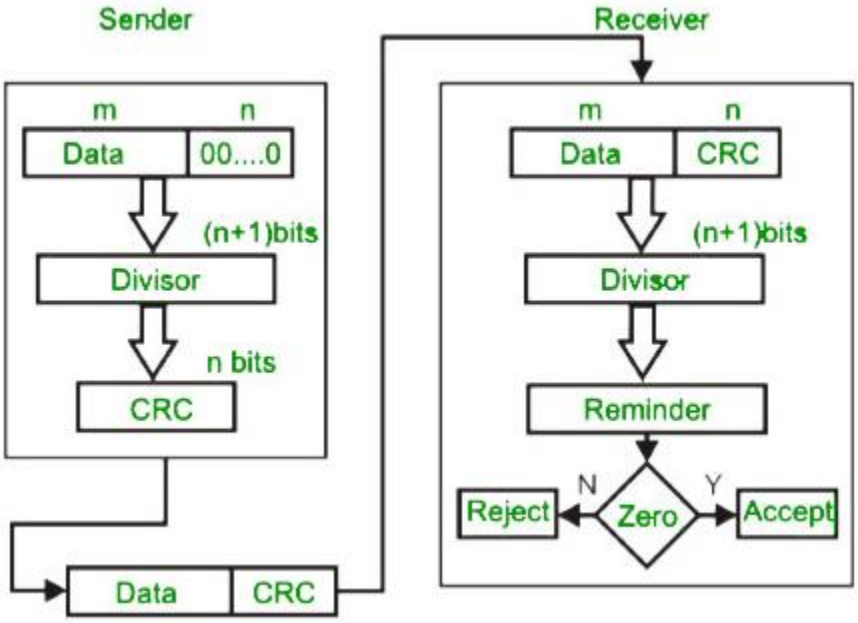




3. **CRC (cyclic redundancy check)**

CRC is based on binary division. In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of data unit so that the resulting data unit

becomes exactly divisible by a second, predetermined binary number. At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted. A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.



This method is commonly used in many forms of communication. It provides a high level of error detection with speed and ease of use.

8.0 NETWORKING DEVICES AND COMPONENTS

Network devices are physical devices that are required for communication and interaction between hardware on a computer network. The network devices work as a group and have a single purpose which securely transfers data as fast as possible. To meet this goal there are several networking devices this include:

- Modem
- Repeater
- Router
- Hub
- Switch,
- Bridge
- Brouter
- Gateway

a) Modem

The main function of the modem is to convert digital signal into analog and vice versa. Modem is a combination of two devices *modulator* and *demodulator*. The modulator converts digital data into analog data when the data is being sent by the computer. The demodulator converts analog data signals into digital data when it is being received by the computer.

b) Repeater

A repeater is an electronic device operates at the physical layer. It has two Ethernet ports. Repeater amplifies the received signal and retransmits the signals in the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. When the signal becomes weak, repeater copy the signal bit by bit and regenerate it at the original strength. Analog repeaters frequently can only amplify the signal while digital repeaters can reconstruct a signal to near its original quality.

c) Hub

Hubs are commonly used to connect segments of a LAN. A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets. There are mainly two types of Hub, they are:

1. **Active Hub:** An Active hub is also known as Concentrator. It requires a power supply and can work as a repeater. Thus, it can analyze the data packets and can amplify the transmission signals, if needed.
2. **Passive Hub:** A passive hub does not need any power supply to operate. It only provides communication between the networking devices and does not amplify the transmission signals. In other words, it just forwards the data as it is.

d) Switch

A Switch is a device that filters and forwards packets between LAN segments. Switches operate at the data link layer (layer 2) and sometimes the network layer (layer 3) of the OSI Reference Model and therefore support any packet protocol. LANs that use switches to join segments are called switched LANs or, in the case of Ethernet networks, switched Ethernet LANs.

Switches are higher-performance alternatives to hubs. Both pass data between devices connected to them. Hubs do so by broadcasting the data to all other connected devices, while switches first determine which device is the intended recipient of the data and then send it to that one device directly via a so-called "virtual circuit."

