Data Communication:

When we communicate we are sharing information. This sharing can be local or remote.

- Local communication occur between individuals (face to face communication.
- Remote communication take place over distance which includ telephony, telegraphy, television means the communication at a distance. (derived from telecommunication)

- Data communication is the exchange of data between two devices via some form of transmission medium such as wire cable.
- For data communication to occur the communicating devices must be a part of communication system made up of a combination of h/w and s/w.
- The effectiveness of a data communication depends on three fundamental characteristic:

i. Delivery: The system must deliver data to correct destination. Data must be received by intended device or user and only by that device or user.

ii. Accuracy: The system must deliver the data accurately Data that have been altered in transmissior and left uncorrected are unusable.

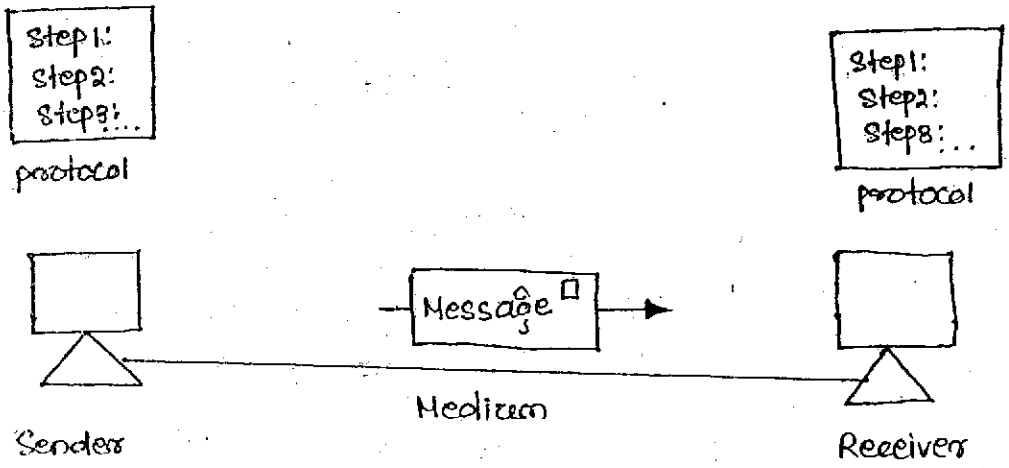
iii. Timelines: The system must deliver data in timely manner. Data delivered late are useless data. Delivering video and audio timely means, in the same order as they are produced.

This kind of delivery is called real-time transmission.

Components:

A data communication system has five components

i. Message
ii. Sender
iii. Receiver
iv. Medium
v. Protocol



FIVE COMPONENTS OF DATA COMMUNICATION

1. Message: Message is the information to be communicated. It can consist of text, numbers, pictures, sound or video, or any combination of these.
2. Sender: The sender is the device that sends the data message. It can be computer, workstation, telephone handset, video camera and so on.
3. Receiver: The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television and so on.
4. Medium: The transmission medium is the physical path by which a message travels from sender to receiver. It can be a twisted-pair cable, co-axial cable,

fiber optic cable or radio waves.

5. Protocol: A protocol is a set of rules that governs data communication. It represents an agreement between the communicating devices. Without a protocol two devices may be connected but not communicating.

Data Representation:

Information can be in different forms such as text, numbers, images, audio and video.

Text:

In data communication text is represented as bit patterns (0s and 1s). The no. of bits depend upon the no. of symbols in the language. Different set of bit patterns have been designed to represent text symbols. Each set is called a code, and the process of representing symbol is called coding.

ASCII:

The American National Standard Institute (ANSI) developed a code called American Standard Code for Information Interchange (ASCII). This uses 7 bit for each symbol. i.e 128 (2^7) different symbols can be defined by this code.

Extended ASCII

To make the size of each pattern 1 byte (8 bits), the ASCII bit pattern are augmented with an extra 0 at the left.

Unicode

To represent the languages other than English, the h/w and s/w manufacturers have designed a code called Unicode that uses 16 bits and can represent upto 65,536 (2^{16}) symbols.

ISO:

The international organization for Standardization (ISO) has designed a code using 32 bit pattern. This code can represent 4,294,967,296 (2^{32}) symbols.

Numbers:

Numbers are also represented by using bit patterns. A code such as ASCII is not used to represent numbers, the no is directly converted to a binary no.

Images:

Images can also be represented by bit patterns. Mechanism of representation is different.

Audio:

Audio is representation of sound. It is continuous not discreate.

Video:

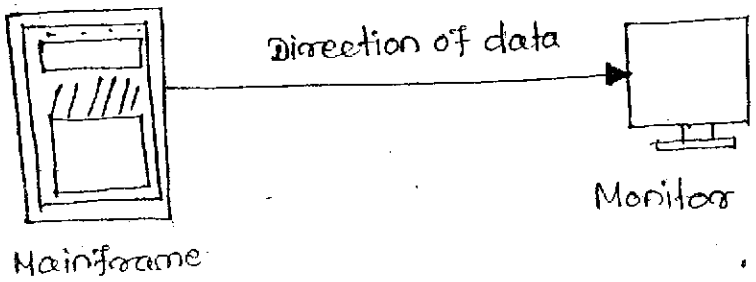
Video can be produced either as a continuous entity or it can be a combination of images, each is a discreate entity, arranged to convey the idea of motion.

Direction of Data Flow: ✓

Communication between two devices can be

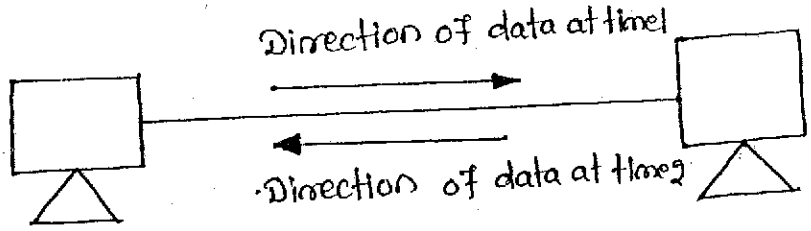
(i) Simplex (ii) Half-duplex (iii) Full Duplex

Simplex:



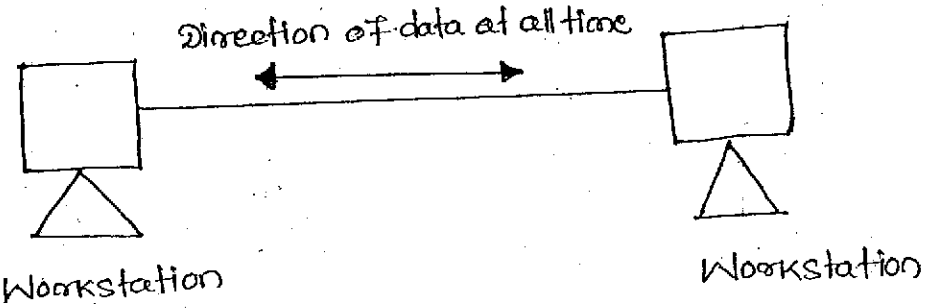
- In simplex mode, the communication is unidirectional as on a one way street.
- Only one of the two device on a link can transmit, the other can only receive.
- Ex: The keyboards and traditional monitors, the keyboard can only introduce I/p, the monitor can only accept O/p.

Half Duplex:



- In half duplex mode each station can both transmit and receive but not at the same time.
- When one device is sending, the other only can receive and vice-versa.
- Its like a one-lane road with two directional traffic. i.e while cars are travelling in one direction cars going on other way must wait.
- The entire capacity of a channel is taken over by which ever the two devices is transmitting at that time.
- Ex: Walkie-talkies and CB (citizens band) radios.

Full-Duplex:



- In full duplex (duplex) both stations can transmit and receive simultaneously. (like a two way street with traffic following both direction at same time).
- Signal going in either direction share the capacity of link.
- The sharing can occur in two ways: Either the link must contain two physically separate transmission path one for sending and other for receiving or the capacity of channel is divided between signals travelling in both direction.
- Ex: Telephone Network.

NETWORKS

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

- Distributed Processing:

Most networks are distributed processing in which a task is divided among multiple computers. Instead of one single machine being responsible for all aspect of a process, separate computer handle a subset.

Network Criteria:

A network must meet certain criteria.

(i) Performance:

- It can be measured in many ways including transmit time and response time.
- Transmit time is the amount of time required for a message to travel from one device to other.

- Response time is the elapsed time between a response and inquiry.

- Performance of a network depend upon many factors like no. of users, types of transmission medium, capabilities of h/w, efficiencies of s/w etc.

- Performance is evaluated by two networking metrics through puts and delay.

- Performance always need more throughput and less delay.

(ii) Relaibility:-

- Network relaibility is measured by the frequency of failure, the time it takes a link to recover from failure.

(iii) Security:-

- Network security include protecting data from unauthorised access, protecting data from damage and developement and implimenting policy and procedures for recovery from breaches and data losses.

Physical Structure:-

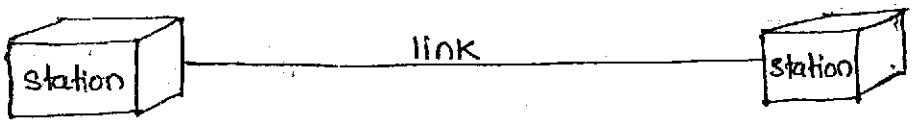
Type of connection:-

- A network is two or more devices connected by a link. A link is a communication path way that transpher data from one device to another.
- There are two posible type of connection.
  - point to point.
  - multipoint.

Point to point:-

- A point to point connection provide a dedicated link between two devices.
- Entire capacity of the link is reserved for transmission between those two devices.
- It use an actual length of wire or cable to connect two ends.
- Eg:

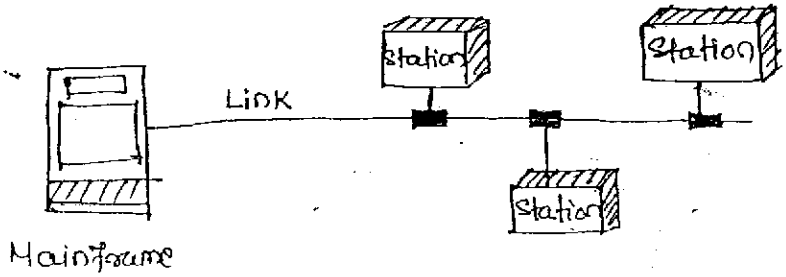
  When TV channels are changed by infrared remote control, a point to point connection is established between the remote control and TV control system.



point to point.

- Multipoint:

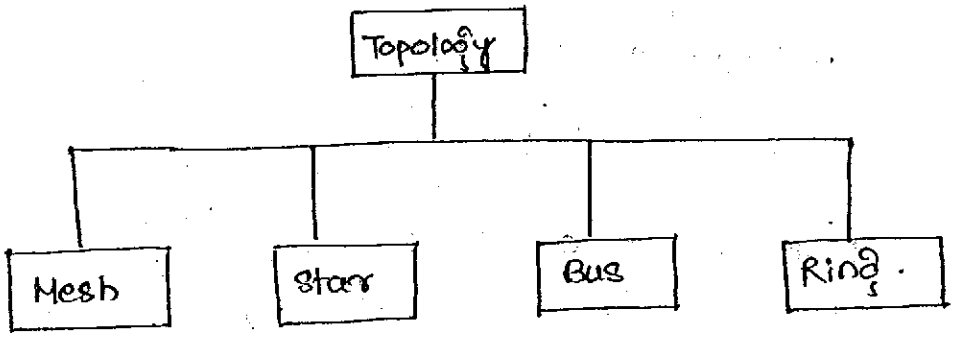
- A multipoint/multidrop connection is one, in which more than two specific device share a single link.
- In a multipoint environment the capacity of the channel is shared either spatially or temporally.
- If several devices can use the link simultaneously it is spatially shared connection.
- If users must take turn, it is time-shared connection.



Multipoint

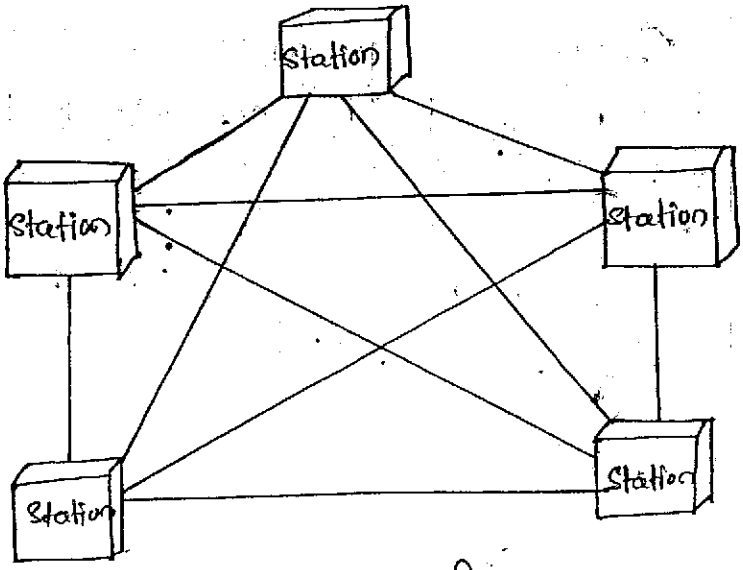
Physical topology:-

- The term physical topology refered to the way in which the n/w is laid out physically.
- Two or more devices connect to link, two or more links form a topology.
- The topology of a n/w is the geometric representation of the relationship of all the links and linking devices to one another.
- type of topology



Mesh Topology:

- In a mesh topology every device has a dedicated point-to-point link to every other device.
- The dedicated means the link carries traffic only between the two devices it connects.



Mesh Topology:

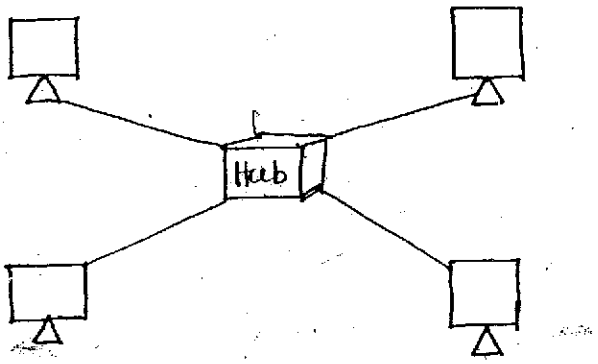
- No. of physical link in a fully connected mesh network with n nodes = $n(n-1)$ i.e in a mesh topology we need $\frac{n(n-1)}{2}$ duplex-mode link.
- Every device on the n/w must have $(n-1)$ no. of I/O ports connected to other $(n-1)$ stations.
- Advantages:
  - It eliminates traffic problems due to the use of dedicated link that carry its own data load.
  - It is robust i.e if one link become unusable, it doesn't incapacitate the entire system.
  - It maintain privacy or security.
- Disadvantages:
  - It requires high amount of cabling and high no. of I/O ports.
  - Installation and reconnection of new devices to the topology are difficult.
  - It is expensive in nature and require more space to be implemented.
- Example:

Connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

For the above reasons mesh topology is used in a limited fashion.

Star Topology:-

- Each device has a dedicated point-to-point link only to a central controller, usually called a hub.
- This device are not directly linked to one another.
- It doesn't allow direct traffic between devices.
- The controller act as an exchanger.
- If one device want to send data to another, it send data to the controller, which then relays the data to other connected device.

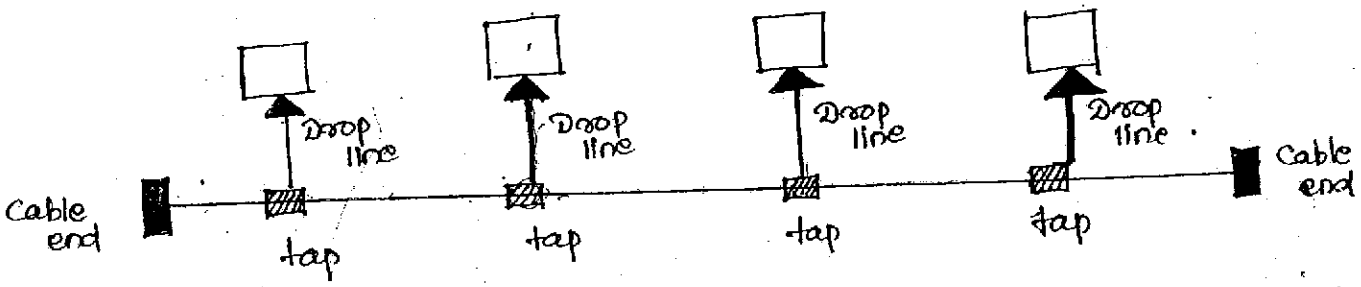


Star Topology:

- Advantage:
  - It is less expensive than a mesh topology as each device needs only one link and one I/O port to connect to any no. of devices.
  - Addition, moving, deletion of devices needs only one connection i.e between the hub and the device.
  - It is robust, because if one link fails only that link is affected.
  - Easy to identify a fault and isolate it.
  - Requirement of cables are more but comparatively less than mesh topology.

Bus Topologys:-

- A bus topology is a example of multipoint connection. One long cable act as a backbone to link all the device in the network.
- Nodes are connected to the bus cable by drop lines or taps.
- A drop line is a connection running between the device and the main cable.
- A tap is a connector that either splices into main cable or punctures the sheathing of a cable to create a contact with metallic core.
- As a single travel, some of its energy is transformed into heat.



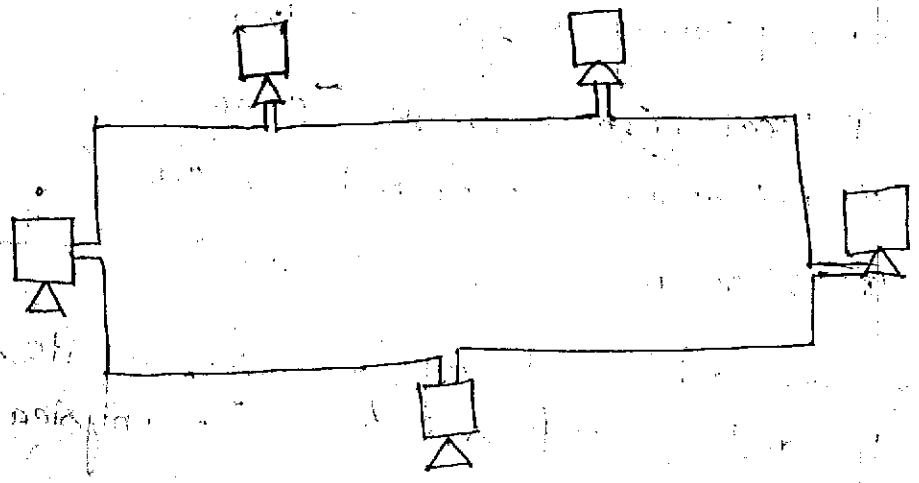
Bus Topology:

- It becomes weaker and weaker as it travels farther and farther.
- So there is a limit on the no. of taps a bus can support and the distance between those taps.
- Advantages:
  - Easy to install
  - A bus topology uses less cables than mesh or star topology

- Disadvantages:
  - It include difficulty in reconnection and fault isolation.
  - Difficult to add new devices to the n/w. Adding devices may require modification or replacement of backbone.
  - Single reflection on the tap cause degradation in quality. It can be controlled by limiting the number and spacing of devices connected to a given length of cable.
  - Fault or break in the bus cable stops all transmission. The damaged area reflects signals back in the direction of origin, creating noise in both direction.

Ring Topology:-

- Each device has a point to point connection only with two devices on either side of it.
- A signal is passed along the ring in one direction from device to device, until it reaches its destination
- Each device in the ring incorporates a repeater.
- When a device receives a signal intended for another device its repeater regenerates the beat and passes them along.



7873034437

- A ring topology is relatively easy to install and configure.
- As each device is linked to its immediate neighbours to add or delete a device requires changing two connection.
- The only constraints are media and no. of traffic considiration.
- Easy to isolate a fault.
- A ring is circulating at all time within the n/w. If one device doesn't receive a signal within a specified period it can issue an alarm.
- The alarm alerts the network operations to the problem and its location.

Disadvantages:—

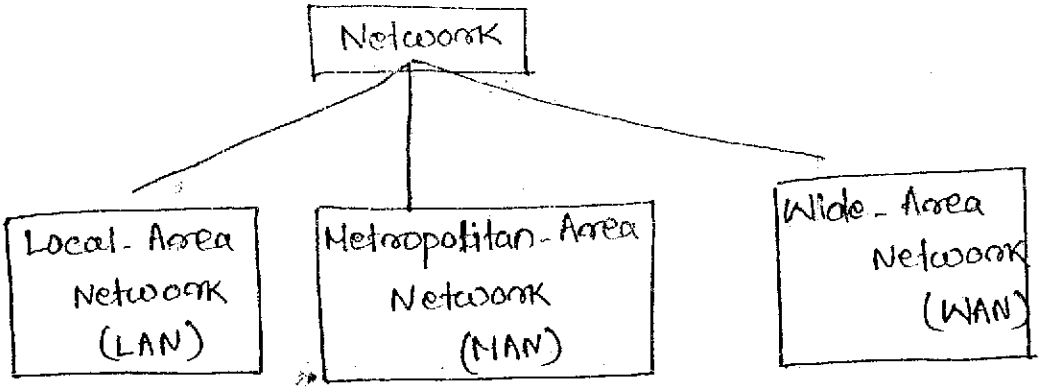
- Unidirectional traffic can be a disadvantage.
- In a ring topology a break in the ring can disable the entire n/w. It can be covered by using a dual ring or switch capable of closing off the break.

Categories of n/w:

There are three primary categories of n/w

(i) Local Area Network (LAN)
(ii) Metropolitan Area Network (MAN)
(iii) Wide Area Network (WAN)

- A n/w comes render which category determined by its size, its ownership, the distance it cover and its physical architecture.



Local_Area Network (LAN):

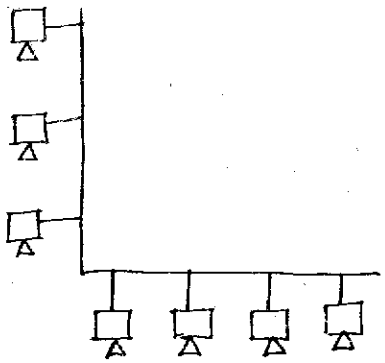
- A LAN is usually privately owned and links the devices in a single office, building or campus.
- LAN size is limited within a few K.m.
- LANs are designed to allow resources to be shared between personal computers or workstations.
- Resources to be shared include h/w (printer) s/w (application program) or data.
- Example:

  Engineering workstations or accounting pcs.

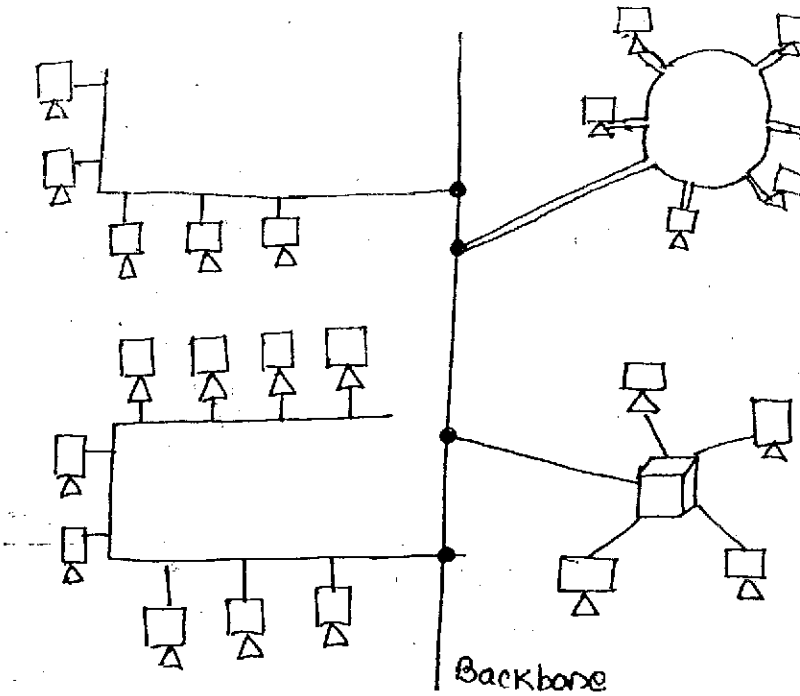
  Here one of the computer may be given a large capacity of disk drive and may become a server to other clients. S/w can be stored in the server and used by the whole group.
- A given LAN will only use one copy of transmission medium.

✓The most common LAN topologies are bus, ring and star.

- LANs have date rates in the 4 to 16 megabits per second. However speeds are increasing and can reach 100 Mbps with gigabits systems in developement.



