

# Data Communication & Computer Networking



Fourth Semester

COMPUTER SCIENCE & ENGG.

**Prepared By: Prasanta Kumar Satapathy**  
(Sr. Lecturer)

# **Data Communication & Computer Network**

## **Contents**

<b>Sl. No.</b>	<b>Topic</b>	<b>Expected Marks</b>
<b>1.</b>	<b>NETWORK&amp; PROTOCOL</b>	<b>15</b>
<b>2.</b>	<b>DATA TRANSMISSION &amp; MEDIA</b>	<b>15</b>
<b>3.</b>	<b>DATA ENCODING</b>	<b>15</b>
<b>4.</b>	<b>DATA COMMUNICATION &amp; DATA LINK CONTROL</b>	<b>20</b>
<b>5.</b>	<b>SWITCHING &amp; ROUTING</b>	<b>20</b>
<b>6.</b>	<b>LAN TECHNOLOGY</b>	<b>15</b>
<b>7.</b>	<b>TCP/IP</b>	<b>10</b>
<b>TOTAL</b>		<b>110</b>

# **CHAPTER 1-**

## **(NETWORK & PROTOCOL)**

### **DATA**

Data is the raw fact or message in the form of text, numbers, alpha numerals, physical quantities (temperature, pressure, voltage, etc), audio file, video file, image and so on.

### **DATA COMMUNICATION**

Data communication is the process of exchange or transfer of data from one communicating device to another.

### **ELEMENTS OF DATA COMMUNICATION**



#### **1-MESSAGE**

Message is the data to be communicated. It may be text, Image , audio, video, or combination of these.

#### **2-SENDER**

Sender is a device which sends data. It can be a computer, workstation, telephone, etc.

### **3-RECIVER**

The receiver is another device that can receive the messages. It can be a computer, mobile phone , etc.

### **4-TRANSMISSION MEDIUM**

A transmission medium is the physical path by which the message travels from sender to the receiver.

It may be a co-axial cable, twisted pair cable, fibre-optic cable or it can be a wireless medium.

## **PROTOCOL**

A protocol is a set of rules that govern data communication. Without a protocol two devices may be connected but cannot communicate with each other.

It represents an agreement between the communicating devices.

## **MODE OF DATA COMMUNICATION**

It is the direction of data flow from sender to reciver or vice versa. There are 3 different modes of data communication.

### **1-SIMPLEX**

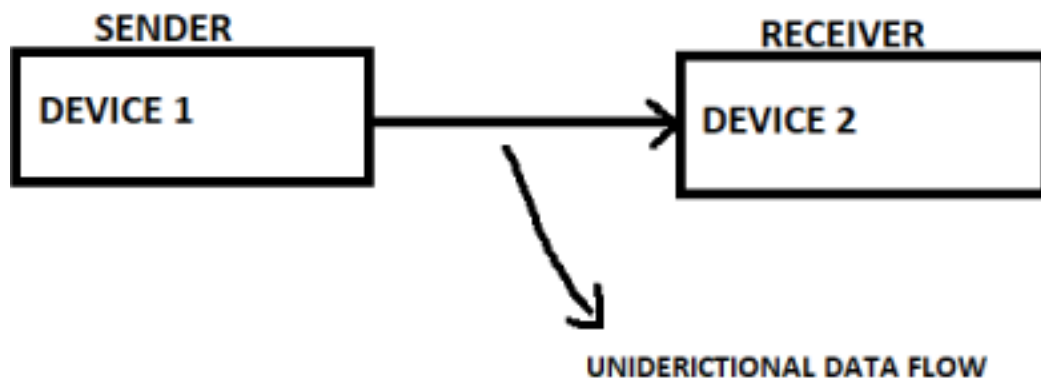
### **2-HALF DUPLEX**

### **3-FULL DUPLEX**

### **1-SIMPLEX MODE OF DATA COMMUNICATION**

In simplex mode the communication is unidirectional.

Only one of the 2 devices on a link can transmit and the other can only receive.



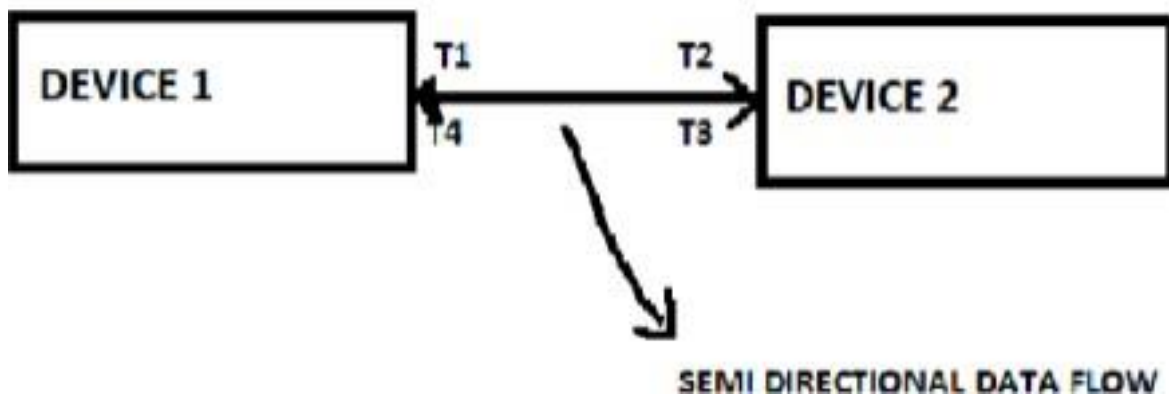
### EXAMPLE-

- (i) A person listening to radio. Here radio is sender and person is receiver.
- (ii) Data flow from keyboard to CPU.

### 2-HALF DUPLEX MODE

In Half duplex mode each station /device has the ability to both transmit and receive but not at the same time.

In this case when one device is sending , the other can only receive and vice versa.

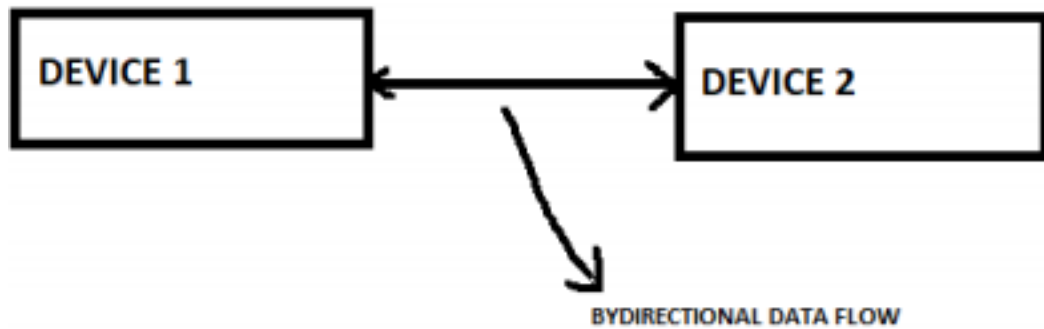


### EXAMPLE

Walky-talky, client-server data exchange, google assistant, etc.

### 3-FULL DUPLEX MODE

In full duplex mode both devices can transmit and receive simultaneously.



## **NETWORK —**

A network is a set of devices or nodes connected by communication links.

A node can be a computer, printer or any other device capable of transmitting and receiving data to or from other nodes on the network with the help of protocol.

### **TYPES OF NETWORKS**

A computer network is mainly of 3 types —

1. LAN (local area network)
2. MAN (metropolitan area network)
3. WAN (wide area network)

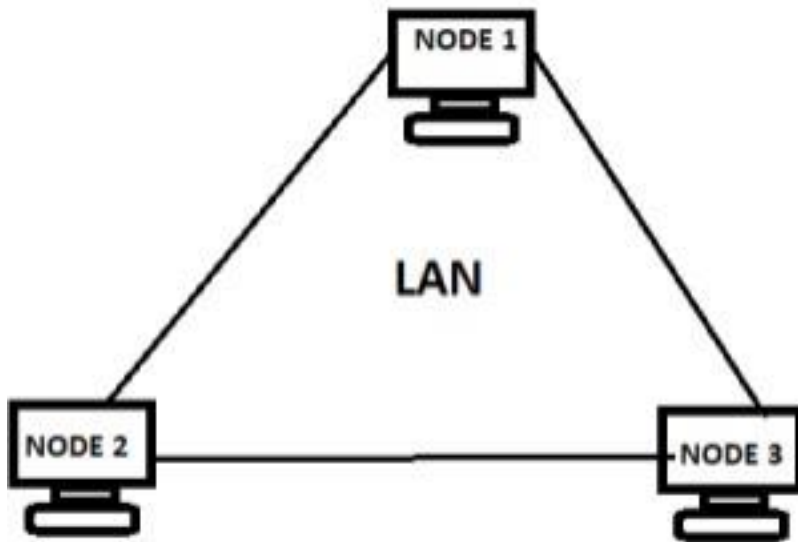
### **LAN:**

LAN is a group of computers connected to each other in a small area such as building, office, etc.

LAN is used for connecting 2 or more PCs through a communication medium such as co-axial cable, twisted pair cable, fibre-optic cable, etc.

It is less costly.

The data is transfer at an extremely faster rate in local area network.



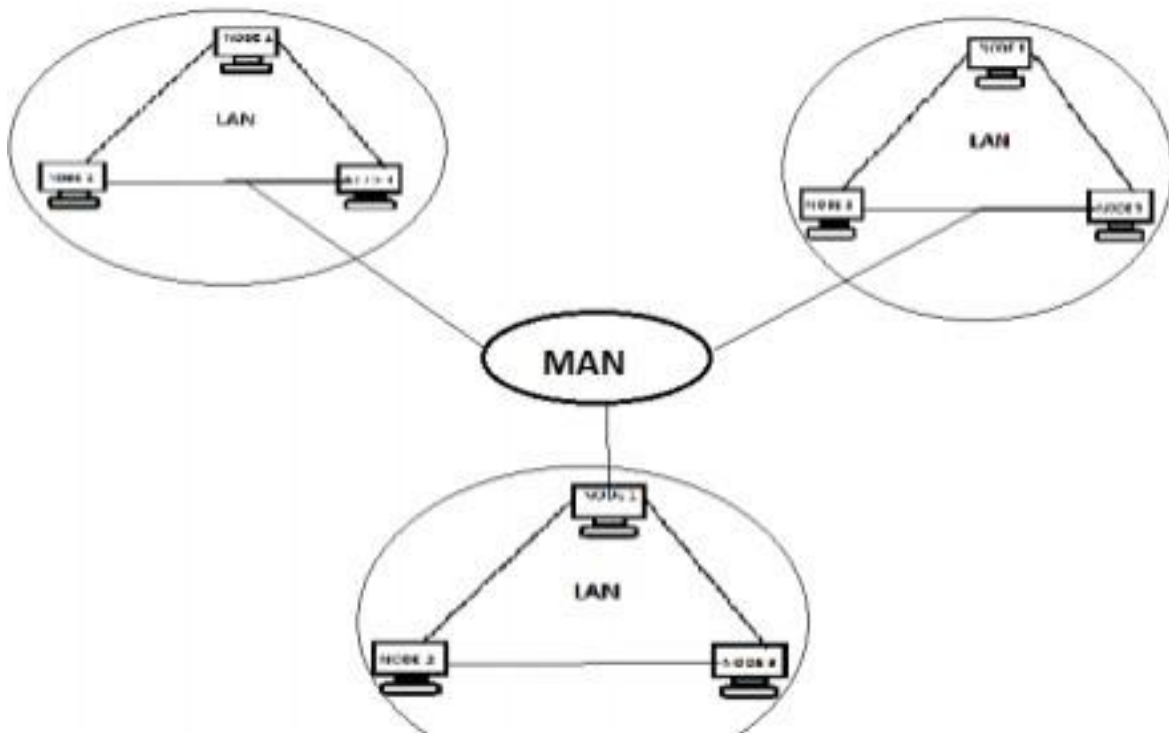
### MAN :

A metropolitan area network is a network that covers a larger geographic area such as a city by interconnecting different LANs to form a larger network.

Government agency uses MAN to connect to cities and industries.

In MAN, various LANs are connected to each other through a telephone exchange line.

It has a high range than LAN.



### **USES OF MAN:**

- MAN is used in communication between banks in a city.
- It can be used in educational institutes within a city.
- It can be used for communicating in military fields.
- It is also used in airline reservation.

### **WAN :**

A wide area network is a network that extends over a large geographical area such as states, countries, continents over the whole world.

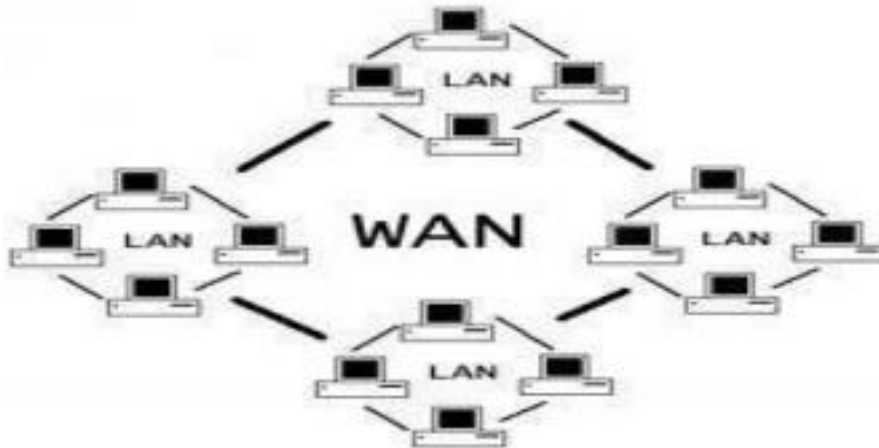
A WAN is a wide bigger network than LAN and MAN.

A WAN is not limited to a single location but it spans over a large area through telephone line, fibre optic cable or satellite links.

The internet is one of the largest WAN in the world.



A WAN is widely used in the field of business, government and education.



### **EXAMPLES OF WAN-**

- A 4G network is widely used across a region or country.
- A telecom company providing internet services to the customer in 100 of cities.

## **Protocol & Architecture, Standards, OSI, TCP/IP**

### **Protocol**

Protocol is a set of rules that governs all aspects of data communication between a number of system.

The elements of protocol are :-

#### **1. Syntax**

It refers to the structure or format of data that should be maintained.

## 2. Semantics

It refers to the meaning of each section of bits.

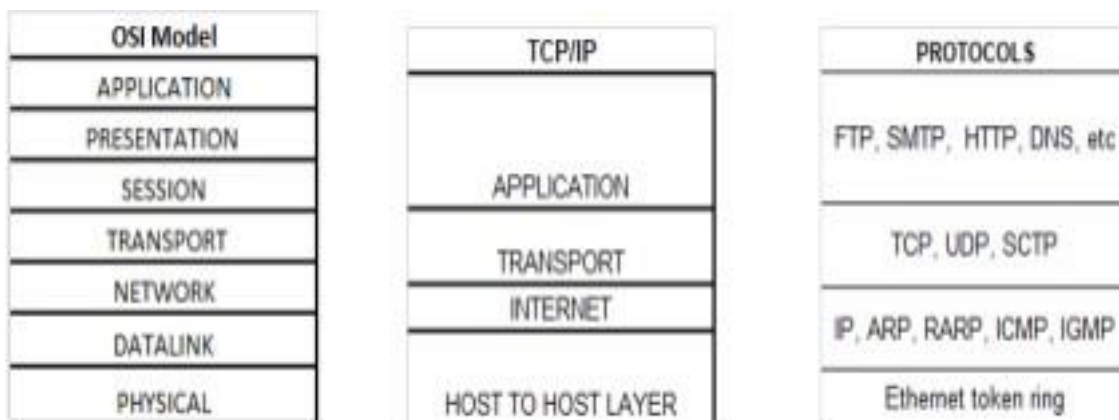
## 3. Timing

It refers to the time and speed of transmitting of data.

- Protocol architecture that are used :-

1- OSI reference model.

2- TCP/IP.



# Trick to remember OSI model — please do not take sales person advice.

### **STANDARD:-**

A standard is an agreed upon way of doing something or measuring something.

Standard are essential in creating and maintaining an open and competitive market for equipment manufacturers and its guarantying national and international inter-operability of data and telecommunication technology and process.

Standard provides guidelines to manufacturer, vendors, government agency and other service providers to ensure the kind of inter-connectivity necessary in communication.

## **STANDARDs ORGANISATION –**

Standards are developed through standards creation committee, forum and government agency.

### **Standards creation committee :**

ISD – International standard organisation.

ANSI – American national standards institute.

IEEE – Institute of electrical and electronics engineers. EIA – Electronics industries association.

### **FORUM:-**

The facilitate standardisation process many special interest groups have developed forums made up of representatives from interested corporation.

### **GOVERNMENT REGULATORY AGENCY :-**

All communication technology is subject to regulation by the government agencies.

## **OSI reference Model :**

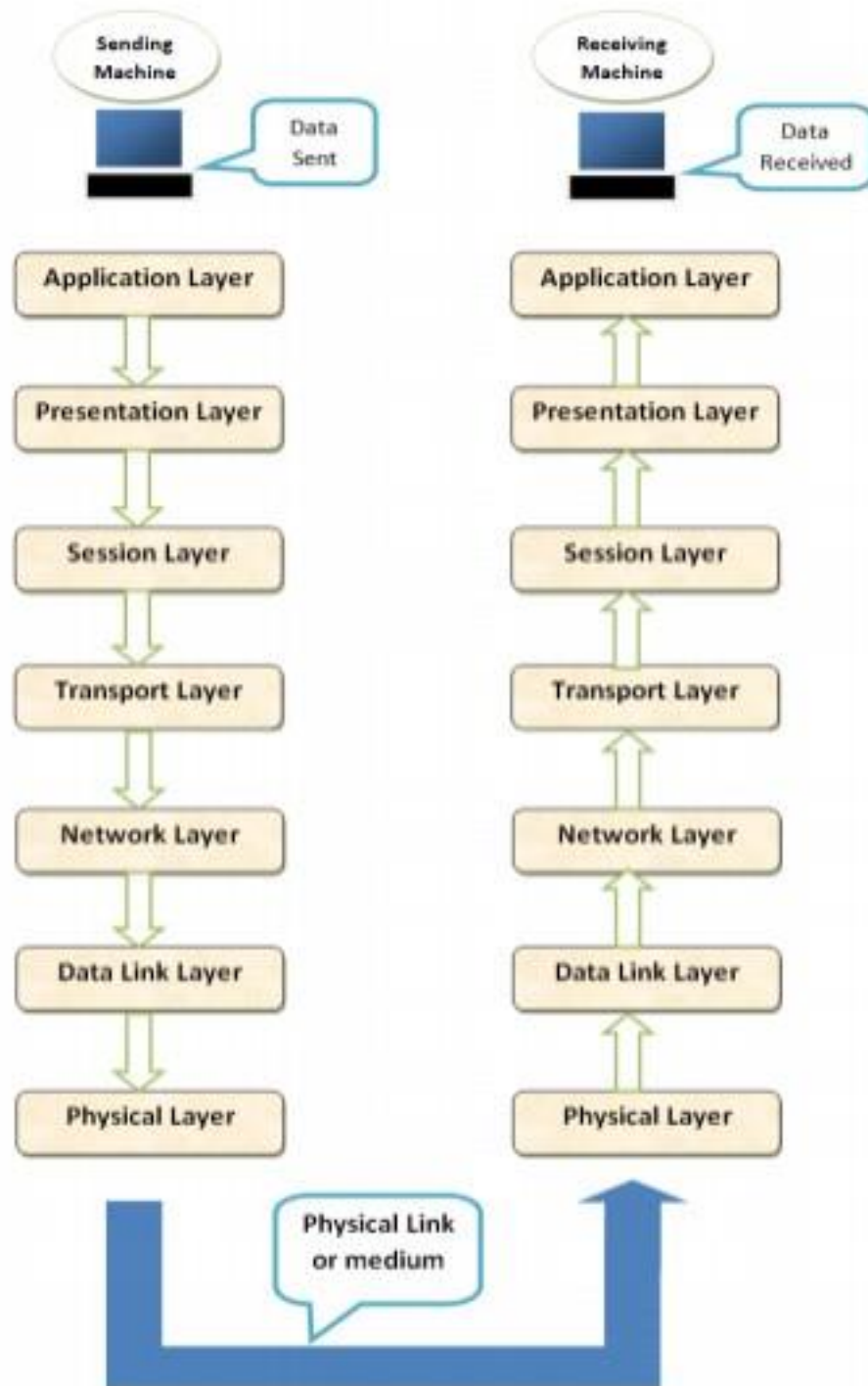
The International Organization for Standardization (ISO) developed the Open

Systems Interconnection (OSI) reference model in 1977 and finally 1983.

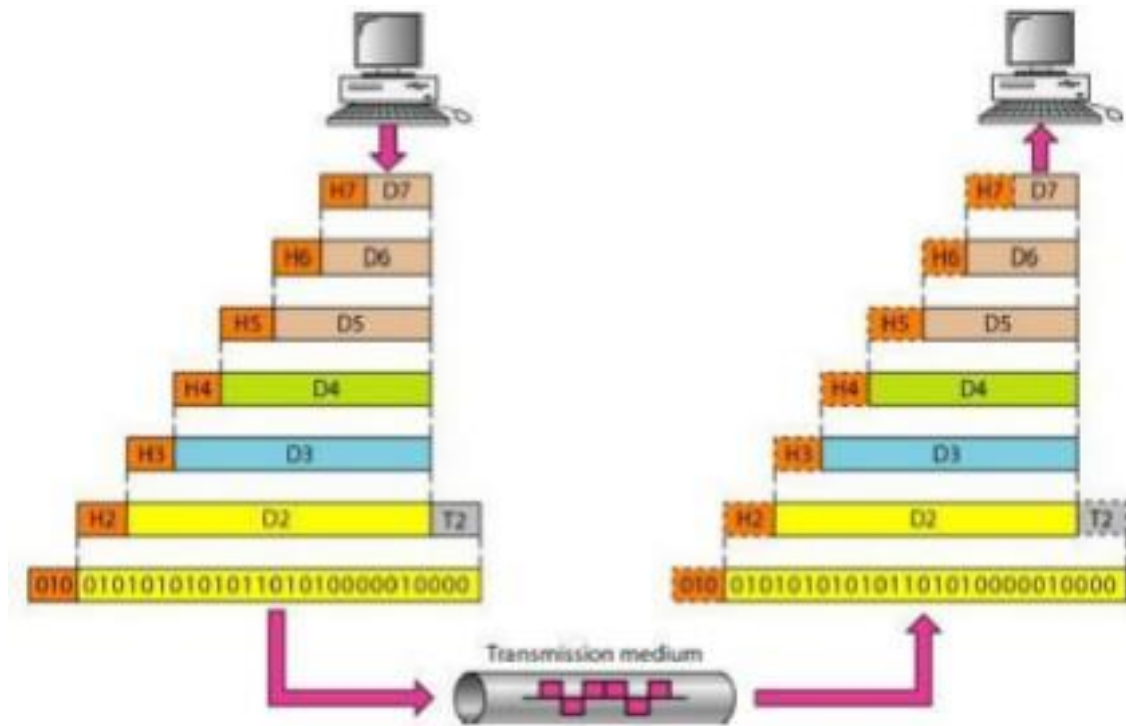
An open system has a set of protocols that allows any 2 different systems to communicate with each other.

OSI model is used to design and understand a network architecture that is flexible, robust and interpretable.

It consist of 7 layer each of which is responsible for moving information across a network.



(OSI Model)



(data exchange using OSI model)

(i) This gives an overall view of data exchange using OSI layers. (ii) D7 means the data unit at layer 7. D6 means the data unit at layer 6 and so on.

(iii) The process starts at layer 7 and moves in descending order. At each layer a header (H) is added to the data unit.

(iv) The trailer is added only at layer 2. When data unit passes through physical layer.

(v) It is changed into electromagnetic signal and transmitted along a physical link.

(vi) After reaching its destination the signal passes into layer 1 and transmitted back into digital form.

(vii) The data unit then moves upward through OSI layer.

(viii) The header and trailer attached to the data unit are removed at their corresponding layer.

(ix) When it reaches layer 7 the message is again in a form appropriate to the application and is available to the receiver.