Switching Methods

Switches use three methods to deal with data as it arrives:

- **Cut-through**: In a cut-through configuration, the switch begins to forward the packet as soon as it is received. No error checking is performed on the packet, so the packet is moved through quickly. The downside of cut-through is that because the integrity of the packet is not checked, the switch can propagate errors. .

- **Store-and-forward:** In a store-and-forward configuration, the switch waits to receive the entire packet before beginning to forward it. It also performs basic error checking.
- **Fragment-free:** Building on the speed advantages of cut-through switching, fragment-free switching works by reading only the part of the packet that enables it to identify fragments of a transmission.

e) Router

The router is a network device. It selects the best path for a data packet. The router is located at any gateway (where one network meets another). Its forward data packets from one network to another based on the address of the destination network in the incoming packet and an internal routing table. It also determines which port (line) to send out the packet (ports typically connect to Ethernet cables).

A router reads its routing table to decide the best available route the packet can take to reach its destination quickly and accurately. The routing table may be of these two types:

- **Static :** In a static routing table the routes are fed manually. So it is suitable only for very small networks that have maximum two to three routers.
- **Dynamic:** In a dynamic routing table, the router communicates with other routers through protocols to determine which routes are free. This is suited for larger networks where manual feeding may not be feasible due to large number of routers.

While hubs, switches, and routers all share similar physical appearance, routers differ substantially in their inner workings and contain significantly more logic. Traditional routers are designed to join together multiple local area networks (LANs) with a wide area network (WAN). Routers serve as intermediate destinations for network traffic. They receive incoming network packets, look inside each packet to identify the source and target network addresses, then forward these packets where needed to ensure the data reaches its final destination. Neither switches nor hubs can do these things.

f) Bridge

A Bridge is a device that connects two local-area networks (LANs), or two segments of the same LAN. The two LANs being connected can be alike or dissimilar. For example, a bridge can connect an Ethernet with a Token-Ring network. Unlike routers, bridges are protocol independent. They simply forward packets without analyzing and re-routing messages. Consequently, they're faster than routers, but also less versatile.

Types of Bridges:

There are mainly three types in which bridges can be characterized:

- **Transparent Bridge:** As the name signifies, it appears to be transparent for the other devices on the network. The other devices are ignorant of its existence. It only blocks or forwards the data as per the MAC address.
- **Source Route Bridge:** It derives its name from the fact that the path which packet takes through the network is implanted within the packet. It is mainly used in Token ring networks.
- **Translational Bridge:** The process of conversion takes place via Translational Bridge. It converts the data format of one networking to another. For instance Token ring to Ethernet and vice versa.

g) Brouter

Brouters are the combination of both the bridge and routers. They take up the functionality of the both networking devices serving as a *bridge* when forwarding data between networks, and serving as a *router* when routing data to individual systems. Brouter functions as a filter that allows some data into the local network and redirects unknown data to the other network.

h) Gateway

Gateways usually work at the Transport layer and Session layer of the OSI model. It connects two networks that may work upon different networking models. Gateway takes data from one system, interpret it, and transfer it to another system. It also is known as protocol converters and

can operate at any network layer. Gateways are generally more complex than switch or router. Gateway deals with numerous protocols and standards from different vendors. It performs all of the functions of routers. A router with added translation functionality is a gateway.

8.1 ROUTING

Routing is a process of selecting path along which the data can be transferred from source to the destination. Routing is performed by a special device known as a router. A Router works at the network layer in the OSI model and internet layer in TCP/IP model. A router is a networking device that forwards the packet based on the information available in the packet header and forwarding table.

The routing algorithms are used for routing the packets. The routing algorithm is nothing but a software responsible for deciding the optimal path through which packet can be transmitted. The routing protocols use the metric to determine the best path for the packet delivery. The metric is the standard of measurement such as hop count, bandwidth, delay, current load on the path, etc. used by the routing algorithm to determine the optimal path to the destination. The routing algorithm initializes and maintains the routing table for the process of path determination.

8.1.1 Types of Routing

1. Static routing

Static Routing is also known as Nonadaptive Routing. It is a technique in which the administrator manually adds the routes in a routing table. A Router can send the packets for the destination along the route defined by the administrator.