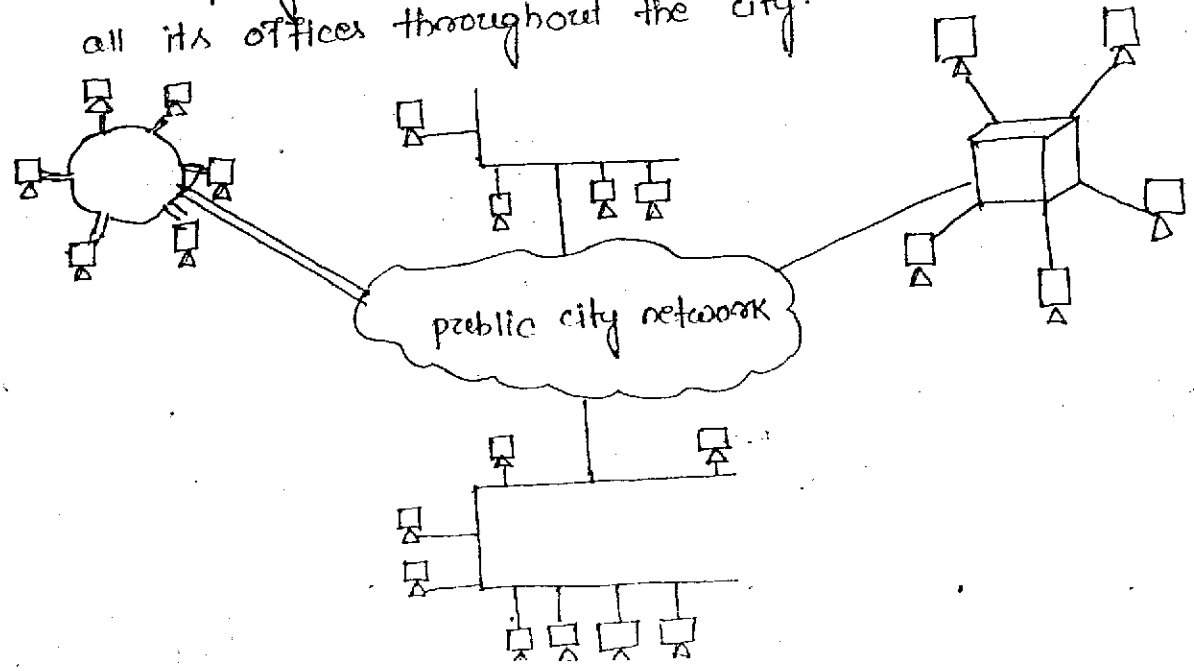
Single building LAN



Multiple building LAN

Metropolitan Area Network:-

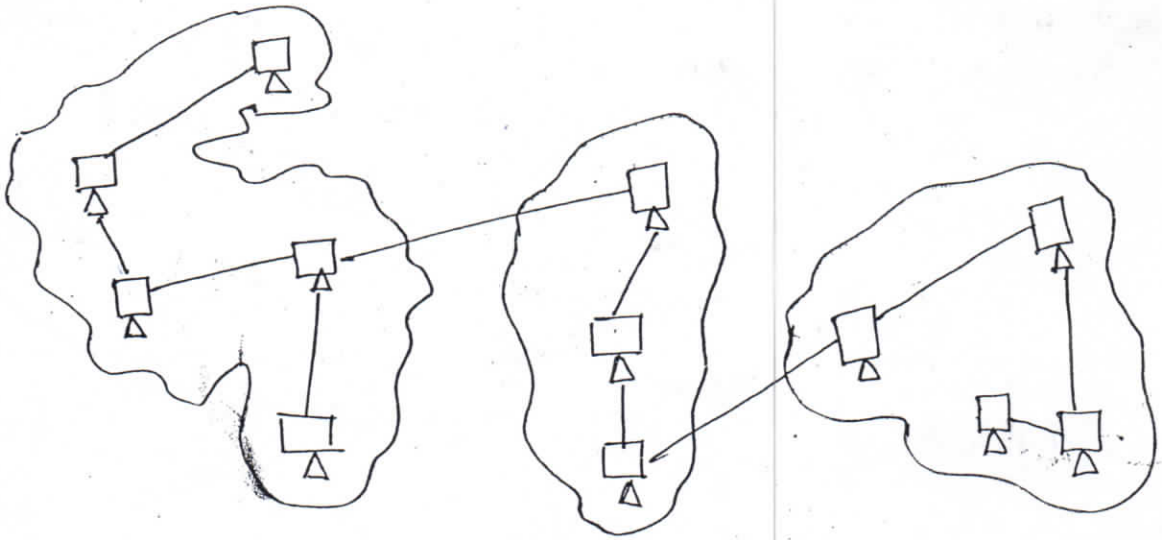
- It is designed to extend over the entire city.
- It may be a single n/w such as cable television n/w or it may be a means of connecting a no. of LANs into a larger n/w so that resource may be shared LAN to LAN as well as device-to-device.
- Example:-
  A company can use a MAN to connect the LANs in all its offices throughout the city.



- A MAN may be wholly owned and operated by a private company or it may be a service provided by public company, such as a telephone company. Many telephone companies provid a popular MAN service called Switched Multi-megabit Data Services (SMDS)

Wide Area Network (WAN):

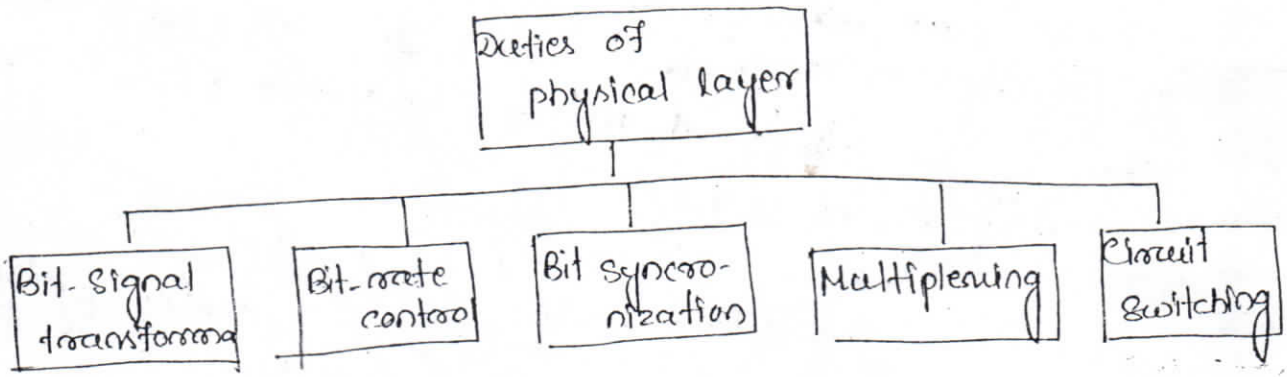
- It provides long distance transmission of data, voice, images and video information over large geographic areas, that may comprise a country, a continent or even the whole world.
- WAN utilize public leased or private communication equipme in combination and can therefore span an unlimited no. of miles.
- A WAN that is wholly owned and used by single compa is often refered to as enterprise network.
- When two or more networks are connected they become a internetwork or internet.



PHYSICAL LAYER

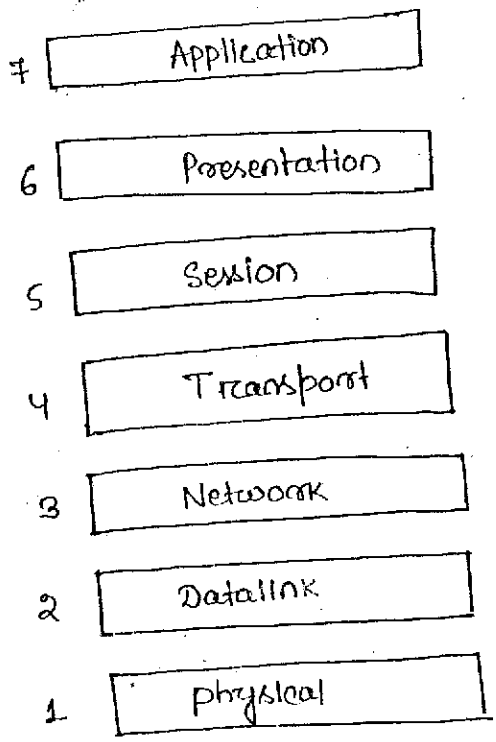
- Physical layer is the bottom most layer of internet model which actually interacts with the transmission media.
- It physically carries information from one node to the next in the n/w.
- It provide services for the data link layer. The data in the data link layer consist of 0's and 1's organized into frames that are ready to sent across transmission medium
- This stream of 0s and 1s must first be converted into another entity called signal.
- Physical layer create a signal that represent this stream of bits.
- Physical layer take care of physical network, control the transmission medium and decides the direction of data flow.

Services:-



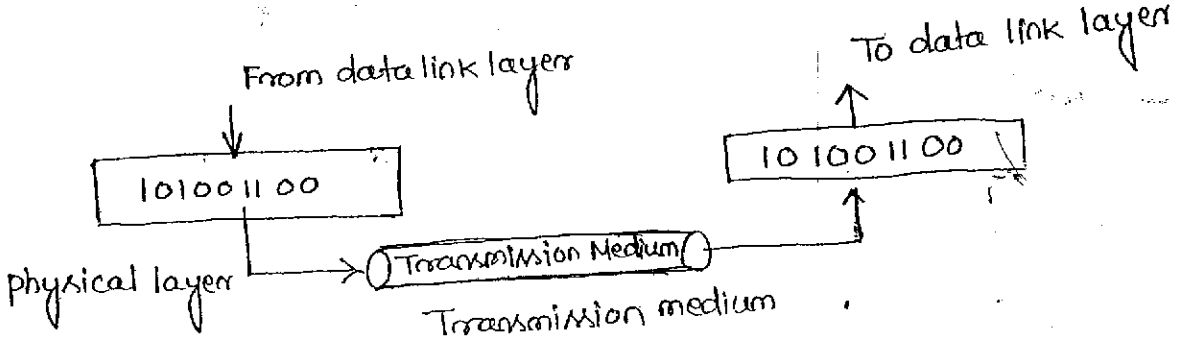
OSI MODEL

- An open system interconnection or osi model was designed by ISO.
- osi model is a theoretical model designed to show how a protocol stack should be implemented.
- osi model consist of 7 layers.



Physical Layer:-

- physical layer co-ordinates the functions required to transpher a bit stream over a physical medium. It deals with the mechanical and electrical specification of the interface and transmission media and defines the procedure and functions that physical device and medium has to perform for transmission to occur.



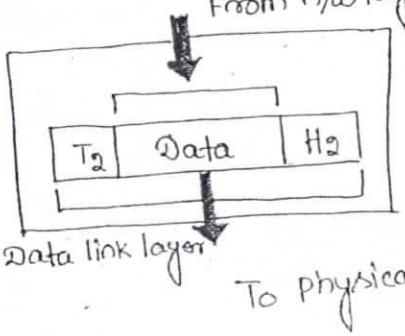
- physical layer is responsible for transmitting individual bits from one node to next.

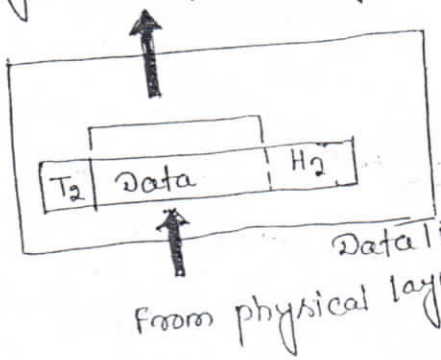
MAJOR DUTIES:

- physical characteristics of interface and media:
  → It defines the characteristics of the interface between the device and transmission media.
  → It also defines the types of transmission medium.
- Representation of bits:
  → physical layer data consist of 0's and 1's. To be transmitted bits must be converted to signal (electrical or optical)
  → It defines the types of representation. (how 0's and 1's are changed to signal.
- Data Rate:
  → Transmission rate: the no. of bits for each second is also defined by physical layer. Defines the duration of bits
- Syncronization of Bits.
  → The sender and receiver must be syncronized at bit level. Sender and Receiver clocks must be syncronized.

Data link layer:-

Data link layer is responsible for transmitting frames from one node to the next. It make the physical layer appear error free to the upper layer.





MAJOR DUTIES:

- Framing:
  → The data link layer devides the stream of bits received from the n/w layer into manageable data units called frames.
- Physical addressing:
  → If frames are distributed to different systems on the n/w the data link layer adds a header to the frame to define the sender and/or receiver of the frame.
  → If the frame is intended for a system outside the sender network, the receiver address is the address of connecting device that connects the n/w to the next one.
- Flow control:
  → If the rate at which the data are absorbed by the receiver is less than the rate produced in the sender the data link layer imposes a flow control mechanism
- Error control:
  → The data link layer adds relaibility to the physical layer by adding mechanism to detect and retransmit damaged or lost frames, and also to prevent duplication of frames.
  → It is achived through a trailer added to the end of the frame.
- Access control:
  → When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

Network layer:-

It is responsible for source to destination delivery of a packet across multiple networks, where data link layer is responsible for delivery of the packets between two systems in the same network.

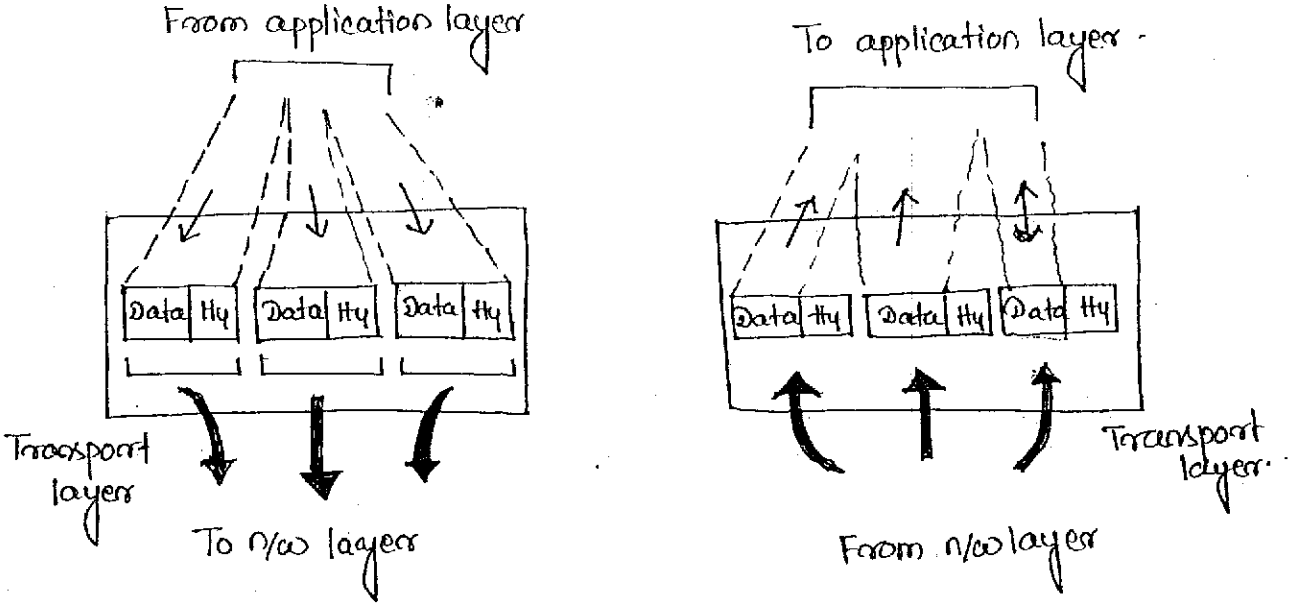
Network layer is responsible for the delivery of packets from original source to final destination.

MAJOR DUTIES:

- **Logical Addressing:**
  - → If a packet passes a network boundary, we need another addressing system to help to distinguish the source and destination system.
  - → The n/w layer adds a header to the packet coming from the upper layer, includes the logical addressing of the sender and receiver.
- **Routing:**
  - → When independent n/ws or links are connected to create an internetwork (network of network) the connecting devices (routers or switches) route or switch the packets to their final destination. One of the function of n/w layer is to provide this mechanism.

Transport layer:-

- Transport layer is responsible for process to process delivery of the entire message, whereas as the n/w layer oversees host-to-destination delivery of individual packets.



MAJOR DUTIES:

- **Port Addressing:**
  - → Computers often run several processes at the time. A process-to-process delivery means delivery not only from one computer to the next but also a specific process on one computer to a specific process on other. The transport layer must therefore include a type of address called a port address.
- **Segmentation and reassembly:**
  - → A message is divided into transmittable segments each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arrival at the destination and to identify and replace packets that were lost in the transmission.
- **Connection Control:**
  - → A transport layer can be either connection less or connection oriented.

→ A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine.

→ A connection oriented transport layer makes a connection with the transport layer at the destination machine first before delivering packets. After all the data are transfered, the connection is terminated.

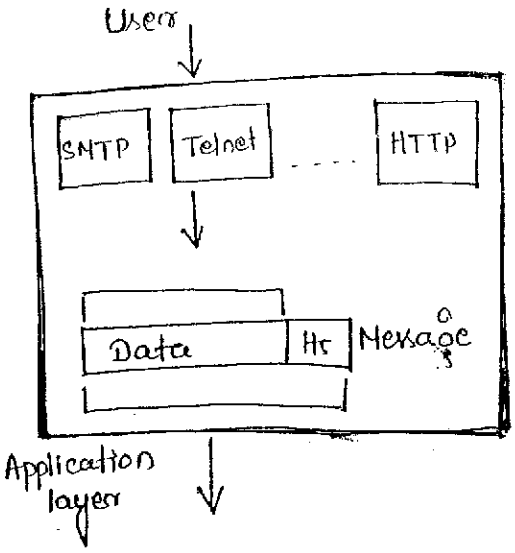
- Flow control:
  → Flow control at this layer is performed end to end rather than a single link.

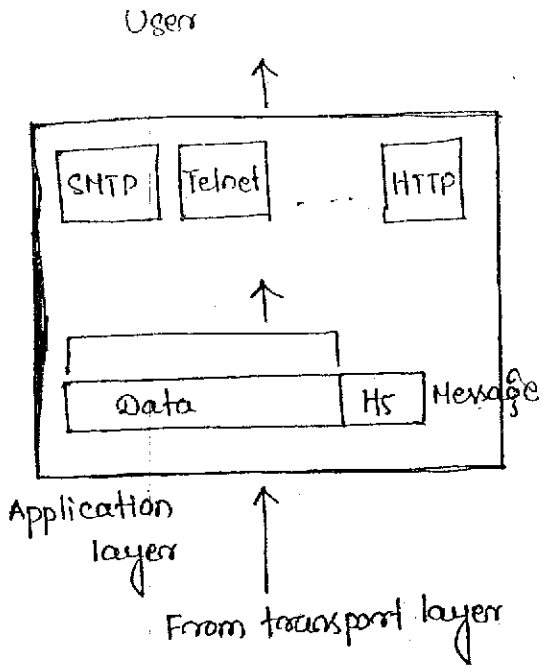
- Error Control:
  → Error control at this layer is performed end to end rather than a single link.

- Session layer:
  → Session layer is the n/w is the n/w diabo controller.
  → It was designed to establish, mentain and syncronize the interaction between communicating system.

- presentation layer:-
  → It was designed to handle the syntax and semantics of information exchanged between the two system
  → Designed for data translation, encryption, decryption and compression.

- Application layer:
  Application layer enables the user to access the n/w. It is responsible for providing services like e-mail, remote file access and transpher, access to WWW and so on.





MAJOR DUTIES:

- Mail Services:
  → This application is the basis for email forwarding and storage
- File Transfer and Access:
  → This application allows a user to access files in a remote host (to make changes or read data), to receive files from a remote computer for user in a local computer and to manage or control files in a remote computer locality.
- Remote log in:
  → A user can log in to remote computer and access the resources of that computer.
- Accessing the World Wide Web:
  → The most common application today is the access of WWW.

MAJOR DUTIES OF SESSION LAYER:

- Dialog Control:—
  → It allows two system to enter into a dialog. It allows the communication between two processes to take place either in half duplex or full duplex mode. e.g: dialog bet^n a termina

connected to a mainframe can be half-duplex.

- Synchronization:

→ The session layer allows a process to add checkpoints (synchronization points) into a stream of data.

→ eg: If a system is sending a file of 2000 pages, it is advisable to add checkpoints after every 100 pages to ensure that 100 page unit is received and acknowledged independently. So this case if crash happens during the transmision of page 523, the only pages that need to be resent after system recovery are pages 501 to 523.

MAJOR DUTIES OF PRESENTATION LAYER:

Translation:—

→ The processes in two systems are usually exchanging info in the form of character strings, number and so on. The information must be changed to bit streams before being transmitted. Because different computers use different encoding system, the presentation layer is responsible for interportability between different encoding methods.

→ Presentation layer at the sender changes the information from its sender dependent format to a common format

→ Presentation layer at the receiving machine changes the common format into receiver dependent format.

Encryption:→

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

Compression:

Data compression reduces the no. of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio and video.

-o-

Bit to Signal Transmission:-

- The physical layer of two adjacent nods provides a logical pipe through which the bits can travel, which act as the transmission medium.
- Since the transmission medium can't carry bits we need to represent bits by a signal, electomagnetic energy that can propagate through a medium.

Bit rate control:-

- physical layer controols the data transferred in bits per second (data rate).

Bit Synconization:-

- As the timing of bit transfer is crucial in data transmission, physical layer governs the synconization of bits by providing clocking mechanism that control both sender and receiver.

Multiplexing:-

- Multiplexing is the proces of dividing a link, the physical medium into logical channels for better efficiency.

Switching:-

- Switching in data communication can be done in several layes. We have
  - (i) Circuit switching
  - (ii) Packet switching
  - (iii) Message switching.

ANALOG AND DIGITAL

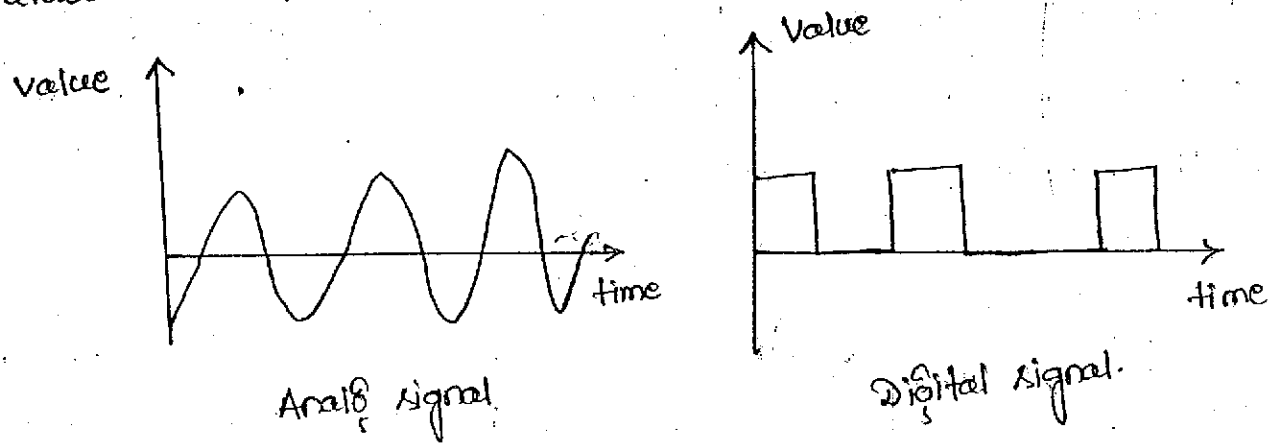
Both data and the signals that represent them can either be analog or digital form.

Analog and digital data:-

- Data can be analog or digital. Human voice is analog data. Data stored in computer in the form of 0's and 1's are digital data.

Analog and Digital Signal:-

- Signal can either be analog or digital.
- An analog signal has infanitely many level of intensity over a period of time. e.g: electrical signal, telephone voice.
- A digital signal can only have a limited no of defined values as simple as 0's and 1's.



Analog signal

Digital signal.

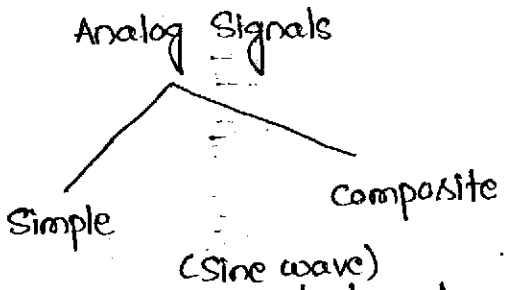
Periodic and Aperiodic Signals:-

- Both analog and digital signal can take one of two forms
  - (i) Periodic
  - (ii) aperiodic.

- A periodic signal completes a pattern within a measureable time ~~period~~ frame, called a period, and repeat that pattern over subsequent identical periods.

- The completion of one full pattern is called a cycle.
- An aperiodic signal changes without exhibiting a pattern or cycle that repeats over time.
- In data communication we commonly use periodic and aperiodic analog signals to send data from one point to another.

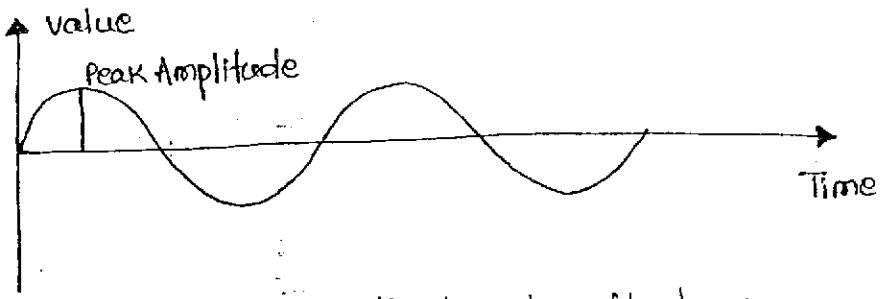
ANALOG SIGNALS

- 

- A simple analog signal cannot be decomposed into simpler signal.
- A composite analog signal is composed of multiple sine waves.

Sine Wave

A sine wave is the most fundamental form of a periodic analog signal.



A sine wave can mathematically described as

$$s(t) = A \sin(2\pi f t + \phi)$$

$s \rightarrow$ instantaneous amplitude

$A \rightarrow$ peak amplitude

$f \rightarrow$ frequency

$\phi \rightarrow$ phase.

Remember:-

- Peak Amplitude of a signal represent the absolute value of its highest intensity
- Period is the amount of time it takes in seconds, a signal needs to complete one cycle. (in seconds)
- Frequency refers to the no. of periods in one second (in hertz)

$$F = \frac{1}{T} \quad T = \frac{1}{F}$$

[Period is inverse of frequency and frequency is inverse of period].

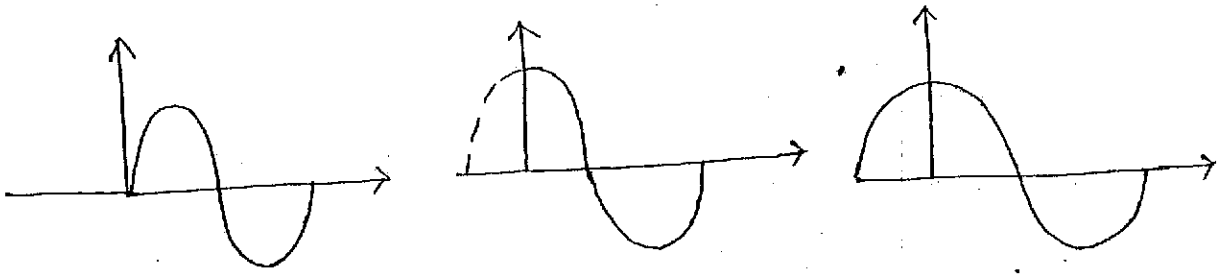
If Six periods in 1s

So F = 6Hz.