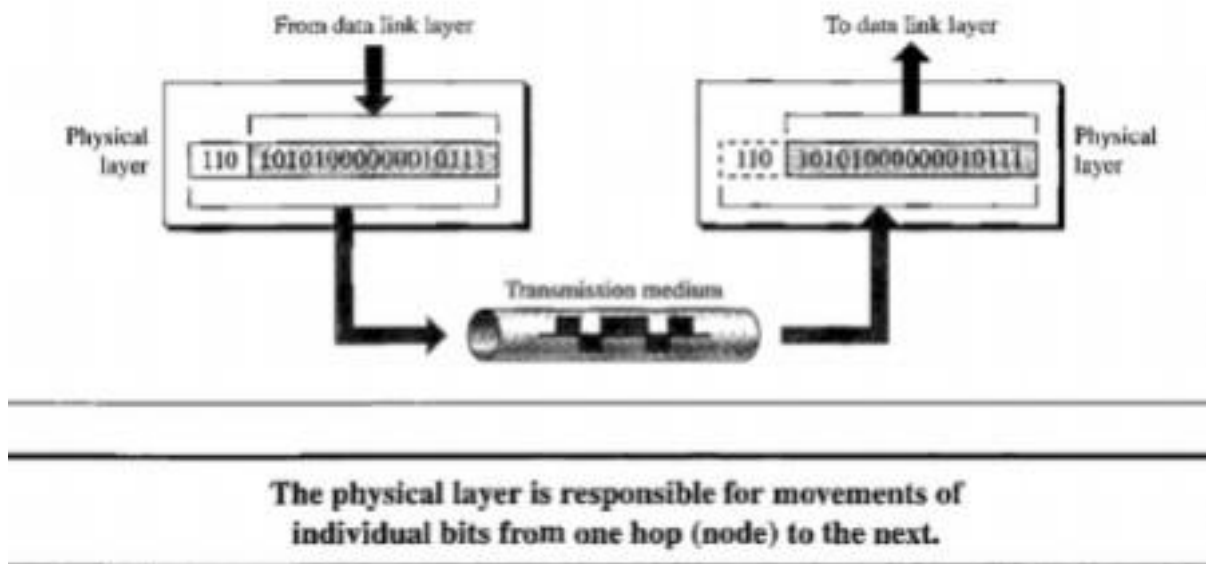
## LAYERS IN OSI MODEL

### PHYSICAL LAYER

The physical layer is responsible for movement of individual bits from 1 node to the next.

It coordinates the functions required to carry a bit stream over a

physical medium.



Other responsibility of physical layer are –

1. Physical characteristics of interface or medium.
2. Representation of bits.
3. Data rate.
4. Synchronisation of bits.

5. Line configuration.
6. Physical topology.
7. Transmission mode.

## **DATALINK LAYER –**

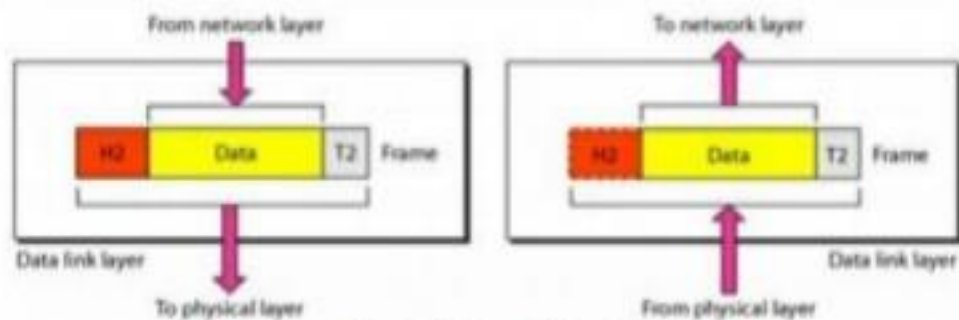
The data link layer is responsible for transmitting group of bits between the adjacent nodes.

The group of bits is called frame.

The network layer passes the data to the datalink layer and here the datalink layer adds the header and trailer information to the data.

The header contains the physical address or MAC address and the other control information of the adjacent node in the network.

It makes the physical layer appear error free to the upper layer.



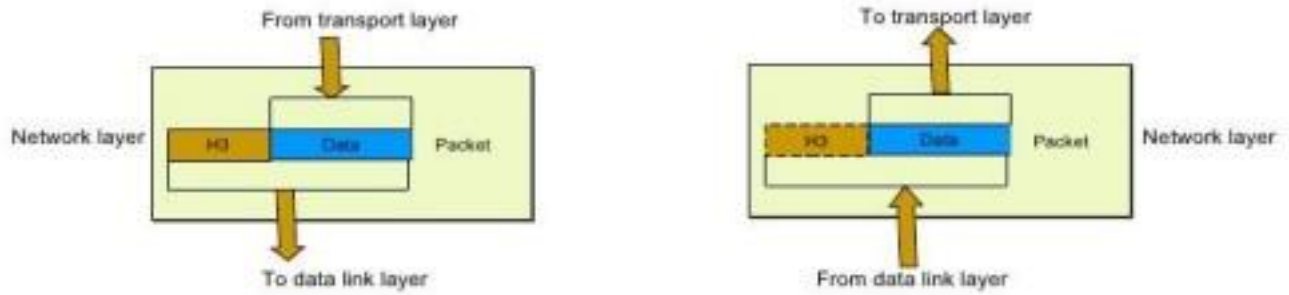
**Fig. Data Link Layer**

The other responsibility of datalink layer include:-

1. Physical addressing – the datalink layer adds a header to the frame defining the address of sender and receivers.
2. Flow control – the datalink layer impose flow control mechanism to avoid over whelming the receiver.
3. Error control – error control is achieved by adding a trailer to the end of the frame. It acts as a mechanism to detect and retransmit damaged or lost



# Network Layer (Source to Destination)



- The network layer is responsible for the delivery of individual packets from the source host to the destination host.
- Concerned:
  - Logical addressing (IP Address)
  - Routing (Source to destination transmission between networks)

8

It has 2 main features :-

1. Logical addressing
2. Routing

## LOGICAL ADDRESSING –

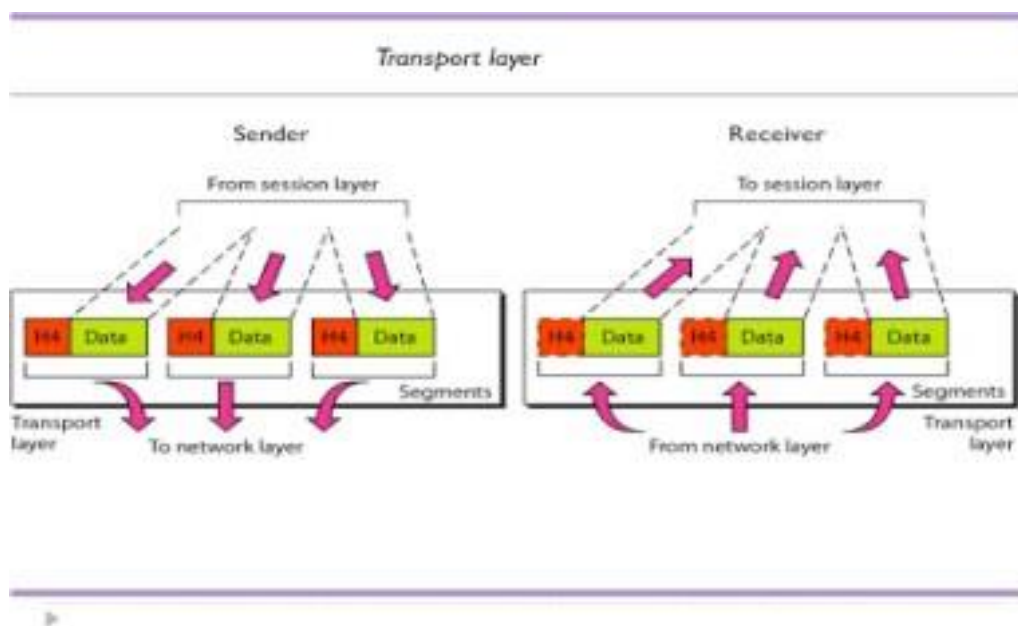
1. The network layer adds a header to the packet defining the logical address of sender and receivers.

## ROUTING –

When independent networks are connected to create a large network the connecting devices are called routers which routes or switches the packets to their final destinations.

## TRANSPORT LAYER:-

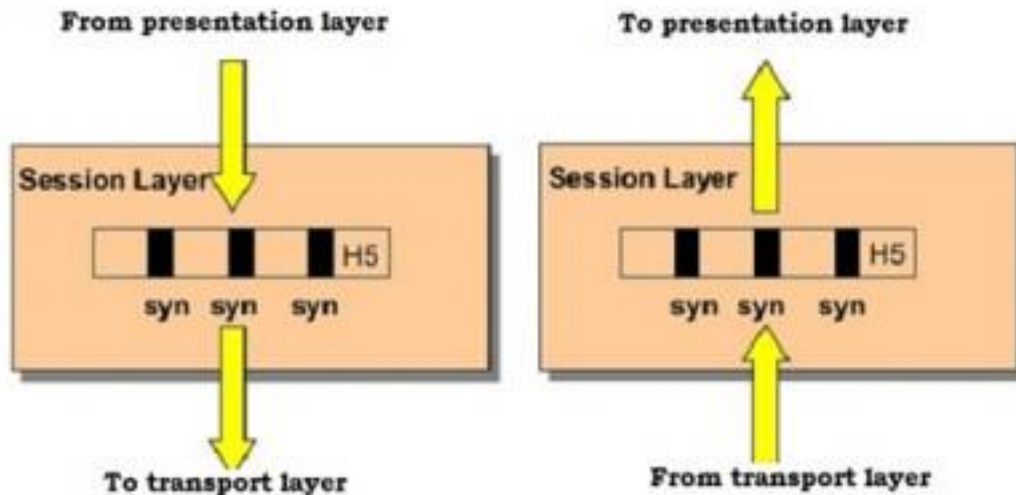
- Transport layer is responsible for the process to process delivery of an entire message.
- A process is an application program running on a host.
- The transport layer ensures that the whole message arrives in order. ➤ It provides error control & flow control mechanism at source to destination level.



## SESSION LAYER :-

- A session layer is the network dialogue controller.

- It establishes, maintains & synchronises the introduction among communicating systems.



### **Dialogue control**

The session layer allows 2 system to enter into a dialog that means it allows the communication between 2 processes to take place either in half duplex or in full duplex mode.

### **Synchronisation**

The session layer allows the processes to add synchronisation points to a string of data which helps in resending the data in between the synchronous point at the time of error.

### **PRESENTATION LAYER :-**

The presentation layer is responsible for translation , compression and encryption.

It is also concerned with the syntax and semantics of the information exchanged between 2 systems.



### **APPLICATION LAYER :-**

It is responsible for providing services to the user. The figure shows the application like ( directory services, FTAM(file transfer access management) and x.400(message handling service)



).

Using network virtual terminal in application layer a user can login to remote host.

### **Advantages-**

- Easier application development.
- Layering breaks the computer task into sub tasks. Each layer handles a specific subset of tasks.
- Layered architecture simplified the network design.
- The network layer follows a set of rule for protocol.

### **TCP/IP :-**

- TCP/IP protocol suite is the internet model for data communication.
- TCP/IP protocol provides reliable data transfer data between packets between 2 stations.

➤ ===O===

## **Short Questions with answer**

### **Q1. What is computer network?**

- (i) A network is a set of devices or nodes connected by communication links.
- (ii) A node can be a computer, printer or any other device capable of transmitting and receiving data to or from other nodes on the network with the help of protocol.

### **Q2. What is data communication?**

Data communication is the process of exchange or transfer of data from one communicating device to another.

### **Q3. Define TCP/IP**

- (i) TCP/IP protocol suite is the internet model for data communication.
- (ii) TCP/IP protocol provides reliable data transfer or data packets between 2 stations.

## **Long Questions**

**Q1. Explain 7 layers of OSI model.**

**Q2. Define data communication. Explain different types of data communication.**

## CHAPTER 2

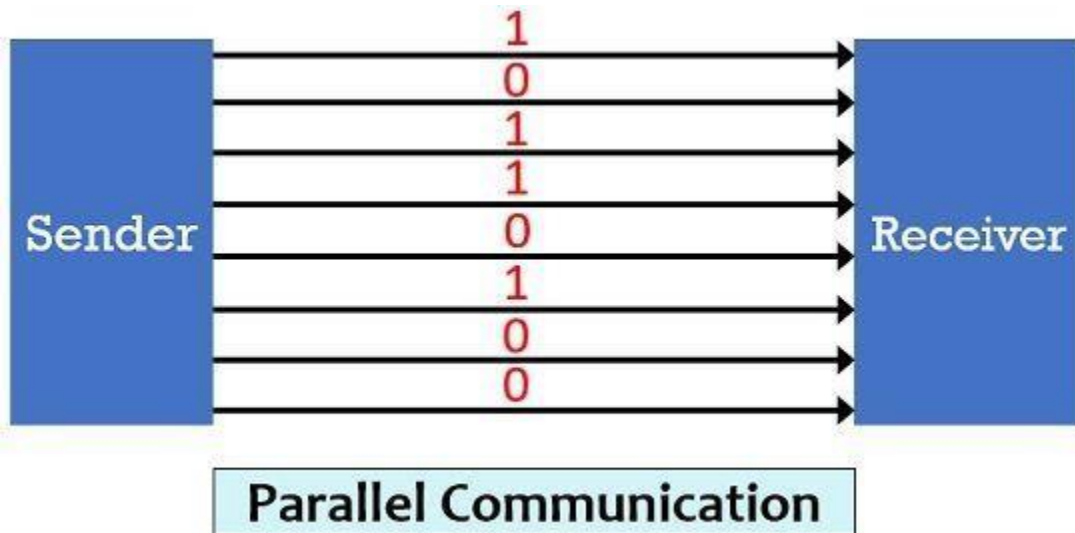
### DATA TRANSMISSION & MEDIA

#### DATA TRANSMISSION:-

Data transmission is the process by which data can be transmitted from one communicating device to another.

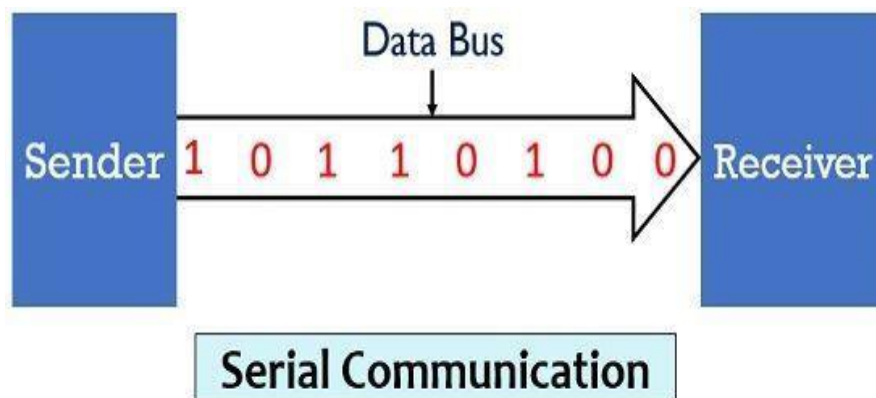
Data transmission occurs in 2 different modes –

##### 1. Parallel



Circuit Globe

##### 2. Serial



Circuit Globe



PARALLEL TRANSMISSION	SERIAL TRANSMISSION
n links required	only one links required
faster in speed	slower in speed
more expensive	less expensive
short distance communication	long distance communication

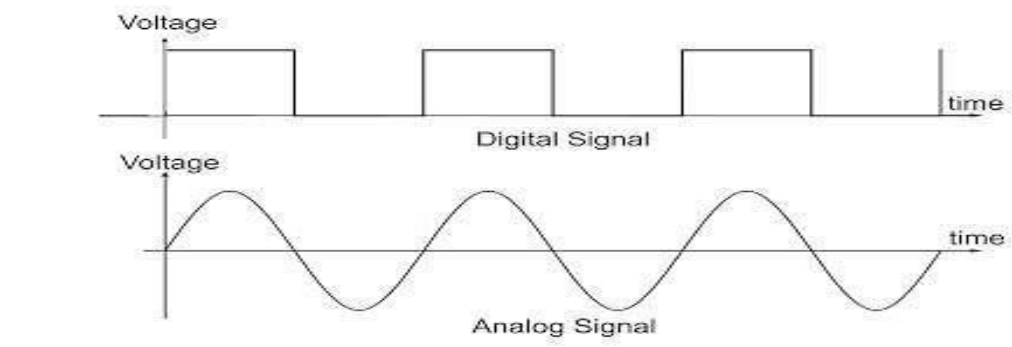
#Serial transmission is of 2 types-

1. Synchronous
2. Asynchronous

## ANALOG AND DIGITAL DATA TRANSMISSION:-

### Analog data transmission –

1. Analog data transmission is a transmission method of sending information using continuous signal which varies in amplitude, phase or some of the property of that information .
2. Analog transmission occurs in twisted pair cable, fibre optic cable, co-axial cable & also in space.



## **Digital data transmission –**

1. Digital transmission transmits data directly.
2. The data/message are represented by a sequence of pulses via a line code.
3. They are presented using a digital modulation method.
4. The computer are the originators of digital data.

## **TRANSMISSION IMPAIRMENTS, CHANNEL CAPACITY**

### **Transmission impairments-**

In communication system, the signals transmitted in a transmission media tends to deteriorate the quality of original signal.

This imperfection causes signal impairments that is the received signal is not same as the signal that has been sent.

The cause of impairment are-

1. ATTENUATION
2. DISTORTION
3. NOISE

### **ATTENUATION-**

1. It means loss of energy. The strength of the signal decreases with increasing distance which cause loss of energy in overcoming the resistance of the medium.
2. This is known as attenuation for attenuated signal. Amplifiers are used to amplify those signals.

## **DISTORTION-**

1. It means the change in the shape of the signal.
2. This is generally seen in composite signals with different frequency.
3. Each frequency components has its own propagation speed.
4. Every frequency component arrived at different time which leads to distortion.

## **NOISE-**

1. Noise is unwanted electrical or electromagnetic energy that degrades the quality of signals and data.
2. Noise occurs in both digital and analog signals.

## **Channel capacity-**

The maximum rate at which data can be transmitted over a given communication path or channel under given condition is refer to as channel capacity.

## **Data rate-**

1. The rate at which data can be transmitted is known as data rate.
2. It is represented in bits per second (BPS).

## **BANDWIDTH-**

The bandwidth of a transmitted signal is the difference between highest to lowest frequency.

It is expressed in hertz(Hz).

## Error rate-

The rate at which error occurs where an error is a receiving of 1 when a 0 is transmitted or vice versa.

## Signal rate-

1. It is the number of signal element send in one second.
2. A signal element is a shortest unit of the digital signal.
3. The unit of signal rate is baud. It is also known as baud rate.

Where  $n$  = data rate.

$S$  = no of signal element per second.

$C$  = case factor.

$R$  = ratio of number of data elements/number of signal elements.

**Example** - A signal is carrying data in which one data element is encoded as one signal element. If signal rate is 50 kilo Baud , what is the average value of bit rate if  $C$  is  $\frac{1}{2}$ .

Answer-

$$S = 50$$

$$C = \frac{1}{2}$$

$$R = 1$$

Applying formula  $s = c * n * 1/r$

$$\Rightarrow 50 * \frac{1}{2} * n * 1/1$$

$$\Rightarrow 50000 = n/2$$

$$\Rightarrow 50000 * 2$$

⇒ 100000

⇒  $N = 100 \text{ kbps}$ .

### Formula to calculate data rate-

There are 2 formula to calculate data rate for -

1. Noiseless channel
2. Noise channel

### Noiseless channel – ( Nyquist data rate ) -

$$\text{Bit rate} = 2 * B * \log_2 L$$

Where  $B$  = Bandwidth.

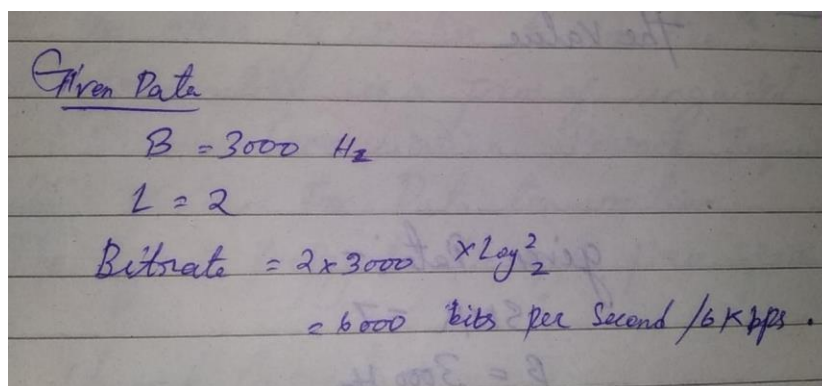
$L$  = Labels of the signal.

**Example-** Consider a noiseless channel with a bandwidth 3000 Hz, transmitting a signal with 2 signal labels what is the maximum bit rate.

Given Data-

$$B = 3000 \text{ Hz}$$

$$L = 2$$



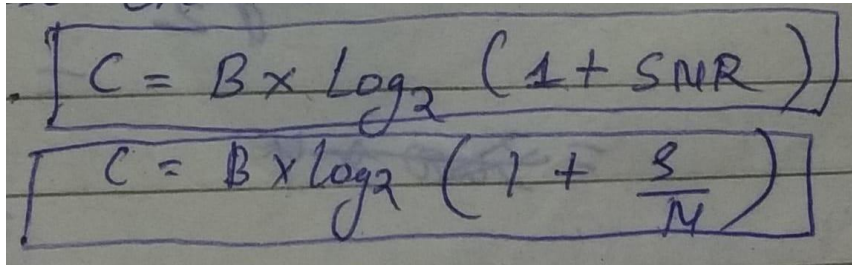
Handwritten calculation on lined paper:

Given Data

$$B = 3000 \text{ Hz}$$
$$L = 2$$
$$\text{Bitrate} = 2 \times 3000 \times \log_2 2$$
$$= 6000 \text{ bits per Second / 6 Kbps.}$$

## Noise channel - ( shannon's capacity ) –

It is used to determine the theoretical highest data rate of a noise channel.



The image shows two versions of the Shannon capacity formula written in blue ink on lined paper. The top formula is  $C = B \times \log_2 (1 + \text{SNR})$  and the bottom formula is  $C = B \times \log_2 (1 + \frac{S}{N})$ . Both formulas are enclosed in hand-drawn rectangular boxes.

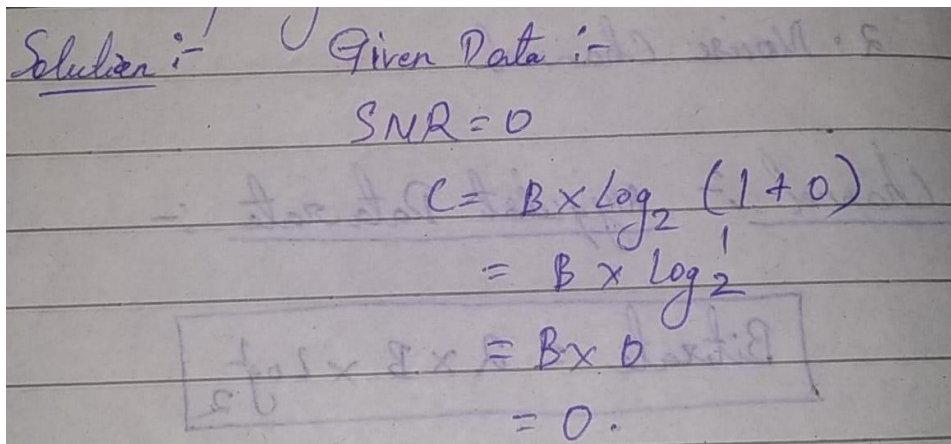
SNR = Signal to noise ratio.

Where **C** = capacity of the channel.

**B** = Bandwidth of the channel.

### Example –

Consider an extremely noise channel in which the value of the signal to noise ratio is almost '0'. Calculate the channel capacity.



The image shows a handwritten solution in blue ink on lined paper. It starts with 'Solution :-' followed by 'Given Data :-' and 'SNR = 0'. Then, the formula  $C = B \times \log_2 (1 + 0)$  is written, followed by  $= B \times \log_2 1$ . A final boxed calculation shows  $\log_2 1 = 0$ , leading to  $C = B \times 0 = 0$ .

This means the capacity of this channel is 0 regardless of the bandwidth.

In other words we cannot receive any data through this channel.

## ***TRANSMISSION MEDIA :-***

In data transmission system, it is the path between the sender & receiver.

The transmission media can be classified into 2 categories –

- 1. Guided media (wired)**
- 2. Unguided media (wireless)**

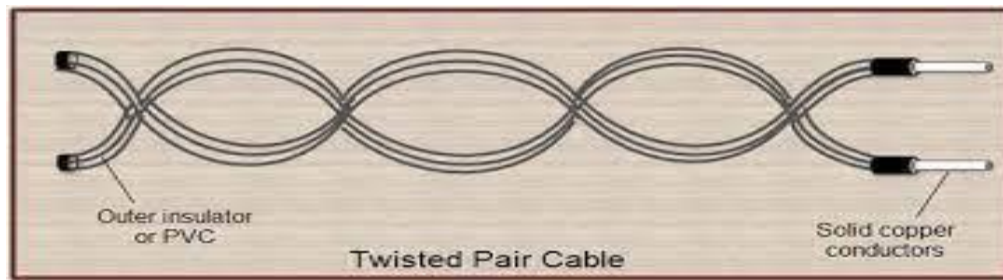
## **GUIDED MEDIA-**

In case of guided media , electromagnetic signals are guided along a solid path.

It is of 3 types-

- 1. Twisted pair cable**
- 2. Co-axial cable**
- 3. Fibre optic cable**

## **Twisted pair cable-**



- Twisted pair cable Consist of two insulated copper conductor twisted over one another.
- Wires in a twisted pair cable had Thickness 0.016 To 0.036 inches.
- Here One of The Wires is used to to carry signal to the receiver and the other is used as a ground reference.
- The receiver receives the difference between the two signals.
- In addition to the signal sent in one of the wires, noise & crosstalk may affect both the wires and create unwanted signals.
- The receiver operates only on the difference between the unwanted signals.
- This means if 2 wires are affected equally then difference is '0' & the receiver receives the original signal.
- If the 2 wire are parallel, the effect of unwanted signals will not be same in both wires.
- By twisting the pair of cable, balance is maintained.