Advantages

i. No routing overhead for router CPU which means a cheaper router can be used to do routing.
ii. It adds security because only administrator can allow routing to particular networks only.
iii. No bandwidth usage between routers.

Disadvantage

i. For a large network, it is a hectic task for administrator to manually add each route for the network in the routing table on each router.
ii. The administrator should have good knowledge of the topology. If a new administrator comes, then he has to manually add each route so he should have very good knowledge of the routes of the topology.

2. Default Routing

Default Routing is a technique in which a router is configured to send all the packets to the same hop device, and it doesn't matter whether it belongs to a particular network or not. A Packet is transmitted to the device for which it is configured in default routing. Default Routing is used when networks deal with the single exit point.

It is also useful when the bulk of transmission networks have to transmit the data to the same hp device. When a specific route is mentioned in the routing table, the router will choose the specific route rather than the default route. The default route is chosen only when a specific route is not mentioned in the routing table..

1. **Dynamic Routing**

Dynamic routing makes automatic adjustment of the routes according to the current state of the route in the routing table. Dynamic routing uses protocols to discover network destinations and the routes to reach it. RIP and OSPF are the best examples of dynamic routing protocol. Automatic adjustment will be made to reach the network destination if one route goes down.
A dynamic protocol have following features:

- The routers should have the same dynamic protocol running in order to exchange routes.
- When a router finds a change in the topology then router advertises it to all other routers.

Advantages

i. Easy to configure.
ii. More effective at selecting the best route to a destination remote network and also for discovering remote network.

Disadvantage

i. Consumes more bandwidth for communicating with other neighbors.

ii. Less secure than static routing.

8.2 SWITCHING

Switched communication networks are those in which data transferred from source to destination is routed between various intermediate nodes. Switching is the technique by which nodes control or switch data to transmit it between specific points on a network. There are 3 common switching techniques:

- Message switching
- Packet Switching
- Circuit Switching

8.2.1 Message Switching

Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded. In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.

Message switches are programmed in such a way so that they can provide the most efficient routes. Each and every node stores the entire message and then forward it to the next node. This type of network is known as *store and forward network***.** Message switching treats each message as an independent entity.

Advantages of Message Switching

Message switching has the following advantages:

i. As message switching is able to store the message for which communication channel is not available, it helps in reducing the traffic congestion in network.
ii. In message switching, the data channels are shared by the network devices.
iii. It makes the traffic management efficient by assigning priorities to the messages.
iv. The size of the message which is sent over the network can be varied. Therefore, it supports the data of unlimited size.

Disadvantages of Message Switching

Message switching has the following disadvantages:

i. Message switching cannot be used for real time applications as storing of messages causes delay.
ii. In message switching, message has to be stored for which every intermediate devices in the network requires a large storing capacity.

8.2.2 Packet Switching

The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually. The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.Every packet contains some information in its headers such as source address, destination address and sequence number.

Packets will travel across the network, taking the shortest path as possible. All the packets are reassembled at the receiving end in correct order. If any packet is missing or corrupted, then the message will be sent to resend the message. If the correct order of the packets is reached, then the acknowledgment message will be sent.

Approaches of Packet Switching:

There are two approaches to Packet Switching:

- Datagram packet switching
- Virtual packet switching

1. **Datagram Packet switching:**

It is a packet switching technology in which packet is known as a datagram, is considered as an independent entity. Each packet contains the information about the destination and switch uses this information to forward the packet to the correct destination. The packets are reassembled at the receiving end in correct order.

In Datagram Packet Switching technique, the path is not fixed. Intermediate nodes take the routing decisions to forward the packets. Datagram Packet Switching is also known as connectionless switching.

2. **Virtual Circuit Switching**

Virtual Circuit Switching is also known as connection-oriented switching. In the case of Virtual circuit switching, a preplanned route is established before the messages are sent. Call request and call accept packets are used to establish the connection between sender and receiver. In this case, the path is fixed for the duration of a logical connection.