- A phase describes the position of the waveform relative to time zero. It indicates the status of first cycle. (measures in degrees or radians)

$$360^\circ = 2\pi \text{ rad}$$

$$\Rightarrow 1^\circ = \frac{2\pi}{360} \text{ rad} \quad \text{and} \quad 1 \text{ rad} = \frac{360^\circ}{2\pi}.$$



0° phase shift

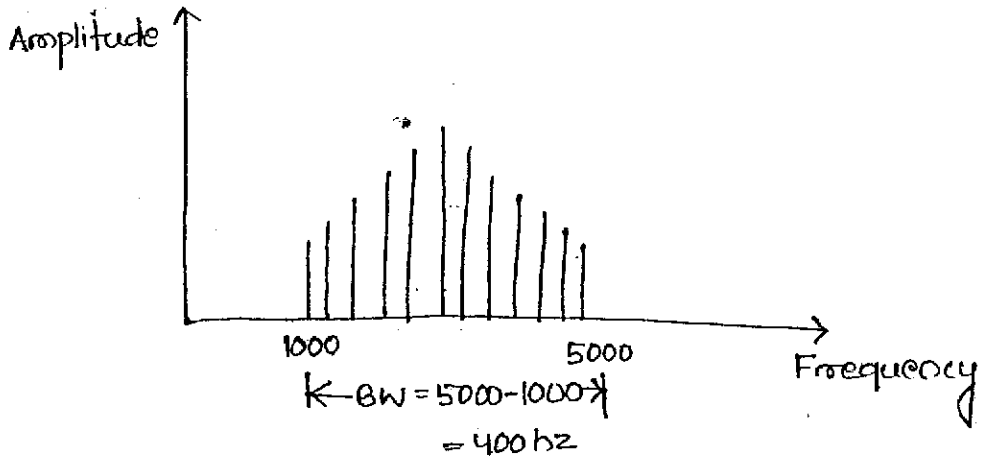
90° phase shift

180° phase shift.

- A range of frequency that a medium can pass is called its bandwidth, because no medium can pass or block all frequencies. Bandwidth refers to a range of frequencies that a medium can pass without loosing one-half of the power contained in the signal.

Example:

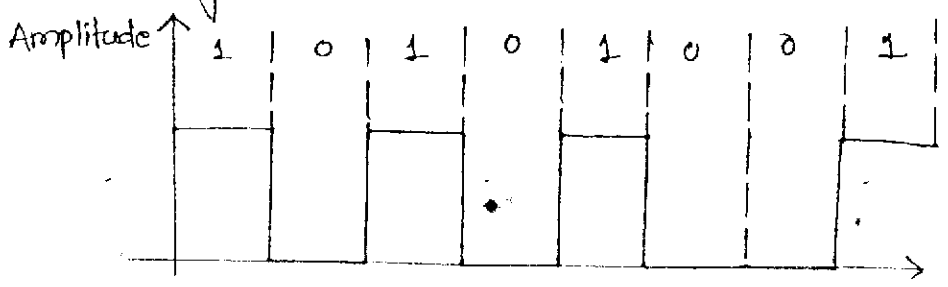
If a medium can pass frequencies between 1000 to 5000 without loosing most of the power contained in this range, then its bw is 5000 − 1000 or 4000



"BW is a property of a medium. It is the difference between the highest and lowest frequency that the medium can satisfactorily pass."

DIGITAL SIGNALS

- Digital signals are not continuos i.e they change in indivisual steps.
- They consist of pulses or digits with discrete values. The value of each pulse is constant, but there is an abrupt change from one digit to the next.
- Digital signal have two amplitude level called nodes, the value of which are specified as one of the two possibilities '1' or '0', i.e 'high' or 'low'. In reality the value are anywhere within specify range.



Bit interval and Bit Rate:

- Bit interval is the time required to send one single bit.
- Bit rate is the no of bit intervals per second expressed in bps (bits per second)

- Example

A digital signal has a bit rate 200 bps. What is the duration of each bit. (Bit interval)

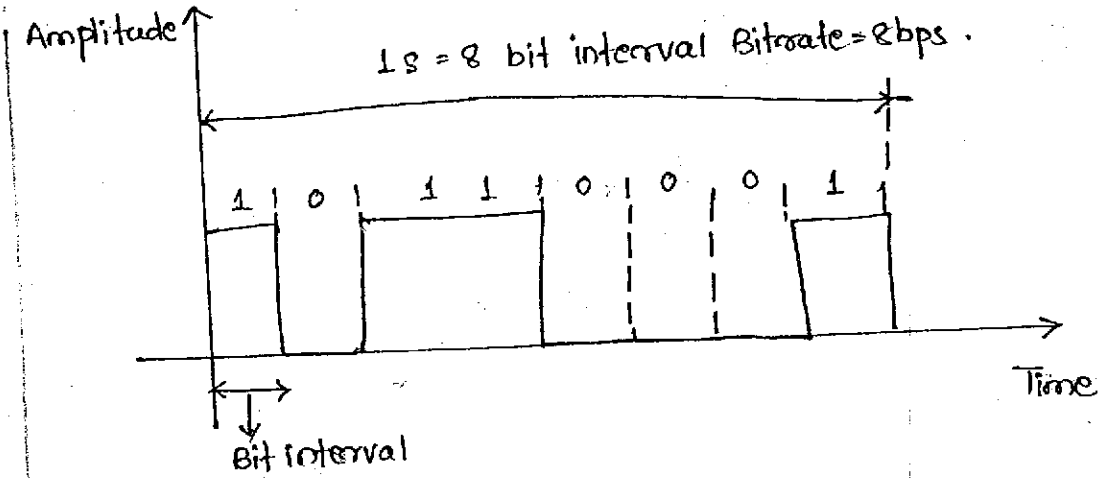
Solution

$$\text{Bit interval} = \frac{1}{\text{Bit rate}} = \frac{1}{2000} = 0.0005$$

$$= 0.000500$$

$$= 0.000500 \times 10^6 \mu s$$

$$= 500 \mu s$$



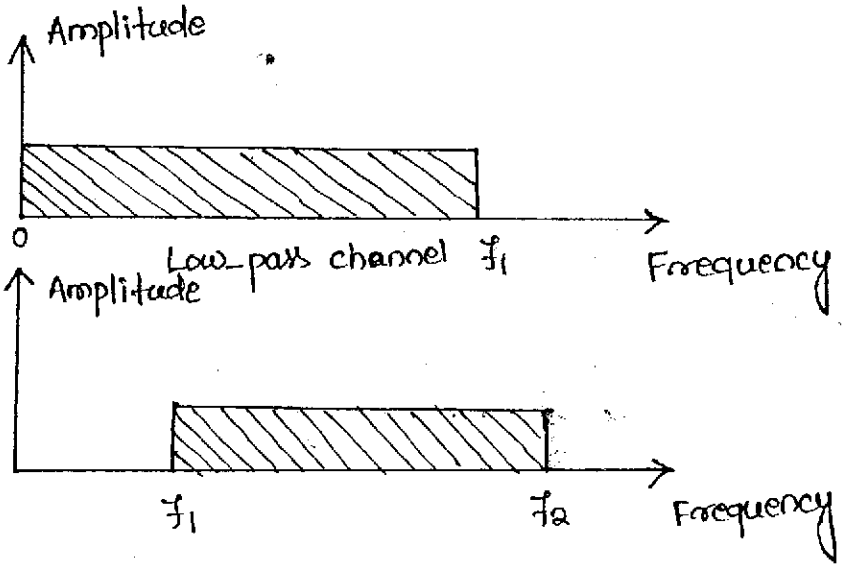
ANALOG VERSUS DIGITAL

The use of analog or digital signal depends upon the situation or the bw available.

Low pass and band pass:

- A channel or link is either low pass or band-pass.

- A low-pass channel has a band-width with frequency between 0 to f_1 i.e the lower limit is 0. the upper limit can be any frequency.
- A band-pass channel has a bandwidth with frequency bet^n f_1 and f_2



Digital Transmission:

- A digital signal theoritically needs a bandwidth bet^n 0 to ∞. We have a low pass channel if the medium is dedicated to two devices or shared bet^n several devices in time (not in frequency). e.g: Wired Local area Network.

Analog Transmission:

- An analog transmission has a narrower bw then a digital signal with frequency between f_1 and f_2. i.e a analog signal requires a band pass channel. The bw of a medium can be devided into several band pass channels to carry several analog transmission.

  e.g: Limited Telephony

DATA RATE LIMITS

Data rate depends upon 3 factor

(i) The bw available.
(ii) The level of signals we can use.
(iii) The quality of channel (level of noise)

Two theoritical formal has been developed to calculate the data rate.

(i) Nyquist for a noiseless channel
(ii) Shannon capacity for a noisy channel.

Noiseless channel: Nyquist Bitrate:

Nyquist bitrate defines the theoritical maximum bit rate

$$\text{Bitrate} = 2 * \text{Bandwidth} * \text{Log}_2^L$$

L → No of signal levels used to represent the data

Bitrate is the bitrate in bps.

Noisy channel: Shannon Capacity:

Shanon capacity to determine the theoritical highest datarate for a noisy channel

$$\text{Capasity} = \text{Bandwidth} * \log_2(1+\text{SNR})$$

SNR → Signal to noise ratio

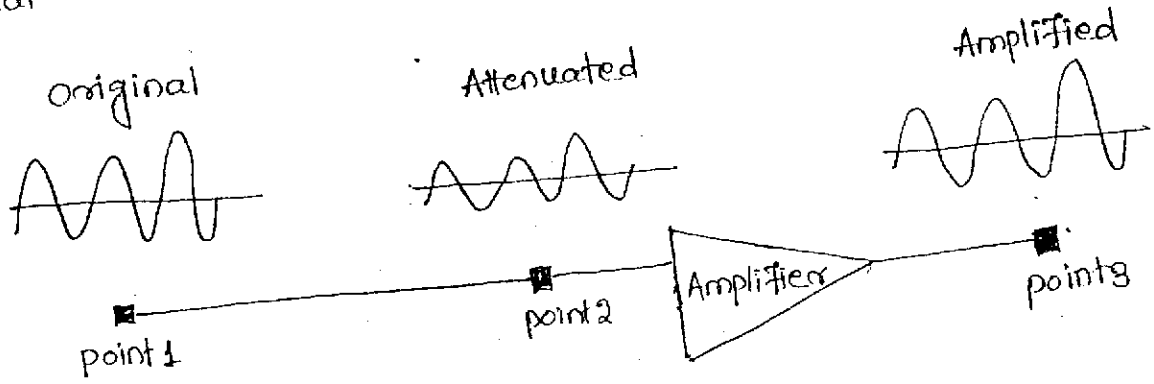
capacity → capacity of channel in bps.

TRANSMISSION IMPAIRMENT

- Signal travel through transmission media, which are not perfect. The imperfection cause impairement in the signal. i.e What is sent is not what is received
- Three types of impairement usually occur
  - Attenuation
  - Distortion
  - Noise

Attenuation:

- Attenuation mean loss of energy.
- When a signal, simple or composite travels through the medium it losses some of its energy so that it can overcome the resistance of the medium.
- Some of the electrical energy in the signal is converted to heat.
- To compensate this loss amplifiers are used to amplify the signal.



Attenuation

Note

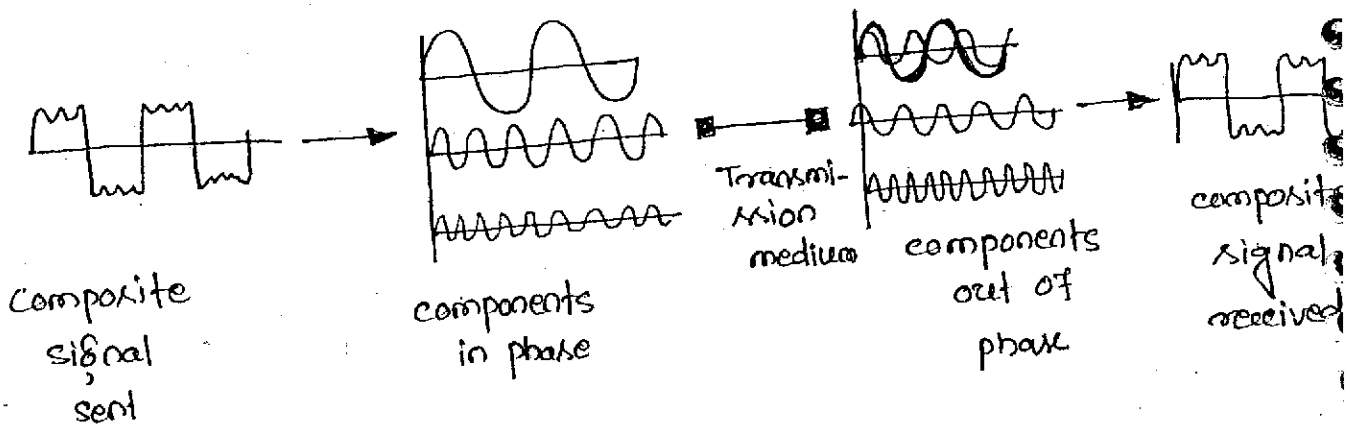
To show that a signal has lost or gained strength, engineer used the concept of decibel. The decibel (dB) measures the relative strength of two signal at two different

points of the decibel is negative, if a signal is attenuated and positive if a signal is amplified.

$$dB = 10 \log_{10} (P_2/P_1)$$

Distortion:-

- Distortion means the signal changes its form or shape.
- Distortion occur in a composite signal made of different frequencies.
- Each signal component has its own propagation speed through a medium. Therefore its own delay in arriving the final destination.

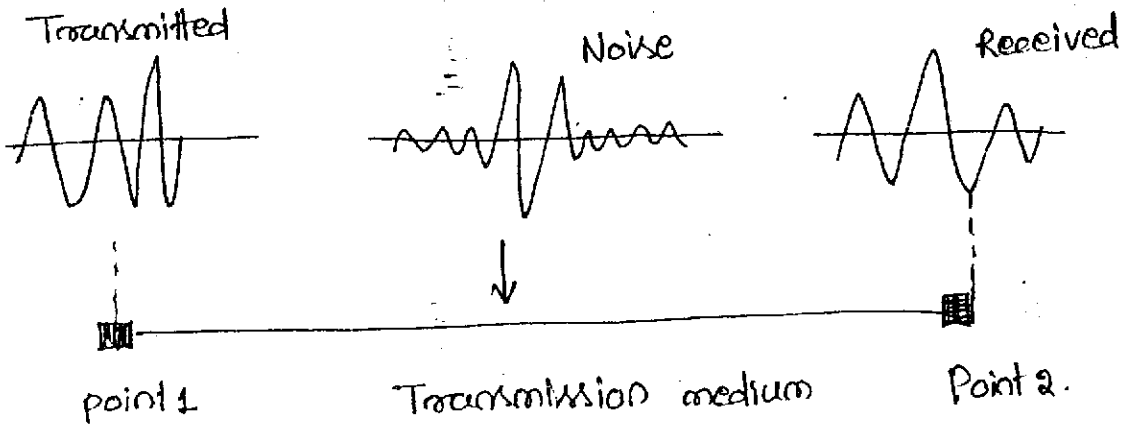


Distortion:

Noise:-

- Noise is another problem, Several types of noise such as thermal noise, induced noise, cross talk and impulse noise may corrupt the signal.
- Thermal noise is the random motion of electrons in a wire which creates an extra signal not originally sent by the transmitter.

- Induced noise comes from sources such as motors and appliances. These devices act as a sending antenna and transmission medium act as a receiving antenna.
- Cross talk is the effect of one wire on the other. One wire act as a sending antenna and other act as a receiving antenna.
- Impulse noise is a spike (a signal with high energy and a very short period of time) that comes from power lines lightning and so on.



Noise

✓ More About Signals (Basic properties of signal)

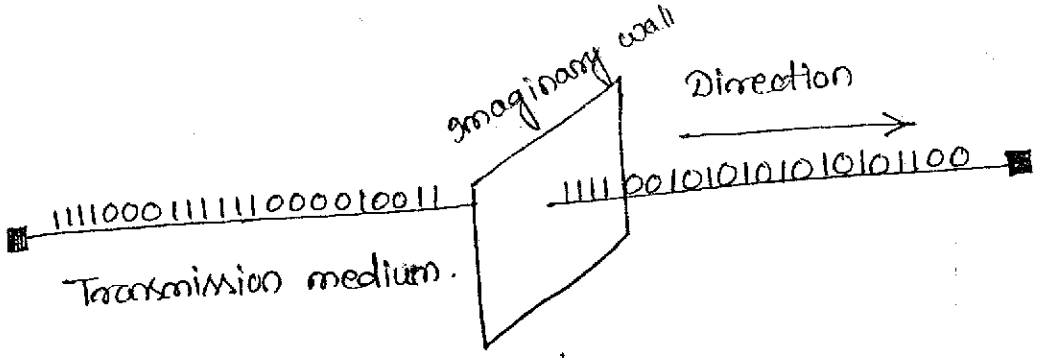
Four other measurement used in data transmission are

(i) Throughput (iii) Propagation Time
(ii) Propagation Speed (iv) Wavelength.

Throughput:

- Throughput is the measurement of how fast data can pass through an entity. (point / Network)
- If we consider this entity as a wall through which bits pass

throughput is the no of bits that can pass this wall in one sec.



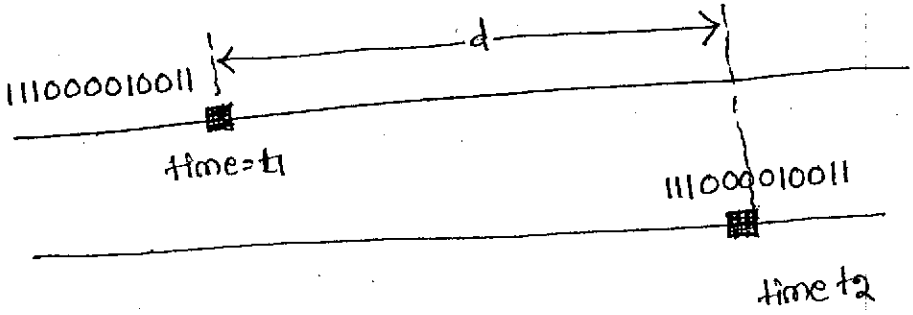
Propagation Speed:—

- Propagation speed measures the signal or a bit can travel through a medium in one second.
- The propagation speed of electromagnetic signal depends upon the medium and frequency of the signal.

Example: Propagation speed of light in a vaccume 3×10^8.

Propagation Time:-

- Propagation time is the time required for a signal to travel from one point of the transmision medium to another.
- $$\text{propagation time} = \frac{\text{Distance}}{\text{Propagation Speed}} = t_2 - t_1$$

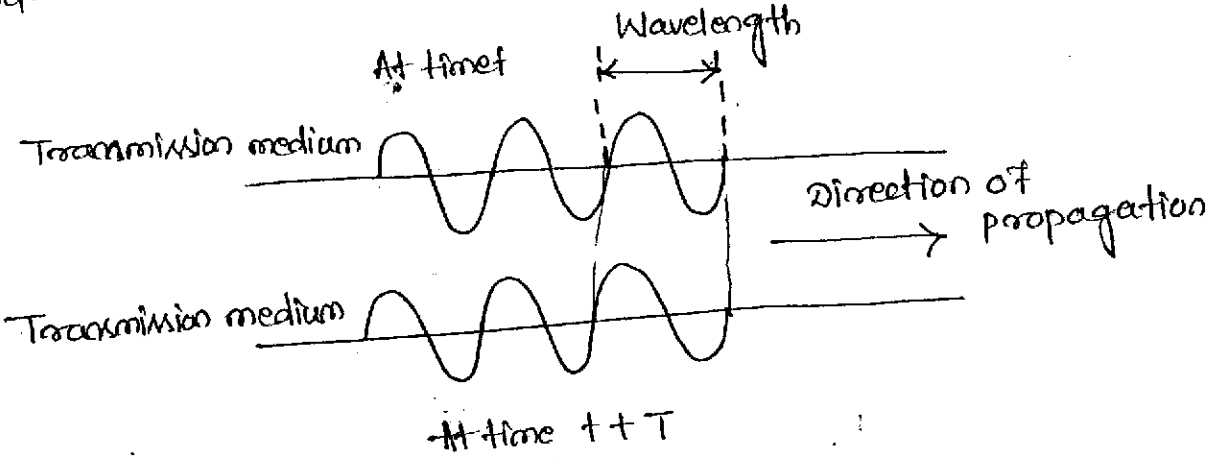


Wavelength:

- Wavelength binds the period or the frequency of a simple sine wave to the propagation speed of the medium.

i.e while the frequency of the signal is independent of the medium the wavelength depends on both the frequency and the medium.

- Wavelength is the distance a simple signal can travel in one period.



$$\text{Wavelength} = \text{propagation speed} \times \text{period}$$

$$= \text{propation speed} \times \frac{1}{\text{frequency}}$$

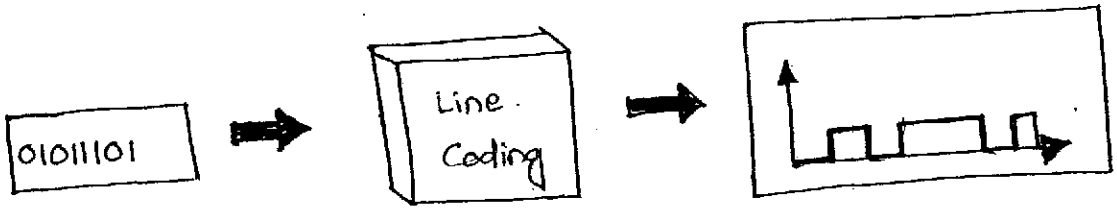
$$= \frac{\text{Propagation speed}}{\text{frequency}}$$

$$\text{i.e} \quad \lambda = \frac{c}{f}$$

DIGITAL TRANSMISSION

LINE CODING

- Line coding is the process of converting binary data to a digital signal.
- Example: Data, text, numbers, graphical images, audio and video that are stored in computer memory are all sequences of bits.



Line Coding

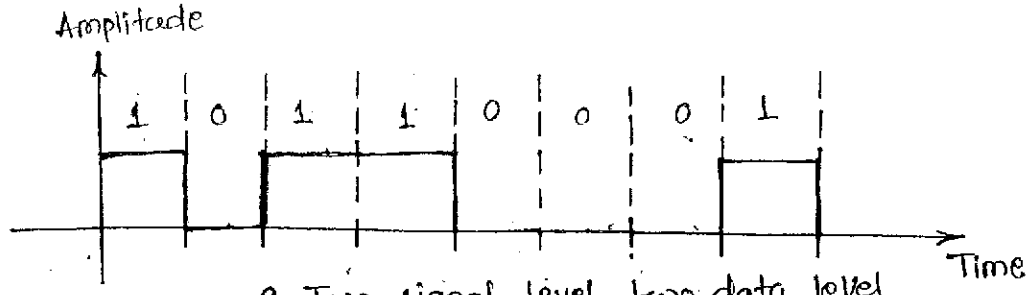
- Line coding convert a sequence of bits to digital signal.

Chareeteristic of Line Coding:

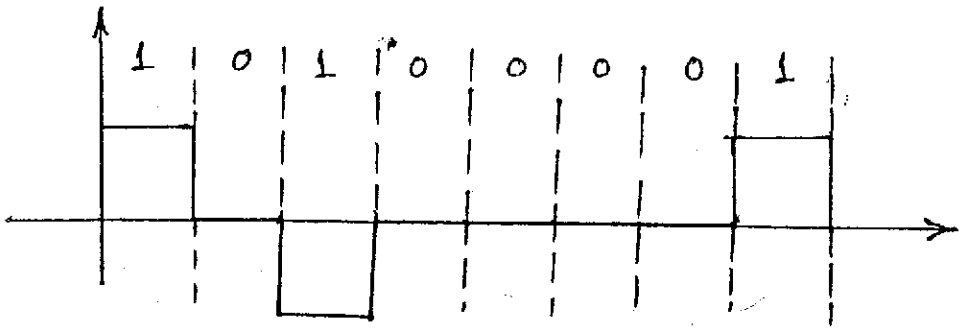
* Single level versus data level
* Pulse rate versus bit rate
* D.C component.
* Self Sycronization.

Single level vesesus data level:

- A digital data can have a limited no. of values, only some of these values can be used to represent data. The rest are used for other purposes.
- We refer to the number of values allowed in a perticular signal as the no. of signal level.
- We refer to the no. of values used to represent data as the



a. Two signal level, two data level



b. Three signal level, two data level.

Pulse Rate versus Bit Rate:

- The pulse rate defines the number of pulses per second.
- A pulse is the minimum amount of time required to transmit a symbol.
- The bit rate defines the no. of bits per second.
- If the pulse carries only one bit, the pulse rate and bit rate are same.
- In general

$$\text{Bit rate} = \text{Pulse Rate} \times \log_2 L$$

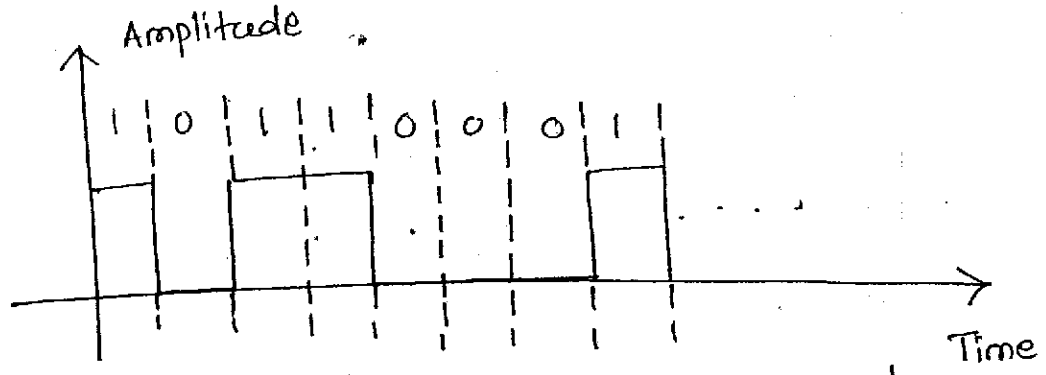
L → No. is data levels of the signal

DC Components:

- Some line coding schemes have a residual direct current (dc) component. (zero frequency). This component is undesirable for two reasons.