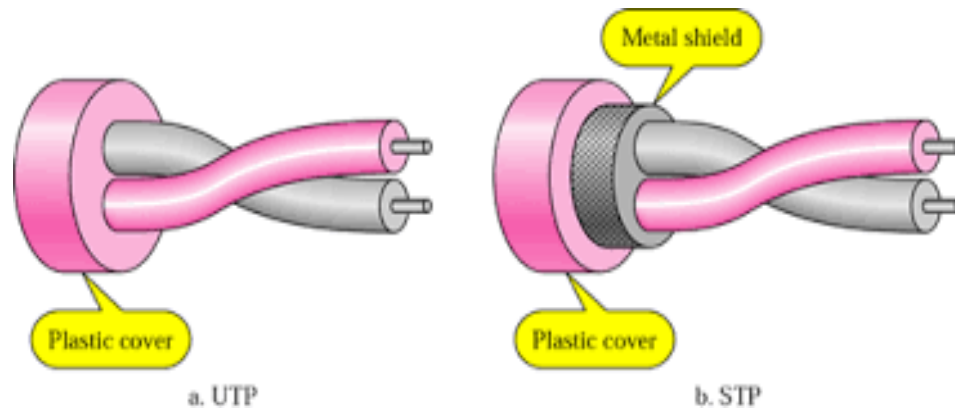
It is of 2 types:-

1. **Unshielded twisted pair cable (UTP)**
2. **Shielded twisted pair cable (STP)**

**UTP-**



- It is the ordinary telephone wire.
- It is cheap, flexible and easy to install.
- It suffers from external electromagnetic interference.



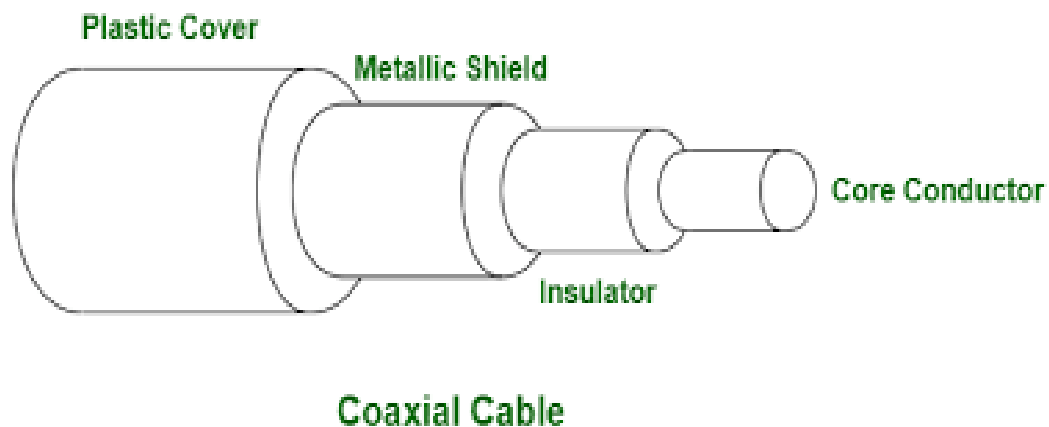
## STP-

- STP is developed by IBM for its use.
- STP cable has a metal foil covering the pair of insulated wires.
- The metallic wiring prevents the penetration of electromagnetic signal into it.
- It eliminates cross talk.

## Application of twisted pair cable-

- It is used in telephone line.
- It is used for digital signaling
- It is used in private branch exchange system.

## Co-axial cable-



- Coaxial have 2 conductors-
  1. Inner conductor
  2. Outer conductor
- It operates over a wide range of frequency.
- It consist of hollow outer cylindrical conductor, inner conductor is placed by a solid dielectric material.
- A single co-axial cable has a diameter from 0.4 to 1 inch.
- The outer conductor is also enclosed in an insulating sheet and the whole cable is protected by plastic cover.

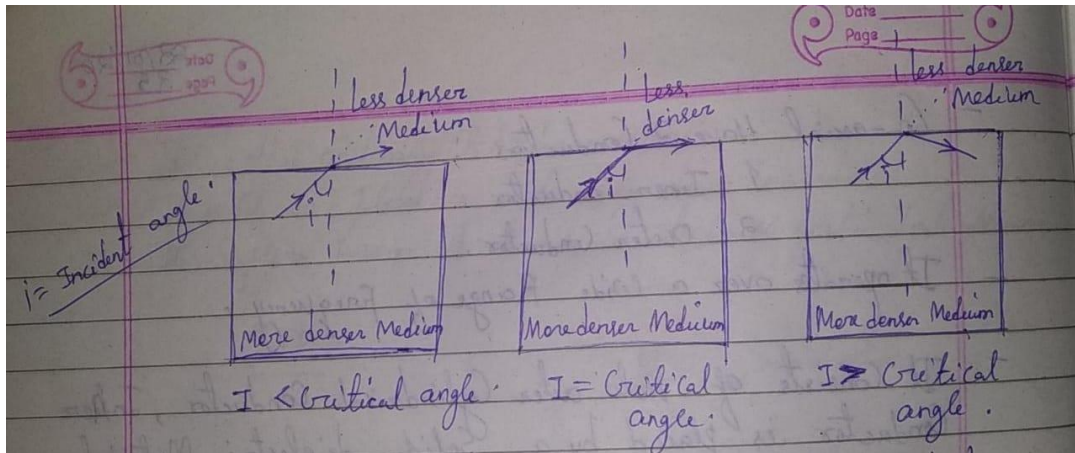
### Application-

- Used in TV cable network
- Used in Ethernet LAN
- Used in high speed computer data busses

- Used as higher frequency & supports high data rate

## FIBRE OPTIC CABLE-

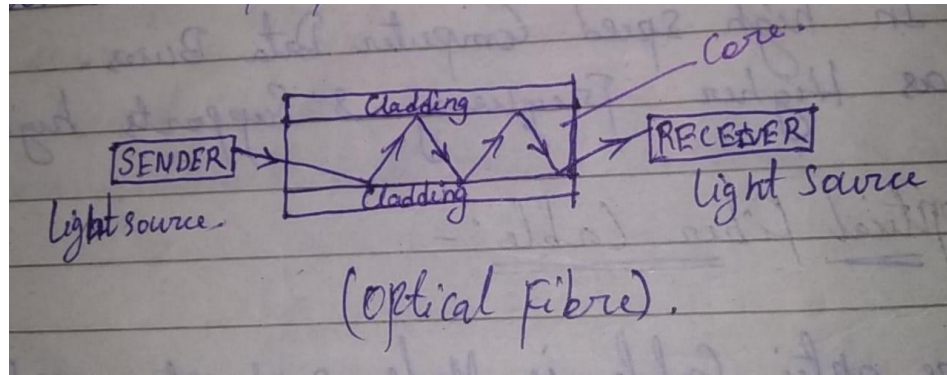
1. A fibre optic cable is made up of glass or plastic and transmit signal in the form of light.
2. Light travels in straight line when it moves along a single uniform substance, if a ray of light travelling through one substance, suddenly enters into another substance then the ray changes its direction.



In the above figure , if the angle of incidence is less than the critical angle then the light ray refracts and moves closer to the surface.

If the angle of incidence  $i$  is equal to the critical angle, then the light bends along the surface.

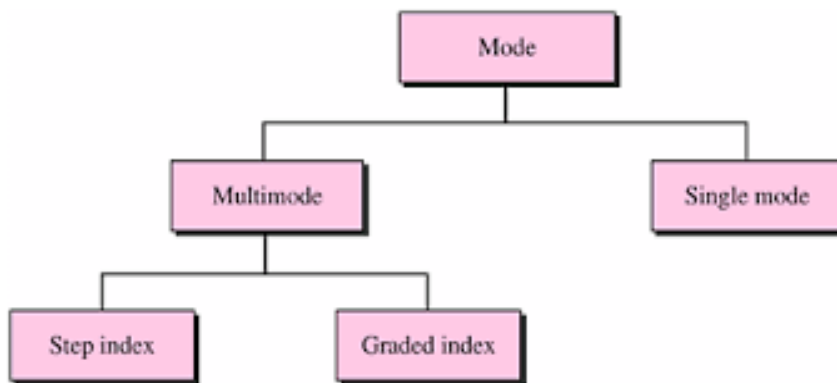
If the angle of incidence is greater than the critical angle then the ray **R** effects and moves closer to the denser substances.



A glass or plastic core is surrounded by cladding means less dense glass or plastic.

The difference in density of the 2 materials must be such that a ray of light moving through the core is reflected at the cladding instead of refracted into it.

## PROPAGATION MODES-



### Multimode propagation-

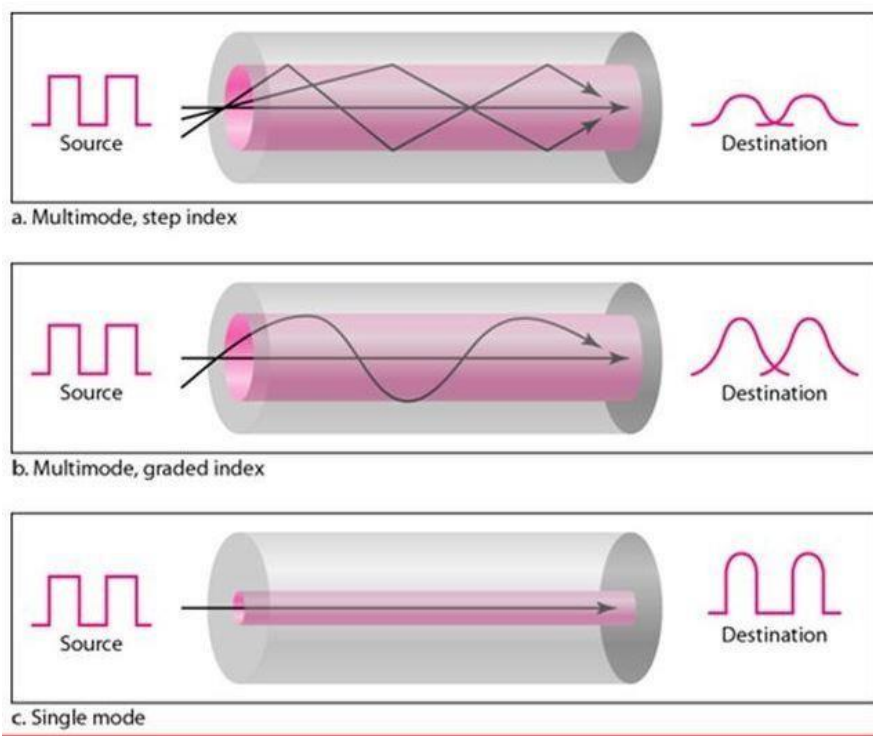
Multimode is so named because multiple beams of light move through the core in different paths.

## Multimode step index-

- In this mode the density of the core remains constant from the centre to edges.
- A beam of light moves through the constant density in a straight line until it reaches the interference of core and cladding.
- The term step index refers to the sudden change of angle at the interface.
- It may contribute to distortion.

## Multimode graded index-

- This type of fibre is of varying density.
- Density is high at the centre of the core & decreases gradually towards the edge so there is a change in the signal.
- It decreases the distortion of the signal through the cable.



## **Single mode-**

- It uses step index fibre and highly focused source of light that limits beams to small range of angle all close to horizontal.
- The decrease in density result in a critical angle that is closed enough to  $90^\circ$  to make the propagation of beams almost horizontal.
- All beams arrive at the destination together.

## **Application-**

- Optical fibre provides backbone structure.
- LAN also uses fibre optic cables.
- Some cable TV company also uses this.

## **Advantages-**

- Higher data rate and bandwidth.
- Immune to electromagnetic interference.
- Less signal attenuation
- Light weight

## **Disadvantage-**

- Installation and maintenance is difficult.
- It is expensive.
- It unidirectional in nature.

## **UNGUIDED MEDIA-**

1. It transmits electromagnetic waves without using a physical conductor.
2. This type of communication refers to as wireless communication.
3. Signals are normally broadcast through free space and thus are available to anyone who has a device capable of transmitting and receiving it.

### **Different types of wireless communication are as follows-**

1. Satellite communication.
2. Infrared communication.
3. Broadcast radio.
4. Micro wave communication.
5. Wi-fi communication.

### **Satellite communication-**

1. Satellite communication allows user to stay connected almost anywhere in the earth.
2. When a signal is received by a satellite it amplifies the signal & forwards to the receiver antenna which is located on the surface of earth.

### **Infrared communication-**

1. IR wireless communication communicates information to a device or a system through IR radiation.
2. It is used for security control, TV remote control & short-range communication.

3. In electromagnetic spectrum, IR radiation lies between microwaves & visible lights.

### **Broadcast radio-**

1. Broadcast Radio uses a transmitter which is used to transmit data in the form of radio waves to receiving antennas.
2. Radio broadcasting may occur via cable, FM, and satellites.
3. A broadcast sends information over long distances.

Examples- **AM**- amplitude modulation

**FM**- frequency modulation

### **Micro wave communication-**

- This is an effective type of communication which uses radio waves.
  - In this communication data or information can be transmitted using 2 methods.
1. Satellite method
  2. Terrestrial method

### **Wi-fi communication-**

1. Wireless fidelity is a popular wireless networking technology.
2. WI-FI is invented by NCR corporation in Netherlands in 1991.
3. WI-FI has been developed for mobile computing devices such as laptop but now it is used for mobile application, TV & digital camera etc.



### **Short Questions with answers**

**Q1. Define signal rate.**

**Signal rate-**

1. It is the number of signal element send in one second.
2. A signal element is a shortest unit of the digital signal.
3. The unit of signal rate is baud. It is also known as baud rate.

**Q2. Define Channel capacity-**

The maximum rate at which data can be transmitted over a given communication path or channel under given condition is refer to as channel capacity.

**Q3. Define Data rate.**

1. The rate at which data can be transmitted is known as data rate.
2. It is represented in bits per second (BPS).

### **Long Questions**

**Q1. Describe transmission impairments.**

**Q2. Explain different types of transmission media.**

## CHAPTER-03

# Data Encoding

### **Data Encoding**

- **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.

### **Data Encoding**

- Data Encoding is the process of using various patterns of voltage or current levels to represent 1s and 0s of the digital signals on the transmission link.

### **Types of data encoding techniques-**

1. Digital data digital signals
2. Digital data analog signals
3. Analog data analog signals
4. Analog data digital signals

### **Digital data digital signals**

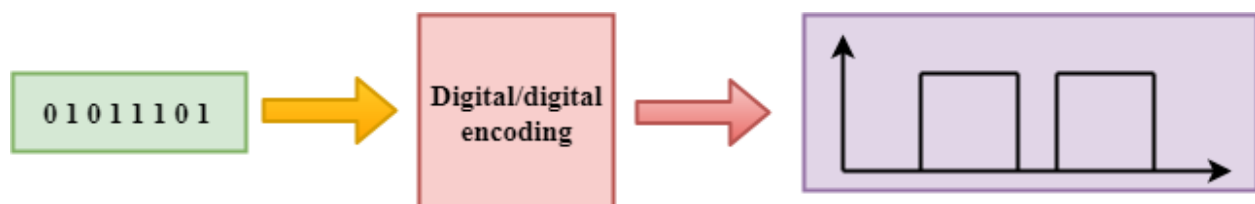
- It is the digital to digital conversion technique which represents the digital data into digital signals.
- A digital signal is a sequence of discrete, discontinuous voltage pulses where each pulse is a signal element.
- Binary data are transmitted by encoding each data bit into a signal element.
- Encoding scheme maps data bits to signal elements.

## Key terms of data transmission :-

TERMS	UNIT	DEFINITION
Data element	Bit	A single binary 0 or 1
Data rate	Bits/sec(bit rate)	The rate at which data elements are transmitted
Signal element	-	It is the shortest unit of a digital signal
Signal rate	Signal elements per second(baud)	The rate at which signal elements are transmitted

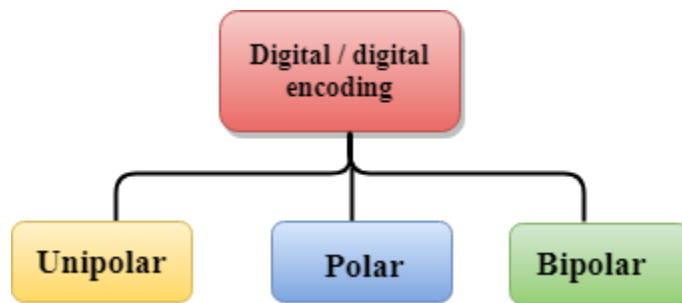
## DIGITAL-TO-DIGITAL CONVERSION

- 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.



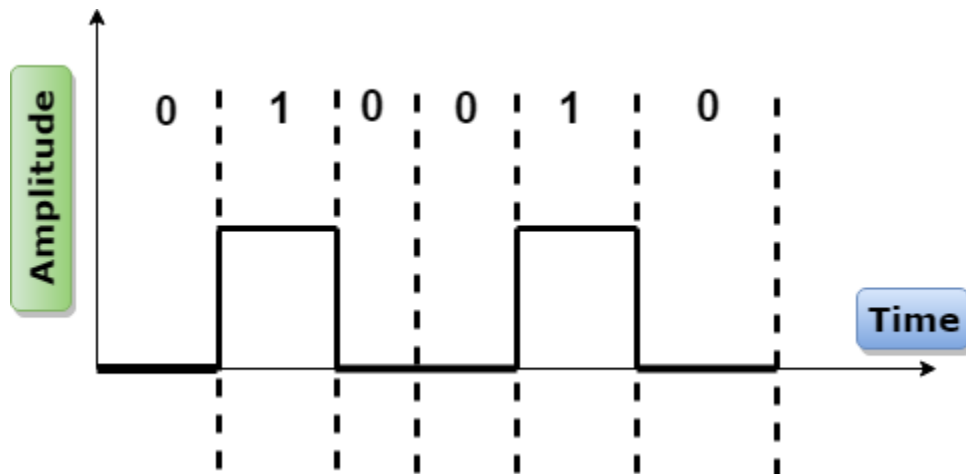
**Digital-to-digital encoding is divided into three categories:**

- **Unipolar Encoding**
- **Polar Encoding**
- **Bipolar Encoding**



## Unipolar

- Digital transmission system sends the voltage pulses over the medium link such as wire or cable.
- In most types of encoding, one voltage level represents 0, and another voltage level represents 1.
- The polarity of each pulse determines whether it is positive or negative.
- This type of encoding is known as Unipolar encoding as it uses only one polarity.
- In Unipolar encoding, the polarity is assigned to the 1 binary state.
- In this, 1s are represented as a positive value and 0s are represented as a zero value.
- In Unipolar Encoding, '1' is considered as a high voltage and '0' is considered as a zero voltage.
- Unipolar encoding is simpler and inexpensive to implement.



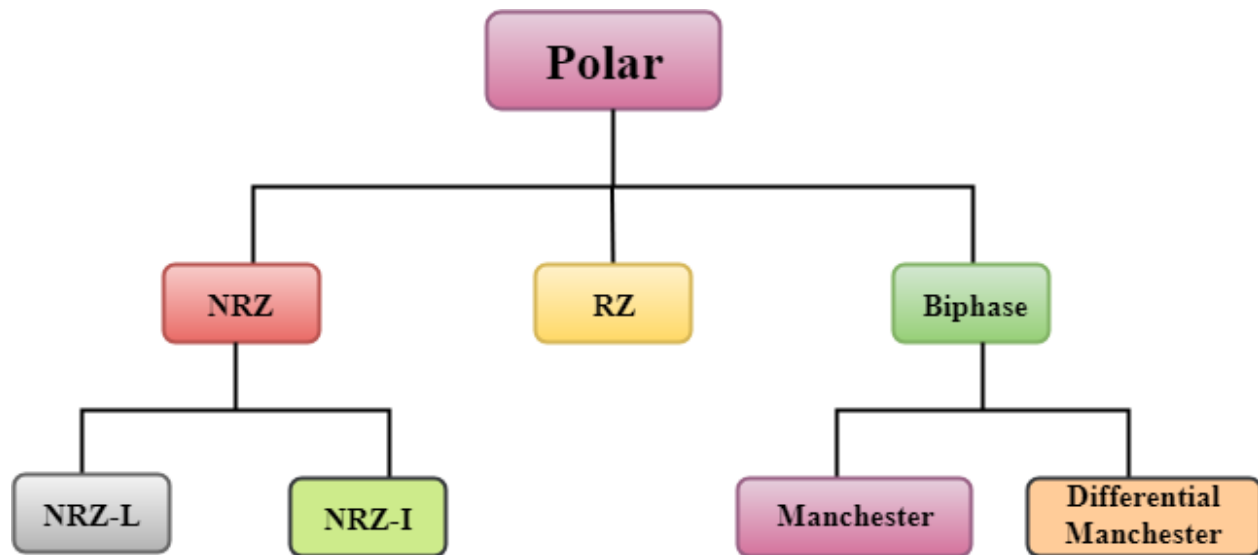
**Unipolar encoding has two problems that make this scheme less desirable:**

- **DC Component**
- **Synchronization**

---

## Polar

- Polar encoding is an encoding scheme that uses two voltage levels: one is positive, and another is negative.
- By using two voltage levels, an average voltage level is reduced, and the DC component problem of the unipolar encoding scheme is alleviated.



## NRZ

- NRZ stands for Non-return zero.
- In NRZ encoding, the level of the signal can be represented either positive or negative.

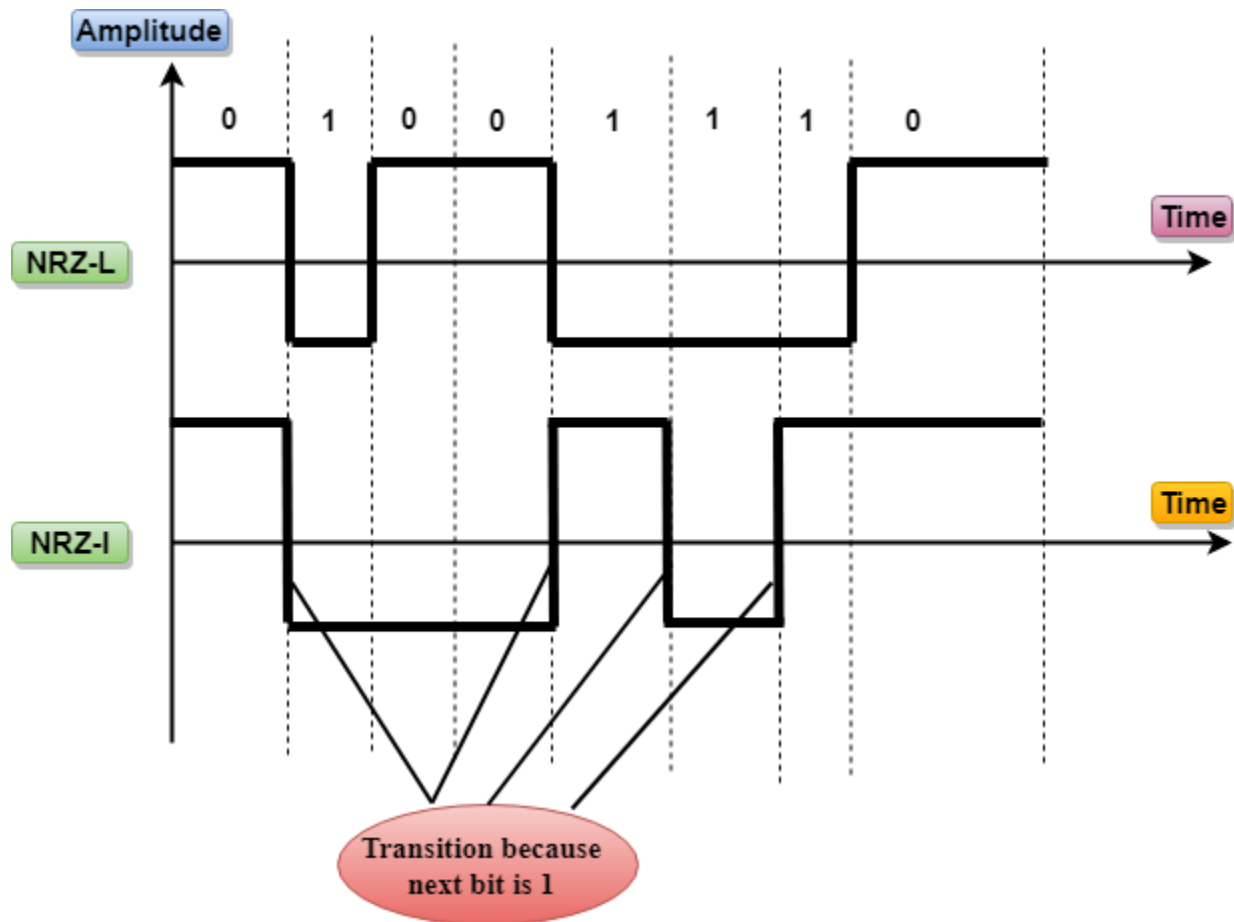
## The two most common methods used in NRZ are:

### NRZ-L:

- In NRZ-L encoding, the level of the signal depends on the type of the bit that it represents.
- If a bit is 0 or 1, then their voltages will be positive and negative respectively.
- Therefore, we can say that the level of the signal is dependent on the state of the bit.