Advantages of Packet Switching

i. Delay in delivery of packets is less, since packets are sent as soon as they are available.

ii. Switching devices don't require massive storage, since they don't have to store the entire messages before forwarding them to the next node.

iii. Data delivery can continue even if some parts of the network faces link failure. Packets can be routed via other paths.

iv. It allows simultaneous usage of the same channel by multiple users.

v. It ensures better bandwidth usage as a number of packets from multiple sources can be transferred via the same link.

Disadvantages of Packet switching

i. They are unsuitable for applications that cannot afford delays in communication like high quality voice calls.

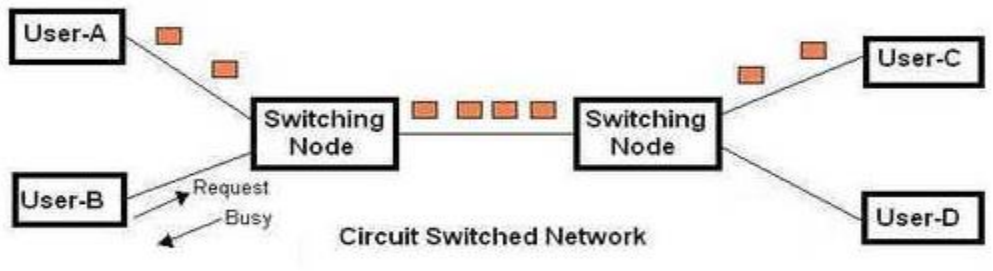
ii. Packet switching high installation costs.

iii. They require complex protocols for delivery.

iv. Network problems may introduce errors in packets, delay in delivery of packets or loss of packets. If not properly handled, this may lead to loss of critical information.

8.2.3 Circuit Switching

Circuit switching network establishes a fixed bandwidth circuit (channel) between nodes before the users may communicate, as if the nodes were physically connected with an electrical circuit. The bit delay is constant during the connection, as opposed to packet switching, where packet queues may cause varying delay.



Each circuit cannot be used by other callers until the circuit is released and a new connection is set up. Even if no communication is taking place in a dedicated circuit then, that channel still remains unavailable to other users. Channels that are available for new calls to be set up are said to be idle. Telephone network is example of circuit switching system.
Virtual circuit switching is a packet switching technology that may emulate circuit switching, in the sense that the connection is established before any packets are transferred, and that packets are delivered in order.

Advantages of circuit switching

Following are the advantages of circuit switching :

i. As there is very less delay for the call to be established and also during the conversation, the circuit switching network is widely used for realtime voice services throughtout the world since years. There is almost no waiting time at voice switches used for the call.

ii. It will have realistic voice communication and consecutively speaking persons are easily identified due to higher sampling rates used.

iii. Once the connection is established between two parties, it will be available till end of the conversation. This guarantees reliable connection in terms of constant data rate and availability of resources (Bandwidth, channels etc.). Hence it is used for long distance and long duration calls without any sort of tiredness.

iv. No loss of packets or out of order packets here as this is connection oriented network unlike packet switched network.

v. The forwarding of information is based on time or frequency slot assignments and hence there is no need to examine the header as in the case of packet switching network. As there is no header requirement, there is low overhead in circuit switching network.

Drawbacks or disadvantages of circuit switching

Following are the **disadvantages of circuit switching**:

i. As is it designed for voice traffic, it is not suitable for data transmission.

ii. The channels and bandwidth used in the connection are not available till the convesation or call is broken. Due to this, even if they are not utilized, they can not be used for any other purpose (e.g. connections). Hence circuit switching is inefficient in terms of resource utilization (i.e. channels, bandwidth etc.). Moreover due to this, if there are many users than the available channels, it leads to dropped calls or calls not being established.

iii. The connection requires call setup delay and it is not instantaneous. This means there is no communication until connection is established and resources are available.

iv. It is more expensive compare to other techniques due to dedicated path requirement. Consecutively, the call rates are also higher.

9.0 NETWORKING PROTOCOLS

Network protocols are sets of established rules that dictate how to format, transmit and receive data so computer network devices from servers and routers to endpoints can communicate regardless of the differences in their underlying infrastructures, designs or standards. To successfully send and receive information, devices on both sides of a communication exchange must accept and follow protocol conventions. Support for network protocols can be built into software, hardware or both.