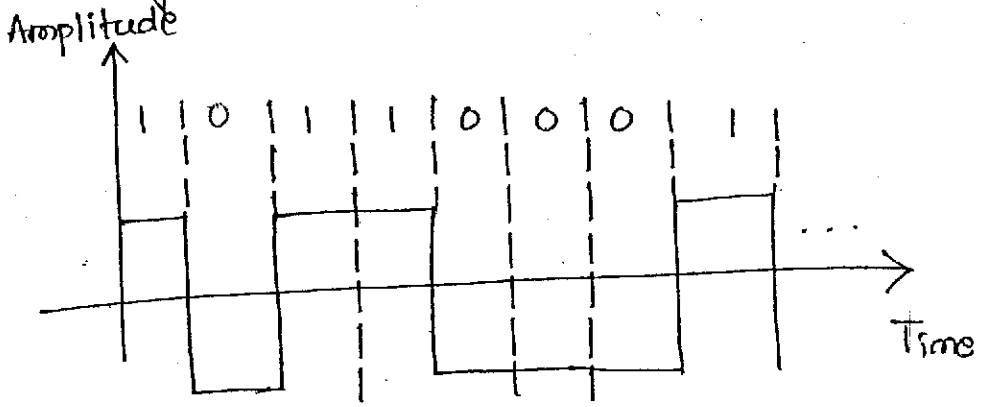
(i) If the signal is to pass through a system that doesn't allow the passage of dc component, the signal is distorted and may create errors in output.

(ii) The component is extra energy residing on the line and is useless.



a. A signal with dc component.

(It has a dc component, the positive voltage are not canceled by the negative voltage. It doesn't pass through a transformer properly)



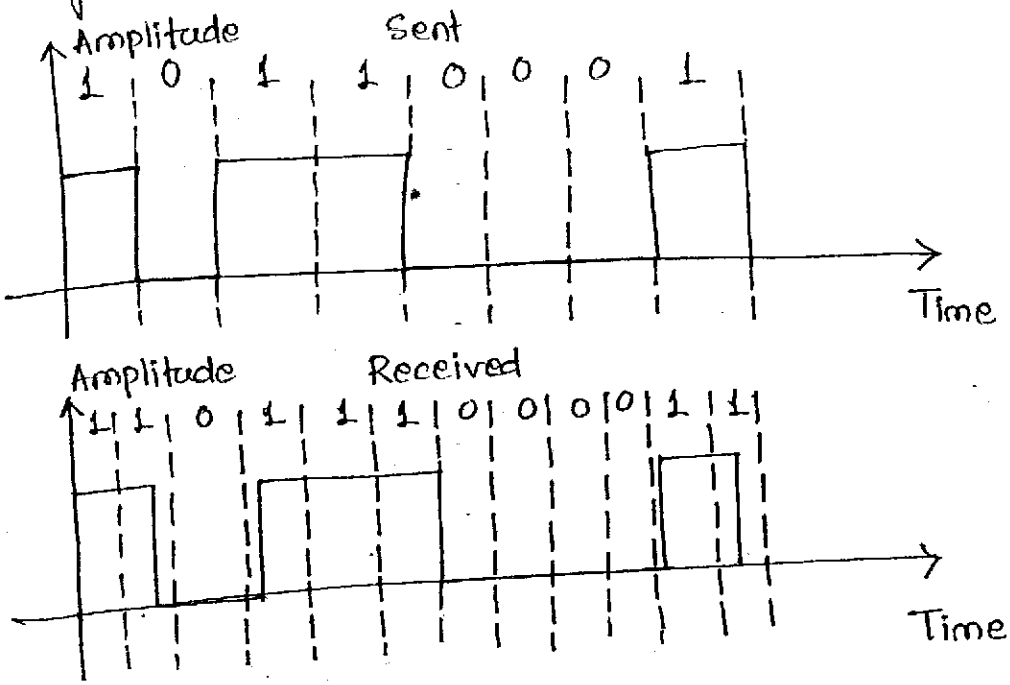
b. Signal without dc component

(It has no dc component, the +ve voltage are canceled by the negative voltage. It pass through a transformer)

Self Synchronization:

- To correctly interpret the signals received from the sender, the receivers bit intervals must correspond exactly to the sender's bit interval.

- If the receiver clock is faster or slower, the bit intervals are not matched, the receiver might interpret the signal differently.



(It shows a situation in which receiver has a shorter bit duration. Here the sender sends 10110001, while the receiver receives 110111000011)

Line Coding Schemes:

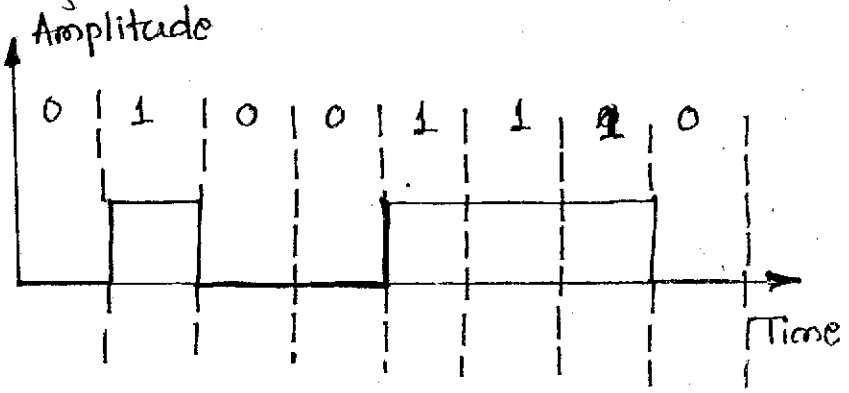
We can devide the line coding scheme into three broad categories

(i) Unipolar
(ii) Polar
(iii) Bipolar.

Unipolar:-

- Unipolar encoding is very simple and preemitive.
- It allows us to examine the kinds of problems that any digital transmission system must over come.
- Digital transmission system works by sending voltage pulses along a medium link, usually a wire or cable.

- In many types of encoding, one voltage level stands for binary 0 and other level stands for binary 1.
- The polarity of pulses refer to wheather it is positive or negative.
- Unipolar encoding is so named because it uses only one polarity. This polarity is assigned to one of the two binary states, usually the 1, The other state 0, is represented by zero voltage.



Unipolar Encoding

- Here 1s: are encoded as positive value
  0s: are encoded as negative value.
- It is expensive to implement. Main problems: A DC component and lack of synchronization.
- Average amplitude of unipolar encoded signal is nonzero which creates a dc component. If the data contains a long sequence of 0s and 1s, there is no change in the signal during this duration, that can alert receiver to potential synchronization problem.

Polar

- Polar encoding uses two voltage levels, one positive and one negative
- By using two levels in most polar encoding methods the average voltage level on the line is reduced and the dc component problem seen in unipolar encoding is elivated.
- Of the many existing variation of polar encoding, there are four of the most popular polar encoding.

(i) Nonreturn to zero (NRZ)
(ii) Return to zero (RZ)
(iii) Manchester
(iv) Differential Manchester.

Non Return to Zero:

- In NRZ encoding the value of the signal is always either positive or negative.
- There are two popular forms of NRZ.

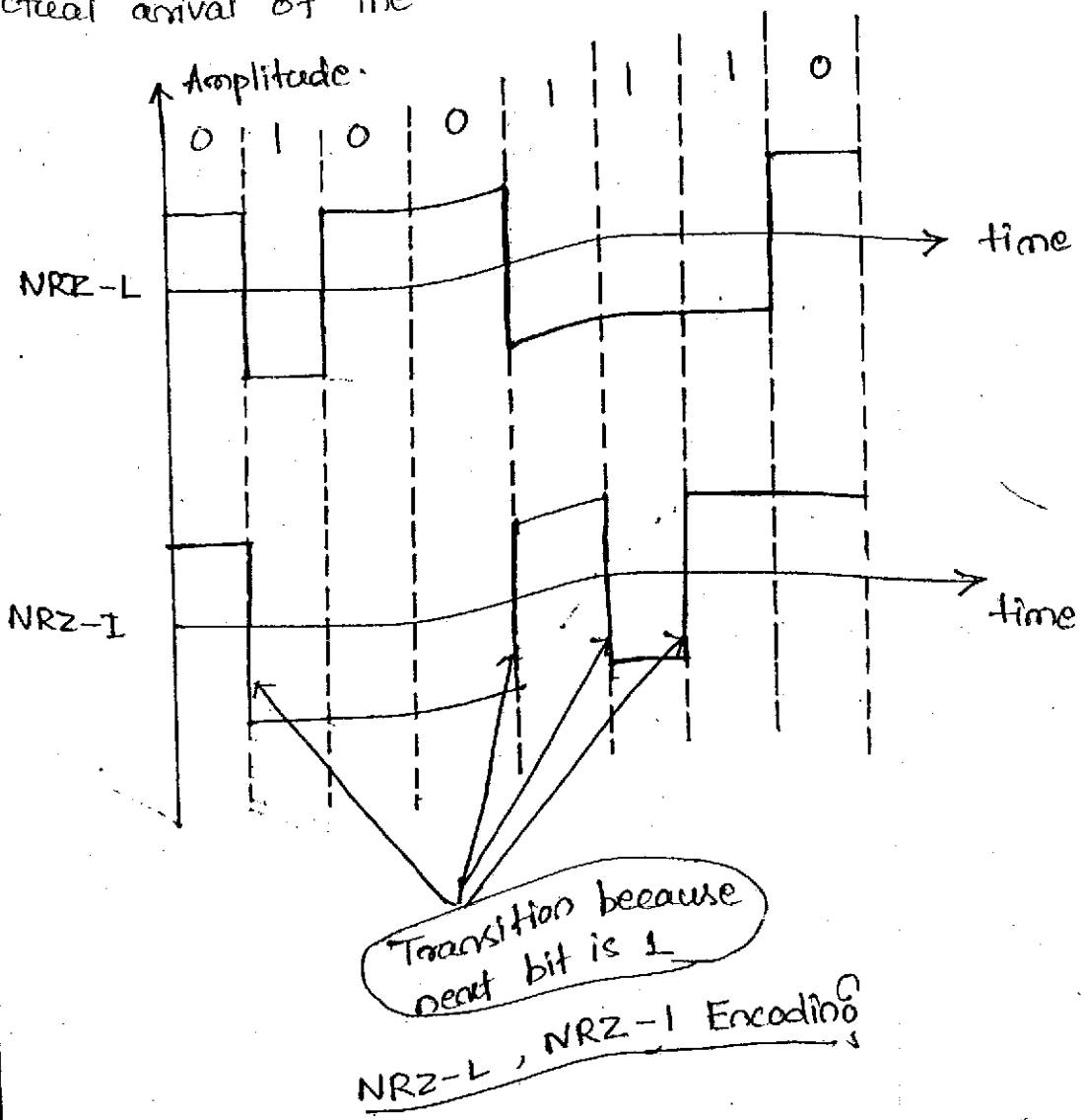
(i) NRZ-L (NRZ-Level)
(ii) NRZ-I (NRZ-invert)

- In NRZ-L encoding the level of signal depends upon the type of bit that it represents.

A +ve voltage means the bit is 0, while the -ve voltage means the bit as 1, thus the problem can arise when the data contain a long stream of 0s and 1s. The receiver receives a continuous voltage and determines how many bits are sent by relaying on its clock which may not be synchronized with sender clock.

- In NRZ-I, an inversion of voltage level represent a 1 bit.

It is the transition between a positive and negative voltage, not the voltage itself that represent 1 bit. A 0 bit is represented by no change. NRZ-I is superior to NRZ-L due to synchronization provided by the signal change each time a 1 bit is encountered. The existence of 1s in the data stream allows the receiver to synchronize its timer to the actual arival of the transmission.

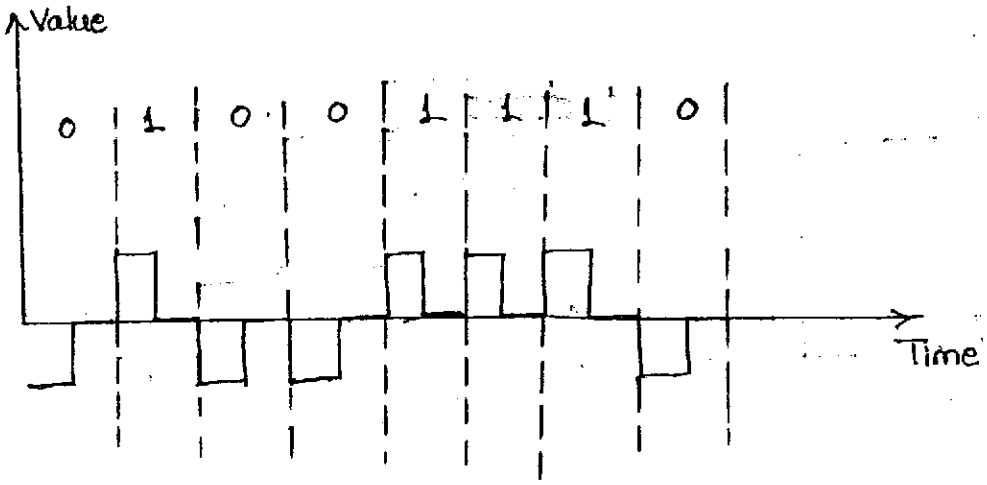


NRZ-L, NRZ-I Encoding

Return to zero:

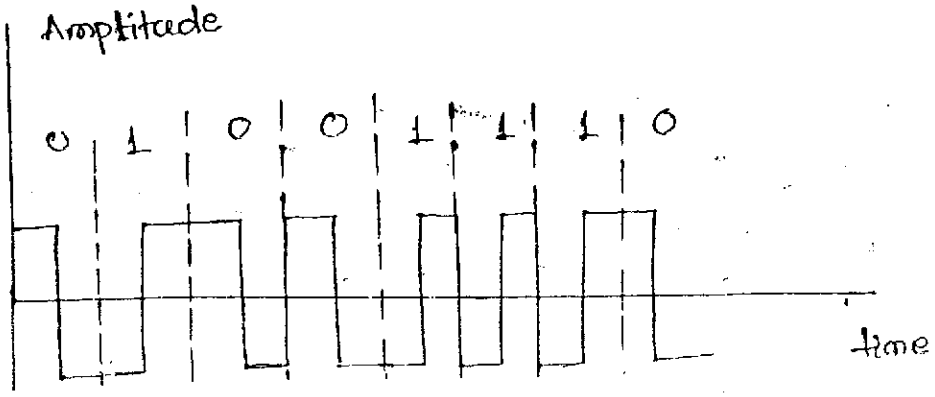
- To ensure synchronization, there must be a signal change for each bit. The receiver can use these changes to build up, update and synchronize its clock.
- NRZ-I accomplishes this for sequence of 1s but to change with every bit we need more than just two values. One soln is RZ-encoding.

- It uses three values: positive, negative and zero. Here signal changes not between bits but for each bit.
- A 1 bit is represented by +ve to zero and a 0 bit by -ve to zero rather than by +ve and -ve alone.
- Disadvantage: It requires two signal changes to encode 1 bit and therefore occupais more bandwidth.
- A good encoded digital signal must contain a provision for synchronization.



Manchester:

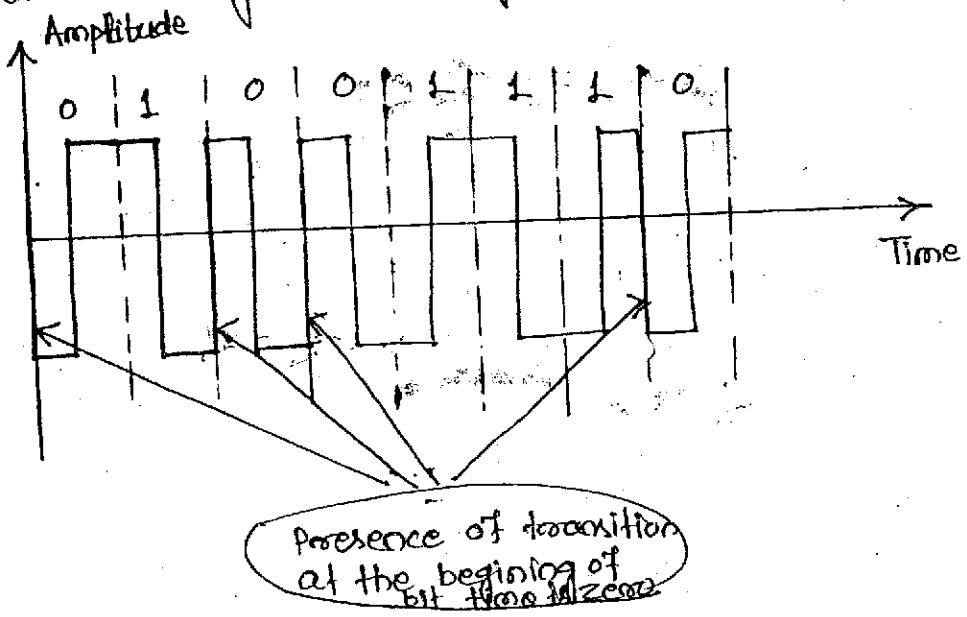
- Manchester encoding uses an inversion at the bit of each bit interval, for both synchronization and bit representation.
- A negative-to-positive transition represents binary 1 and a positive-to-negative transition represents binary 0.
- By using a single transition for a dual purpose, manchester encoding achives the same level of synchronization as Rz but with two levels of amplitude.



Differential Manchester:

Here the inversion at the middle of the bit interval is used for synchronization, beat the presence or absence of an additional transition at the begining of the interval is used to identify the bit.

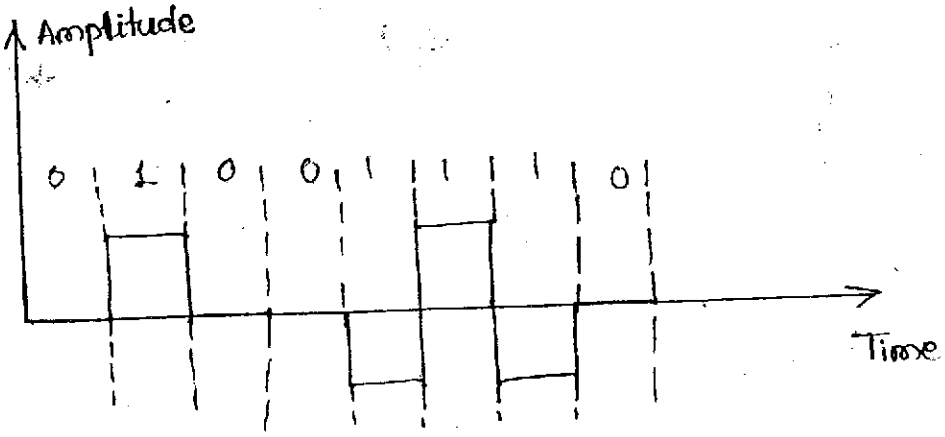
- A transition means binary 0 and no transition means binary 1.
- Differential manchester encoding requires two signal changes to represent binary 0 beat only 1 to represent binary 1.



Bipolar:

- Bipolar encoding like Rz uses three voltage levels: positive, negative and zero.
- However the zero level in bipolar encoding is used to represent binary 0. The 1s are represented by alternating +ve and -ve voltage.
- If the first 1 bit is represented by the positive amplitude and second will be represented by -ve amplitude, the third by +ve amplitude and so on.
- Alternation occur even when the 1bit are not consecutive
- A common bipolar encoding is called bipolar alternate mark

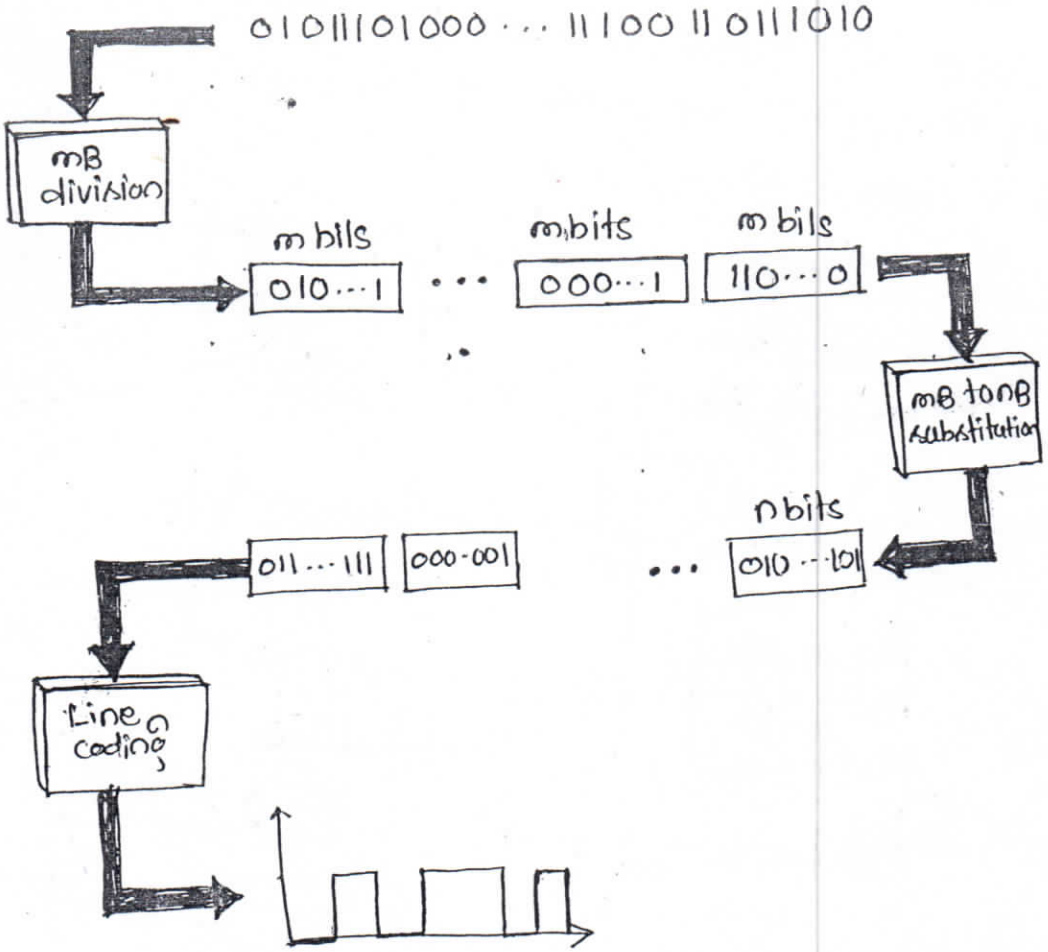
- The word mark comes from telegraphy and means 1. So AMI means alternate 1 inversion. A natural zero voltage represents binary 0. Binary 1s are represented by alternating positive and negative voltages.
- A modification of bipolar AMI has been developed to solve the problem of synchronization of sequential 0's. especially for long distance transmission.
- It is called (BnZS (bipolar n-zero substitution). Here when n consequtive zeros occur in the sequence, some of the bits in these n bits become positive or negative which helps synchronization



Bipolar AMI encoding

BLOCK CODING:

- To improve the performance of line coding, block coding was introduced



Steps in transmission:

In this method there are three steps: division, substitution and line coding.

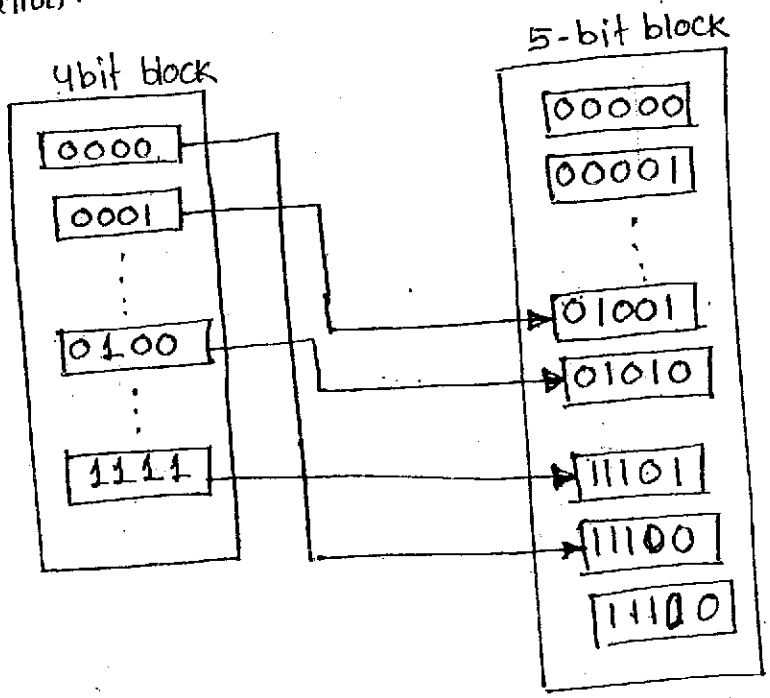
Step 1: Division:

- In this step, the sequence of bits is divided into groups of m bits
- e.g.: In 4B/5B encoding, the original bit sequence is divided into 4 bit groups.

Step 2: Substitution:

- In this step, we substitute an m bit code for n bit substi-

- e.g: In 4B/5B encoding we substitute a 5 bit code for a 4 bit code.
- With a 4 bit code, we can have $2^4 = 16$ different groups. With a 5 bit code, we can have $2^5 = 32$ possible codes. i.e we can map a 5 bit group to 4 bit group.
- As some of the 5 bit code are not used a strategy or policy is applied to choose only the 5-bit code that help in synchronization.



Substitution in block coding

- To achive synchronization, we can apply the policy that we do not have more than three consecutive 0's or 1's in 5-bit code.
- Block coding help in error detection, Because only a subset of the 5-bit codes is used, if one or more of the bits in the block is changed in such a way that one of the unused code is received, the receiver can easily detect the error.

Step3 : Line coding:

- After the substitution, we can use one of the line coding schemes to create a signal.
- A very simple line coding scheme is choosen because the

block coding procedure provides two desirable features of complex line coding scheme.