### NRZ-I:

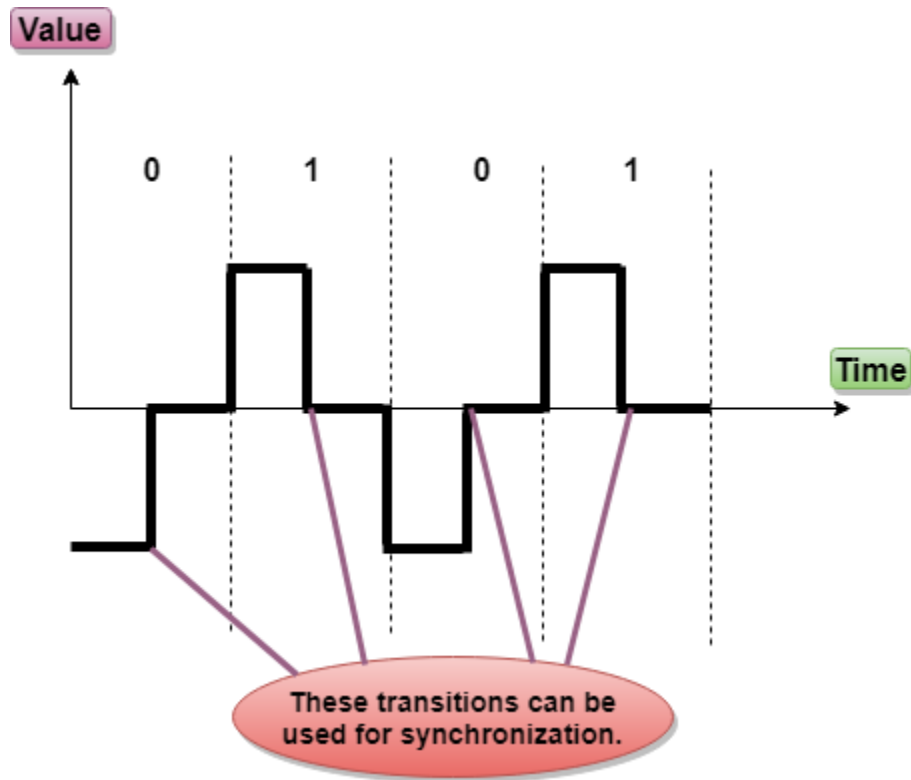
- NRZ-I is an inversion of the voltage level that represents 1 bit.
- In the NRZ-I encoding scheme, a transition occurs between the positive and negative voltage that represents 1 bit.
- In this scheme, 0 bit represents no change and 1 bit represents a change in voltage level.



## RZ

- RZ stands for Return to zero.
- There must be a signal change for each bit to achieve synchronization. However, to change with every bit, we need to have three values: positive, negative and zero.
- RZ is an encoding scheme that provides three values, positive voltage represents 1, the negative voltage represents 0, and zero voltage represents none.
- In the RZ scheme, halfway through each interval, the signal returns to zero.

- In the RZ scheme, 1 bit is represented by positive-to-zero and 0 bit is represented by negative-to-zero.



#### Disadvantage of RZ:

It performs two signal changes to encode one bit that acquires more bandwidth.

#### Biphase

- Biphase is an encoding scheme in which signal changes at the middle of the bit interval but does not return to zero.



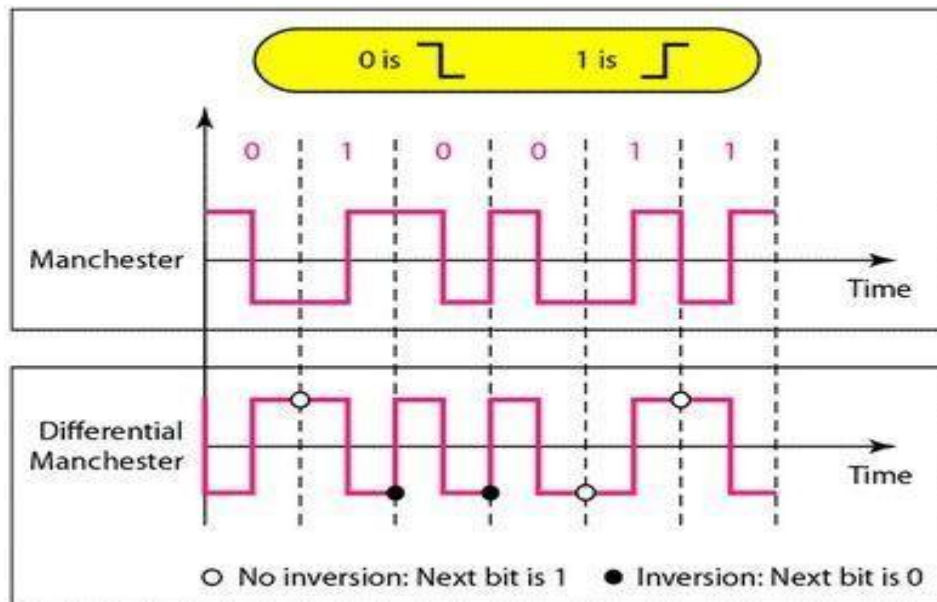
## **Biphase encoding is implemented in two different ways:**

### **Manchester**

- It changes the signal at the middle of the bit interval but does not return to zero for synchronization.
- 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.

### **Differential Manchester**

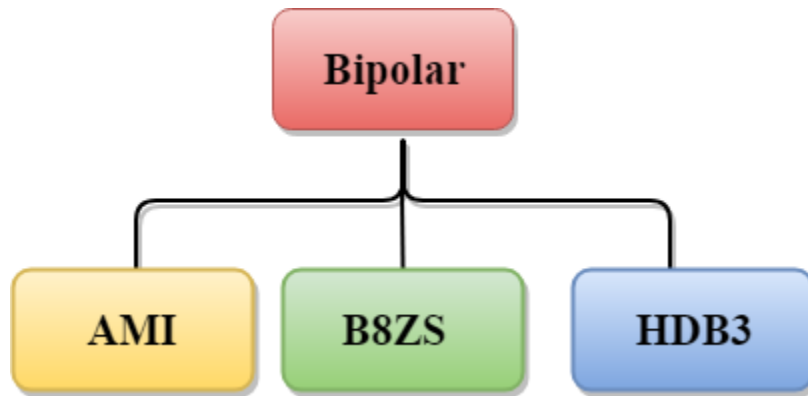
- It changes the signal at the middle of the bit interval for synchronization, but the presence or absence of the transition at the beginning of the interval determines the bit.
- A transition means binary 0 and no transition means binary 1.
- In the Manchester Encoding scheme, two signal changes represent 0 and one signal change represents 1.



## Bipolar

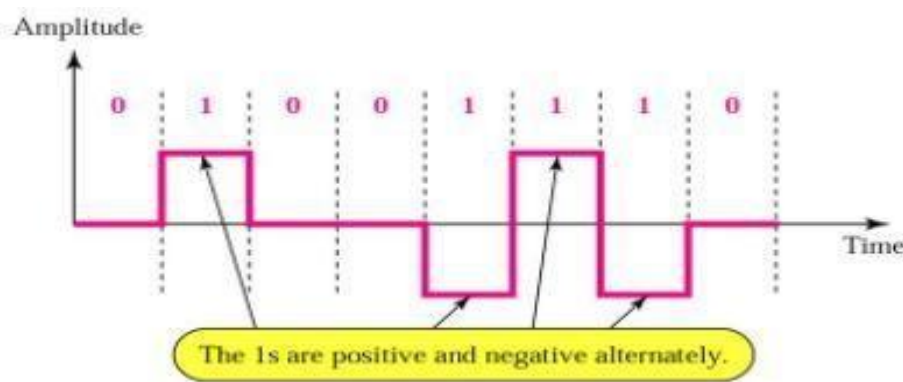
- Bipolar encoding scheme represents three voltage levels: positive, negative, and zero.
- In Bipolar encoding scheme, zero level represents binary 0, and binary 1 is represented by alternating positive and negative voltages.
- If the first 1 bit is represented by positive amplitude, then the second 1 bit is represented by negative voltage, the 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:**



### AMI

- **AMI stands for *alternate mark inversion* where mark work comes from telegraphy which means 1. So, it can be redefined as alternate 1 inversion.**
- **In Bipolar AMI encoding scheme, 0 bit is represented by zero level and 1 bit is represented by alternating positive and negative voltages.**



**Advantage:**

- **DC component is zero.**
- **Sequence of 1s bits are synchronized.**

**Disadvantage:**

- **This encoding scheme does not ensure the synchronization of a long string of 0s bits.**

## B8ZS

- B8ZS stands for Bipolar 8-Zero Substitution.
- This technique is adopted in North America to provide synchronization of a long sequence of 0s bits.
- In most of the cases, the functionality of 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 the 0 string pattern.
- When eight 0 occurs, then B8ZS implements some changes in 0s string pattern based on the polarity of the previous 1 bit.
- If the polarity of the previous 1 bit is positive, the eight 0s will be encoded as zero, zero, zero, positive, negative, zero, negative, positive.

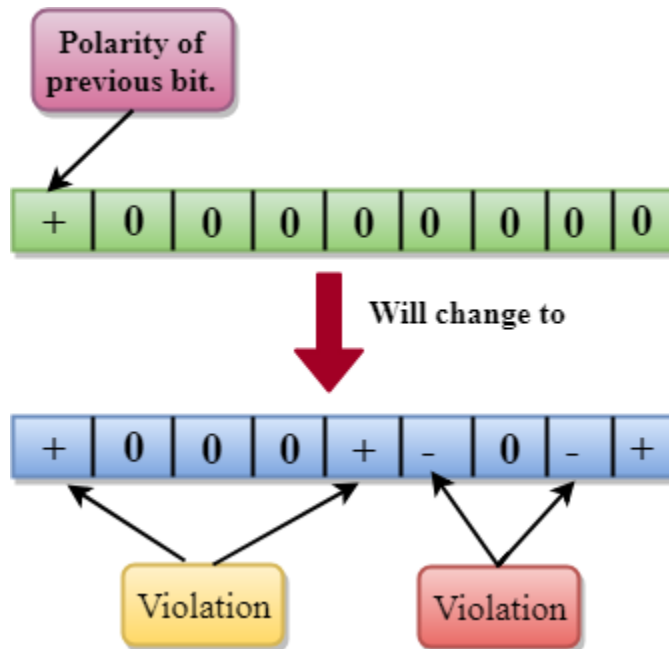
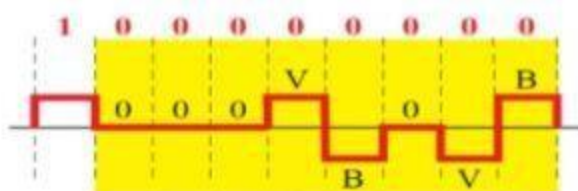
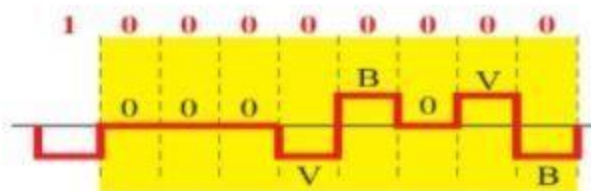


Figure: Two cases of B8ZS scrambling technique



a. Previous level is positive.



b. Previous level is negative.

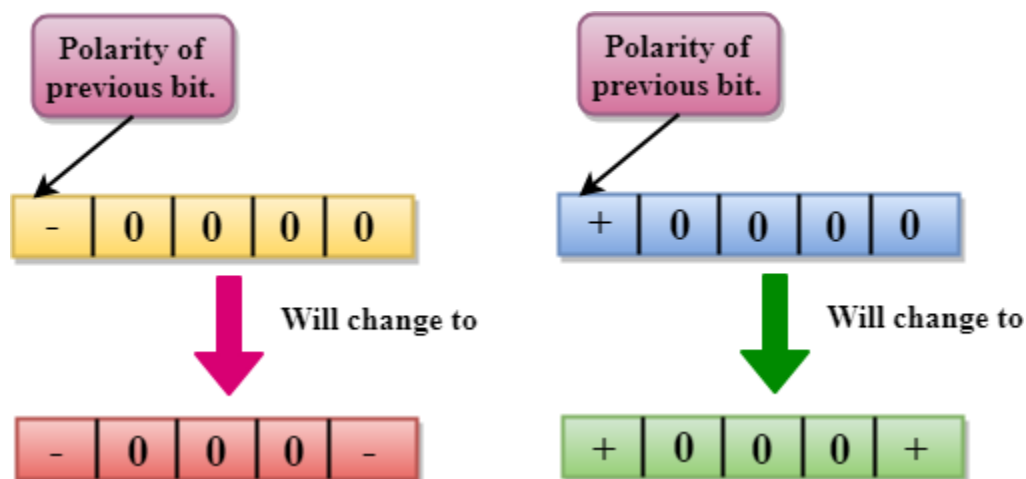
- V means the same polarity as the polarity of previous non zero pulse
- B means the polarity opposite to the polarity of previous non zero pulse

- If the polarity of previous 1 bit is negative, then the eight 0s will be encoded as zero, zero, zero, negative, positive, zero, positive, negative.

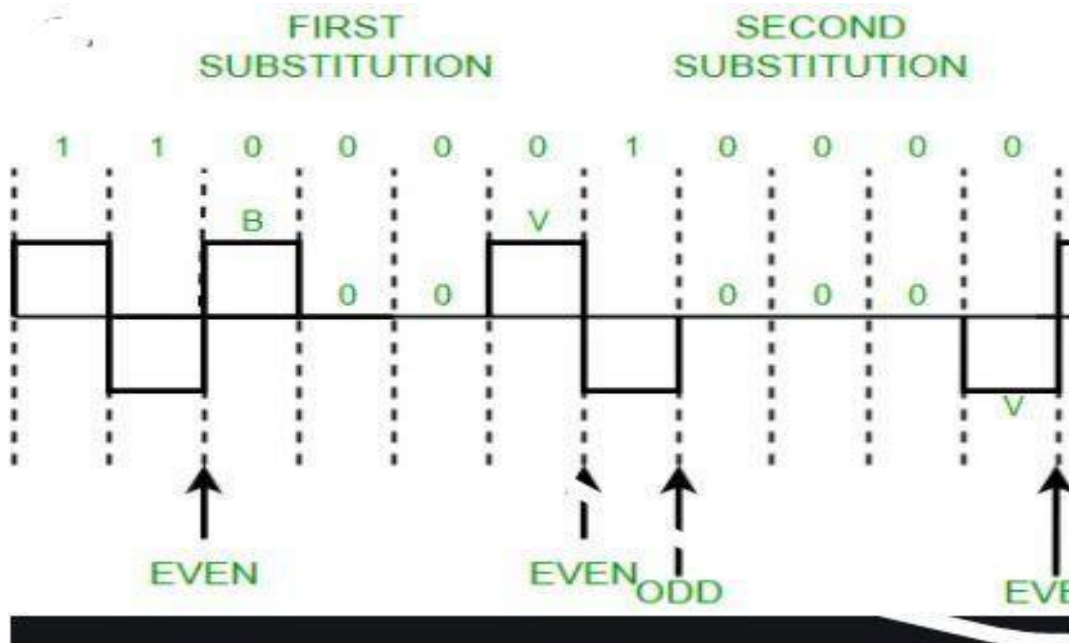
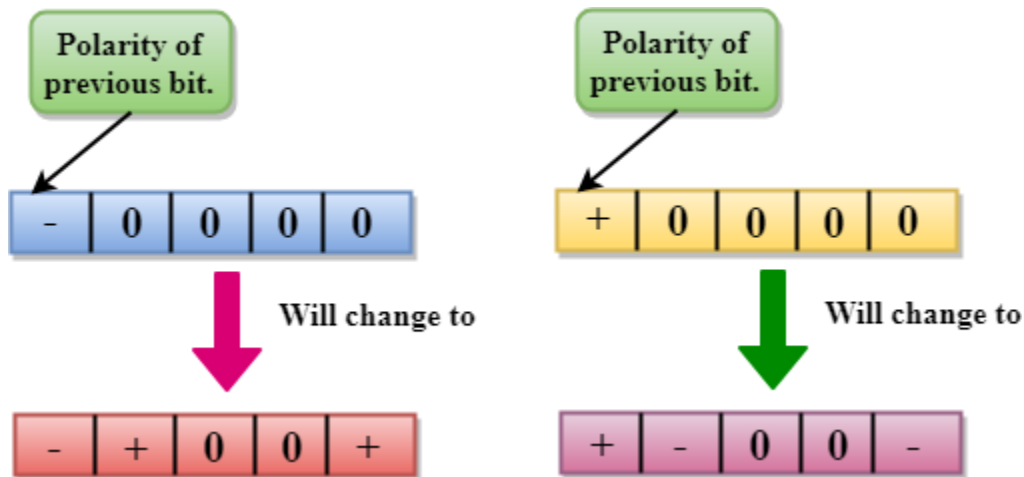
## HDB3

- HDB3 stands for High-Density Bipolar 3.
- HDB3 technique was first adopted in Europe and Japan.
- 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 that occurred since the last substitution.
- If the number of 1s bits is odd, then the violation is made on the fourth consecutive of 0. If the polarity of the previous bit is positive, then the violation is positive. If the polarity of the previous bit is negative, then the violation is negative.

**If the number of 1s bits since the last substitution is odd.**



- If the number of 1s bits is even, then the violation is made in the place of the first and fourth consecutive 0s. If the polarity of the previous bit is positive, then violations are negative, and if the polarity of the previous bit is negative, then violations are positive.
- If the number of 1s bits since the last substitution is even.

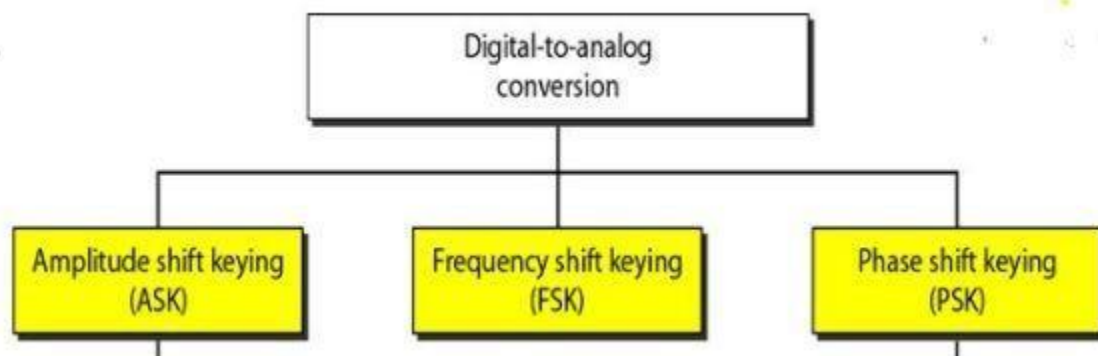


## Digital data analog signal

Digital data can be converted to analog signal by changing one of the characteristics such as –

- Amplitude
- Frequency
- Phase

There are 3 different mechanisms that convert digital data into analog signals.

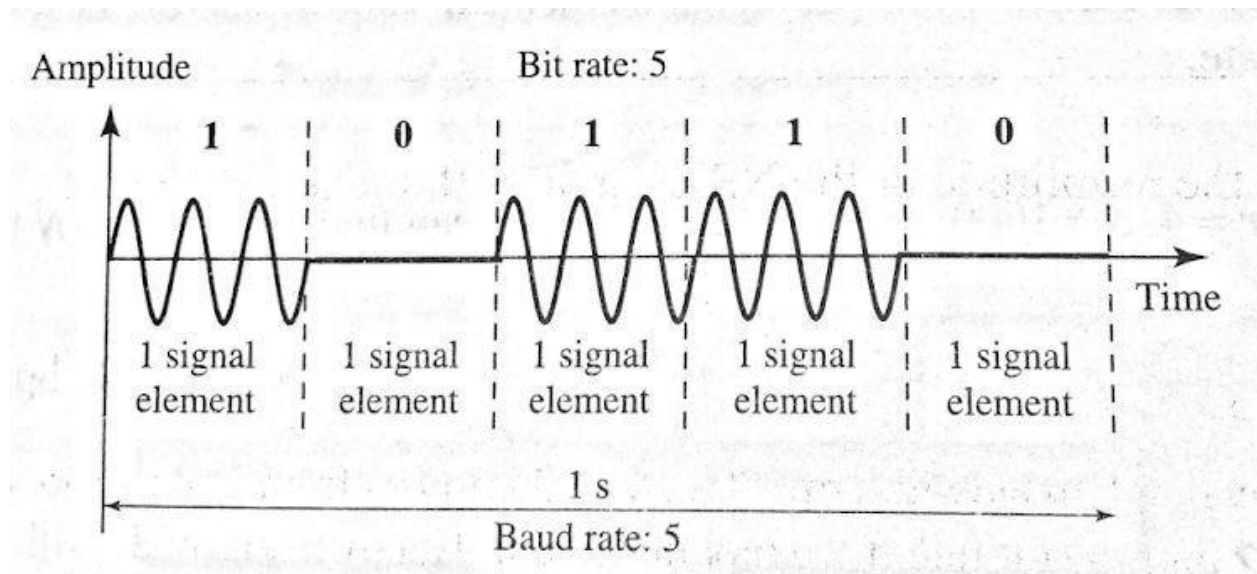


1. Amplitude shift keying
2. Frequency shift keying
3. Phase shift keying

### **Amplitude shift keying-**

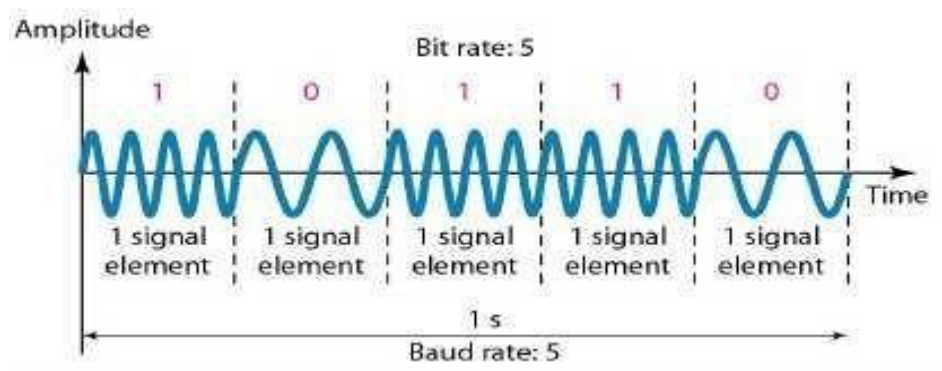


In ASK the amplitude of the carrier signal is varied to create signal elements keeping both frequency & phase constant.



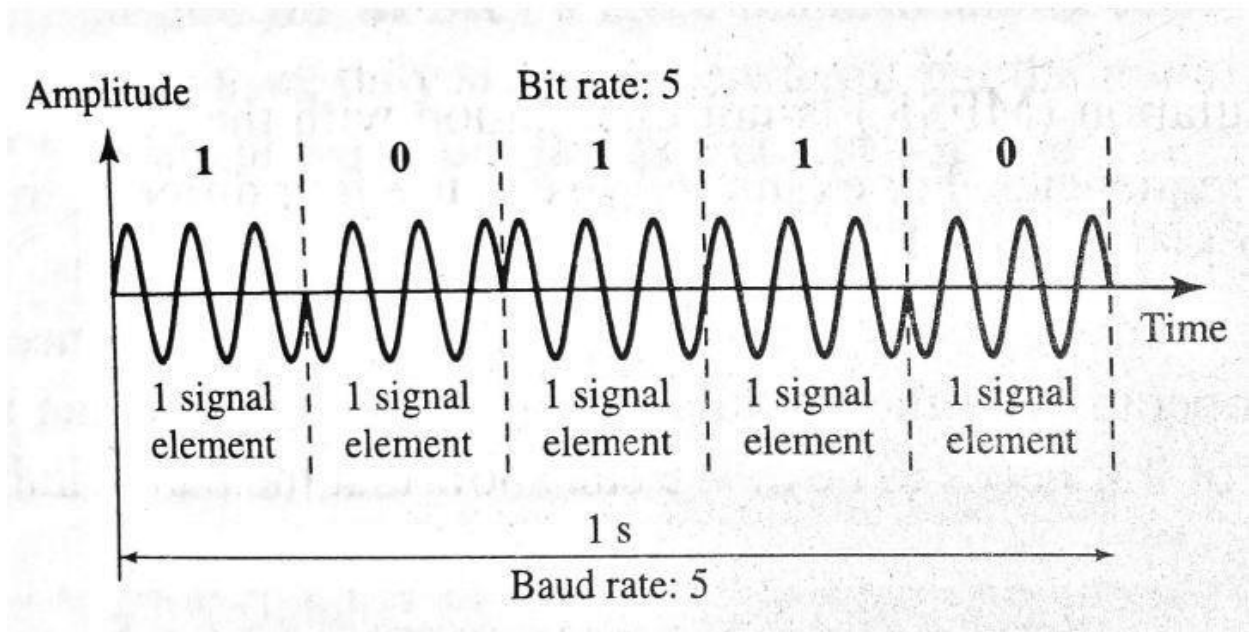
### Frequency shift keying-

- If the frequency of a sinusoidal carrier wave is varied (switched) depending upon the digital input signal then it is known as the Frequency shift keying.
- Here amplitude and phase remain constant.