Standardized network protocols provide a common language for network devices. Without them, computers wouldn't know how to engage with each other. As a result, except for specialty networks built around a specific architecture, few networks would be able to function, and the internet as we know it wouldn't exist. Virtually all network end users rely on network protocols for connectivity.

9.1 Elements of a protocol

The key elements of a protocol are as follows:

1. **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 be the address of the receiver, and the rest of the stream to be the message itself.
2. **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?.
3. **Timing:** Timing refers to two characteristics: when data should be sent and how fast they can be sent. For example, if a sender transmits data at 100 Mbps but the receiver can receive data at only 1 mbps, this transmission will overload the receiver and data will be largely lost.

9.2 A protocol performs the following functions:

1. **Data sequencing**. It refers to breaking a long message into smaller packets of fixed size. Data sequencing rules define the method of numbering packets to detect loss or duplication of packets, and to correctly identify packets, which belong to same message.

2. **Data routing**. Data routing defines the most efficient path between the source and destination.

3. **Data formatting**. Data formatting rules define which group of bits or characters within packet constitute data, control, addressing, or other information.

4. **Flow control**. A communication protocol also prevents a fast sender from overwhelming a slow receiver. It ensures resource sharing and protection against traffic congestion by regulating the flow of data on communication lines.

5. **Error control**. These rules are designed to detect errors in messages and to ensure transmission of correct messages. The most common method is to retransmit erroneous message block. In such a case, a block having error is discarded by the receiver and is retransmitted by the sender.

6. **Precedence and order of transmission**. These rules ensure that all the nodes get a chance to use the communication lines and other resources of the network based on the priorities assigned to them.

7. **Connection establishment and termination**. These rules define how connections are established, maintained and terminated when two nodes of a network want to communicate with each other.

8. **Data security**. Providing data security and privacy is also built into most communication software packages. It prevents access of data by unauthorized users.

9. Log information. Several communication software are designed to develop log information, which consists of all jobs and data communications tasks that have taken place. Such information may be used for charging the users of the network based on their usage of the network resources.

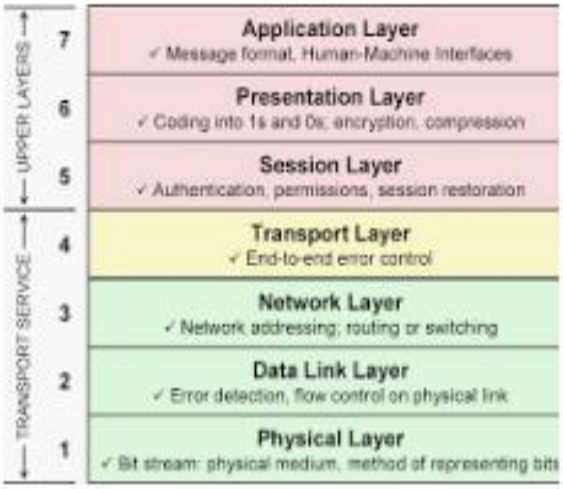
9.3 NETWORK MODELS

A network model reflects a design or architecture to accomplish communication between different systems. Network models are also referred to as network stacks or protocol suites. Examples of network models includes TCP/IP, Sequenced Packet Exchange/Internet Packet Exchange (SPX/ IPX) used by Novelle Netware, the Network Basic Input Output System (NetBIOS), which comprises the building blocks for most Microsoft networking and network applications; and AppleTalk, the network model for Apple Macintosh computers.

A network model usually consists of layers. Each layer of a model represents specific functionality. Within the layers of a model, there are usually protocols specified to implement specific tasks. Thus, a layer is normally a collection of protocols. There are a number of different network models. Some of these models relate to a specific implementation, such as the TCP/IP network model. Others simply describe the process of networking, such as the International Organization for Standardization/Open System Interconnection Reference Model (ISO/ OSI-RM, or more simply, OSI-RM).