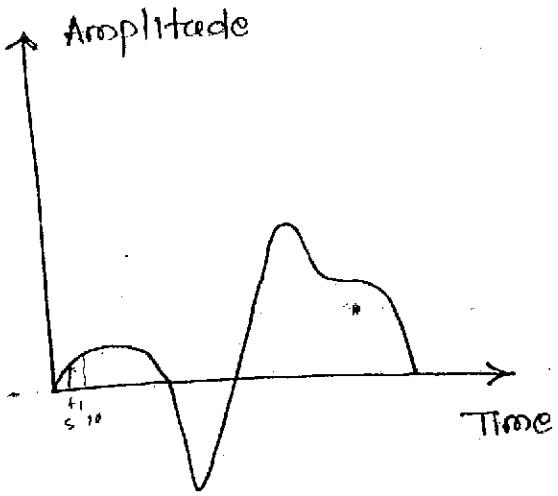
SAMPLING

- While sending an analog signal, we have to store it in a computer and send it digitally, so we have to change it through a process called sampling.
- After the analog signal is sampled, we can store the binary data in the computer or use line coding (or a combination of line coding or block coding) to further change the signal to a digital one, so it can be transmitted digitally.

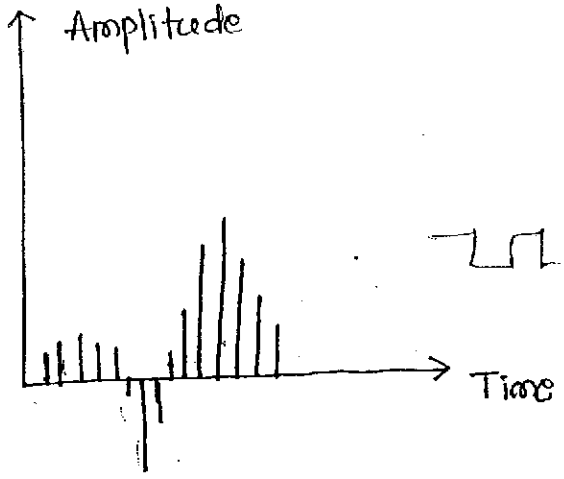
Pulse Amplitude Modulation:

- One of the method to convert analog to digital signal is called pulse amplitude modulation (PAM).
- This technique takes an analog signal, sampled it and generated a series of pulses based on the result of the sampling.
- The term sampling means "Measuring amplitude of the signal at equal intervals".
- PAM is the foundation of an analog to digital conversion method called pulse code modulation (PCM)
- PAM uses a technique called sample and hold. At a given moment the signal is read, then held briefly.
- The sampled value occurs only instatenously in the actual waveform, but is generated over a still short but measurable period in the PAM result.
- Disadvantages: PAM is not useful to data communication, even though it translates the original waveform to series of pulses. these pulses are still of any amplitude. (Still an analog signal not digital). To make them digital, we must modify them using pulse code modulation.

Pulse Code Modulation:



a. Analog Signal

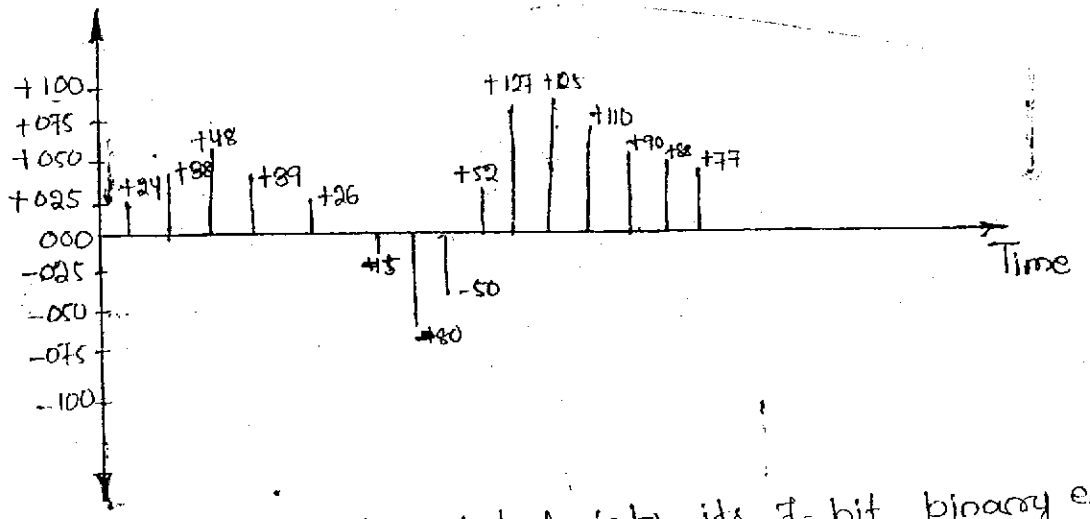


b. PAM Signal

PAM

- PCM modifies the pulses created by PAM to create completely digital signal. To do so, PCM first quantizes the PAM pulses.
- "Quantization is a method of assigning integral value in a specific range to sampled instances.

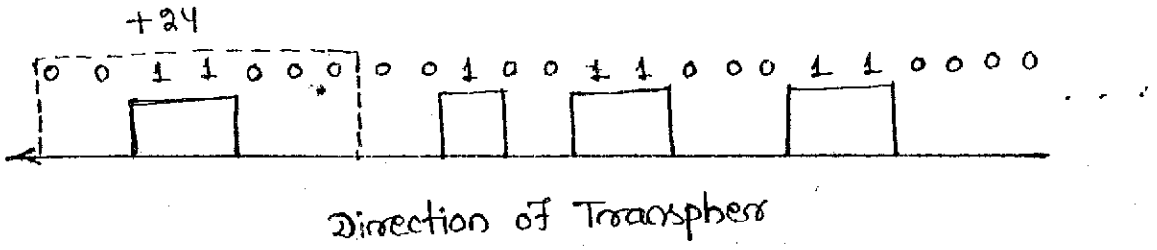
Result of Quantization



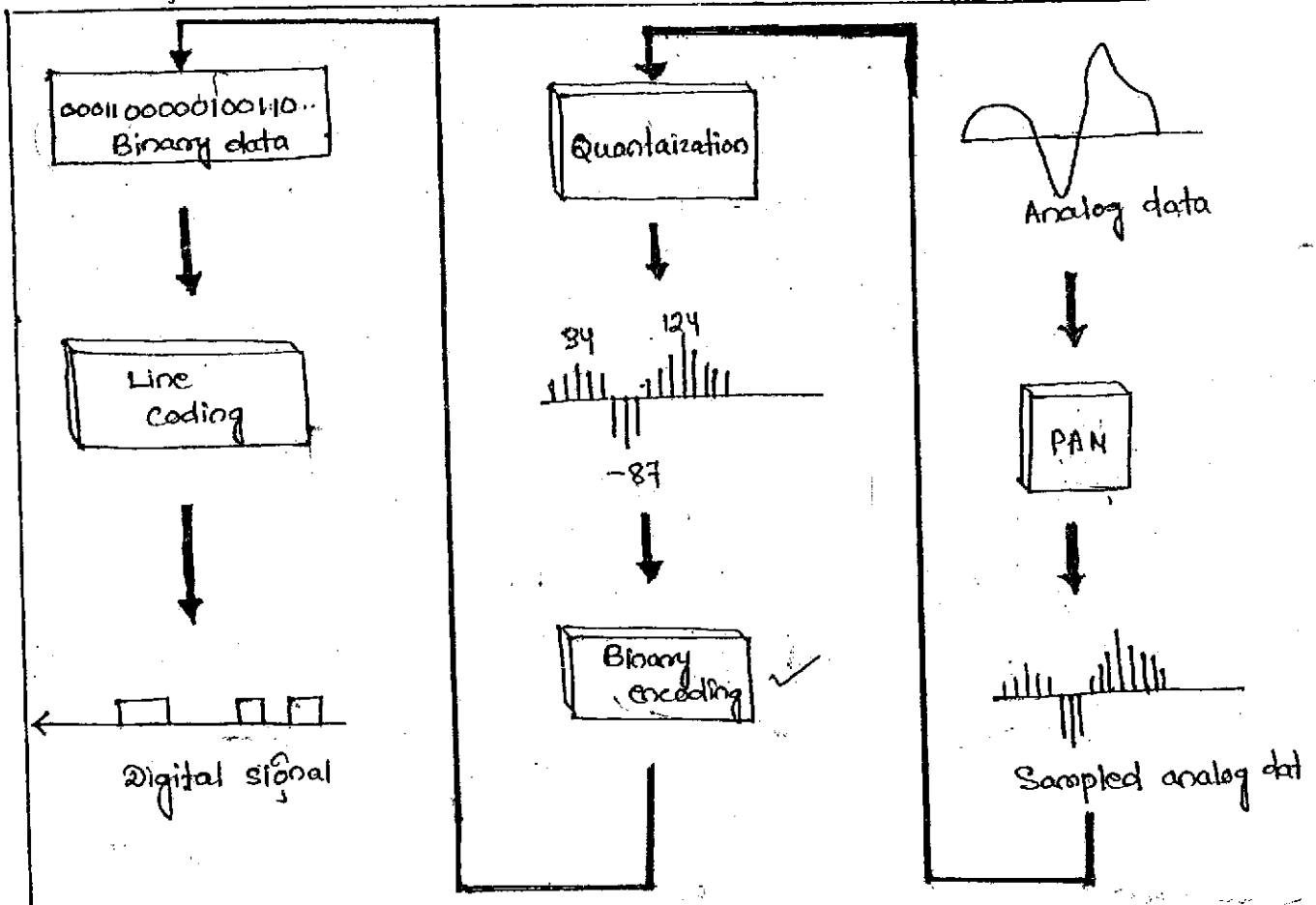
- Now each value is translated into its 7-bit binary equivalent. The eight bit indicate the sign.

+024 - 00011000 +039 - 00100111 -050 - 10110010 +125 - 01111101 ← Sign Bit
+038 - 00100110 +26 - 00011010 +052 - 00110110 +110 - 01101110
+048 - 00110000 -015 - 10001111 +127 - 01111111 +090 - 01011010
+088 - 01011000

- The binary digits are then transformed to a digital signal by using one of the line coding technique.
- PCM of the original signal encoded finally into a unipolar signal Here the first three sample valued are shown



- PCM is actually made up four separate process: PAM, Quantaization, binary encoding and line coding.
- Following figure shows the entire process in graphical form.

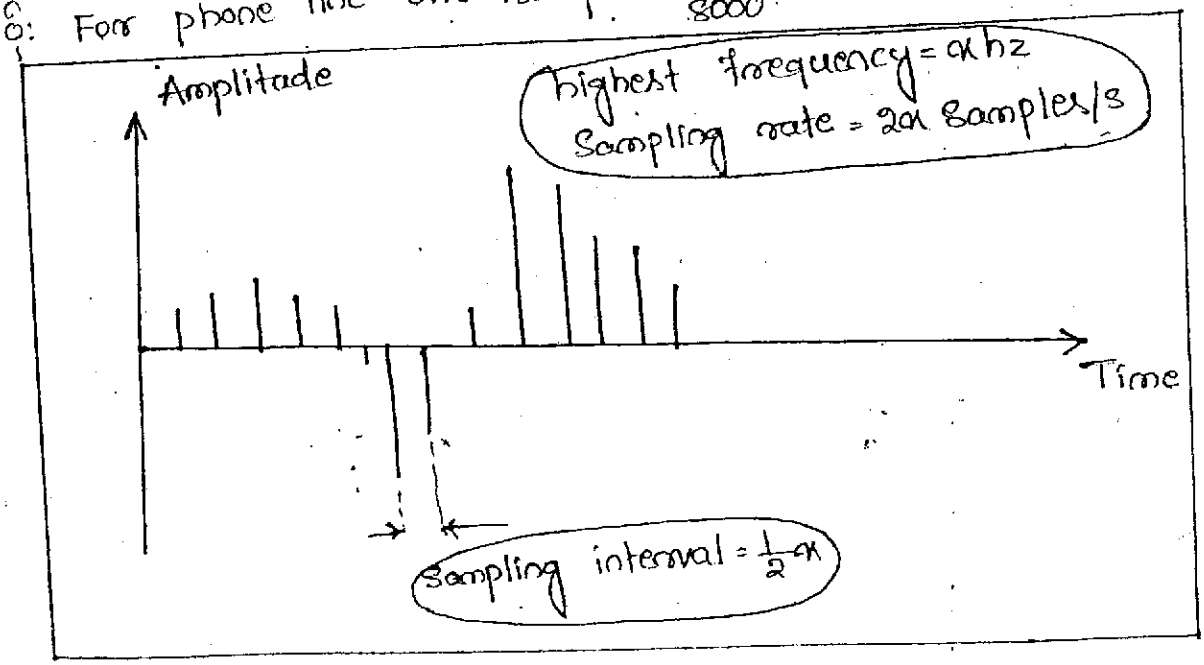


From analog signal to PCM digital Code

Sampling Rate: Nyquist Theorem:

- The accuracy of any digital reproduction of an analog signal depends upon the no. of samples taken.
- Using PAM and PCM, we can reproduce the waveform exactly by taking infinite samples or we can reproduce the barest generalization of its direction of change by taking three samples
- Nyquist Theorm:

  "Acc. to Nyquist theorm" to ensure accurate reproduction of an original analog signal using PAM, the sampling rate must be at least twice the highest frequency of the original signal"
- e.g.: If we want to sample telephone voice with maximum frequency 4000 hz, we need sampling rate of 8000 samples per second.
- A sampling rate of twice the frequency of α hz means that the signal must be sampled every $\frac{1}{2\alpha}$ seconds
- e.g.: For phone line one sample $\frac{1}{8000}$ s.



Note

We can always change a band-pass signal to a low pass signal before sampling, there the sampling rate is twice the b

TRANSMISSION MODE

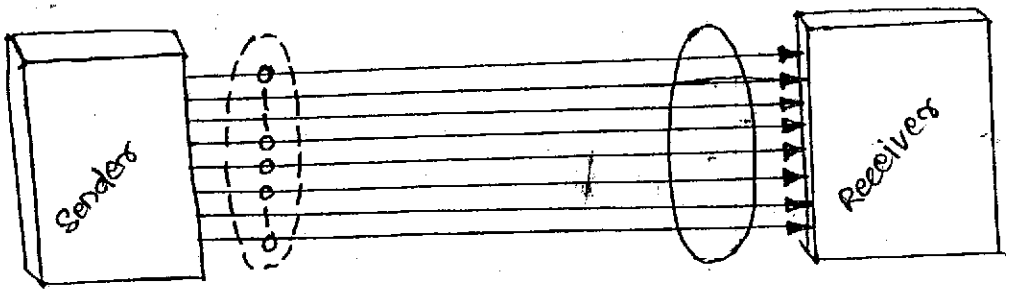
- When we are considering the transmission of data from one device to another, ~~we are considering~~ wiring as the primary media. when we are considering wiring is the data stream.

Data Transmission

- Parallel
- Serial
  - Synchronous
  - Asynchronous

Parallel Transmission

- The transmission of binary data through parallel mode, multiple bits, are sent through each clock tick.
- Here binary data consisting of 1s and 0s may be organized into groups of n bits each.
- By grouping we can send data n bits at a time instead of 1. This is called parallel transmission.
- It uses n wires to send n bits at one time. That way each bit has its own wire, and all n bits of one group can be transmitted with each clock tick from one device to another.
- Following figure shows a parallel transmission of n=8, Eight wires are bundled in a cable with connector at each end.

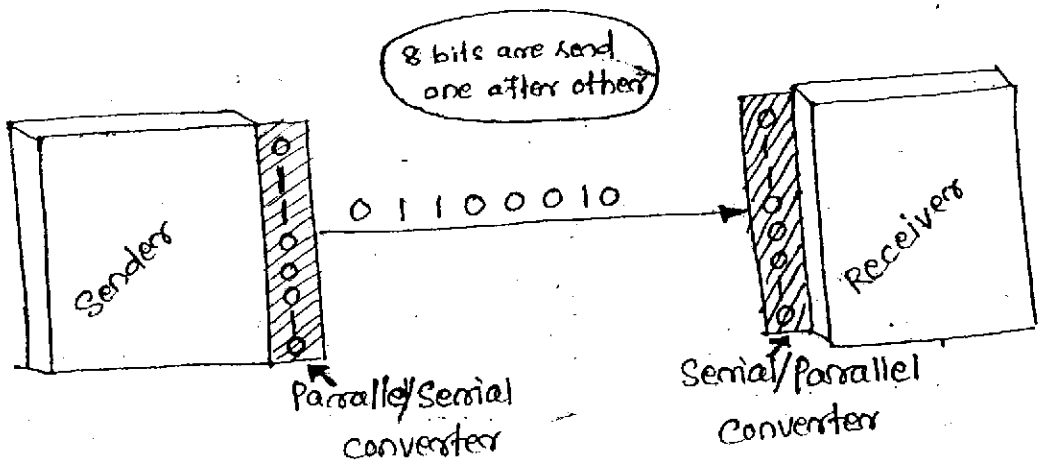


Parallel transmission

- Advantage:
  - Transmission is speed. It can increase the transmission speed by n over serial transmission.
- Disadvantage:
  - Cost, Parallel transmission requires n communication lines just to transmit the data stream.
  - Limited to short distance.

Serial Transmission

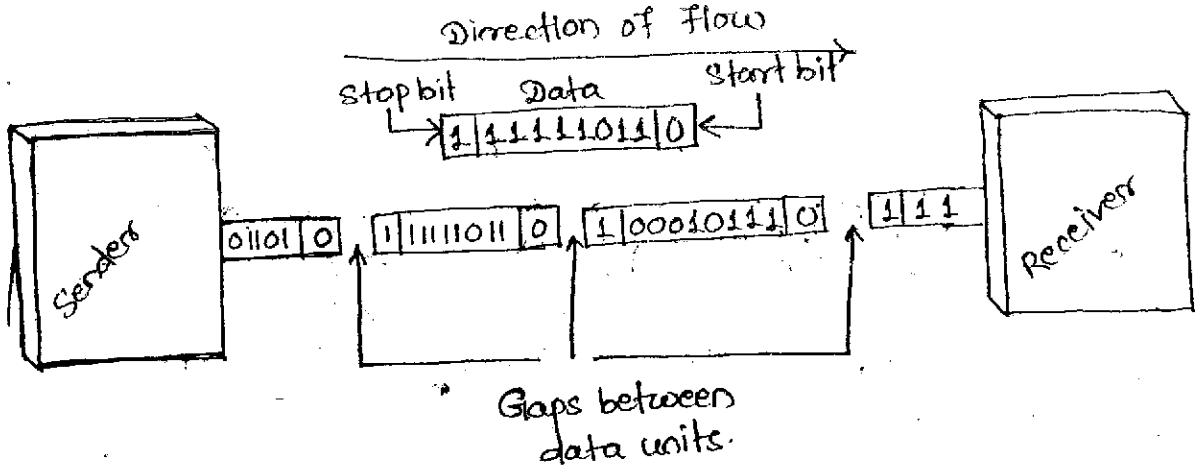
- In serial transmission one bit follows another, so we need only one communication channel rather than n to transmit data between two communicating devices.
- Advantage:
  - As only one communication channel is used, it reduces the cost of transmission over parallel by roughly a factor of n.
  - Since communication within devices is parallel, conversion devices are required at the interface between the sender and the line, and between the line and receiver.



- Serial Transmission is of two types
  - Asynchronous Transmission
  - Synchronous Transmission.

Asynchronous Transmission:

- It is named so because the timing of signals unimportant.
- Information is received and translated by agreed upon patterns. As long as those patterns are followed, the receiving device can retrive the information, without regard to the rhythm in which it is sent.
- A group of 8 bits (=1 byte) is sent along the link as a unit.
- The sending system handle each group independently whenever ready without regarding about the timer.
- To alert the receiver about the arival of a new group an extra bit is added at the beginig of each byte. This bit is '0' called a start bit.
- To let the receiver know that the byte is finished 1 additional bit is added to the end of the byte. This bit usually 1s are called stop bit.
- So the byte size is increased to 10 bits. 8 are information and and 2 or more are signal to the receiver.
- The transmission of each byte may then be followed by a gap of varying duration.
- This gap can be represented either by an idle channel or by a stream of additional stop bits.
- This mechanism is called asyncronores, because at the byte level, sender and receiver dont have syncronized, bcet within each byte, the receiver must still be syncronized for the incoming bit stream. It resyncronizes at the onset of new byte.
- When the receiver detects a start bit, it gets the timer and begins counting bit as they come in. After n bits the receiver look for stop bit. As soon as it detects the stop bit it waits until it detects the next start bit.



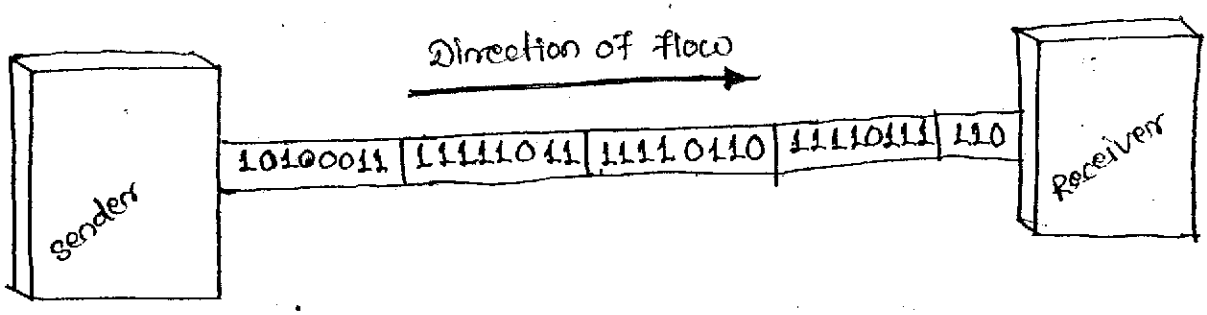
- On the example the start bit are 0s, the stop bit is and the gap is represented by an idel line rather than by additional stop bit.
- The additional stop bit and start bit and insertion of gap bet? the bit streams make asynchronous transmission slower than forms of transmission that can operate without the addition of control information.
- It is cheap and effective.
- Low-speed communication.

Synchronous Transmission:

- Here the bit stream is combined into longer frames, which may contain multiple bytes.
- Each byte however is introduced onto the transmission link without a gap between the one and next one.
- It is left to the receiver to separate the bit stream into bytes for decoding purposes, receiver separates that string into bytes or characters, it needs to reconstruct the information.
- It contains no start bit or stop bit.
- Even really those division doesn't exist, the sender puts its data onto the line as one long string.
- If the sender wishes to send data in separate bursts, the

gaps between bursts must be filled with special sequence of 0s and 1s that means idle.

- The receiver counts the bits as they arrive and groups them in 8-bit units.



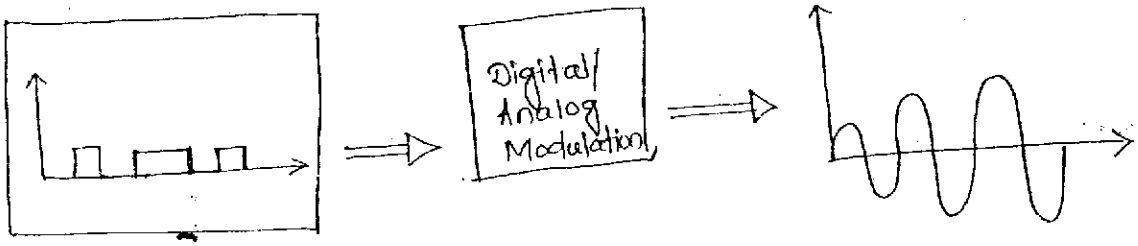
- Timing becomes very important, therefore, because the accuracy of the received information is completely dependent on the ability of the receiving device to keep an accurate count of the bits as they come in.

- Advantage:
  - Transmission is speed.
  - Synchronous transmission is faster than asynchronous transmission, as the extra bits are absent.
  - Useful for high speed transmission such as transmission from one computer to another.
  - It is accomplished in data link layer.

ANALOG TRANSMISSION

MODULATION OF DIGITAL DATA:

- Modulation of binary data or digital-to-analog modulation is the process of changing one of the characteristic of an analog signal based on the information in a digital signal (0s and 1s).
- e.g: When you transmit data from one computer to another across a public across a phone line, suppose original data are digital, bad because telephone wires carry analog signals, the data must be converted. The digital data must be modulated on an analog signal that has been manipulated to look like two distinct values corresponding to binary 1 and binary 0.
- A wave can be defined by 3 different characteristics
  - Amplitude
  - Frequency
  - phase.
- Any of the three characteristics can be altered using 3 mechanism for modulating digital data into an analog signal
  - Amplitude shift keying (ASK)
  - Frequency shift keying (FSK)
  - phase shift keying (PSK)
- There is a fourth mechanism that combines changes in both amplitude and phase called quadrature amplitude modulation (QAM).