### Phase shift keying-

- In phase shift keying ,the phase of the carrier wave is switched as per the input digital signal.
- The amplitude & frequency remains constant.



## Analog data digital signals

## ANALOG-TO-DIGITAL CONVERSION

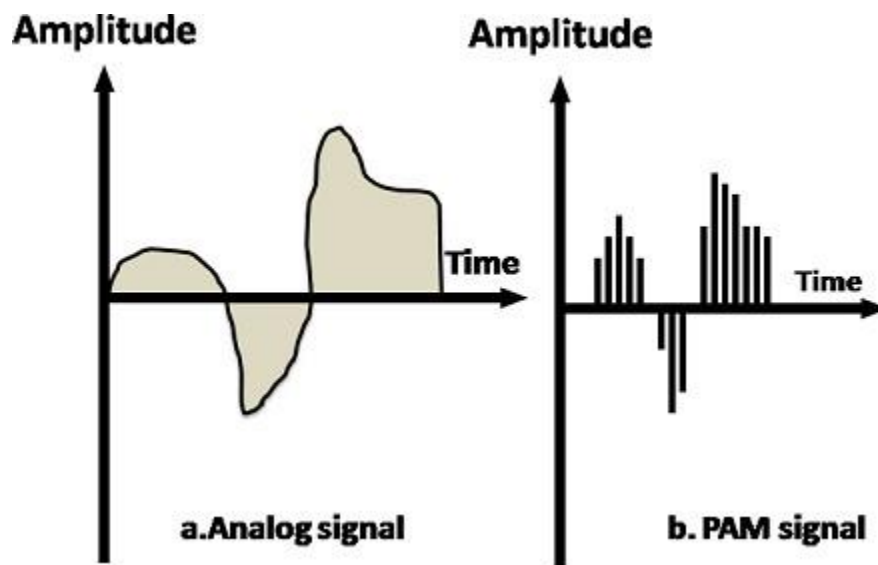
- When an analog signal is digitalized, this is called an analog-to-digital conversion.
- Suppose human sends a voice in the form of an analog signal, we need to digitalize the analog signal which is less prone to noise. It requires a reduction in the number of values in an analog message so that they can be represented in the digital stream.

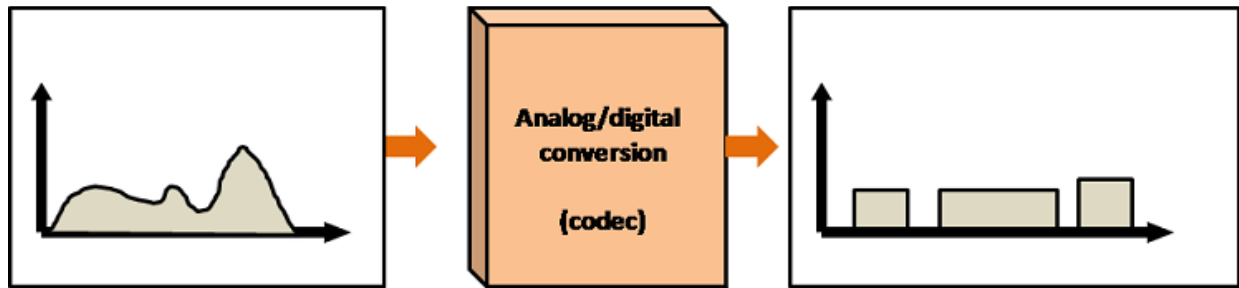
- In analog-to-digital conversion, the information contained in a continuous wave form is converted in digital pulses.

## Techniques for Analog-To-Digital Conversion

### PAM

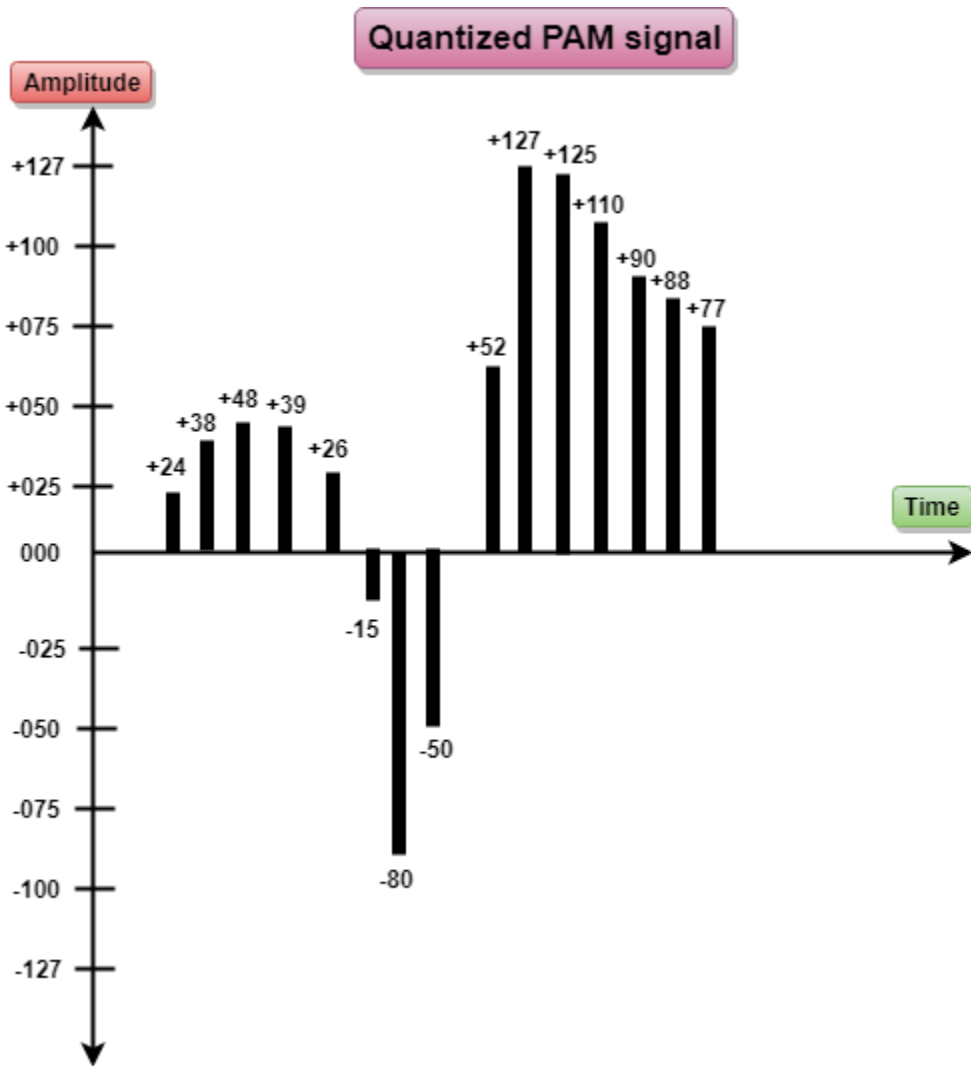
- PAM stands for pulse amplitude modulation.
- PAM is a technique used in analog-to-digital conversion.
- PAM technique takes an analog signal, samples it, and generates a series of digital pulses based on the result of sampling where sampling means measuring the amplitude of a signal at equal intervals.
- PAM technique is not useful in data communication as it translates the original wave form into pulses, but these pulses are not digital. To make them digital, PAM technique is modified to PCM technique.





## PCM

- **PCM stands for Pulse Code Modulation.**
- **PCM technique is used to modify the pulses created by PAM to form a digital signal. To achieve this, PCM quantizes PAM pulses.**
- **Quantization is a process of assigning integral values in a specific range to sampled instances.**
- **PCM is made of four separate processes: PAM, quantization, binary encoding, and digital-to-digital encoding.**



## PCM



## **Analog data analog signal :-**

- **It is also known as analog modulation.**
- **It represents the analog information in analog signal.**

### **Modulation-**

**Modulation is the process of varying any of the 3 characteristics such as amplitude, frequency, or phase of carrier signal.**

**Analog to analog conversion takes place in 3 ways-**

- 1. Amplitude modulation.**
- 2. Frequency modulation.**
- 3. Phase modulation.**

### **Amplitude modulation-**

- **It is the modulation technique in which carrier amplitude varies based on analog baseband signal to be transmitted using wireless medium.**
- **One of the 1<sup>st</sup> application is radio broadcasting.**
- **It is the simplexed type modulation.**
- **Hardware design of both transmitter is very simple & cost effective.**

### **Frequency modulation-**

- **FM is the modulation technique in which carrier frequency varies based on analog baseband information signal using wireless medium.**
- **FM radio broadcast is an example.**
- **Modulation and demodulation does not catch any channel noise.**

### **Phase modulation-**

- It is the modulation technique in which carrier phase varies based on analog baseband information signal to be transmitted using wireless medium.

**Example- satellite communication.**

## **Short Questions with answers**

### **Q1. What is Data Encoding?**

Data Encoding is the process of using various patterns of voltage or current levels to represent 1s and 0s of the digital signals on the transmission link.

### **Q2. What is digital to digital conversion?**

- 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.

## **Long Questions**

**Q1. Explain Manchester and differential manchester encoding.**

**Q2. Explain NRZ-L and NRZ-I technique.**

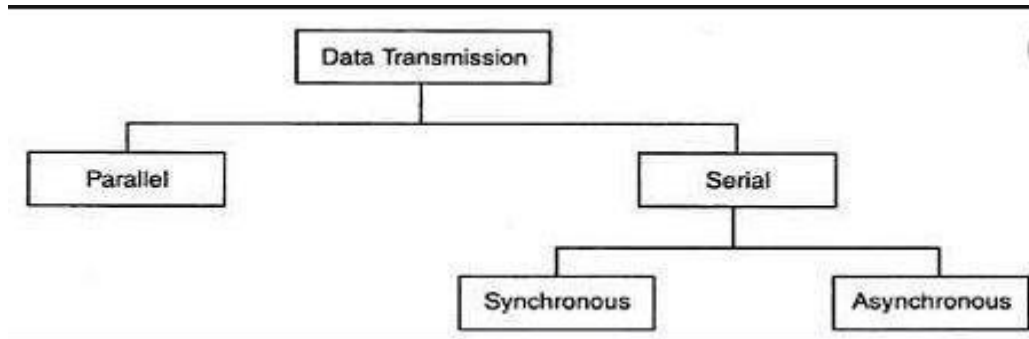
**Q3. Describe different techniques of digital to analog conversion technique.**



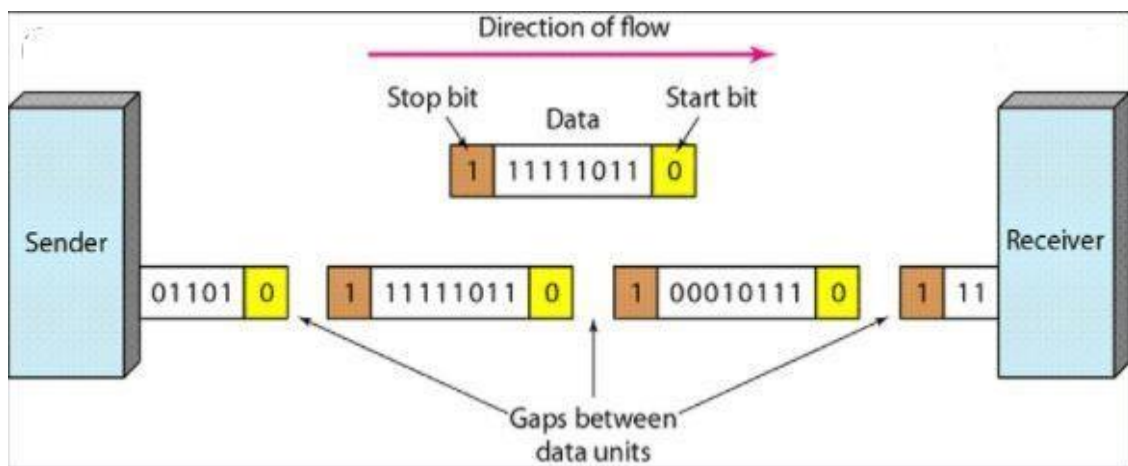
# Chapter – 04

## Data communication & data link control.

### Asynchronous and Synchronous Transmission



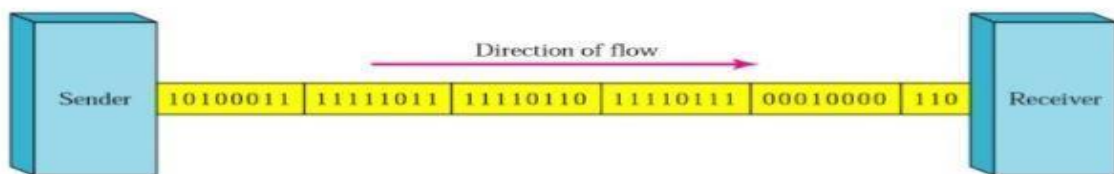
### Asynchronous transmission –:



- It is so named because the timing of a signal is not important in this case i.e. the receiver can't predict when the next data byte will arrive.
- To alert the receiver of a few byte, an extra bit is added at the beginning of each byte that is 0(zero) called the start bit.
- To let the receiver know the byte is finished, one or more extra bits are added at the end of each byte i.e. 1(one) called as stop bit.

- By this method each byte is increased in size to at least 10 bits of which 8 bits are information and 2 bits are signal to the receiver.
- In addition to this, transmission of each byte may be followed by a gap of varying duration. This gap may be represented either by an idle channel or by a string of stop bits.
- The start bit, stop bit and the gap alert the receiver about the beginning and end of each byte and allow to synchronized with data string.

## Synchronous Transmission



- In synchronous transmission the bit string is combined into a longer frame which may contain multiple bytes
- Each byte is introduced in the transmission link without a gap between it and the next one.
- It is left to the receiver to separate the bit strings into bytes for decoding purpose. The receiver counts the string of bits and groups them into 8 bit units. In this case timing is important.
- The advantage of synchronous transmission is speed.
- It is used in high speed communication such as transmission of data from one computer to another.

## Error detection:

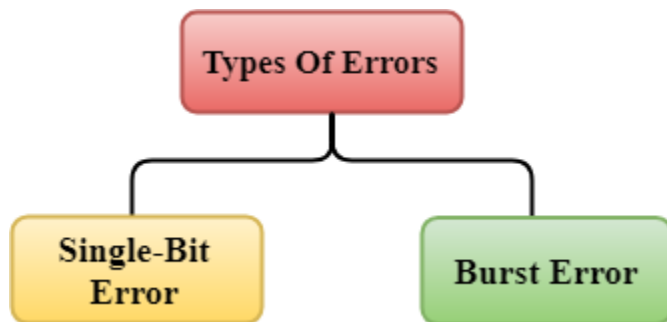
### Error –

- Data may be corrupted during the time of transmission, is known as error.
- In other words, if the data bits received at the receiver is different from the data bits sent by the sender, then error is said to have occurred.

### Types of error –

There are 2 types of errors-

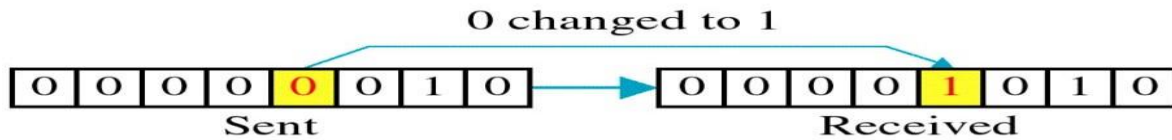
- i. Single bit error
- ii. Burst error



### **Single bit error –**

It means that only one bit of the sent data unit is changed from '0' to '1' or '1' to '0' at the receiver.

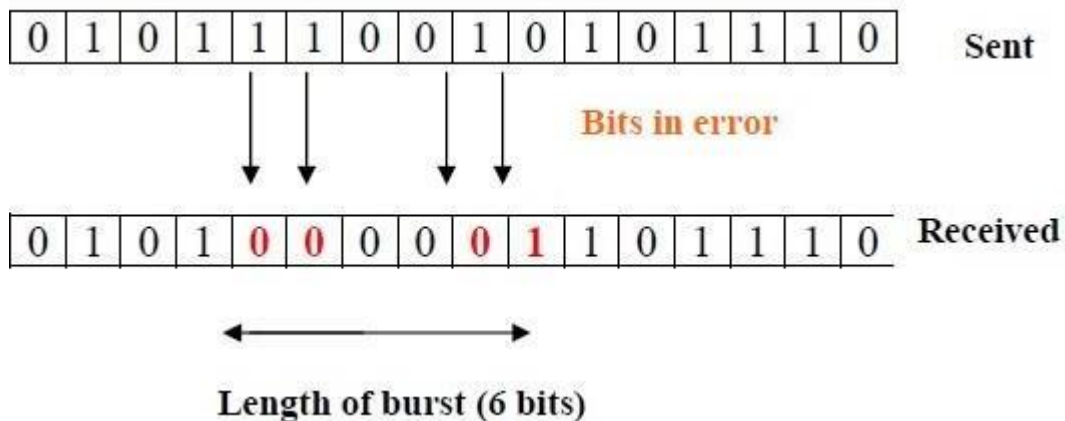
## Single-bit error



3

### Burst error –:

It means that 2 or more bits from a sent data unit is changed from 0 to 1 or vice versa at the receiver.



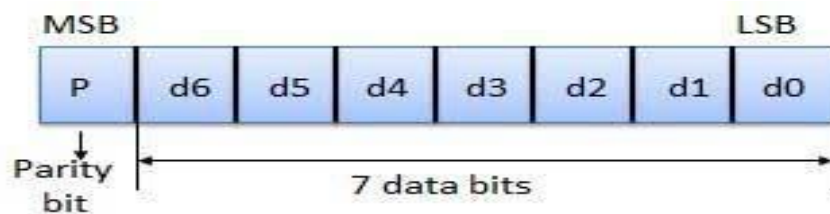
### Error detection methods –

The major error detection methods are –

1. Parity checking.
2. Checksum error detection method.
3. Cyclic redundancy check method.

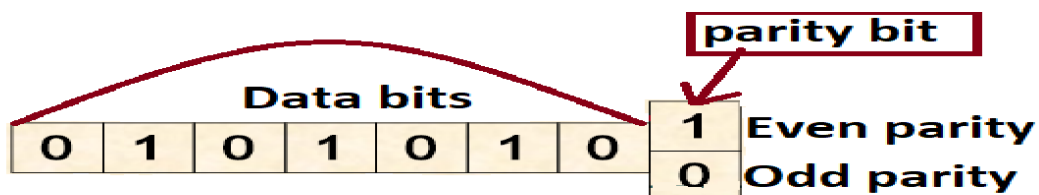
## Parity checking –

- A **parity bit** is a check **bit**, which is added to a block of data for error detection purposes.
- It is used to validate the integrity of the data.
- The value of the **parity bit** is assigned either 0 or 1 that makes the number of 1s in the message block either even or odd depending upon the type of **parity**.



- The parity of the 8 bit transmitted data bits can be either even parity or odd parity.
- Even parity means number of 1's including parity bit must be even.  
Ex- 2,4,8,10 etc.
- Odd parity means number of 1's in the given word including parity bit must be odd.  
Ex- 1,3,5,7 etc.
- FORMULA  
 $P = (\text{Sum of all bits}) \% 2$ .

### Even parity example-



parity bit = **1** (in case of even parity setting)  
parity bit = **0** (in case of odd parity setting)

- The parity bit is chosen by the formula  $p = (d_7, d_6, d_5, d_4, d_3, d_2, d_1, d_0) \% 2$ .
- If the number 1's is even then result will be 0.
- If the number of 1's is odd, the result will be 1.
- The code word may be corrupted during the transmission.
- The checker at the receiver performs a similar operation like sender.
- The addition is done over all the bits of the code word and modulo division('%') by 2 is performed.
- If the result is '0' then the code word is correct otherwise it has errors.

### **Checksum error detection method :-**

- It is another error detection method.
- It based on the concept of redundancy.

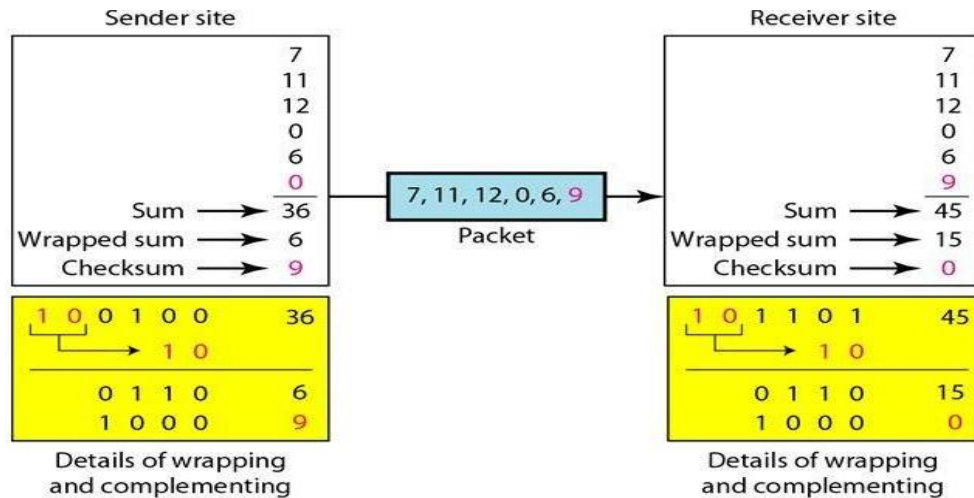
#### At the sender side –

The sender calculates the checksum by the following steps-

1. The message is divided into 'n' bit words
2. The value of the checksum is set to 0
3. All words including the checksum are added using 1's compliment method.
4. The sum is complimented & becomes the checksum
5. The checksum is sent with the data words

#### At the receiver side –

1. The message including checksum are added using 1's compliment addition
2. The sum is complimented & becomes the checksum
3. If the value of the checksum is 0, the message are accepted , otherwise it is rejected.



**Homework** – consider the data words 5,14,13,8,2 is to be transmitted to the receiver using checksum error detection method. Calculate the checksum at the sender side & verify all the data words at the receiver side received correctly or not.

### **Modular arithmetic –**

- In modulo 'n' arithmetic we will use all integers in the range of 0 to n-1 inclusive.
- Here addition and subtraction are same.
- As there is no carry when two digits are added and there is also no borrow when one digit is subtracted from another.
- In modulo-2 arithmetic, additions and subtractions are like this-

Addition	Subtraction
0+0=0	0-0=0
0+1=1	0-1=1
1+0=1	1-0=1
1+1=0	1-1=0

### **Cyclic redundancy check (CRC) :-**

#### **At the sender side –**

- There is an encoder that contains the data word of  $k$  bits & the codeword of  $n$  bits.
- The size of the data words is augmented by adding  $(n-k)$  0's to the right side of data word.
- The  $n$  bit result is fed into a generator. The generator uses a divisor of size  $n-k+1$ , pre-defined & agreed upon.
- The generator divides the augmented data word by  $\%2$  division.
- The remainder is appended to the data word to create code word.

#### **At the receiver side –**

- Here the decoder receives the possibly corrupted code word.
- A copy of all  $n$  bits is fed to the checker which is a replica of the generator.
- The remainder produced by the checker is a syndrome of  $n-k$  bits.
- If the syndrome bits are all 0's , the code word is correct. Otherwise there is error.

#### **Example-**

Given

Data word = 1001 =(k bits = 4)

Code word = data bits + CRC =n bits

Devisor = 1011 = (d bits=4)

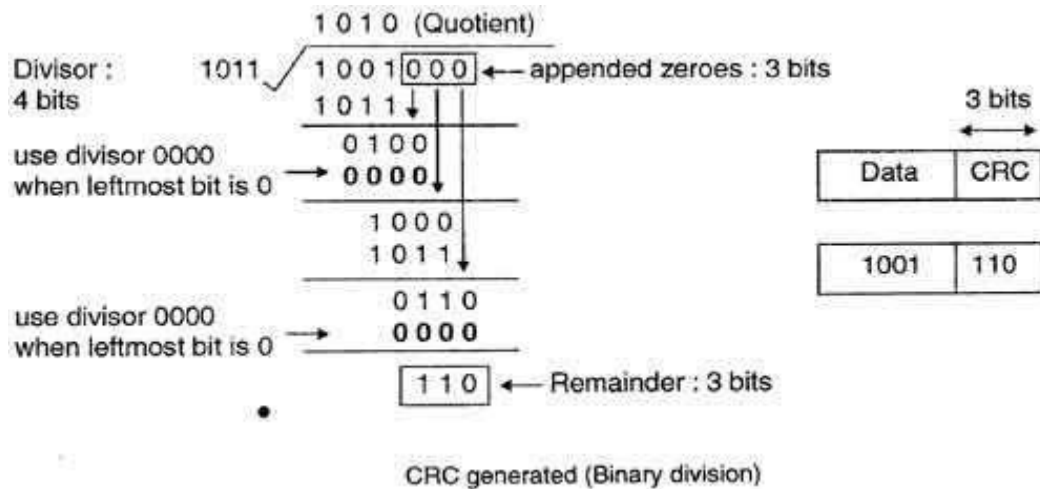
Using CRC method, generate the code word of the data word 1001 & divisor 1011.