9.3.1 Open System Interconnection (OSI) Model

In 1947, the International Standards Organization (ISO) proposed a network model that covers all network communications .This model is called Open Systems Interconnection (OSI) model. An open system is a model that allows any two different systems to communicate regardless of their underlying architecture. The OSI model is built of seven layers.



Physical layer (Layer 1)

The physical layer is the lowest layer of the OSI hierarchy and coordinates the functions required to transmit a bit stream over a physical medium. It also defines the procedures and functions that physical devices and interfaces have to perform for transmission occur. The physical layer specifies the type of transmission medium and the transmission mode (simplex, half duplex or full duplex) and the physical, electrical, functional and procedural standards for accessing data communication networks.

Data Link (Layer 2)

The data link layer transforms the physical layer, a raw transmission facility, to a reliable link and is responsible for node-to-node delivery. It makes the physical layer appear error free to the upper layer (network layer). The data link layer packages data from the physical layer into groups called blocks, frames or packets. If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the physical address of the sender (source address) and/or receiver (destination address) of the frame. The data-link layer provides flow-control, access-control, and error-control.

Network layer (Layer 3)

The network layer provides details that enable data to be routed between devices in an environment using multiple networks, subnetworks or both. This is responsible for addressing messages and data so they are sent to the correct destination, and for translating logical addresses and names (like a machine name FLAME) into physical addresses. This layer is also responsible for finding a path through the network to the destination computer.

The network layer provides the upper layers of the hierarchy with independence from the data transmission and switching technologies used to interconnect systems. Networking components that operate at the network layer include routers and their software.

Transport Layer (Layer 4)

The transport layer controls and ensures the end-to-end integrity of the data message propagated through the network between two devices, providing the reliable, transparent transfer of data

between two endpoints. Transport layer responsibilities include: message routing, segmenting, error recovery and two types of basic services to an upper-layer protocol: connection oriented and connectionless.

The transport layer is the highest layer in the OSI hierarchy in terms of communications and may provide data tracking, connection flow control, sequencing of data, error checking, and application addressing and identification.

Session Layer (Layer 5)

Session layer, some times called the dialog controller provides mechanism for controlling the dialogue between the two end systems. It defines how to start, control and end conversations (called sessions) between applications. Session layer protocols provide the logical connection entities at the application layer. These applications include file transfer protocols and sending email.

Session responsibilities include: network log-on and log-off procedures and user authentication. Session layer characteristics include virtual connections between applications, entities, synchronization of data flow for recovery purposes, creation of dialogue units and activity units, connection parameter negotiation, and partitioning services into functional groups.

Presentation Layer (Layer 6)

The presentation layer provides independence to the application processes by addressing any code or syntax conversion necessary to present the data to the network in a common communications format. It specifies how end-user applications should format the data. The presentation layer translated between different data formats and protocols.

Presentation functions include: data file formatting, encoding, encryption and decryption of data messages, dialogue procedures, data compression algorithms, synchronization, interruption, and termination.

Application Layer (Layer 7)

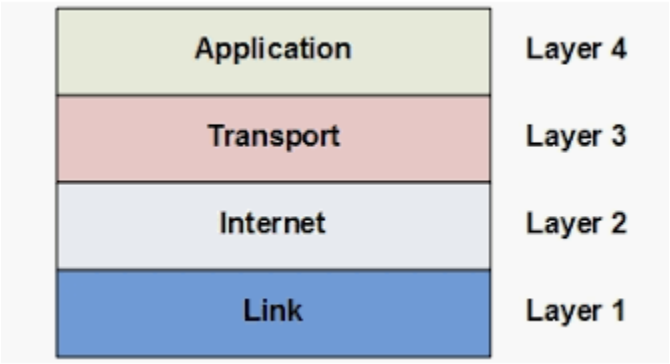
The application layer is the highest layer in the hierarchy and is analogous to the general manager of the network by providing access to the OSI environment. The applications layer

provides distributed information services and controls the sequence of activities within and application and also the sequence of events between the computer application and the user of another application.

The application layer communicates directly with the user's application program. User application processes require application layer service elements to access the networking environment. The service elements are of two types: CASEs *(common application service elements)* satisfying particular needs of application processes like association control, concurrence and recovery. The second type is SASE (*specific application service elements)* which include TCP/IP stack, FTP, SNMP, Telnet and SMTP.