Aspects to digital-to-analog conversion:

Two basic issues of digital-to-analog modulation

(i) bit and baud rate

(ii) Carrier signal

Bit rate and Baud rate:

- Two terms used frequently in data communication
  (i) Bit rate, (ii) Baud rate.
- Bit rate is the no. of bits translated in 1 sec.
- Baud rate refers to the number of signal units per second that are required to represent those bits.
- A signal unit is composed of one or more bits.
- Baud rate determines the bandwidth required to send the signal.
- Bit rate equals the baud rate times the number of bits represented by each signal unit
- Bit rate is always equal to or greater than baud rate

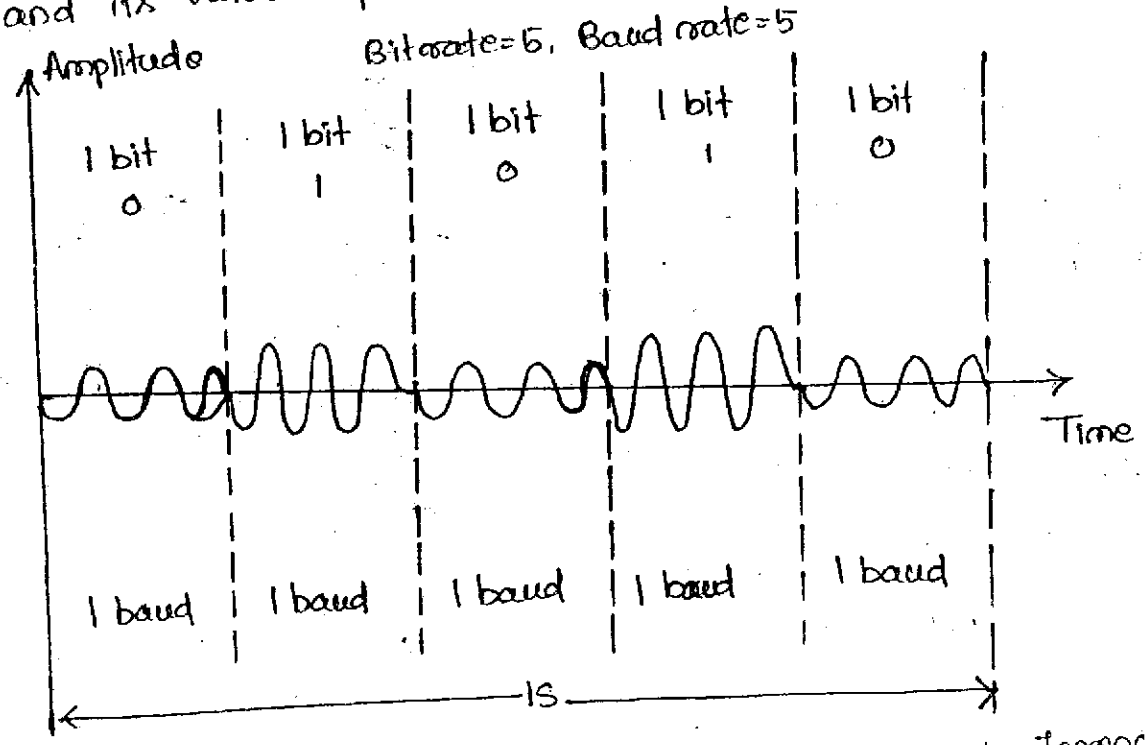
$$\text{Baud rate} = \frac{\text{Bit rate}}{\text{No of bits per signal unit.}}$$

Carrier Signal:

- In analog transmission, the sending device produces a high frequency signal that acts as a basic for the information signal.
- This base signal is called carrier signal or carrier frequency.
- The receiving device is tuned to the frequency of the carrier signal that it expects from the sender.
- Digital information then modulates the carrier signal by modifying one or more of its characteristic (i.e amplitude, frequency or phase). This kind of modification is called modulation.

Amplitude Shift Keying (ASK):

- In ASK, the strength of the carrier signal is varied to represent binary 1 or 0.
- Both frequency and phase remain constant while the amplitude changes.
- A bit duration is the period of time that defines 1 bit.
- The peak amplitude of the signal during each bit duration is constant, and its value depends on the bit (0 and 1)



- ASK transmission is highly susceptable to noise interference
- The term noise refers to unintentional voltages introduced onto a line by various phenomena such as heat or electromagnetic induction created by other sources.
- This unintentional voltage combine with the signal to change the amplitude. A 0 can be changed to 1 or a 1 to 0.
- ASK is the modulation method for the signal most affected by noise.
- A popular ASK technique is called on/off keying (OOK). In OOK one of the bit value represented by no voltage. The advantage is a reduction in the amount of energy required to transmit

Bandwidth for ASK:

- When we decompose a ASK modulated signal, we get a spectrum of many simple frequencies.
- BW requirement for ASK are calculated using the formula

$$BW = (1+d) \times N_{baud}$$

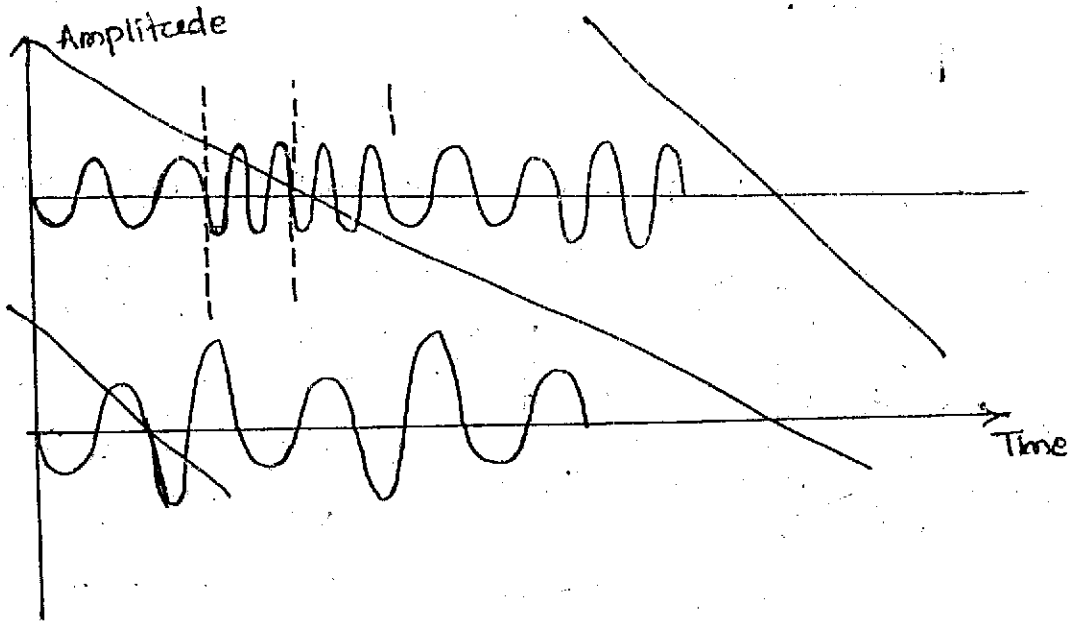
N_{baud} → Baud rate

d → Factor related to modulation process

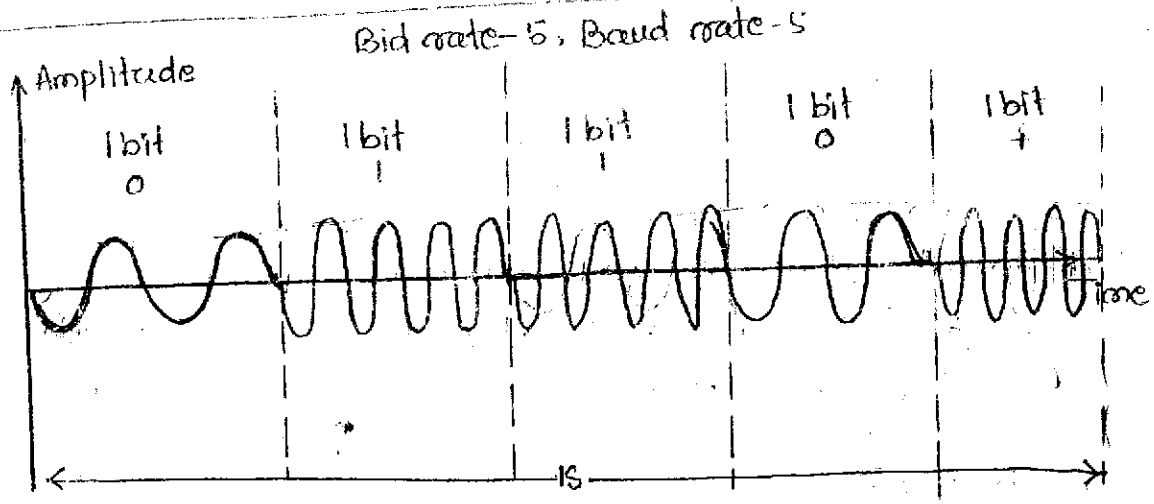
- Here minimum bandwidth required for transmission is equal to baud rate

Frequency Shift Keying: (FSK)

- In FSK the frequency of carrier signal varied to represent binary 1, or 0.
- The frequency of the signal during each bit duration is const, and its value depend on the bit 0 and 1.
- Here both peak amplitude and phase remain const.



- FSK avoids most of the problems from noise, because the receiving device is looking for sp. frequency change over a given no. of period. It can ignore voltage spikes.
- ~~It can ignore~~ Limiting factor are physical capabilities of the carrier.



Bandwidth for FSK:

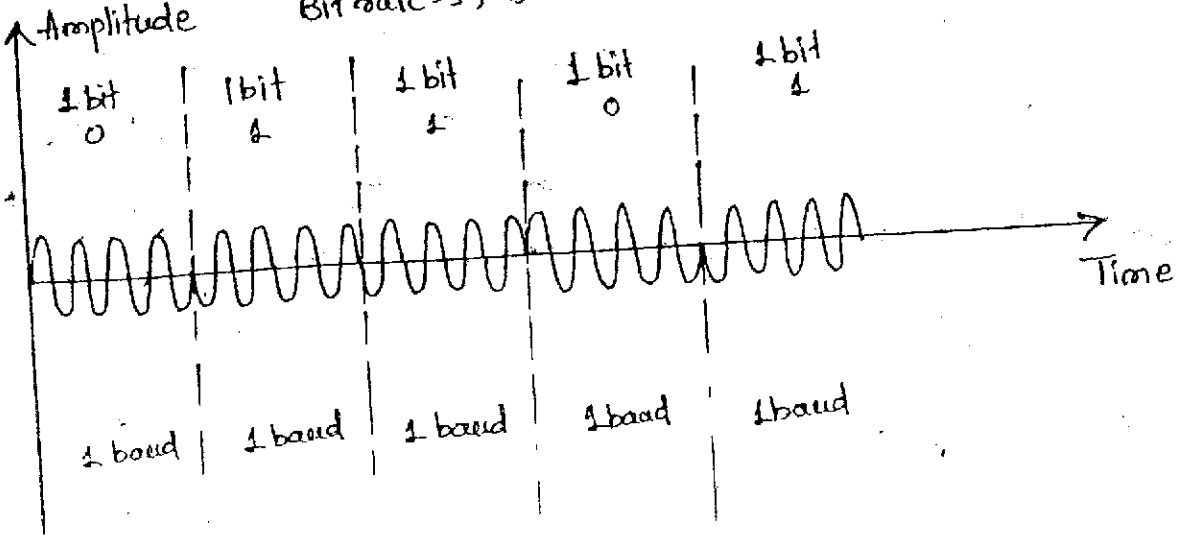
- FSK spectrum is a combination of two ASK spectra centered on f_{c0} and f_{c1}.
- The bw required for FSK transmission is equal to the baud rate of the signal plus the frequency shift

$$BW = f_{c1} - f_{c0} + N_{baud}$$

- Although there are only two carrier frequency, the process of modulation produces a composite signal that is a combination of many simple signals.

phase Shift Keying (PSK):

- In PSK, the phase of the carrier is varied to represent binary 1 or 0.
- Both peak amplitude and frequency remain constant as the phase change.

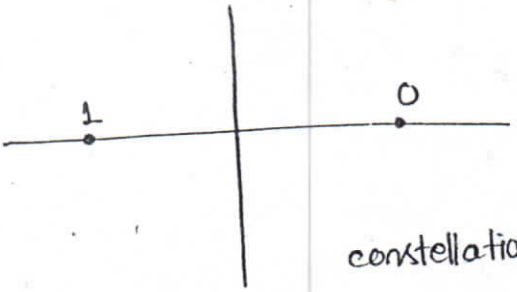


e.g.: If we start with a phase of 0° to represent binary 0, we can change the phase to 180° to send binary 1.

- The phase of the signal during each bit duration is constant.
- The above method is often called 2-PSK or binary PSK, because two different phases 0° and 180° are used.
- A second diagram called constellation or phase state diagram shows the same relationship illustrating only the phases.

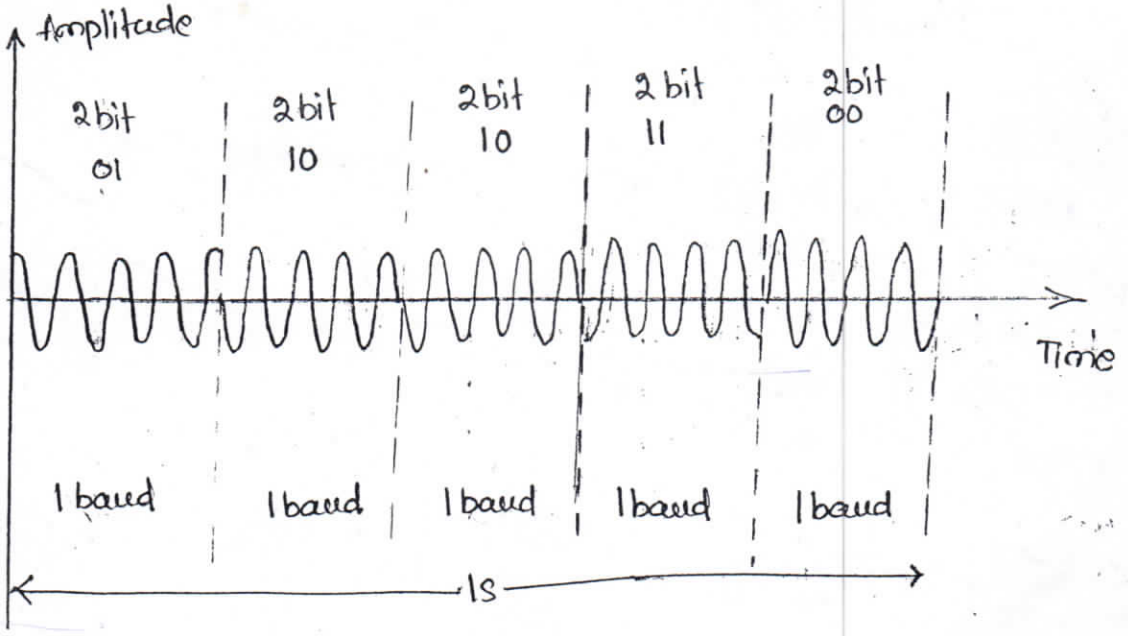
PSK Constellation —

Bit	phase
0	0
1	180



constellation diagram.

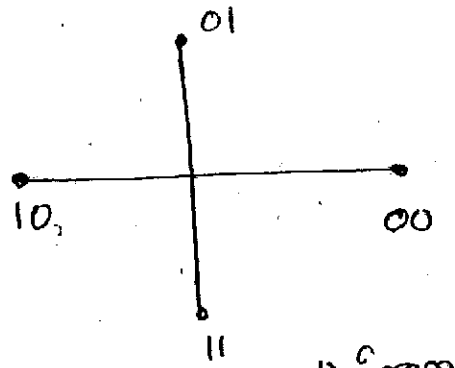
- PSK is not susceptable to noise degradation that affects ASK or to the bw limitation of FSK. A small variation in the signal can be detected by receiver.
- We can represent 4-variation and let each phase shift represent 2 bits



- This technique is called 4-PSK or Q-PSK. The pair of bits represented by each phase is called a dibit. We can transmit data twice as efficiency using 4-PSK as we can using 2-PSK.

4-PSK characteristics

Dibit	Phase
00	0
01	90
10	180
11	270

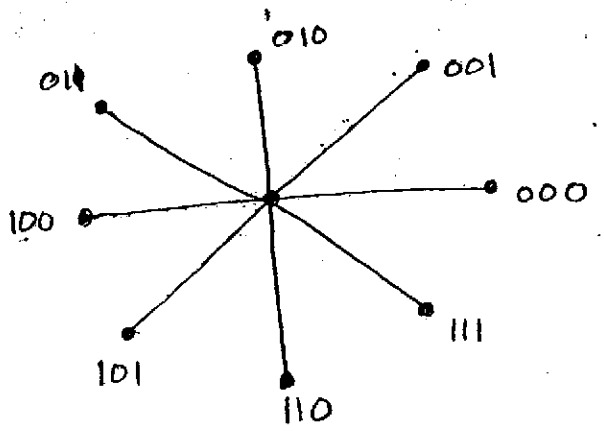


Constellation diagram.

- We can extend 4-PSK to 8PSK, where we vary the signal by shifts of 45°. Bits represent by each phase called Tribit.

8-PSK characteristics

Tribit	Phase
000	0
001	45
010	90
011	135
100	180
101	225
110	270
111	315

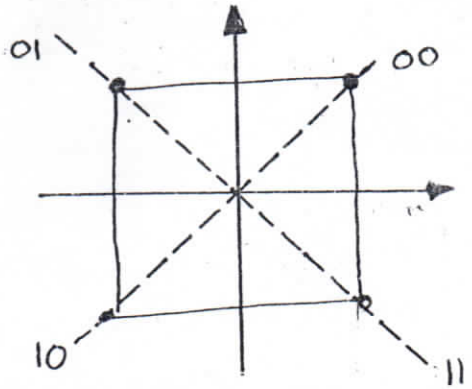


Bandwidth for PSK

- Min^m Bandwidth required for PSK transmision = Bandwidth required for ASK transmision.
- PSK bit rates using the same bandwidth can be 2 or more ~~times~~ greater; while the maximum baud rate for PSK and ASK are the same.

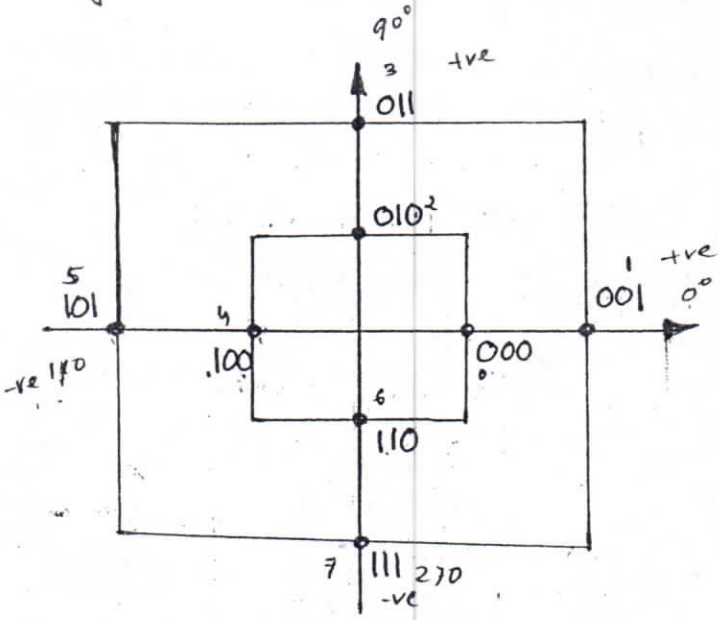
Quadrature Amplitude Modulation:

- PSK is limited by the ability of the equipment to distinguish small differences in phase. The factor limits its potential bit rate.
- QAM is a combination of ASK and PSK, so that a maximum contrast between each signal unit (bit, debit, tribit and so on).
- We have two possible configuration i.e 4-QAM and 8-QAM because amplitude changes are susceptible to noise and, require greater shift differences than phase changes, the number of phase shift used by a QAM is always larger than no. of amplitude shifts.



4-QAM

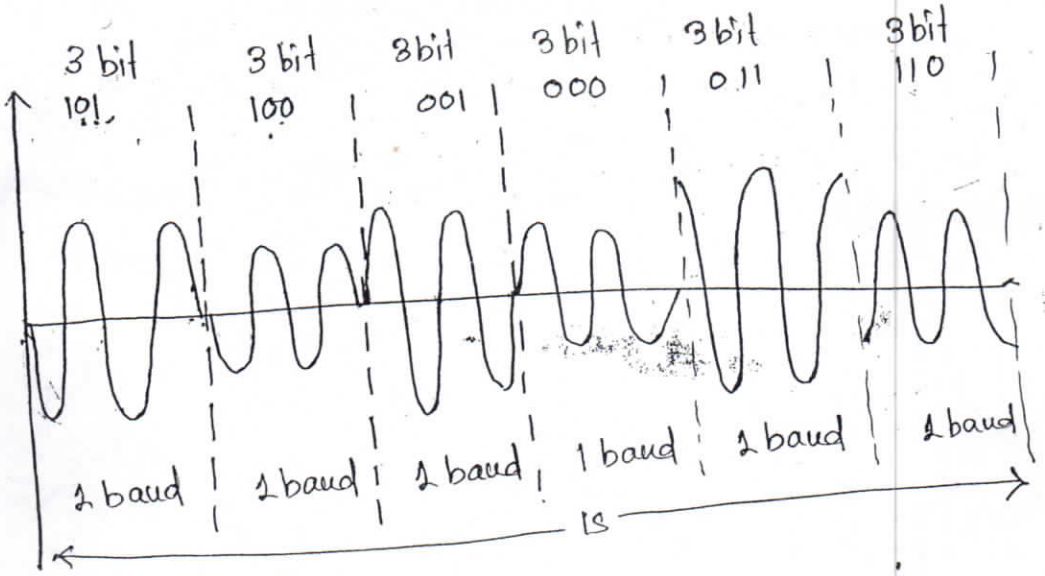
1 amplitude, 4 phase



8-QAM

2 amplitude, 4 phase

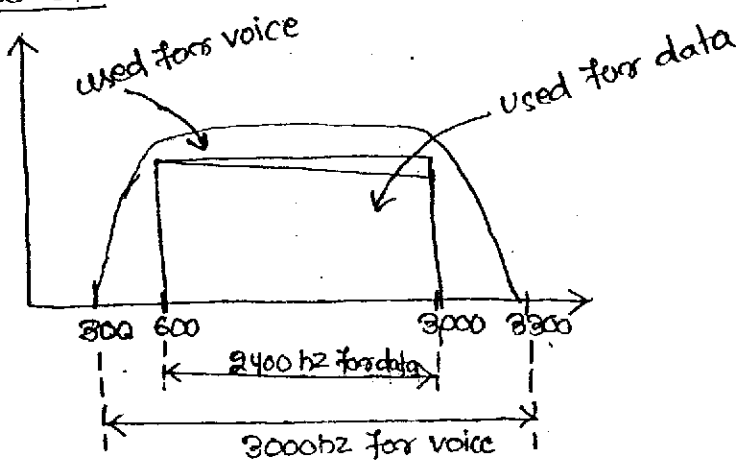
4-QAM and 8-QAM constellation



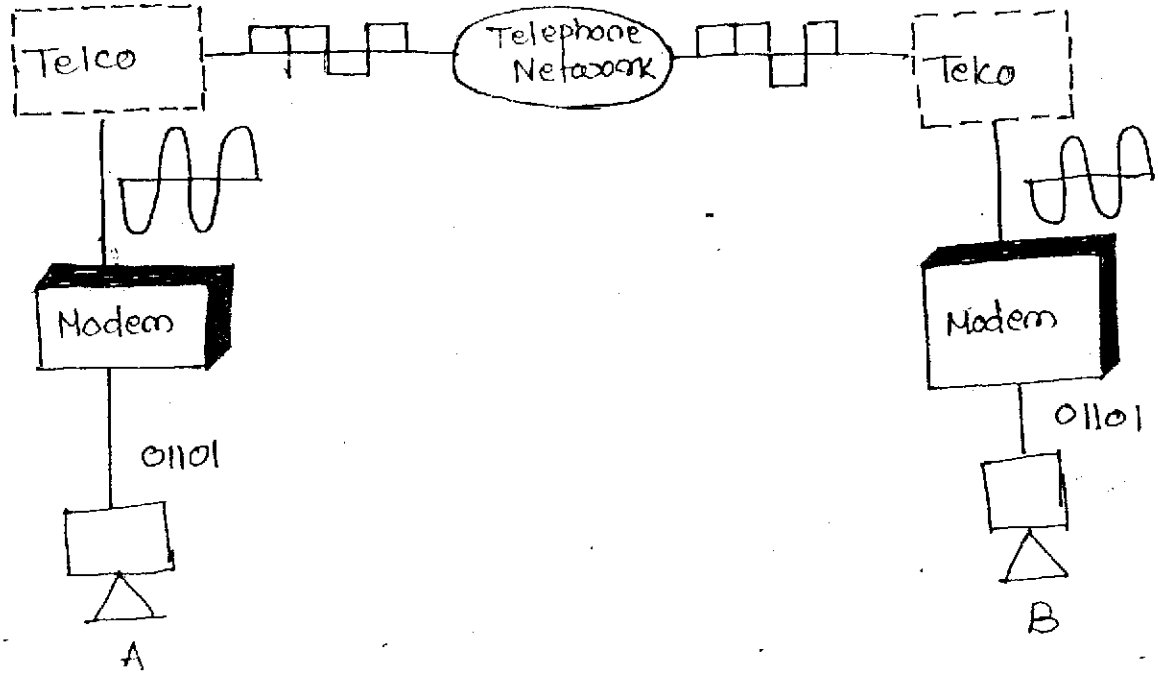
TELEPHONE MODEMS

- Traditional telephone lines can carry frequencies 300 and 3000hz. A telephone line has a bw of almost 2400 hz of data transmission.
- This bandwidth defines a baseband nature, which means we need to modulate if we want to use this bw for data transmission, Device that were traditionally used to do so are called modems.
- Modem is a coined word refers to the two functional entities that make up the device: a signal modulator and a signal demodulator.
- A modulator creates a band-pass analog signal from binary data. A demodulator recovers the binary data from the modulated signal

- Telephone line bw



- Modem stands for Modulation/Demodulation

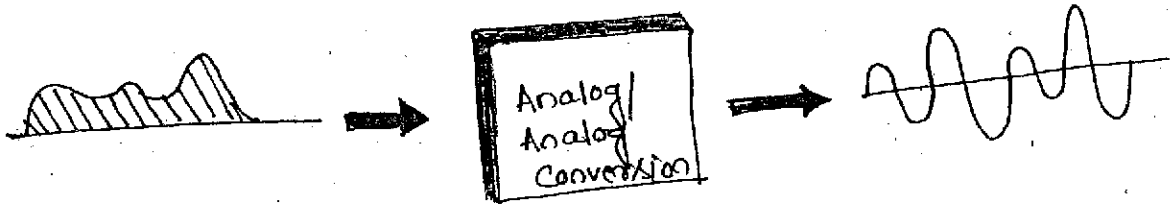


It shows the relationship of modems to a communication link. The computer on the left send binary data to the modulator portion of the modem. The data is sent as an analog signal on the telephone lines. The modem on the right receives the analog signal demodulates it through its demodulator, which means the computer on the right can also send data to the computer on the left using the same modulation/demodulation process.

MODULATION OF ANALOG SIGNALS

Modulation of an analog signal or analog-to-analog conversion is the representation of analog information by an analog signal. Though we have analog signal modulation is needed if the medium has a band-pass nature and the analog signal available is low-pass-signal.