Upon reaching at the destination the code word will be checked & show that the code word is correct. (Assuming no error)

#### **Answer-**

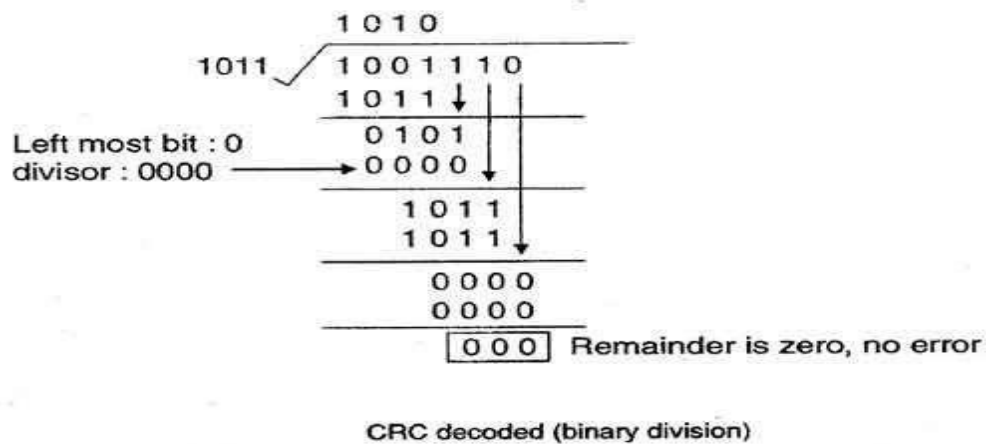
- By appending  $(d-1)$  0s at the right hand side of the data word we will get augmented data word as 1001000
- After getting augmented data word, code word can be generated.





Now the code word=1001110 is transmitted over the network to receiver.

### At the Receiver



As the remainder is all 0s , the code word is correct.

**Q. A bit stream 1101011011 is transmitted using standard CRC method. The generator polynomial is  $x^4 + x + 1$ . what is the actual bit stream (code word) transmitted?**

Answer-

Given –

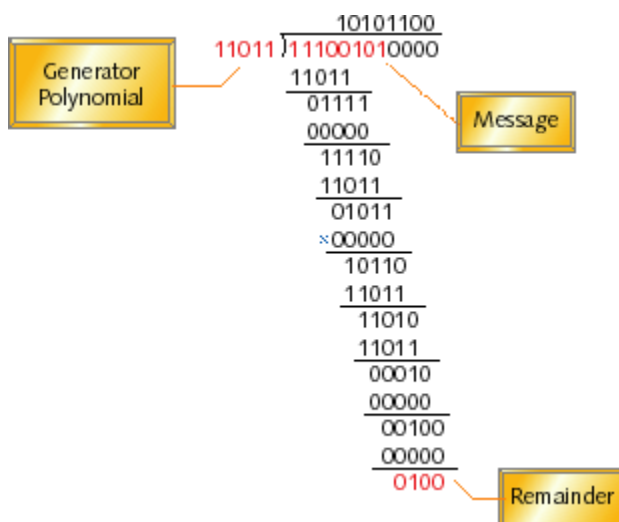
bit stream = 11100101

generator polynomial =  $x^4 + x^3 + x + 1$

=  $1.x^4 + 1.x^3 + 0.x^2 + 1.x^1 + 1.x^0$

Divisor = 11011

Now augmented data word = 111001010000



Hence the bit stream (code word) transmitted is **111001010100**

## **HAMMING DISTANCE –**

It is a concept in coding for error control.

The hamming distance between 2 code words (of the same size) is the number of differences between corresponding bits.

It is represented as  $D(x, y)$  where  $x$  &  $y$  are 2 code words.

Hamming distance is calculated by applying ex-or operation on the 2 words and counting the no. Of 1's in the result.

$$D(x, y) = x + y.$$

Ex – let  $x = 01011$

$Y = 11001$

= 2 bits are error.

Hamming distance –  $d(x, y) = x + y = 2$ .

01011

11001

---

10010

No of 1's = 2.

### **Minimum hamming distance –**

The minimum hamming distance is the smallest hamming distance between all possible pairs in a set of words.

Q. find the minimum hamming distance between the following set of words.

Given code words =  $\{(0000), (0101), (1011), (1101)\}$

$D(w, x) = 0000 \oplus 0101 = 2$

$$D(w, y) = 0000 \oplus 1011 = 3$$

$$D(w, z) = 0000 \oplus 1101 = 3$$

$$D(x, y) = 0101 \oplus 1011 = 3$$

$$D(x, z) = 0101 \oplus 1101 = 1$$

$$D(y, z) = 1011 \oplus 1101 = 2$$

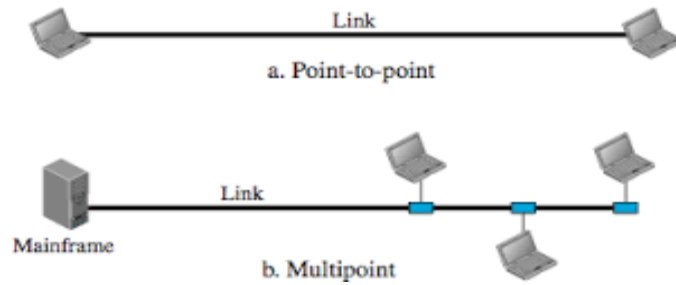
The minimum hamming code = 1.

## Line configuration

- A network is two or more devices connected through a link.
- A link is a communication pathway that transfer data from one device to another. Devices can be a computer, printer or any other device that is capable to send and receive data.
- For communication to occur, two devices must be connected in some way to the same link at the same time.
- There are two possible types of connections:

**1. Point-to-Point Connection**

**2. Multipoint Connection**



### 1. Point-to-Point Connection:

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

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

### 2. Multipoint Connection

1. It is also called Multidrop configuration. In this connection two or more devices share a single link.
2. More than two devices share the link that is the capacity of the channel is shared now. With shared capacity, there can be two possibilities in a Multipoint Line configuration:

**Spatial Sharing:** If several devices can share the link simultaneously, its called Spatially shared line configuration.

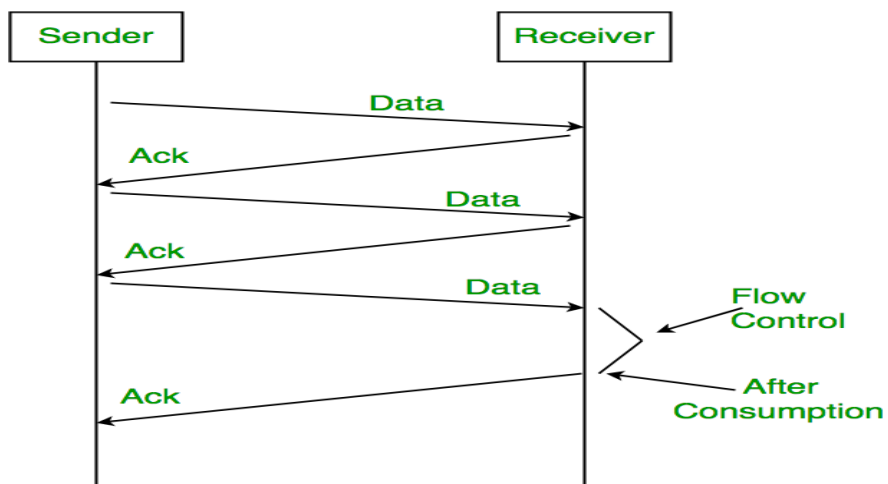
**Temporal (Time) Sharing:** If users must take turns using the link , then its called Temporally shared or Time Shared Line configuration.

### Flow Control

- In data communications, **flow control** is the process of managing the rate of data transmission between two nodes to prevent a fast sender from overwhelming a slow receiver.
- Data link layer uses feedback based flow control mechanisms. There are two main techniques –



## Stop and Wait Protocol



This protocol involves the following transitions –

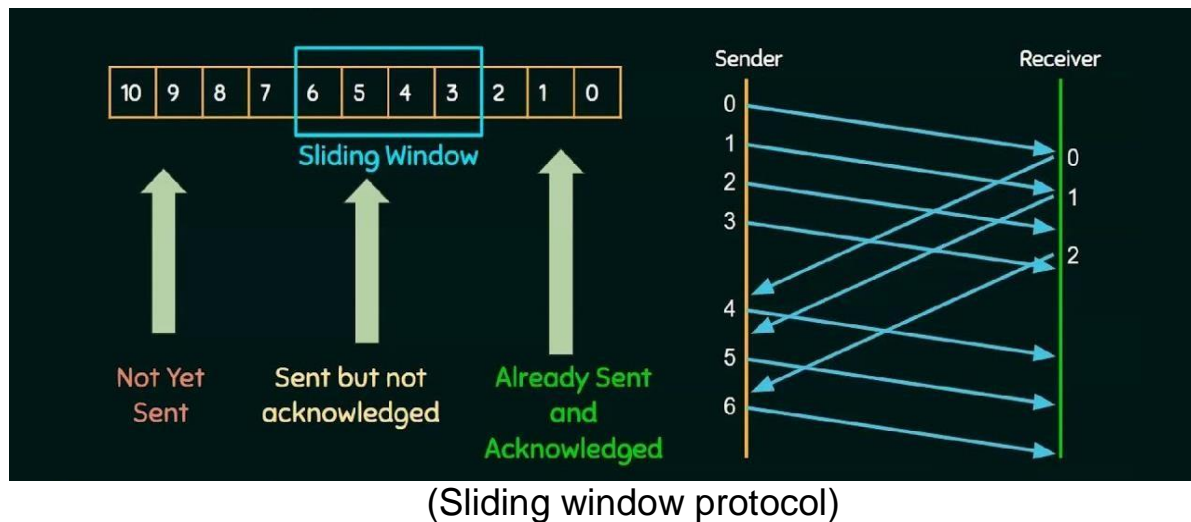
- The sender sends a frame and waits for acknowledgment.
- Once the receiver receives the frame, it sends an acknowledgment frame back to the sender.
- On receiving the acknowledgment frame, the sender understands that the receiver is ready to accept the next frame. So it sends the next frame in queue.

## Sliding Window

This protocol improves the efficiency of stop and wait protocol by allowing multiple frames to be transmitted before receiving an acknowledgment.

The working principle of this protocol can be described as follows –

- Both the sender and the receiver has finite sized buffers called windows. The sender and the receiver agrees upon the number of frames to be sent based upon the buffer size.
- The sender sends multiple frames in a sequence, without waiting for acknowledgment. When its sending window is filled, it waits for acknowledgment. On receiving acknowledgment, it advances the window and transmits the next frames, according to the number of acknowledgments received.



Error Control

**Error control –**



Error control mechanism are –

1. Automatic request for retransmission.
2. Forward error correction.

### **Automatic request for retransmission –**

- It is a technique in which the receiver detects the occurrence of errors and asked the sender to resend the message.
- Resending is repeated until a message arrives at the receiver which is completely error free.

### **Forward error correction –**

- It is a process in which the receiver tries to guess the message by using redundant bits.
- This is possible if the number of errors are small.

### **Error correction technique –**

#### **Hamming code –**

- Hamming code is used to detect & correct a code.
- In hamming code 'k' parity bits( $k > 1$ ) are added to 'n' bit data words.
- The new words ie. Codeword formed is of  $(n+k)$  bits.
- The bit position are from 1 to  $(n+k)$ .
- Example- in a 7 bit hamming code there are 3 parity bits –  $p_1, p_2, p_4$  & 4 bit data positions are –  $d_3, d_5, d_6, d_7$ .

- Position of parity bit are  $2^n$  where  $n = 0,1,2..etc.$

d7	d6	d5	p4	d3	p2	p1
----	----	----	----	----	----	----

### Question-

To transmit 8 bit data word what should be the length of hamming code.

Ans- given data bit = 8

d12	d11	d10	d9	d8	d7	d6	d5	p4	p3	p2	p1
-----	-----	-----	----	----	----	----	----	----	----	----	----

Parity bit = 4

Length of the hamming code =  $8+4 = 12$  bit.

### Question 2-

Construct a 7 bit hamming code using a data word 1011.

Ans-

d7	d6	d5	d4	d3	p2	p1
----	----	----	----	----	----	----

To find p1 -

To find p2 –

### Question 3 –

During the transmission of a hamming code we obtained the code word – 1001110011001. Find out whether the code word is correct or not.

d13	d12	d11	d10	d9	d8	d7	d6	d5	d4	d3	p2	p1
1	0	0	1	1	1	0	0	1	1	0	0	1

**To find p1 –**

$P1 \ d3 \ d5 \ d7 \ d9 \ d11 \ d13 = p1 = 1.$

**To find p2 –**

$P2 \ p3 \ d6 \ d7 \ d10 \ d11 = p2 = 1. \text{ (error)}$

**To find d4 –**

$d4 \ d5 \ d6 \ d7 \ d12 \ d13 = d4 = 0. \text{ (error)}$

**To find d8 –**

$D8 \ d9 \ d10 \ d11 \ d12 \ d13 = d8 = 1.$

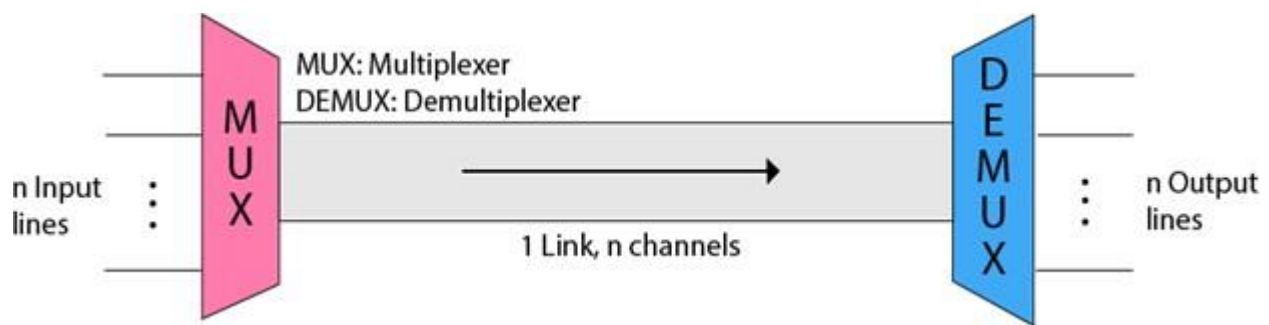
$p2+p4=6 = d6$ is error bit.
------------------------------

The correct codeword is 10011**1**011001.

Multiplexing

- Multiplexing is a technique used to combine and send the multiple data streams over a single medium. The process of combining the data streams is known as multiplexing and hardware used for multiplexing is known as a multiplexer.
- Multiplexing is achieved by using a device called Multiplexer (**MUX**) that combines  $n$  input lines to generate a single output line. Multiplexing follows many-to-one, i.e.,  $n$  input lines and one output line.
- Demultiplexing is achieved by using a device called Demultiplexer (**DEMUX**) available at the receiving end. DEMUX separates a signal into its component signals (one input and  $n$  outputs). Therefore, we can say that demultiplexing follows the one-to-many approach.

## Concept of Multiplexing



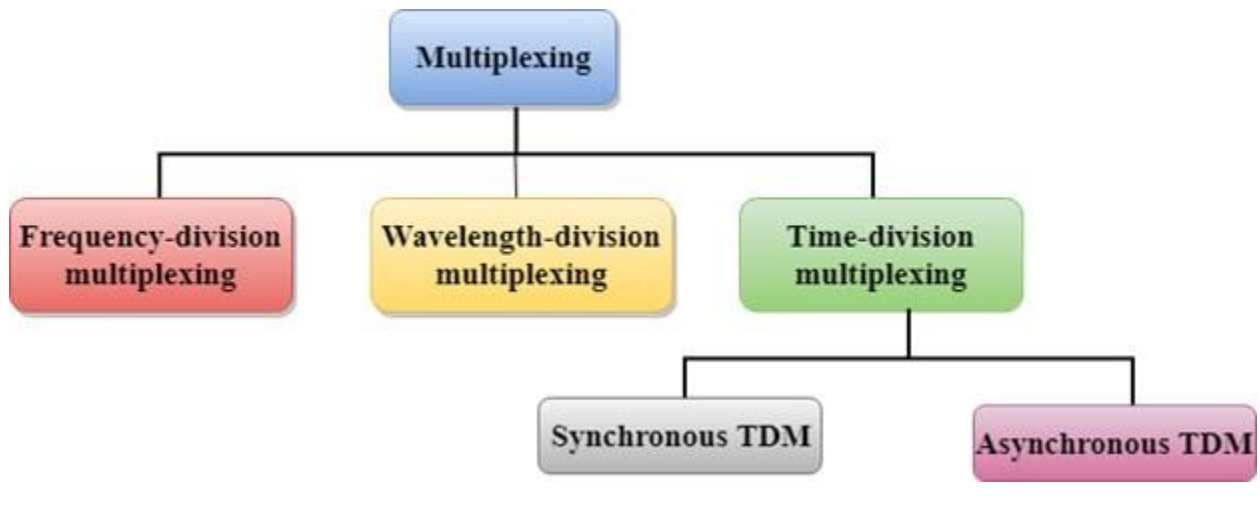
- The ' $n$ ' input lines are transmitted through a multiplexer and multiplexer combines the signals to form a composite signal.
- The composite signal is passed through a Demultiplexer and demultiplexer separates a signal to component signals and transfers them to their respective destinations.

## Advantages of Multiplexing:

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

## Multiplexing Techniques

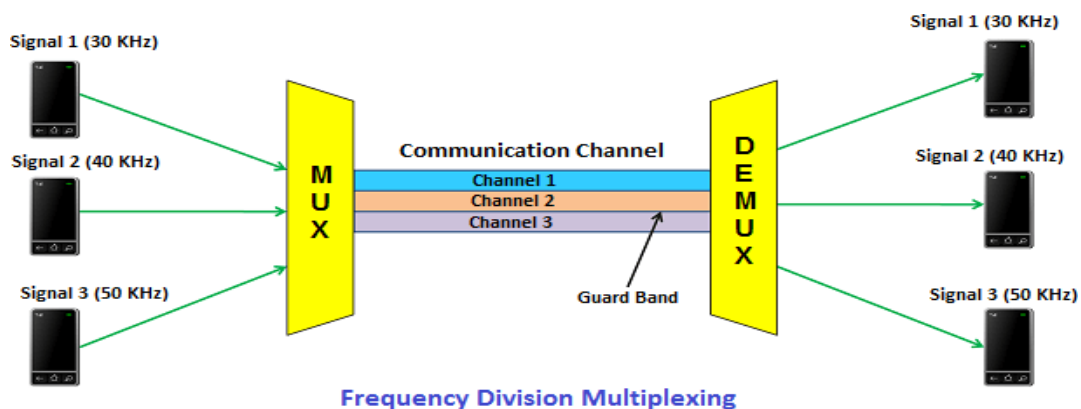
Multiplexing techniques can be classified as:



FDM ,Synchronous TDM

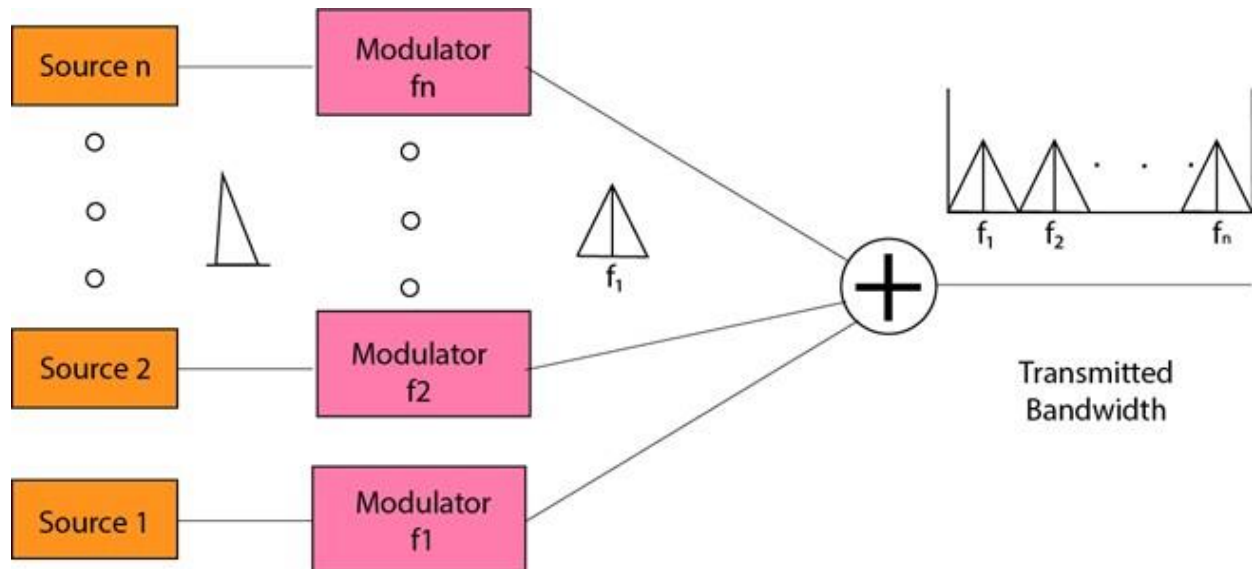
## Frequency-division Multiplexing (FDM)

- It is an analog Multiplexing technique.
- **Frequency Division Multiplexing** is a technique in which the available bandwidth of a single transmission medium is subdivided into several channels.



- The input signals are translated into frequency bands by using modulation techniques, and they are combined by a multiplexer to form a composite signal.

- If  $f_L$  = Bandwidth of the signal and  $f_1, f_2, f_3$  are individual bandwidths of different signals then the condition  $f_L \geq f_1 + f_2 + f_3$  must satisfy for FDM multiplexing.
- **FDM** is mainly used in radio broadcasts and TV networks.



#### Advantages Of FDM:

- FDM is used for analog signals.
- FDM process is very simple and easy modulation.
- A Large number of signals can be sent through an FDM simultaneously.
- It does not require any synchronization between sender and receiver.

#### Disadvantages Of FDM:

- FDM technique is used only when low-speed channels are required.
- It suffers the problem of crosstalk.
- A Large number of modulators are required.
- It requires a high bandwidth channel.

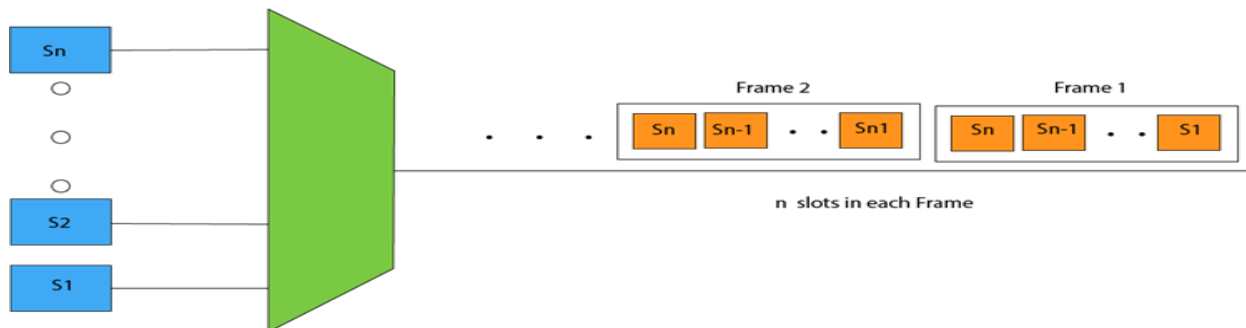
#### Applications Of FDM:

- FDM is commonly used in TV networks.

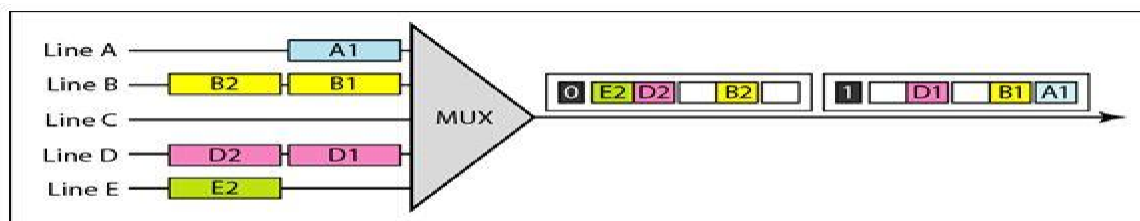
- It is used in FM and AM broadcasting. Each FM radio station has different frequencies, and they are multiplexed to form a composite signal. The multiplexed signal is transmitted in the air.

## Synchronous TDM

- A Synchronous TDM is a technique in which time slot is preassigned to every device.
- In Synchronous TDM, each device is given some time slot irrespective of the fact that the device contains the data or not.
- If the device does not have any data, then the slot will remain empty.
- In Synchronous TDM, signals are sent in the form of frames. Time slots are organized in the form of frames. If a device does not have data for a particular time slot, then the empty slot will be transmitted.
- The most popular Synchronous TDM are T-1 multiplexing, ISDN multiplexing, and SONET multiplexing.
- If there are  $n$  devices, then there are  $n$  slots.