9.3.2 Transmission Control Protocol/Internet Protocol (TCP/IP) Model

The TCP/IP reference model also referred as internet protocol suite is a layered model developed by the Defense Project Research Agency(ARPA or DARPA) of the United States as a part of their research project in 1960. Initially, it was developed to be used by defense only. But later on, it got widely accepted. The main purpose of this model is to connect two remote machines for the exchange of information. These machines can be operating in different networks or have different architecture. The TCP/IP reference model has four layers this includes: Application Layer, Transport Layer, Internet Layer and Network Access Layer.



Each layer of the TCP/IP has a particular function to perform and each layer is completely separate from the layer(s) next to it. The communication process that takes place, at its simplest between two computers, is that the data moves from layer 4 to 3 to 2 then to 1 and the

information sent arrives at the second system and moves from 1 to 2 to 3 and then finally to layer 4.

The Link Layer

The link layer is the lowest layer of the TCP/IP model; it is also referred to as the *network interface* layer. This layer contains the protocols that the computer uses to deliver data to the other computers and devices that are attached to the network. The protocols at this layer perform three distinct functions:

- They define how to use the network to transmit a frame, which is the data unit passed across the physical connection.
- They exchange data between the computer and the physical network.
- They deliver data between two devices on the same network using the physical address.

The network access layer includes a large number of protocols. For instance, the network access layer includes all the variations of Ethernet protocols and other LAN standards. This layer also includes the popular WAN standards, such as the Point-toPoint Protocol (PPP) and Frame Relay.

The Internet Layer

The best known TCP/IP protocol at the internetwork layer is the Internet Protocol (IP), which provides the basic packet delivery service for all TCP/IP networks node addresses, the IP implements a system of logical host addresses called IP addresses. The IP addresses are used by the internetwork and higher layers to identify devices and to perform internetwork routing. IP is used by all protocols in the layers above and below it to deliver data, which means all TCP/IP data flows through IP when it is sent and received, regardless of its final destination.

The basic protocols used at the Internet Layer are:

- **I.P. (Internet Protocol):** It is a protocol used at the internet layer of TCP/IP model by which data is encapsulated and is sent from one computer to another on the Internet.
- **ARP (Address Resolution Protocol):** It is used to map the known I.P. addresses into Physical address.

- **RARP(Reverse Address Resolution Protocol):** It is used to map Physical address into I.P. address
- **I.C.M.P.(Internet Control Message Protocol):** It is used to send error & control Messages in the network
- **I.G.M.P. (Internet Group Management Protocol):** It is a protocol which is used to form multicast groups in a network to receive multicast messages.

The Transport Layer

The protocol layer just below the Application layer is the host-to-host layer (Transport layer). It is responsible for end-to-end data integrity. Transport Layer identifies the segments through Socket address (Combination of Port Number & I.P. address). The two most important protocols employed at this layer are the

- **Transmission Control Protocol (TCP):** TCP provides reliable, full-duplex connections and reliable service by ensuring that data is retransmitted when transmission results in an error (end-to-end error detection and correction). Also, TCP enables hosts to maintain multiple, simultaneous connections.
- **User Datagram Protocol (UDP):** When error correction is not required, UDP provides unreliable datagram service (connectionless) that enhances network throughput at the host-to-host transport layer. It's used primarily for broadcasting messages over a network.