Figure shows the relationship between analog information, the analog to analog conversion hardware, and the resultant analog signal.



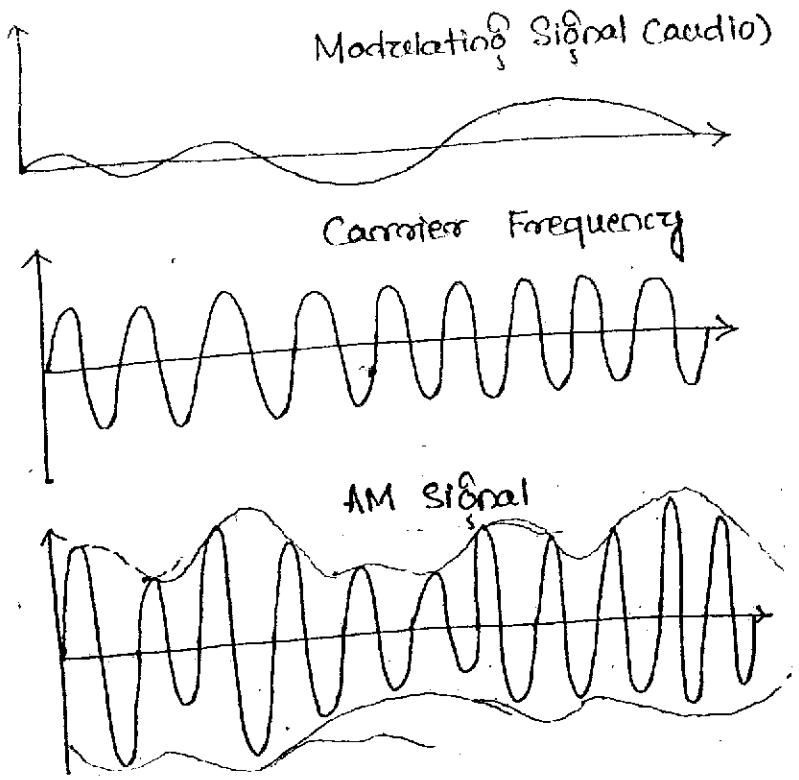
Analog to analog modulation can be accomplished in 3 way

(i) Amplitude Modulation (AM)
(ii) Frequency Modulation (FM)
(iii) Phase Modulation (PM)

Amplitude Modulation:

In AM transmission, the carrier signal is modulated so that its amplitude varies with the changing amplitude of modulating signal.

The phase and frequency of the carrier remain the same.



AM Bandwidth:

- The bw of AM signal is equal to twice the bw of the modulating signal and covers a range centered on the carrier frequency
- BW of audio signal is 5 KHz. So AM radio station needs a minimum bw of 10Khz.
- The total bw required for AM can be determined from the bw of the audio signal

$$\boxed{BW_t = 2 \times BW_m}$$

$BW_m \rightarrow$ BW of the modulating signal

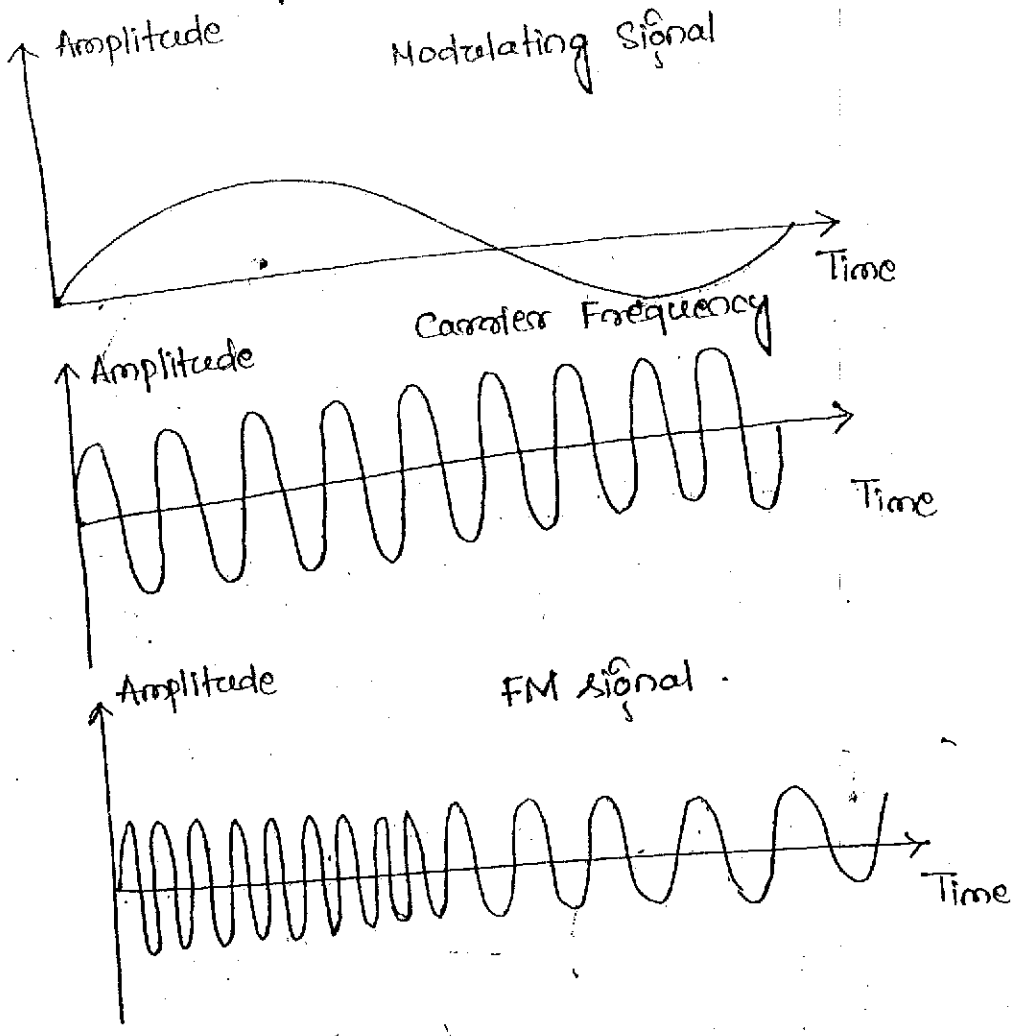
$BW_t \rightarrow$ Total BW

$f_c \rightarrow$ Frequency of the carrier

Frequency Modulation

- On FM modulation the frequency of the carrier signal is modulated to follow the changing voltage level (amplitude) of the modulating signal.

- The peak amplitude and ~~frequency~~ phase of the carrier signal remain constant, the frequency of the carrier changes correspondingly



FM Bandwidth

- The bw of an FM signal is equal to 10 times the bw of the modulating signal
- The bw of an audio signal broadcast is stereo is almost 15 Khz. So each FM radio station therefore needs a minimum bw of 150 Khz.
- The total bw required for FM can be determined from the bw of the audio signal

$$BW_t = 10 \times BW_m$$

$BW_m \rightarrow$ Bw of modulating signal

$BW_t \rightarrow$ total Bw

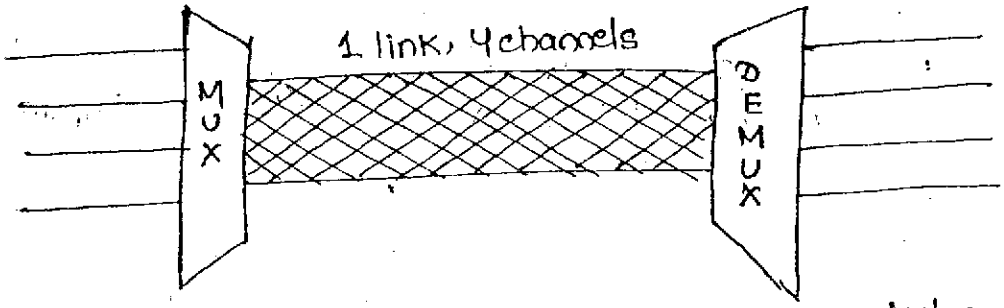
$f_c \rightarrow$ frequency of carrier.

Phase Modulation:

- Due to simpler h/w requirement PM is used in some system as an alternative to FM.
- In PM transmission the phase of the carrier signal is modulated to follow the changing voltage level of the modulating signal.
- The amplitude and frequency remain constant.
- The analysis of modulated signal are similar to those of frequency modulation.

MULTIPLEXING

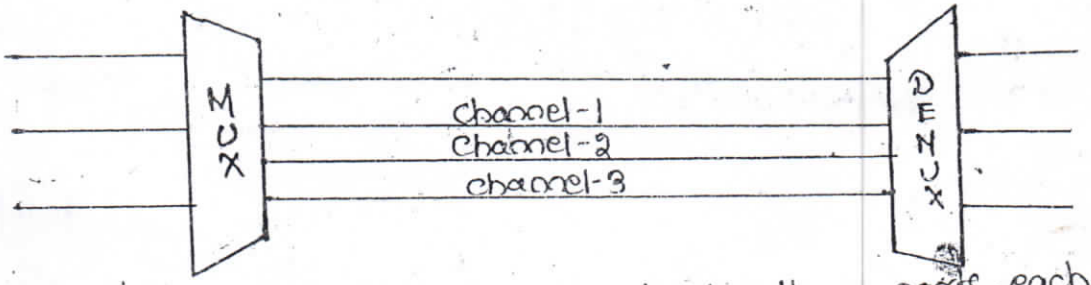
- Multiplexing is the set of technique that allows the simultenious transmision of multiple signal across a single data link.
- In a multiplexed system, n lines share the bw of one link.



- The four lines on the left direct their transmission stream to a multiplexor (MUX), which combines them into a single stream.
- At the receiving end that stream is fed into a demultiplexor (DEMUX), which separate the stream back into its component transmision and direct them to their corresponding lines.
- Link refers to a physical path. The word channel refers to the portion of the link that carries a transmission between a given pair of lines. One link can have n channels.
- Signals are multiplexed by one of the three basic techniques
  - (i) Frequency division multiplexing (FDM) } → Analog
  - (ii) Wave division multiplexing (WDM) }
  - (iii) Time division multiplexing (TDM) } → Digital

Frequency Division Multiplexing: (FDM)

- FDM is an analog technique that can be applied when the bw (in hz) is greater than the combined bw of the signal to be transmitted.
- In FDM, signal generated by each sending device modulate diff. carrier frequency.
- These modulated signals are then ~~connected~~ combined into a single composite signal that can be transported by the link.
- Carrier frequencies are separated by sufficient bw to accomodate the modulated signal. These bw range are the channels through which various signal travel.
- channels must be separated by strips of unused bw (guard bands) to prevent signals from overlapping.
- Carrier frequency must not interface with original data frequency.



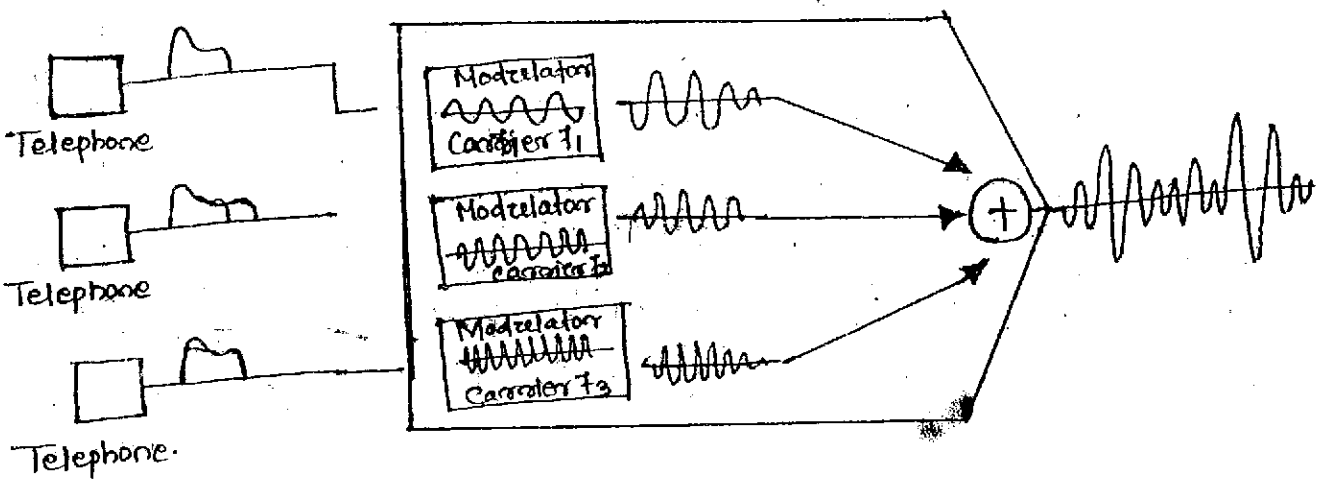
- Here the transmission part is divided into three parts, each corresponding a channel to carry one transmission, without interfering with each other.

Multiplexing Process:-

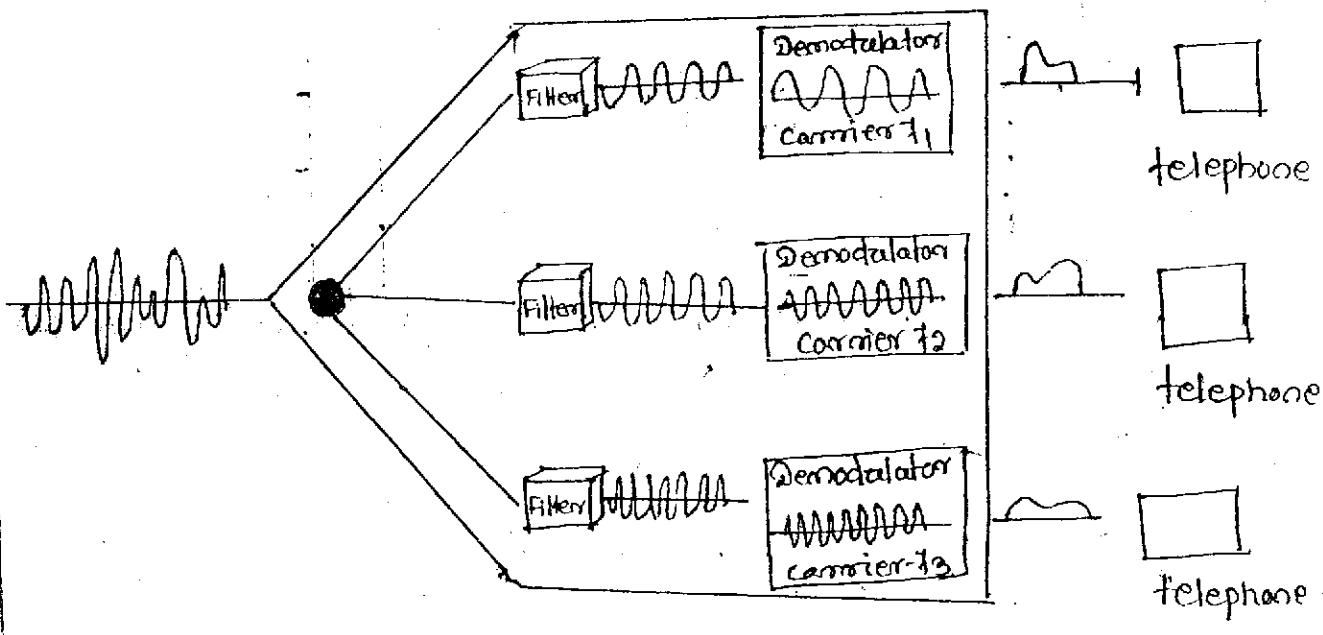
- FDM is an analog process, and the i/p devices used are the telephones.
- Each telephone generate a signal of similar frequency range. Inside the multiplexor, these similar signals are modulated onto different carrier frequencies (f1, f2 and f3)
- These resulting signals are then combined into a composite signal that sent over a link that has enough bw to accomodate

Demultiplexing Process :-

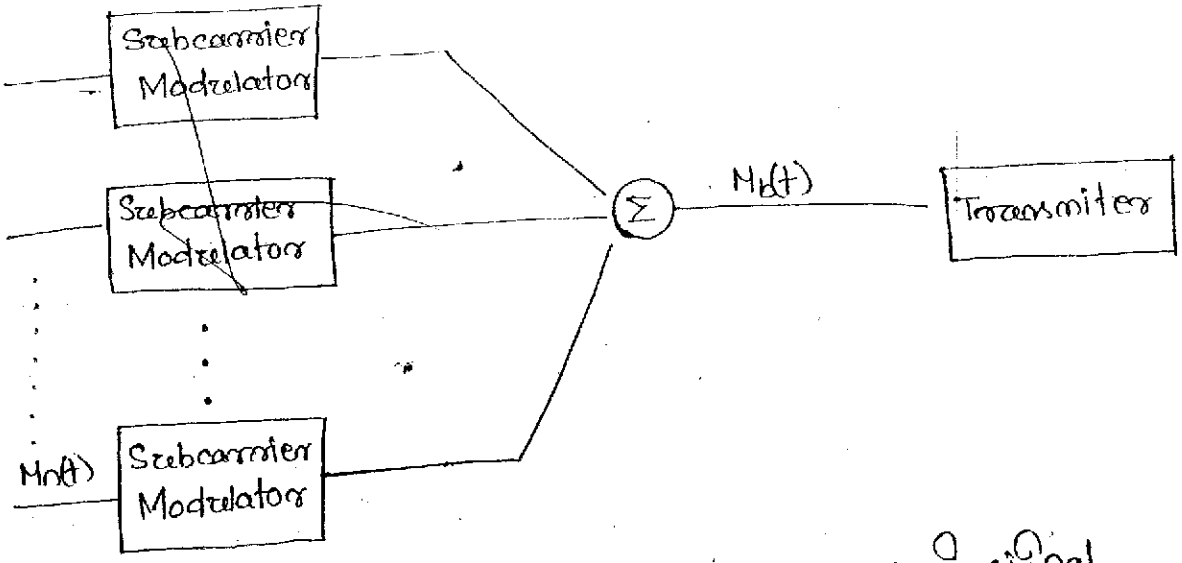
- Demultiplexor uses a series of filters to decompose the multiplexed signal into its constituent component signals. The individual signals are then passed to a demodulator that separates them from their carriers and passes them to the waiting receivers.



FDM Multiplexing process

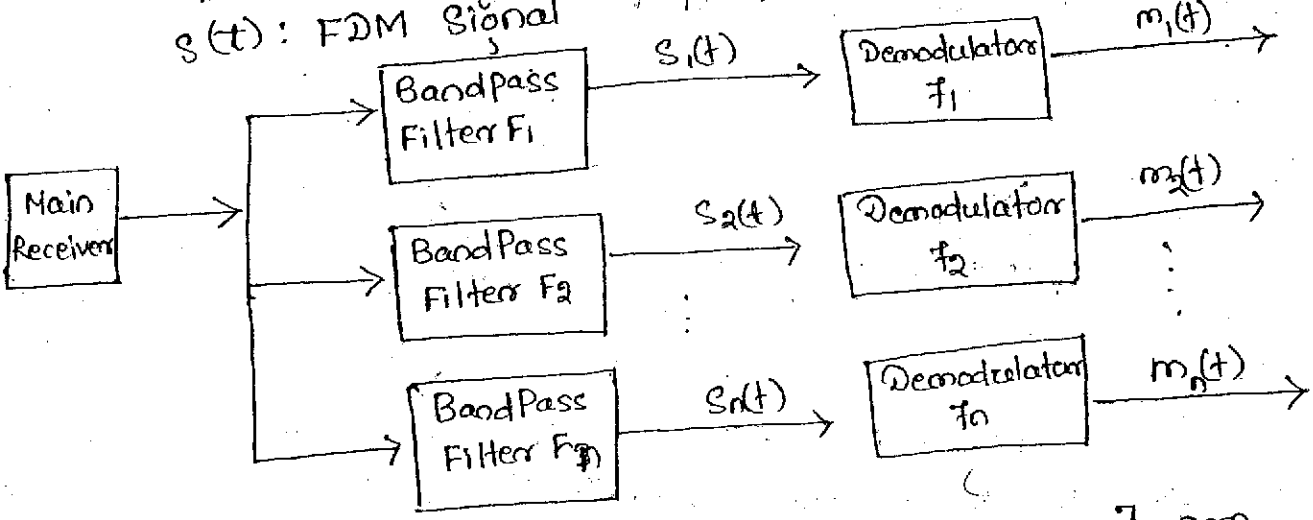


FDM Demultiplexing Process



$m_b(t)$: Composite baseband modulating signal

$s(t)$: FDM signal



× A no. of analog or digital signals $[M_i(t), i \to 1 \cdots n]$ are to be multiplexed. Each signal $M_i(t)$ is modulated onto a carrier f_i, because multiple carriers are to be used, each is refered to a subscriber. The resulting analog modulated signals are then summed to produce a composite bandpass signal $M_b(t)$

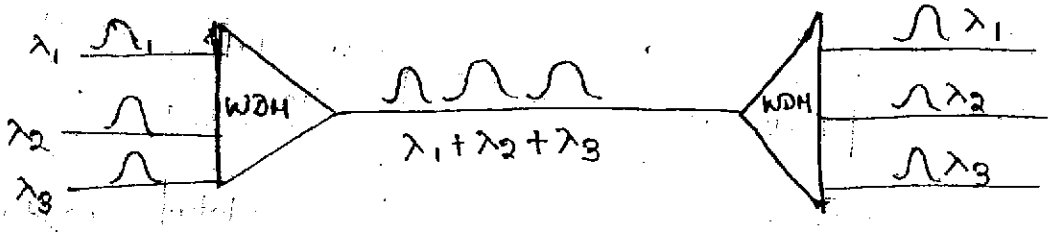
The FDM signal $s(t)$ has a total bw B, where $B > \sum_{i=1}^{n} B_i$

Thus analog signal may be transmitted over a suitable medium. At the receiving end the FDM signal is demodulated to retrive $M_b(t)$, which is then passed through n band pass filters, each filter centered on f_i and having a bw B_i, for $1 \le i \le n$.

- In this way the signal is again split into its component parts. Each component

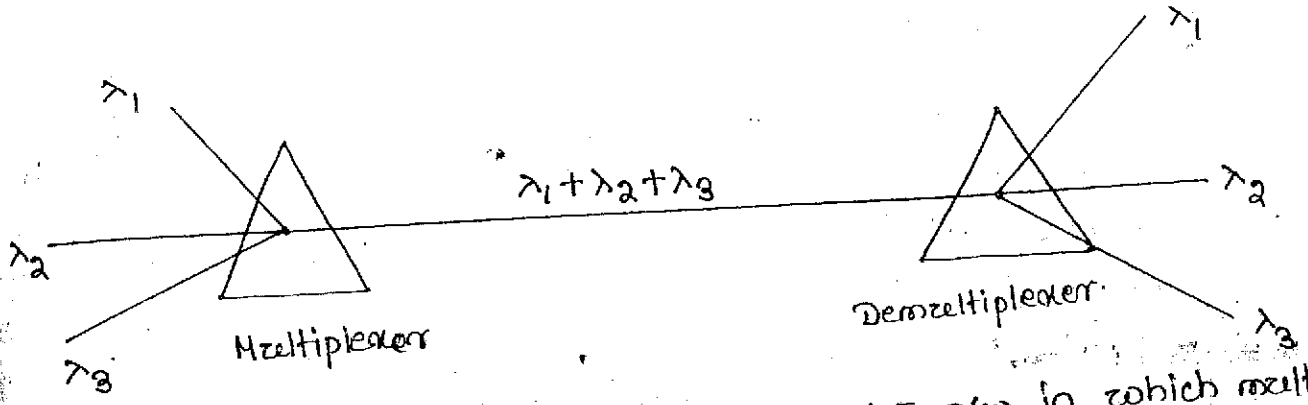
Wave Division Multiplexing: (WDM)

- WDM is designed to use the high data rate capability of fiber optic cable.
- The optical fiber data rate is higher the data rate of metallic transmission cable. The true potential of optical fiber is fully explited.
- When multiple beams of light at different frequencies are transmitted on the same fiber, this is a form of FDM, but is commonly called WDM.



- WDM varies from FDM in the way that multiplexing and demultiplexing involps optical signals transmitted through fiber optic channels.
- In figure very narrow band of light from different sources are combined to make wider band of light. At receiver signals are separated by demultiplexer.
- In WDM we want to combine multiple light sources into one single light at the multiplexor and do the reverse at the demultiplexor. The light streaming through fiber optics consist of many colors or wavelengths.
- Combining and spliting of light sources are easily handled by a prism, because prism bends a beam of light based on the angle of incidence and the frequency.

Using this technique a multiplexer can be made to combine several input beams of light each containing a narrow band of frequencies, into one output stream of a wider band of frequencies.

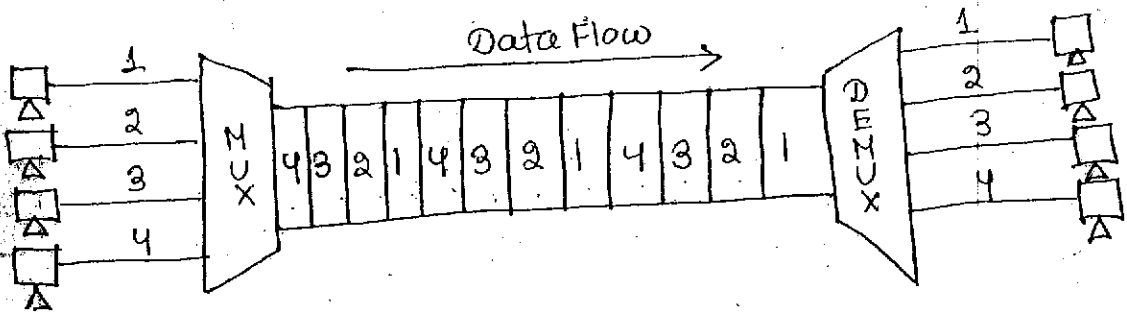


e.g.: one application of WDM is the SONET n/w in which multiple optical fiber lines are multiplexed and demultiplexed.

Time division multiplexing: (TDM)

TDM is a digital process that allows several connection to share the high bw of a link.

Here time is shared. Each connection occupies a portion of time in the link / Link is sectioned by time rather than frequency.