## Concept Of Synchronous TDM



a. Synchronous TDM

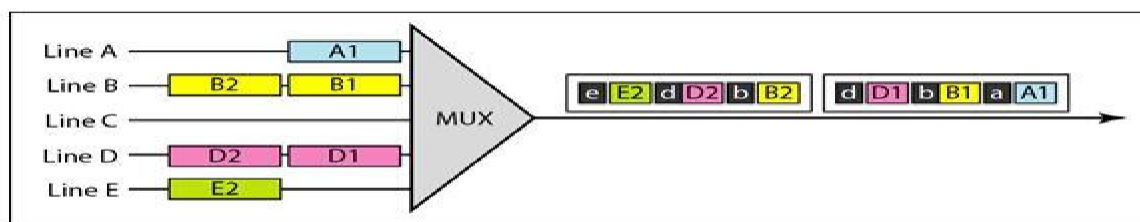
In the above figure, the Synchronous TDM technique is implemented. Each device is allocated with some time slot. The time slots are transmitted irrespective of whether the sender has data to send or not.

### Disadvantages Of Synchronous TDM:

- The capacity of the channel is not fully utilized as the empty slots are also transmitted which is having no data.
- 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.

## Statistical TDM/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.
- In Asynchronous TDM, each slot contains an address part that identifies the source of the data.



b. Statistical TDM



### **Short Questions with answers**

#### **Q1. What is error?**

- Data may be corrupted during the time of transmission, is known as error.
- In other words, if the data bits received at the receiver is different from the data bits sent by the sender, then error is set to have occurred.

#### **Q2. Define Multiplexing.**

- Multiplexing is a technique used to combine and send the multiple data streams over a single medium.
- The process of combining the data streams is known as multiplexing and hardware used for multiplexing is known as a multiplexer.

### **Long Questions**

#### **Q1. Explain different error detection techniques.**

#### **Q2. Explain FDM.**

#### **Q3. What TDM. Explain statistical TDM.**

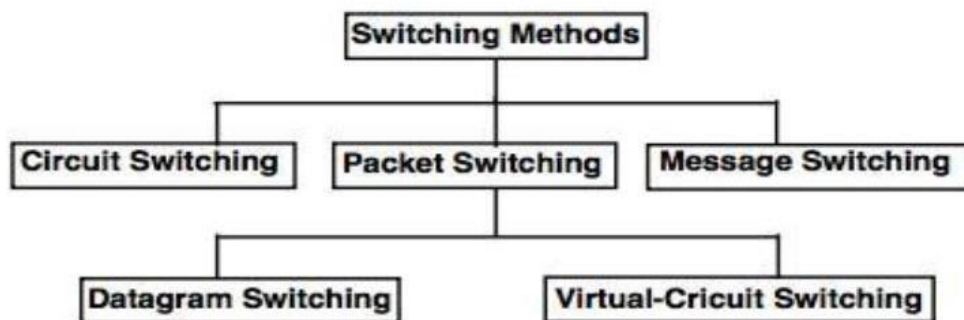
# **CHAPTER-5**

## **Switching & Routing**

### **Switching in Computer Network**

- **Switch** - A switch is a device that links the communicating devices together temporarily.
- **Switching** - In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.

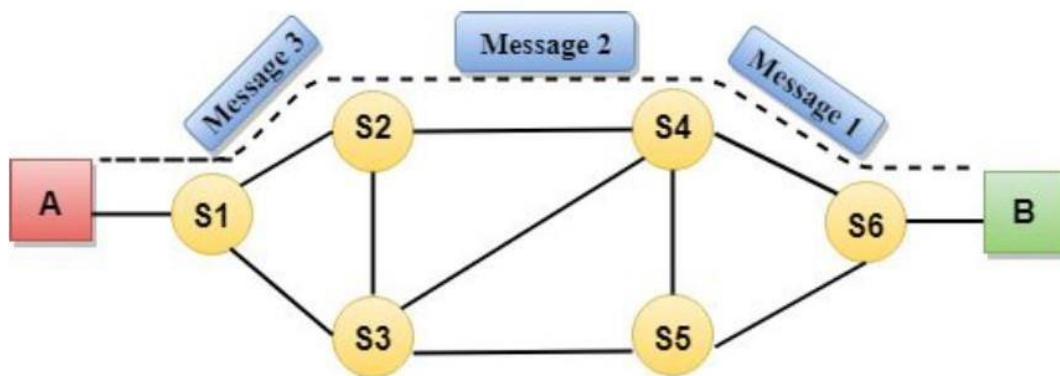
### **Types of Switching Techniques**



### **Circuit Switching Networks-**

- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- In the Circuit Switching Technique, once the connection is established then the dedicated path will exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.

- A complete end-to-end reserved path must exist before the communication takes place.
- In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
- Circuit switching is used in public telephone network. It is used for voice transmission.



Communication through circuit switching has 3 phases.

- **Circuit establishment** - The path is reserved between source & destination.
- **Data transfer** - Data transfer occurs after circuit is established.
- **Circuit Disconnect**- After data transmission completes , the circuit is disconnected.

## **Packet Switching Network-**

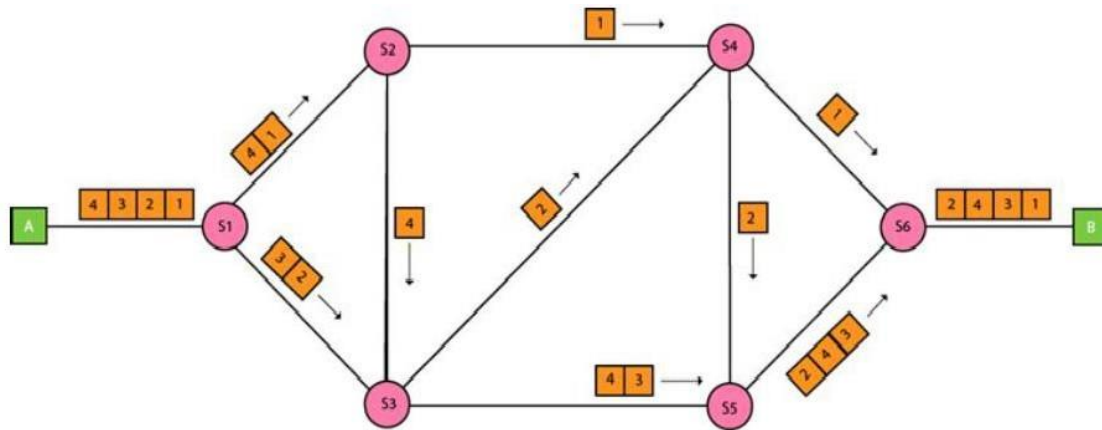
- The packet switching is a switching technique in which the message is divided into smaller pieces known as packets and they are sent individually.
- The packets are given a sequence number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- No dedicated path is established between sender & receiver.
- Packets will travel across the network dynamically , 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 a message will be sent to resend the message.
- If the correct order of the packets is reached, then the acknowledgment message will be sent to the sender.

Packet Switching is of 2 types -

- Datagram packet switching
- Virtual circuit switching

## **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.

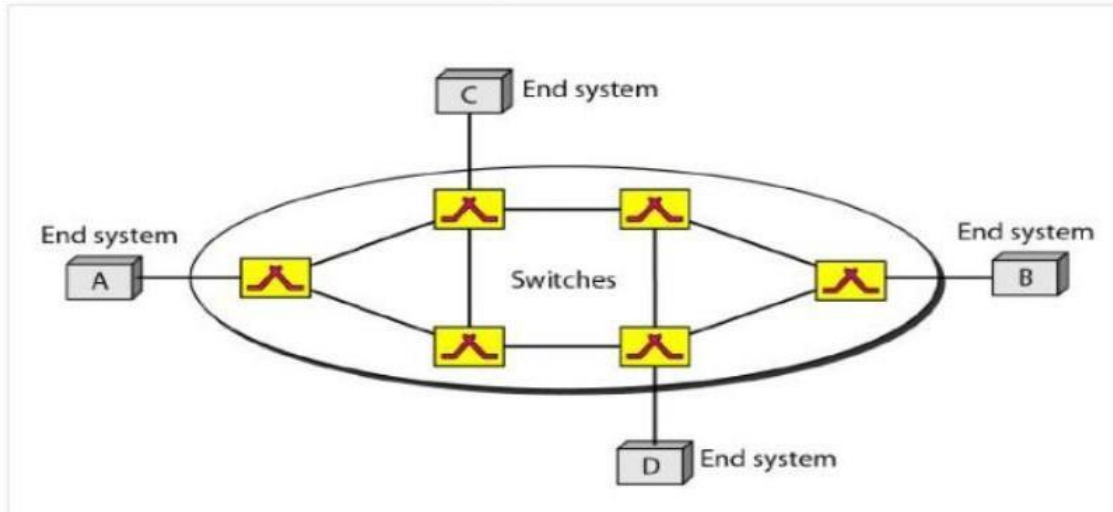


- In Datagram Packet Switching technique, the path is not fixed.
- Intermediate nodes take the routing decisions to forward the packets.
- Datagram Packet Switching is also known as connectionless switching.

## Virtual circuit Network-

- A virtual circuit network is cross between circuit switched & datagram network. It has some characteristics of both.
- As in circuit switching network there are circuit establishment , circuit disconnect phases & as in datagram n/w there is data transfer phase.
- Resources can be allocated during the circuit establishment phase as in circuit switching n/w or during on demand as in datagram n/w.
- As in datagram n/w , data are packetized & travels carrying the destination address & as in circuit switching n/w all packets follow the same path established during connection.
- Virtual ckt n/w is normally implemented in data link layer.

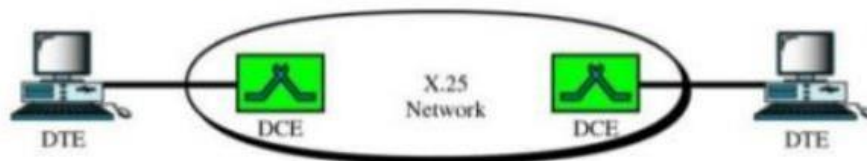
## Virtual-circuit network



### 5.3 X.25

## X.25

- » Packet-switching wide area network developed by ITU-T.
- » X.25 is subscriber network interface (SNI) protocol.
- » Defines how data terminal equipment (DTE) communicates with the network to send packets over it using data circuit-terminating equipment (DCE).
- » It uses virtual circuit approach to packet switching (SVC and PVC).
- » Uses asynchronous TDM to multiplex packets.
- » It describes procedure for establishing, maintaining and terminating connections.



Activate Windows

## Routing in Packet switching

- In packet switching networks, routing is the higher-level decision making that directs network packets from their source toward their destination through intermediate network nodes by specific packet forwarding mechanisms.
- Packet forwarding is the transit of network packets from one network interface to another.

## Congestion

- Network congestion in data networking and queueing theory is the reduced quality of service that occurs when a network node or link is carrying more data than it can handle.
- Typical effects include queueing delay, packet loss or the blocking of new connections.
- A consequence of congestion is that an incremental increase in offered load leads either only to a small increase or even a decrease in network throughput.

## Effects of congestion, congestion control

### Effects of Congestion

- „ Packets arriving are stored at input buffers
- „ Routing decision made
- „ Packet moves to output buffer
- „ Packets queued for output transmitted as fast as possible
- „ Statistical time division multiplexing
- „ If packets arrive too fast to be routed, or to be output, buffers will fill
- „ Can discard packets
- „ Can use flow control
- „ Can propagate congestion through network

## Congestion control

A state occurring in network layer when the message traffic is so heavy that it slows down network response time.

### Effects of Congestion

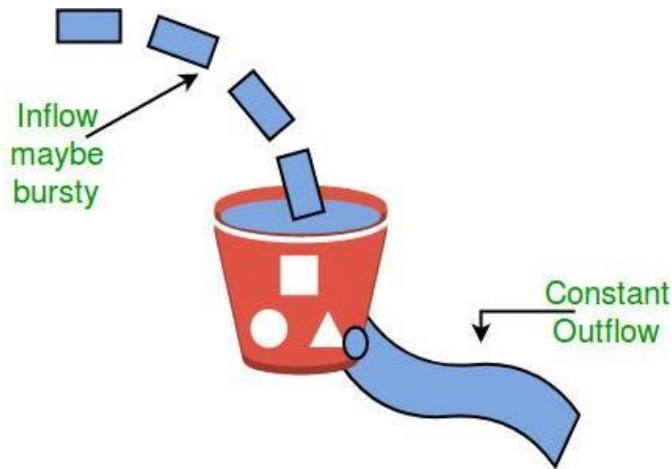
- As delay increases, performance decreases.
- If delay increases, retransmission occurs, making situation worse.

### Congestion control algorithms

- **Leaky Bucket Algorithm**

Let us consider an example to understand

Imagine a bucket with a small hole in the bottom. No matter at what rate water enters the bucket, the outflow is at constant rate. When the bucket is full with water additional water entering spills over the sides and is lost.



Similarly, each network interface contains a leaky bucket and the following **steps** are involved in leaky bucket algorithm:

1. When host wants to send packet, packet is thrown into the bucket.
  2. The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.
  3. Bursty traffic is converted to a uniform traffic by the leaky bucket.
  4. In practice the bucket is a finite queue that outputs at a finite rate.
- **Token bucket Algorithm**

#### **Need of token bucket Algorithm:-**

The leaky bucket algorithm enforces output pattern at the average rate, no matter how burst the traffic is. So, in order to deal with the burst traffic, we need a flexible algorithm so that the data is not lost. One such algorithm is token bucket algorithm.

**Steps** of this algorithm can be described as follows:

1. In regular intervals tokens are thrown into the bucket.
2. The bucket has a maximum capacity.
3. If there is a ready packet, a token is removed from the bucket, and the packet is sent.
4. If there is no token in the bucket, the packet cannot be sent.



## Traffic Management

- Network Traffic Management uses network monitoring tools and management techniques such as bandwidth monitoring, deep packet inspection and application-based routing to ensure optimal network operation.
- In doing so it helps maximise the performance and security of existing networks. It also allows for the identification of network intensive operations that can be incorporated in to network planning and growth strategies.
- Network Traffic Management is used alongside other optimisation techniques like Application Traffic Management as part of an overall Application Delivery Network solution.

## Congestion Control in Packet Switching Network.

- Congestion control in packet-switched data networks is necessary if the performance of the network in the presence of severe overload conditions is to be maintained.
- Such control mechanisms can be functionally divided into: •\* load measurement, •\* informing the users, •\* user reaction, •\* network reaction, if the users do not respond satisfactorily.

## **Short Questions with answers**

### **Q1. What is switching ?**

- In large networks, there can be multiple paths from sender to receiver.
- The switching technique will decide the best route for data transmission.

### **Q2. State the effects of congestion.**

#### **Effects of Congestion**

- As delay increases, performance decreases.
- If delay increases, retransmission occurs, making situation worse.

### **Q3. What is routing in packet switching?**

- In packet switching networks, routing is the higher-level decision making that directs network packets from their source toward their destination through intermediate network nodes by specific packet forwarding mechanisms.
- Packet forwarding is the transit of network packets from one network interface to another

## **Long Questions**

### **Q1. Explain congestion control techniques.**

### **Q2. Differentiate packet switching and circuit switching.**

### **Q3. Explain X.25.**

# ***Chapter-06***

## ***LAN TECHNOLOGY***

### **Network Topology and Transmission Media**

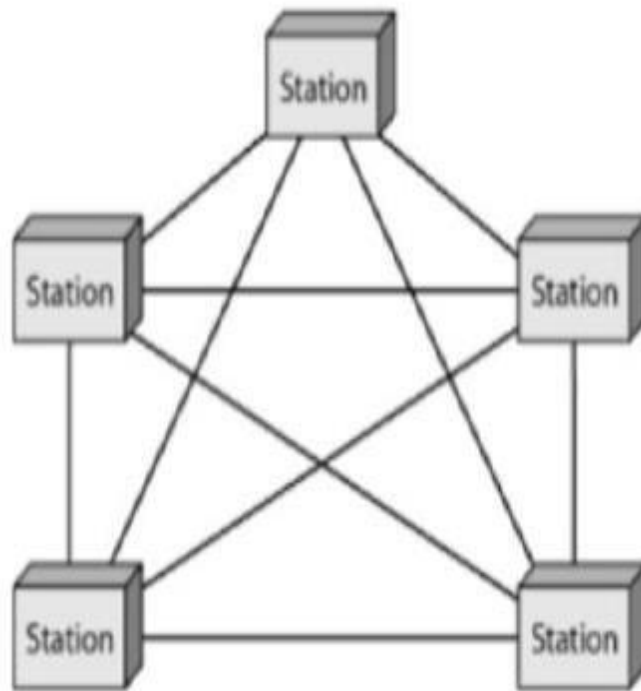
It is the geometric structure of a Network that specifies how the devices are connected with each other through communication links.

- There are 4 types of basic topology.

1. Mesh Topology
2. Star topology
3. Bus topology
4. Ring topology

### **1. Mesh Topology**

- In Mesh Topology , every device has a dedicated point to point link to every other device.
- The term dedicated means the link carries traffic only between the two devices it connects.
- A fully Mesh N/w has  $n(n-1)/2$  no. of physical links to connect  $n$  devices.
- Every device in the N/w must have  $(n-1)$  no. of Input output ports.

**Advantages-:**

- It eliminates traffic problem.
- It is robust in nature.
- It maintains privacy or security.
- Fault identification & fault isolation is easy.

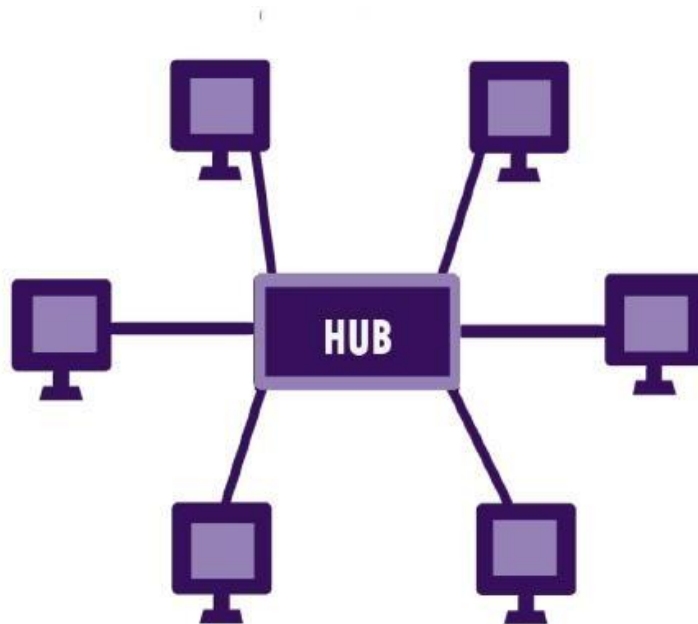
**Disadvantage-:**

- More no. of communication links are needed.
- Installation & reconnection is difficult.

## 2. Star Topology

- In star topology all stations are directly attached to a common central device , known as Hub.

- N links are required to connect N devices in star topology.
- Star topology doesn't allow direct traffic between devices. The hub acts as an exchange.
- If one device wants to send data to another device, it sends data to Hub Which then forwards it to other connected devices.
- The destination device only receives the data.



### **Advantages-:**

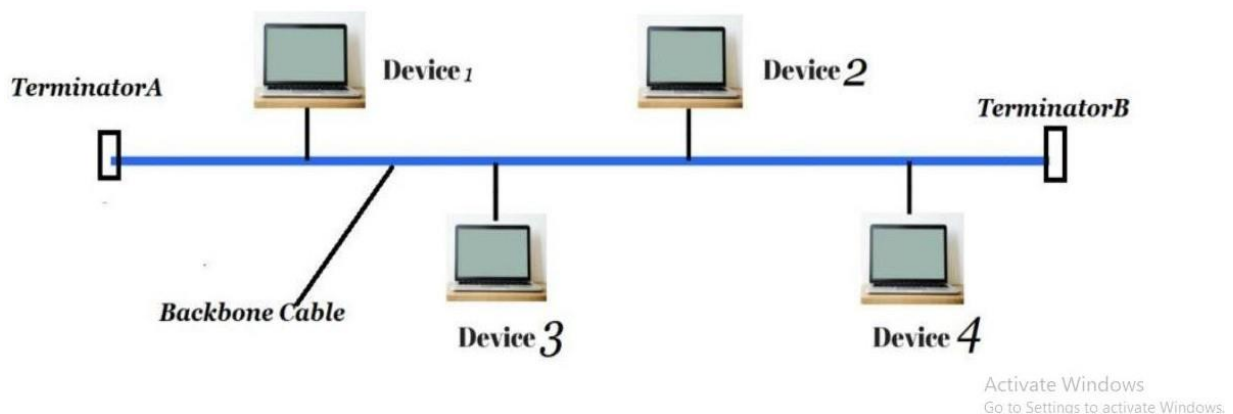
- It is less expensive than mesh topology.
- It is robust in nature.
- Fault identification & isolation is easy.
- Requires less cable than mesh.

### **Disadvantage-:**

- If Hub fails then entire network collapses.

### 3. Bus Topology.

- Bus Topology is a multipoint topology.
- In bus topology there is a main cable and all the devices are connected to this main cable through drop lines.
- There is a device called tap that connects the drop line to the main cable.
- In this topology, the message intended for a device has to pass through other devices present in the network.
- The intended device only receives the message.



#### Advantages:-

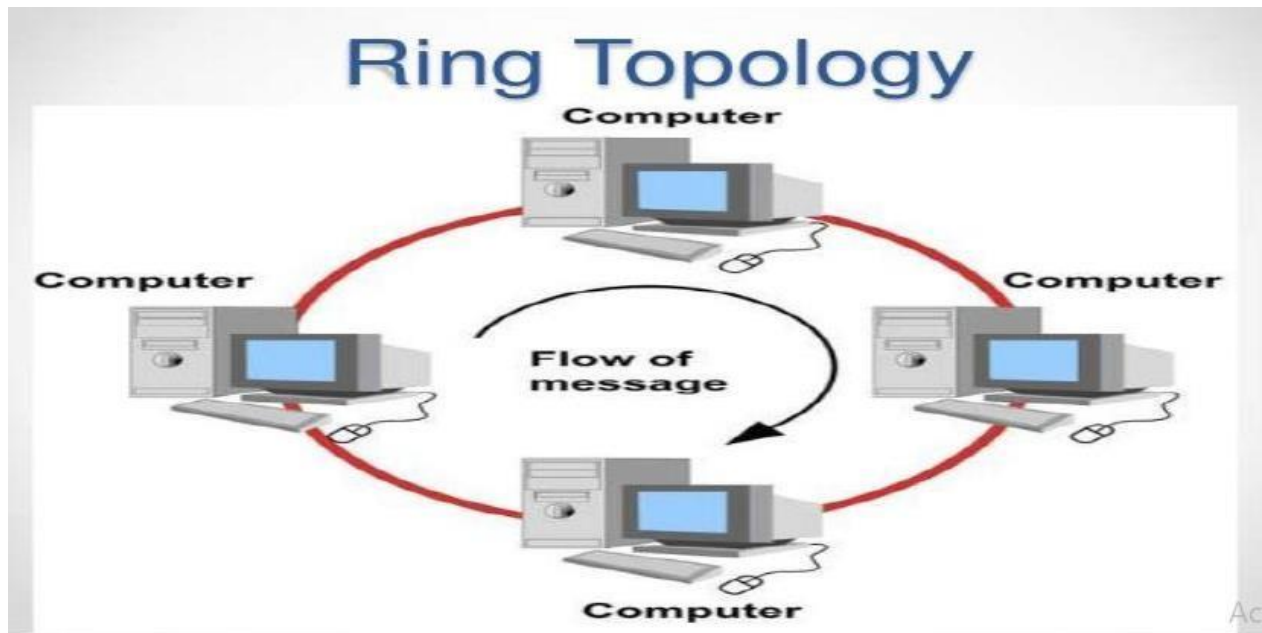
- Installation is easy.
- Less cable is required than Mesh & Star.

#### Disadvantages:-

- Fault detection & isolation is difficult.
- A break in bus cable stops all transmission.

## 4. Ring Topology:

- In ring topology each device is connected with the two devices on either side of it.
- There are two dedicated point to point links a device has with the devices on the either side of it.
- This structure forms a ring thus it is known as ring topology.
- If a device wants to send data to another device then it sends the data in one direction, each device in ring topology has a repeater, if the received data is intended for other device then repeater forwards this data until the intended device receives it.



### Advantages:-

1. Easy to install.

2. Managing is easier as to add or remove a device from the topology only two links are required to be changed.

### **Disadvantages-:**

1. A link failure can fail the entire network as the signal will not travel forward due to failure.
2. Data traffic issues, since all the data is circulating in a ring.