The Application Layer

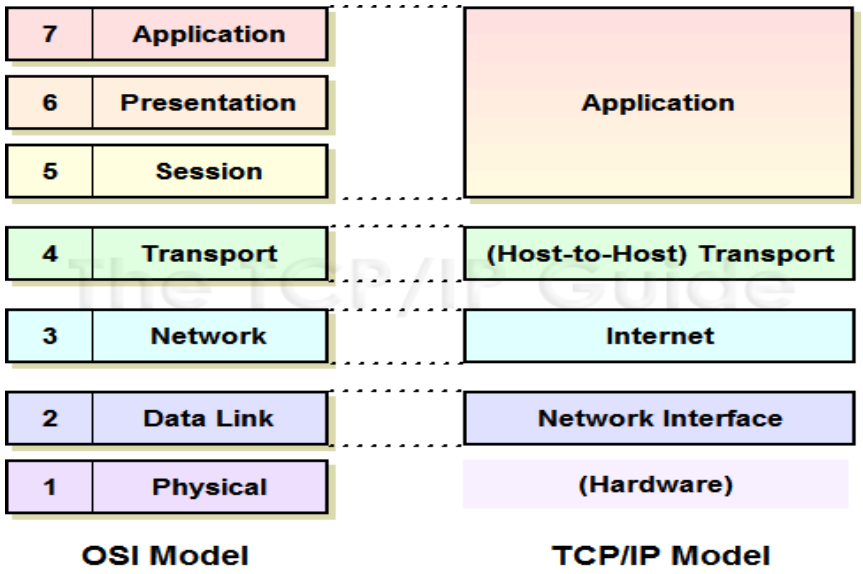
TCP/IP application layer protocols provide services to the application software running on a computer. The application Layer identifies the application running on the computer through Port Numbers. The various protocols that are used at the Application Layer are:

- **Telnet:** Terminal Emulation, Telnet is a program that runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. Port Number :23

- **FTP:** File Transfer Protocol, the protocol used for exchanging files over the Internet. FTP is most commonly used to download a file from a server using the Internet or to upload a file to a server. Port Number : 20(data port) ,21(control port)
- **HTTP:** Hyper Text Transfer Protocol is the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when we enter a URL in the browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. Port Number :80
- **NFS:** Network File System, a client/server application that allows all network users to access shared files stored on computers of different types. Users can manipulate shared files as if they were stored locally on the user's own hard disk. Port Number :2049
- **SMTP:** Simple Mail Transfer Protocol, a protocol for sending e-mail messages between servers. In addition, SMTP is generally used to send messages from a mail client to a mail server. Port Number :25
- **POP3:** Post Office Protocol, a protocol used to retrieve e-mail from a mail server. Most e-mail applications (sometimes called an e-mail client) use the POP, although some can use the newer IMAP (Internet Message Access Protocol)as a replacement for POP3 Port Number :110
- **TFTP:** Trivial File Transfer Protocol, a simple form of the File Transfer Protocol (FTP). TFTP provides no security features. It is often used by servers to boot diskless workstations, X-terminals, and routers. Port Number :69
- **DNS:** Domain Name System (or Service or Server), an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4. Port Number :53
- **DHCP:** Dynamic Host Configuration Protocol, a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. Port Number : 67(Server),68(Client)

- **BOOTP:** Bootstrap Protocol (BOOTP) is utilized by diskless workstations to gather configuration information from a network server. This enables the workstation to boot without requiring a hard or floppy disk drive. Port Number : 67(Server),68(Client)
- **SNMP:** Simple Network Management Protocol, a set of protocols for managing complex networks. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. Port Number :161

9.4 OSI vs TCP/IP Model



9.4.1 Differences between OSI and TCP / IP Reference Models

- OSI model is a generic model that is based upon functionalities of each layer. TCP/IP model is a protocol-oriented standard.
- OSI model distinguishes the three concepts, namely, services, interfaces, and protocols. TCP/IP does not have a clear distinction between these three.
- OSI model gives guidelines on how communication needs to be done, while TCP/IP protocols layout standards on which the Internet was developed. So, TCP/IP is a more practical model.
- In OSI, the model was developed first and then the protocols in each layer were developed. In the TCP/IP suite, the protocols were developed first and then the model was developed.
- The OSI has seven layers while the TCP/IP has four layers.

9.4.2 Similarities between OSI and TCP / IP Reference Models

- Both the reference models are based upon layered architecture.
- The layers in the models are compared with each other. The physical layer and the data link layer of the OSI model correspond to the link layer of the TCP/IP model. The network layers and the transport layers are the same in both the models. The session layer, the presentation layer and the application layer of the OSI model together form the application layer of the TCP/IP model.
- In both the models, protocols are defined in a layer-wise manner.
- In both models, data is divided into packets and each packet may take the individual route from the source to the destination.