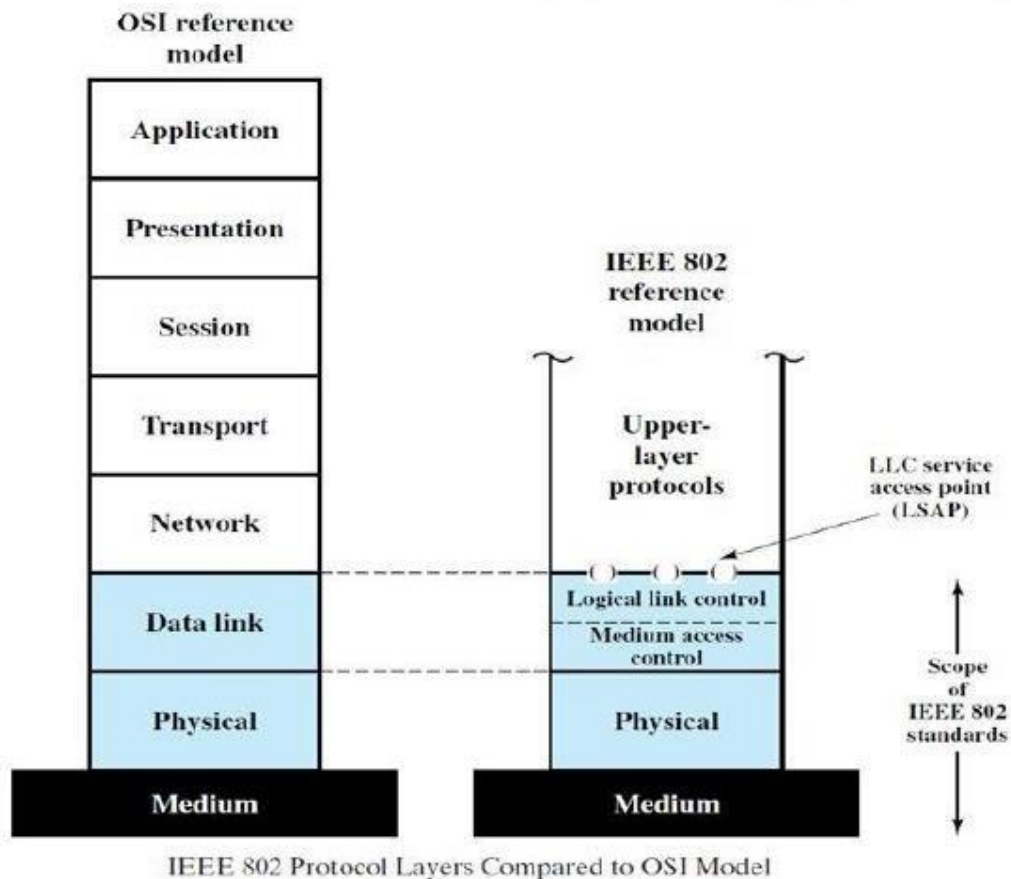
### **Transmission Media**

1. Transmission media is a communication channel that carries the information from the sender to the receiver.
2. Data is transmitted through the electromagnetic signals.
3. The main functionality of the transmission media is to carry the information in the form of bits through LAN(Local Area Network).

## **LAN Protocol Architecture**

- LAN protocol architectures are specified by IEEE 802 reference model.
- In IEEE 802 reference model, there are two separate layers corresponding to data link layer of OSI model.
  - MAC (Medium Access Control) layer.
  - LLC (Logical Link Control) layer.





- **LLC Layer**

- Provide an interface to higher layers
- Flow and error control

- **MAC Layer**

- Interface to physical layer
- Govern access to LAN transmission system
- Sending/receiving frames
- Frame synchronization
- Error detection

- **Physical Layer**

- Specification of the transmission medium and the topology
- Encoding/decoding of signals
- Bit transmission/reception

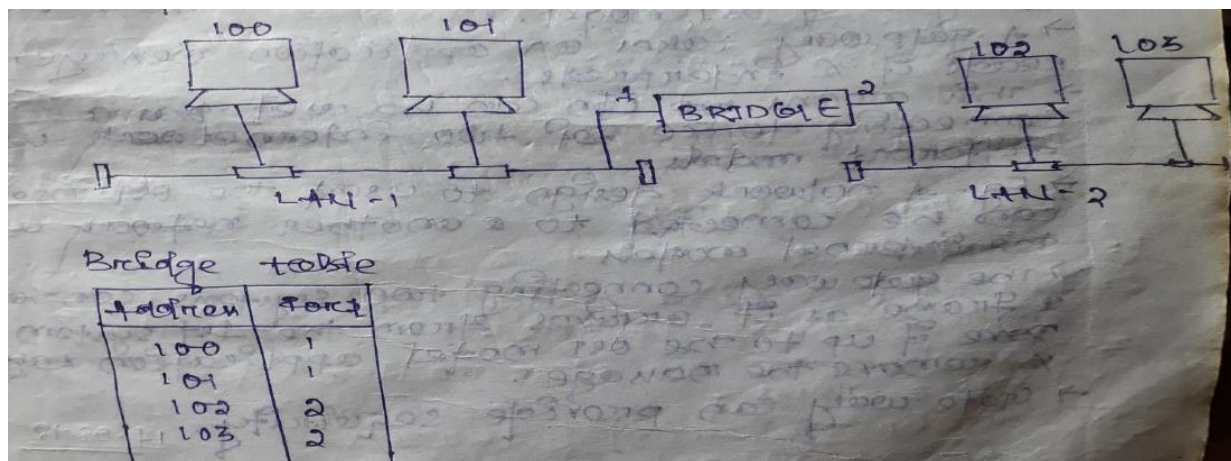
## Medium Access Control

- In Medium Access Control technique , the sender first senses the medium and checks whether the medium is busy or available. If the medium is available , the sender transmits the message over the medium.

## Bridges, Hub, Switch

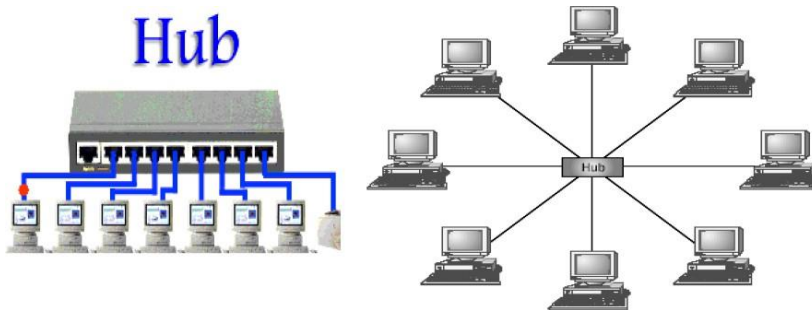
### Bridges:-

- A Bridge operates in both physical & datalink layer.
- As a physical layer device it regenerates the signal it receives , As the datalink layer device , the bridge can check the physical address( Source & Destination) contained in the frame.
- A bridge has filtering capacity which checks the destination address of a frame & decides if the frame should be forwarded or dropped.
- If a frame is to be forwarded , the decision must specify the port.
- A bridge has a table that maps address to ports.
- A bridge can't change the physical address of a frame.



## Hub-:

- Hub is a networking device.
- It works as a repeater.
- Hub performs broadcast, it receives data from 1 port and forwards that to all the ports.
- Now a days people use switches more than hub.
- Hub is not smart as a switch.
- Hub comes with 4,8,16, ports.



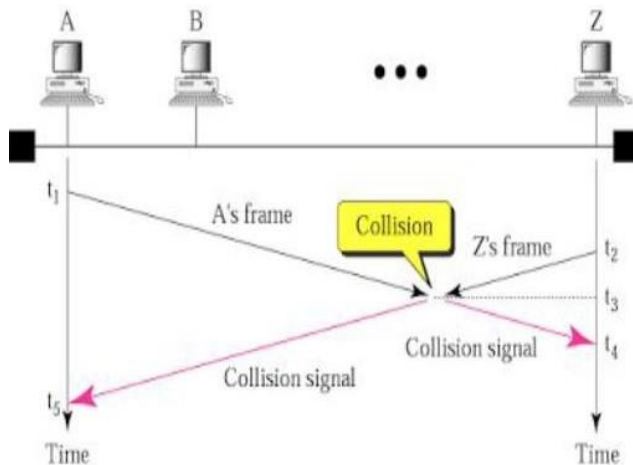
## Switch-:

- A switch is a device in a computer network that connects multiple devices together.
- Switches manage the flow of data across a network by transmitting a received network packet only to the one or more devices for which the packet is intended.
- A switch is more intelligent than an Ethernet hub, which simply retransmits the messages to all other ports connected to it.
- It operates in datalink layer as a layer 2 device as well as in network layer as a router.

## Ethernet (CSMA/CD), Fiber Channel

### Carrier Sense Multiple Access( CSMA)

- It is a medium access control technique .
- Here a station wishing to transmit first senses the medium and transmits only if the medium is available(idle).
- If two or more stations attempt to transmit data at the same time in a single medium , there will be a collision .
- The data from the transmission will be garbled and not received successfully.
- To minimize the chance of collision and to increase the performance, CSMA method was developed.
- By using CSMA method , the station first senses the medium before sending anything to avoid collision.
- CSMA is based on the principle “ **Sense before transmit**” or “**Listen before talk**”.
- **CSMA** can reduce the possibility of collision but can't eliminate it.
- Possibility of collision still exists because of propagation delay.



- At time  $t_1$  station A senses the medium i.e idle so it sends a frame.
- At time  $t_2$  ( $t_2 > t_1$ ) station senses the medium & finds idle because at this time A's frame has not reached station Z due to propagation delay , hence station Z also sends a frame.
- The two signals collide at time  $t_3$  ( $t_3 > t_2 > t_1$ ) which creates a garbled signal or frames are lost.

## WHAT IS CSMA/CD?

```

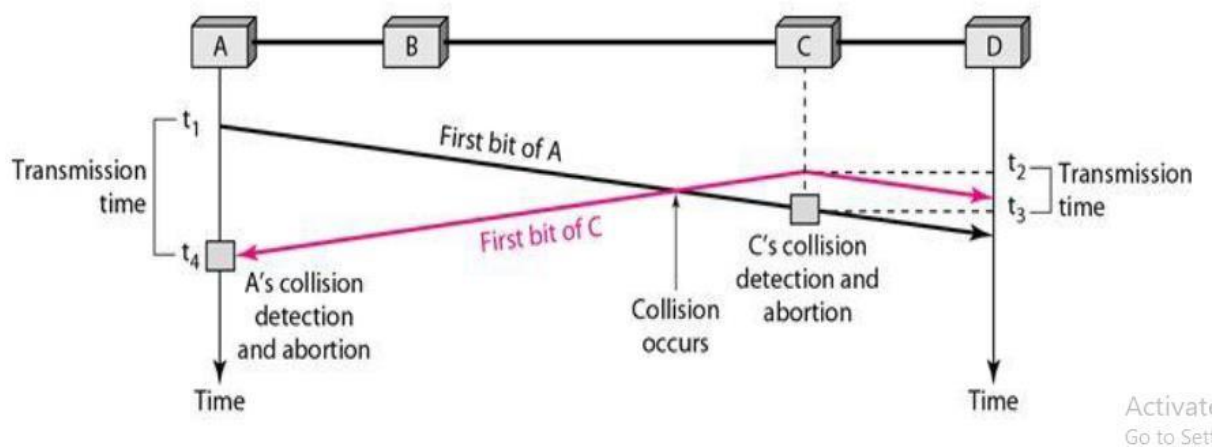
graph LR
    MA[MA] --> CSMA[CSMA]
    CSMA --> CSMA_CD[CSMA/CD]
  
```

- CSMA/CD protocol can be considered as a refinement and modification of pure "Carrier Sense Multiple Access" (CSMA).
- In a CSMA system, the chance of collision can be reduced if a station senses the medium before trying to use it , but it can not eliminate it.
- CSMA/CD is used to improve CSMA performance and it augments the algorithm to handle the collision.

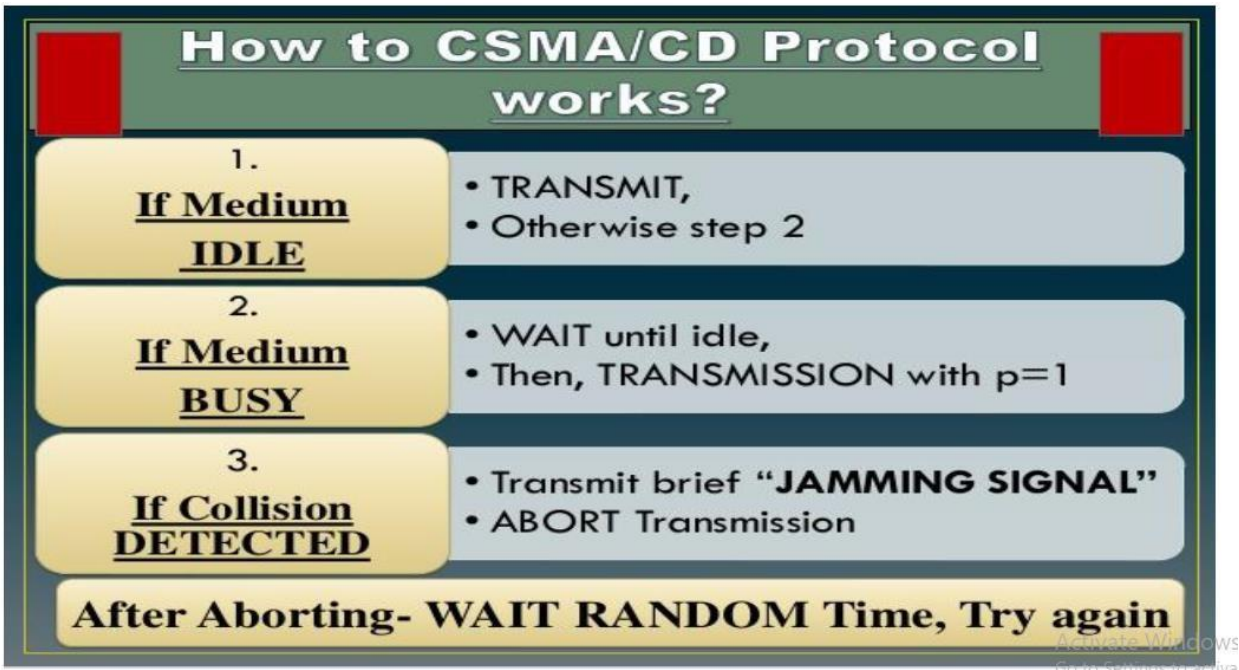
## CSMA/CD - INTRODUCTION

- CARRIER SENSE MULTIPLE ACCESS with COLLISION DETECTION (CSMA/CD) is a MEDIA ACCESS CONTROL method used most notably in early ETHERNET technology for LOCAL AREA NETWORKING.
- This is used in combination with COLLISION DETECTION in which a transmitting station detects collisions by sensing transmissions from other stations while it is transmitting a frame.
- When this collision condition is detected, the station stops transmitting that frame, transmits a jam signal, and then waits for a random time interval before trying to resend the frame.

- In CSMA/CD a station monitors the medium after it sends a frame to see if the transmission is successful. If so the station is finished. If however there is a collision the frame is sent again.







## Wireless LAN Technology

- Wireless technologies enable one or more devices to Communicate without physical connections.
- Wireless technologies use radio frequency transmissions as the means for transmitting data, where as wired technologies use cables.
- Wireless networks are frequently categorized into three groups based on their coverage range:

1. Wireless Wide Area Networks (WWAN),
2. Wireless Local Area Networks (WLAN), and
3. Wireless Personal Area Networks (WPAN).

WLAN is a data transmission system designed to provide location-independent network access between computing devices by using radio waves rather than a cable infrastructure.

## Short questions with answer.

### **Q1. What is network topology?**

It is the geometric structure of a Network that specifies how the devices are connected with each other through communication links.

- There are 4 types of basic topology.

1. Mesh Topology
2. Star topology
3. Bus topology
4. Ring topology

### **Q2. Define MAC.**

1. In Medium Access Control technique, the sender first senses the medium and checks whether the medium is busy or available.
2. If the medium is available, the sender transmits the message over the medium.

### **Q3. Explain wireless LAN technology.**

1. Wireless technologies enable one or more devices to Communicate without physical connections.
2. Wireless technologies use radio frequency transmissions as the means for transmitting data, whereas wired technologies use cables.

## Long Questions

Q1. What is network topology? Explain various types of topology in computer network.

Q2. Explain CSMA/CA

Q3. Explain CSMA/CD



# CHAPTER-07

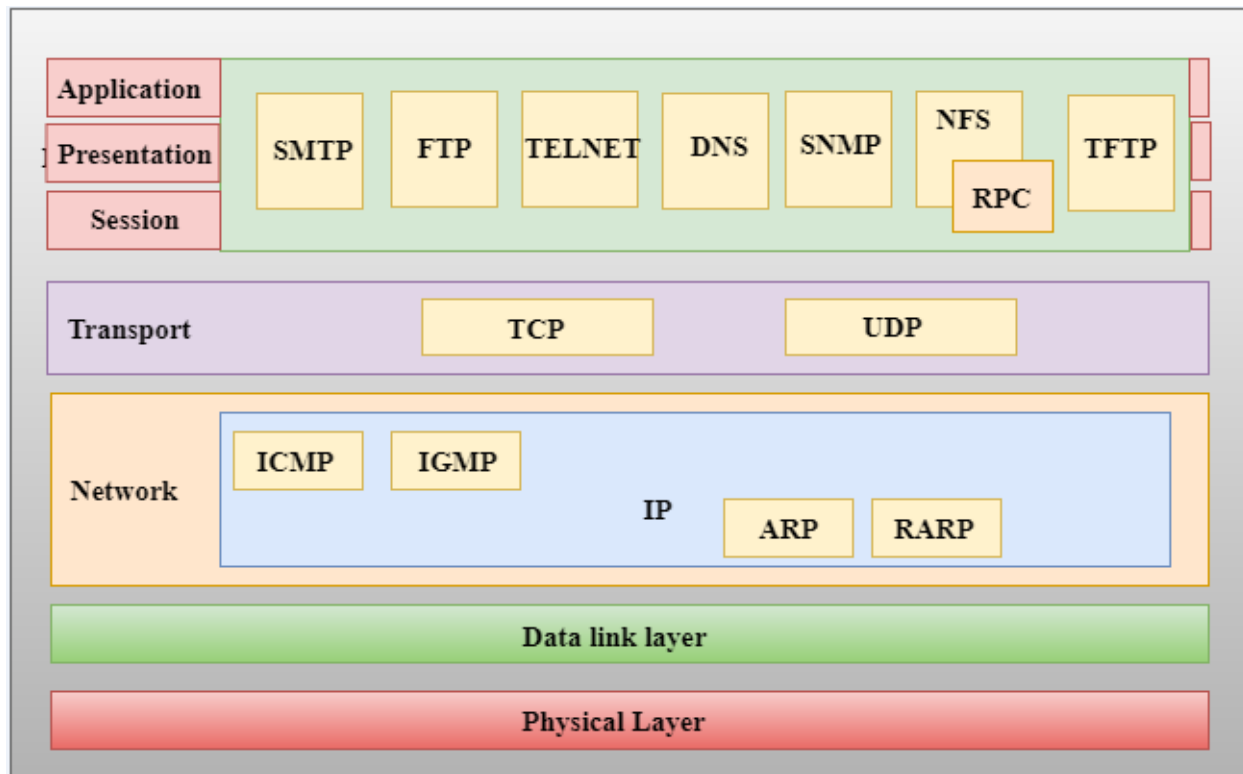
## TCP/IP

### **TCP/IP Protocol Suite**

- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model.
- The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
- The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.
- TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.

Here, hierarchical means that each upper-layer protocol is supported by two or more lower-level protocols.

### **Functions of TCP/IP layers:**



## Basic Protocol functions

### Network Access Layer

- A network layer is the lowest layer of the TCP/IP model.
- A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
- It defines how the data should be sent physically through the network.
- This layer is mainly responsible for the transmission of the data between two devices on the same network.
- The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.

- The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.

## Internet Layer

- An internet layer is the second layer of the TCP/IP model.
- An internet layer is also known as the network layer.
- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.

Following are the protocols used in this layer are:

**IP Protocol:** IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.

Following are the responsibilities of this protocol:

- **IP Addressing:** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.
- **Host-to-host communication:** It determines the path through which the data is to be transmitted.
- **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into a message known as IP datagram.
- **Fragmentation and Reassembly:** The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU). If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the local network. Fragmentation can be done by the sender or intermediate router.

At the receiver side, all the fragments are reassembled to form an original message.

- **Routing:** When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

### **ARP Protocol**

- ARP stands for **Address Resolution Protocol**.
- ARP is a network layer protocol which is used to find the physical address from the IP address.
- **The two terms are mainly associated with the ARP Protocol:**
  - **ARP request:** When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.
  - **ARP reply:** Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header

### **ICMP Protocol**

- **ICMP** stands for Internet Control Message Protocol.
- It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.

- A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.
  - An ICMP protocol mainly uses two terms:
    - **ICMP Test:** ICMP Test is used to test whether the destination is reachable or not.
    - **ICMP Reply:** ICMP Reply is used to check whether the destination device is responding or not.
  - The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.
  - ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the addresses of the source and destination but not of the router that it is passed to.
- 

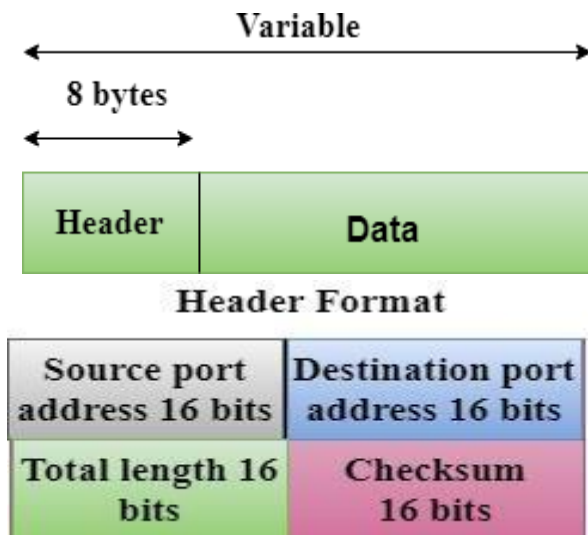
## Transport Layer

The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.

The two protocols used in the transport layer are **User Datagram protocol and Transmission control protocol.**

- **User Datagram Protocol (UDP)**
  - It provides connectionless service and end-to-end delivery of transmission.
  - It is an unreliable protocol as it discovers the errors but does not specify the error.

- User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.
- **UDP consists of the following fields:**
  - Source port address:** The source port address is the address of the application program that has created the message.
  - Destination port address:** The destination port address is the address of the application program that receives the message.
  - Total length:** It defines the total number of bytes of the user datagram in bytes.
  - Checksum:** The checksum is a 16-bit field used in error detection.
- UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment.



- **Transmission Control Protocol (TCP)**

- It provides a full transport layer services to applications.
- It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.

- TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.
  - At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.
  - At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.
- 

## Application Layer

- An application layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- There is an ambiguity occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system. For example: text editor cannot be considered in application layer while web browser using **HTTP** protocol to interact with the network where **HTTP** protocol is an application layer protocol.

Following are the main protocols used in the application layer:

- **HTTP:** HTTP stands for Hypertext transfer protocol. This protocol allows us to access the data over the world wide web. It transfers the data in the form of

plain text, audio, video. It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.

- **SNMP:** SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.
- **SMTP:** SMTP stands for Simple mail transfer protocol. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.
- **DNS:** DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.
- **TELNET:** It is an abbreviation for Terminal Network. It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.
- **FTP:** FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.

## Principles of Internetworking

The Internet Protocol (IP) is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet. The Internet protocol suite is therefore often referred to as TCP/IP.



## Internet Protocol operations

**IP Protocol:** IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.

Following are the responsibilities of this protocol:

- **IP Addressing:** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.
- **Host-to-host communication:** It determines the path through which the data is to be transmitted.
- **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into a message known as IP datagram.
- **Fragmentation and Reassembly:** The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU). If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the local network. Fragmentation can be done by the sender or intermediate router. At the receiver side, all the fragments are reassembled to form an original message.
- **Routing:** When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

## ARP Protocol

- ARP stands for **Address Resolution Protocol**.
- ARP is a network layer protocol which is used to find the physical address from the IP address.
- **The two terms are mainly associated with the ARP Protocol:**
  - **ARP request:** When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.
  - **ARP reply:** Every device attached to the network will accept the ARP request and process the request, but only the recipient recognizes the IP address and sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header

## **ICMP Protocol**

- ICMP stands for Internet Control Message Protocol.
- It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
- A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.
- An ICMP protocol mainly uses two terms:
  - **ICMP Test:** ICMP Test is used to test whether the destination is reachable or not.
  - **ICMP Reply:** ICMP Reply is used to check whether the destination device is responding or not.

- The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.
- ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the addresses of the source and destination but not of the router that it is passed to.

## Internet Protocol

- The **Internet Protocol (IP)** is the principal communications **protocol** in the **Internet protocol** suite for relaying datagrams across network boundaries.
- Its routing function enables internetworking, and essentially establishes the **Internet**. The **Internet protocol** suite is therefore often referred to as **TCP/IP**.

## **Short questions with answer**

### **Q1. Define ARP protocol.**

#### **ARP Protocol**

- ARP stands for **Address Resolution Protocol**.
- ARP is a network layer protocol which is used to find the physical address from the IP address.

### **Q2.What is ICMP?**

- ICMP stands for Internet Control Message Protocol.
- It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.

## **Long Questions**

### **Q1. Explain TCP/IP protocol suite.**

### **Q2. Explain internet protocol operations.**