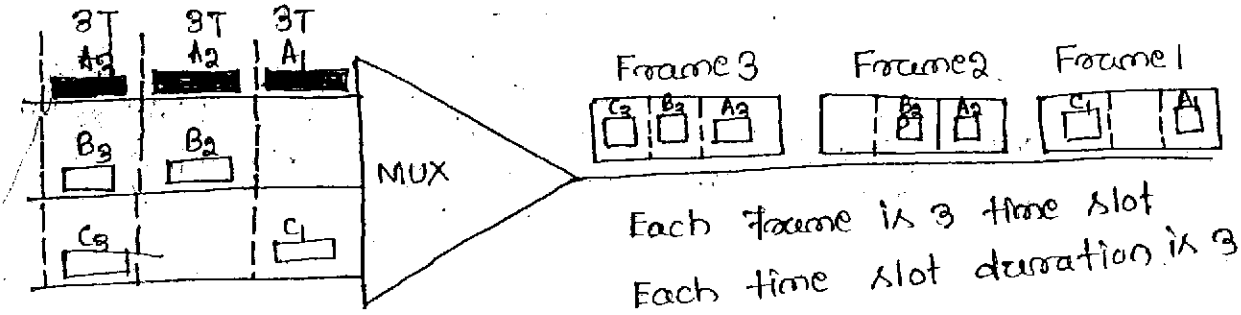
Time Slots and Frames:

The data flow of each connection is devided into units and the link combines one unit of each connection to make a frame.

The size of the unit can be 1 bit or several bits. For n input connections a frame is organized to minimum of

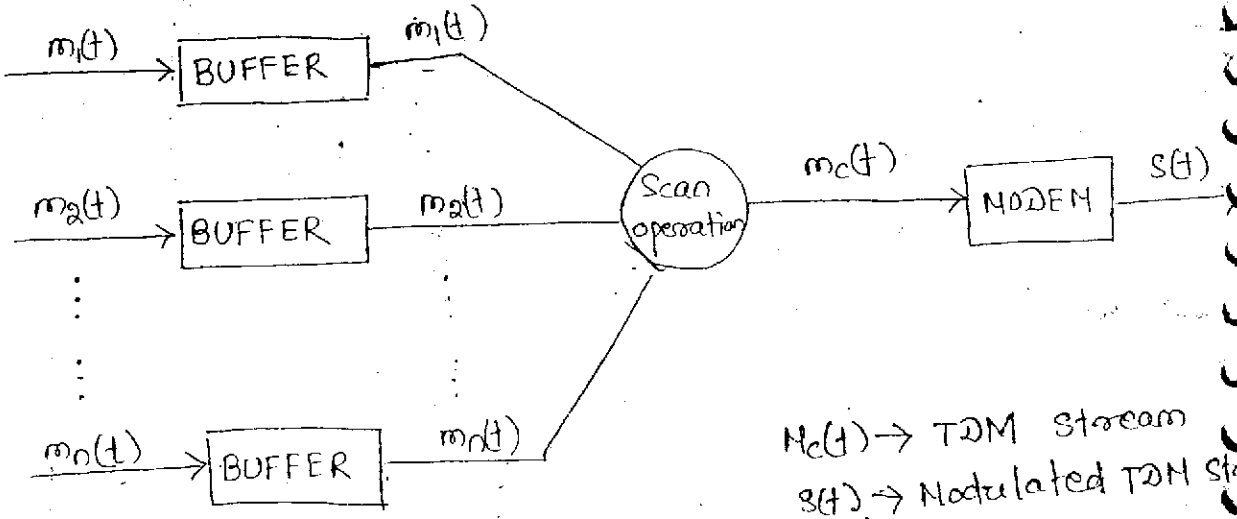
n time slots, each slot carrying one unit from each connection.

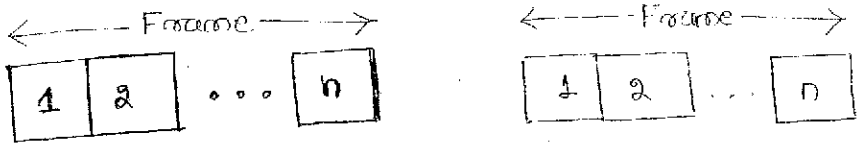
- On a TDM, the data rate of the link is n times faster, & the unit duration is n times shorter.
- Time slots are grouped into frames. A frame consist of one complete cycle of time slots, with one slot dedicated to each sending device.
- On a system with n i/p lines, each frame has n slots, with each slot allocated to carrying data from a sp. i/p line.



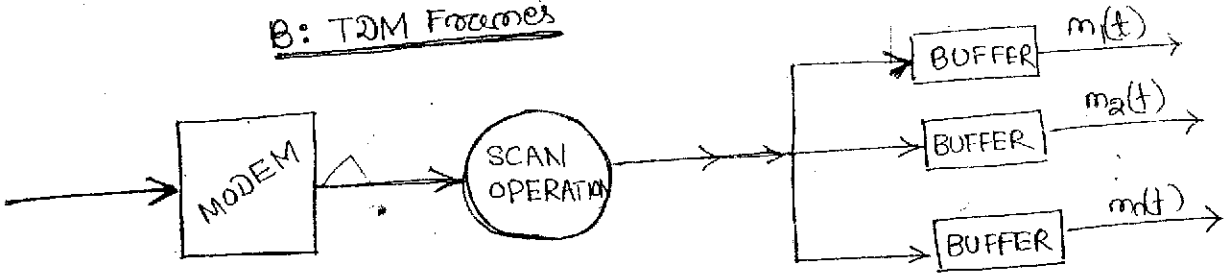
A general description of TDM:

- TDM is possible when the achivable data rate of the medium exceeds the data rate of digital signal to be transmitted.
- Multiple digital signals (or analog signal carrying digital data) can be carried on a single transmission path by interleaving portions of each signal, in time.





B: TDM Frames



C: Receiver

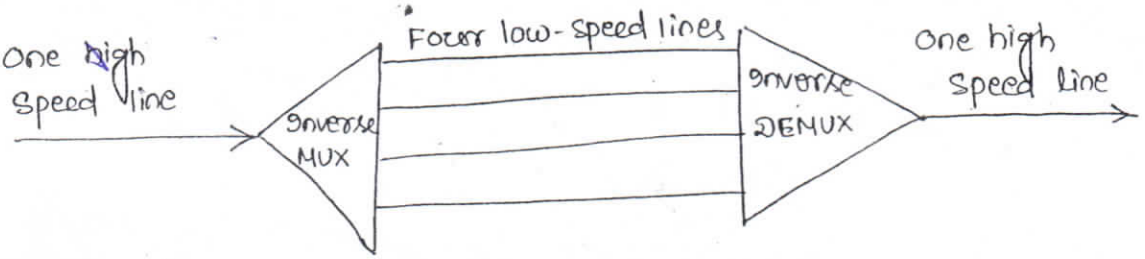
- The no. of signals [mi(t), i = 1 ... n] are to be multiplied onto the same transmission medium.
- The signals carry digital data are generally digital signals.
- The incoming data from each source are briefly buffered. Each buffer is typically one bit
- The scan operation is sufficiently rapid so that each buffer is emptied before more data can arrive.
- Byte interleaving technique is used with asynchronous and synchronous sources. Typically the start and stop bit of each character are eliminated before transmission and reinserted by the receiver, thus improve efficiency.
- At the receiver the interleaved data are demultiplexed and routed to the appropriate destination that will receive the output data at the same rate at which it was generated.

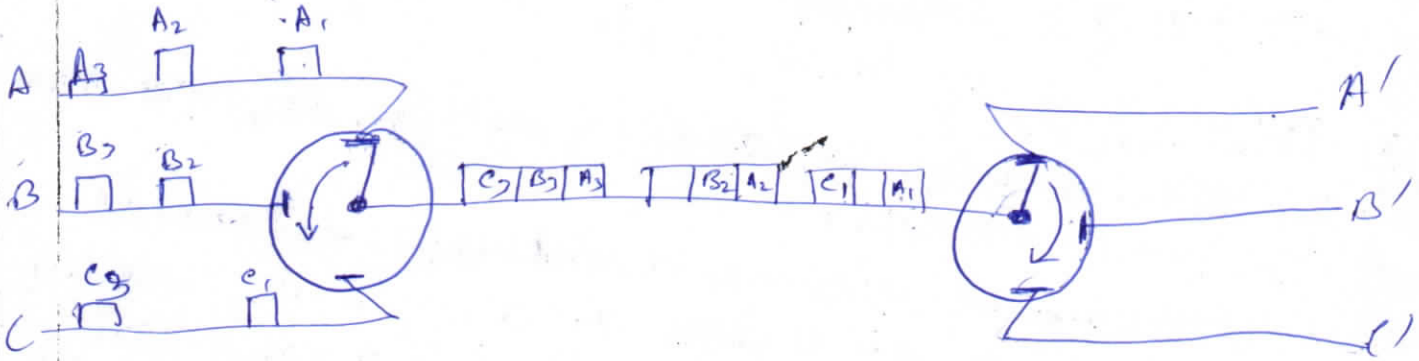
Interleaving:

TDM can be visualised as two fast routing switches, one at the multiplexing side and other at the demultiplexing side. The switches are synchronised and rotate at the same speed but in opposite directions.

Inverse TDM:

In inverse multiplexing, it takes the data stream from one high speed line and breaks it into portion that can be sent across lower speed lines simultaneously with no loss in the collective data rates





TRANSMISSION MEDIA

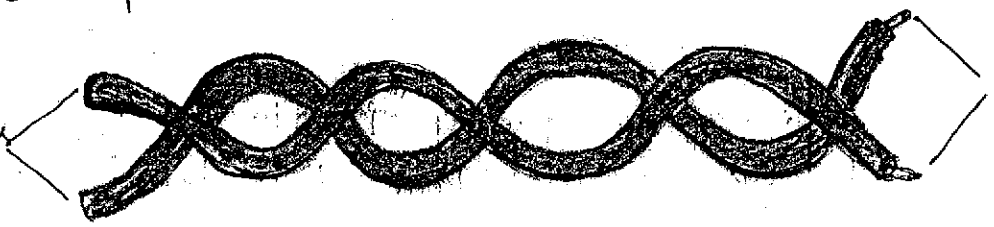
- Transmission media is located below the physical layer and directly controlled by physical layer.
- The signals are transmitted from one device to another in the form of electromagnetic energy which is propagated through transmission media.
- For the purpose of telecommunications, transmission media can be devided into two broad categories
  - (i) Guided
  - (ii) Unguided
- Guided media includes twisted pair cable, co-axial cable and fiber optic cable.
- Unguided medium is usually air.

GUIDED MEDIA:

- Guided media, which are those that provide a conduit (channel) from one device to another.
- It include twisted-pair cable, co-axial cable and fiber-optic cable. Twisted-pair and co-axial cable use metallic conductor that accept and transport signals in the form of electric current. Optical fiber is a glass cable that accepts and transport signal in the form of light.

Twisted-Pair Cable:-

- A twisted pair consists of two conductors (copper) each with its own plastic insulation, twisted together.



Twisted Pair Cable

- One of the wires is used to carry signals to the receiver. and the other is used only as grounded reference.
- The receiver uses the difference between two levels.
- In addition to the signal sent by the sender on one of the wires, interface and crosstalk may affect both wires and create unwanted signal.
- The receiver at the end however, operates only on the difference between those unwanted signals.
- This means that if the two wires are affected by noise or crosstalk equally, the receiver is immune (the difference is zero)
- If two wires are parallel. the effect of these unwanted signal is not same in both the wires because they are at different location relative to noise or crosstalk.
- This result in a difference at the receiver, By twisting the pairs, a balance is maintained.
- Twisting makes it probable that wires are equally affected by external influences (noise or crosstalk). This means that the receiver which calculates the difference between the two receive no unwanted signal. Appl":→ using Telephone n/w Connector→ UTP connector

Unshielded vs Shielded twisted pair cable:—

- The most common twisted pair cable used in communication is refered to as unshielded twisted pair (UTP). IBM has also proceeded a version of twisted pair cable for its use called shielded twisted pair (STP).
- STP cable has a metal foil covering that encases each pair of insulated conductors.
- Although metal improves the quality of cable by preventing the penetration of noise or cross talk, it is bulkier and more expensive.

Performance:

One way to measure the performance of twisted pair cable is to compare attenuation versus frequency and distance.

Application:

- Twisted pair cables are used in telephone lines to provide voice and data channels.

Categories:

- The Electronic Industrial Association (EIA) has developed standards to classify twisted pair cable into seven categories.
- Categories are determined by cable quality with 1 as the lowest and 7 as the highest.

Category 3 and Category 5 UTP:

- Category 3 and category 5 UTP has received the most attenuation for LAN application. Category 3 corresponds to the voice grade cable found in most office breilding.
- UTP cables are associated connecting h/w zobase transmission characteristics are specified upto 16Mhz in category 3 and 100 mhz in category 5.
- Category 5 is a data grade cable that is becoming increasing common for preinstallation.
- A key difference between them is the no. of twists in the cable per unit distance
- Category 5 is more tightly twisted and is more expensive and provides more better performance.

Coaxial Cable:

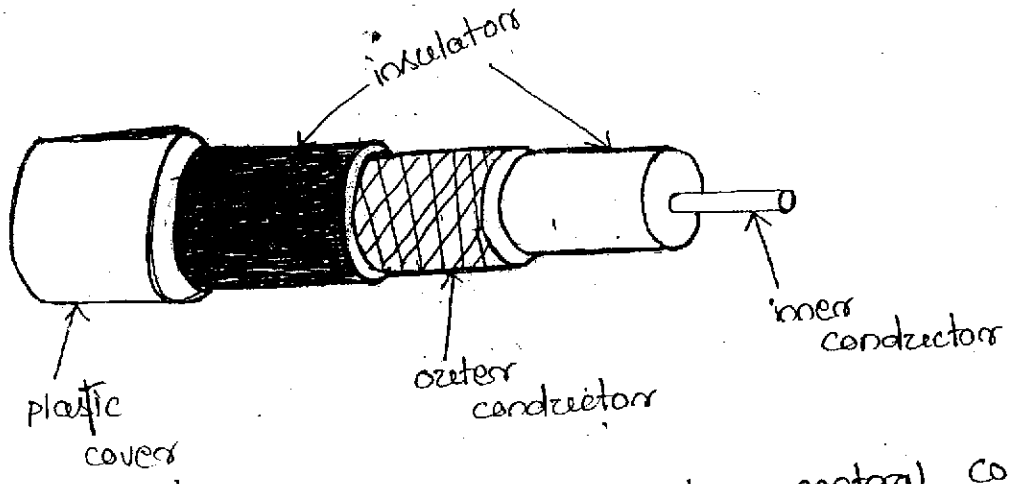
- Coaxial cable carries signal of higher frequency ranges then twisted pair cable, because the two media are constructed differently.

cable TV n/w

connector → BNC connector

Physical description:

- Coaxial cable like twisted pair consist of 2 conductors bcet is constructed differently to permit it to operate over a wide range of frequency.



- Instead of having two-wires coax has central core conductor of solid or standard wire (copper) enclosed in an insulating sheath, which is encased in an outer conductor of metal foil, braid or a combination of the two.
- The outer metallic wrapping serves both as a shield against noise and as a second conductor, which completes the circuit.
- outer conductor is also enclosed in an insulating sheath and the whole cable is protected by plastic cover.
- Coaxial cable can be used over long distance.

Applications

- Coaxial cable is perhaps the most versatile transmission medium and is enjoying wide variety of applications.
  - Television distribution
  - Long distance telephone transmission.
  - Short-run computer system links
  - Local area Networking.

Transmission characteristic:

- Co-axial cable is used to transmit both analog and digital signal.
- Because of its shielded, concentric construction, coaxial cable is much less susceptible to interface and crosstalk than twisted pair.
- For long distance transmission of analog signals amplifiers are needed, every few kilometers with closer spacing required if higher frequencies are required for digital signaling repeaters are needed every kilometer, with closer spacing required for high data rates.

Coaxial Cable Connectors:

- To connect co-axial cable to devices we need, co-axial connectors The most common type of connector used today is Bayone-Neill-Concelman or BNC connector.

Fiber optic Cable:

Fiber optic cable is made of glass or plastic and transmit signals in form of light.

Physical description:-

optical fiber is a thin (.2 to 125) flexible medium capable of guiding an optical ray.

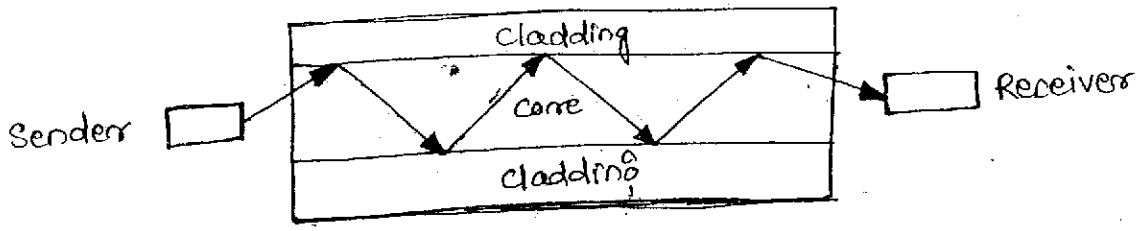
Various glasses and plastics are used to make optical fibers optical fiber cable has a cylindrical shape and consist of three concentric sections

the core, cladding and the jacket.

core is the inner most section and consist of one or very thin strands, or fiber made of glass or plastics. diameter in the range of 8-100 μm.

is surrounded by its own cladding, a glass or that has optical properties different from

- The interface between core and cladding act as a reflector to confine light that would otherwise escape the core.
- The outer most layer, surrounding one and a bundle of cladding fibers is the jacket. The jacket is composed of plastic and material layered for other environmental danger.



Optical fiber

Applications:

- Long distance telecommunication
- Some TV companies use a combination of optical fiber and co-axial cable that creates a hybrid n/w.

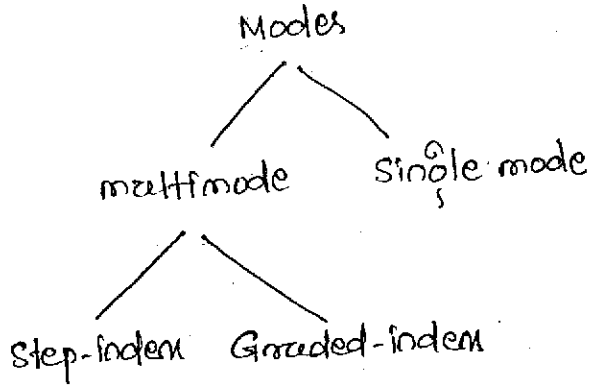
Characteristics:

- Greater capacity
- Smaller size and lighter weight.
- Lower attenuation.
- Electromagnetic isolation.
-

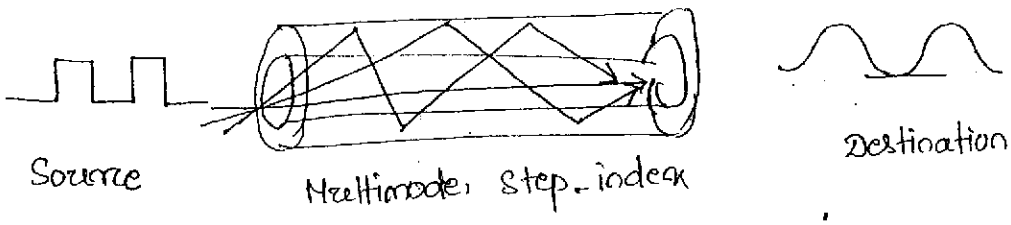
Transmission characteristics: (propagation)

- optical fiber transmits a signal encoded beam of light by means of total internal reflection.
- Total internal reflection can occur in any transparent medium that has a higher index of reflection than the surrounding medium.
- Light from a source enter the cylindrical glass or plastic core rays at shallow angles are reflected and propagated along the fiber, other rays are absorbed by the surrounding material

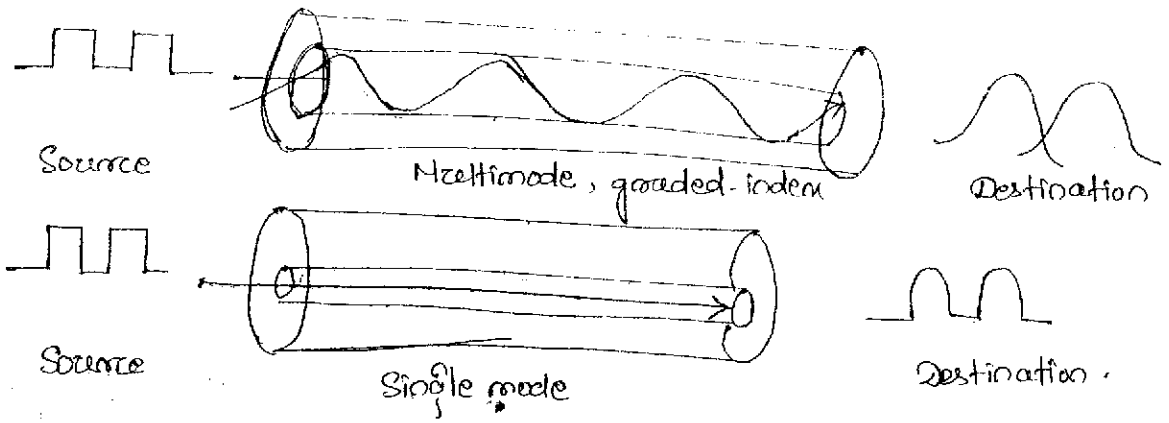
- This form of propagation is called step-index multimode, referring to variety of angles that will reflect.
- With multimedia transmission multiple propagation path exist each with different path length and hence time to traverse the fiber. This cause signal elements (light pulses) to spread out in time, which limits the rate at which data can be accurately received.
- When the fiber core radious is reduced fewer angles will reflect. By reducing the radious of the core to order of wavelength only a single mode can pass the axial ray.
- This single mode propagation provides superior performance for the following reason. Because there is a single transmission path with single mode that is typically used for long distance applications including television and cable television.
- Finally by varying the index of refraction of the core a third type of transmission called as graded index multimode
- The higher refractive index at the center makes the light rays moving down the axis advance more slowly than those near the cladding.



Modes



Multimode, step-index


Source
Multimode, graded-index
Destination

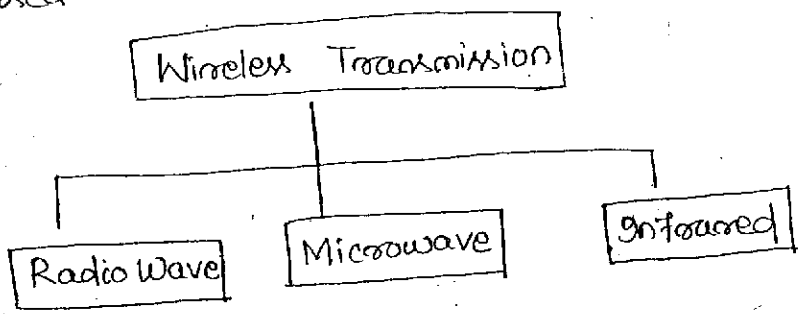
Source
Single mode
Destination

UNGUIDED MEDIA

- Unguided media transport electromagnetic wave without using a physical conductor. This type of communication is referred as wireless communication. Signals are normally broadcast through air and thus are available to anyone who has a capacity of receiving them.

Wireless:

- Unguided signal can travel from source to destination in several ways i.e ground propagation, sky propagation, line-of-sight propagation.
- In ground propagation radio waves travel through the lowest portion of atmosphere. Distance depend upon the amount of power in the signal. The greater the power, the greater the distance.
- In sky propagation, higher frequency radio waves radiate upward into the ionosphere where they are reflected back to earth. It allows for greater distance with lower power o/p.
- In line-of-sight propagation, very high frequency signals are transmitted in straight lines, directly from antenna to antenna. It is tricky because radio transmission cannot be completely focused.



Waves

- ...gnetic waves ranging in frequency between 3 KHz to 1 GHz ...ally called radio waves.
- ...for the most part are omnidirectional. When an ...transmits radiowaves, they propagate in all directions. ...have to be aligned.
- ...are used for long distance broadcasting such as ... they can travel long distances.

- Radio waves with low and medium frequencies can penetrate walls. As the frequency is very low comparatively microwave when divided into subbands lead to low data rate for digital communication.

Microwave

- Electromagnetic wave having frequencies between 1 and 300 Ghz are called microwaves.
- Microwaves are unidirectional. When an antenna transmits microwaves can be narrowly focused. Antenna need to be aligned.
- Microwave propagation is line-of sight. Since the towers with the mounted antennas need to direct sight of each other and to be tall.
- Repeaters are often needed for long distance communication.
- High frequency microwave cannot penetrate walls. This can be a disadvantages if receiver are inside building.
- Microwave band is relatively wide almost 299 Ghz.
- Use of certain portions of the band requires permission from authorities.

Infrared:

- Infrared signals with frequencies 300GHz to 400 THz can be used for short range communication.
- Infrared wave having high frequency cannot penetrate wall.

advantage: a short range communication system in one room cannot be affected by systems in another room.

Disadvantage: Useless for long distance transmission.

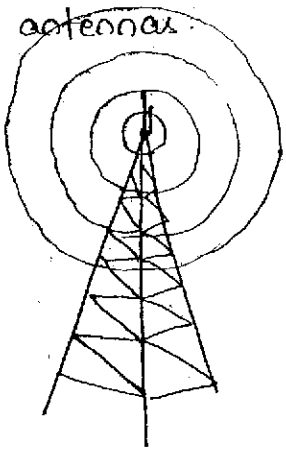
- We cannot use infrared outside the building because rain's ray containing infrared can interfere with communication.

Applications

Radiowave	Microwave	Infrared
on Multicasting purpose where there is one sender and many receiver. - AM, FM radio - Meritime radio - cordless phone	Unicasting comm° where one sender and one receiver is there - Cellular phones - Satellite Network - Wireless LAN	- communication with a PC. - The IrDA port on the keyboard needs to point to PC for transmission

Omnidirectional Antenna

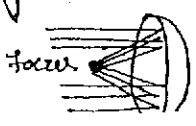
- Radio waves use omnidirectional antennas that send out signals in other directions.
- Based on wavelength, strength and purpose of transmission we have several antennas.

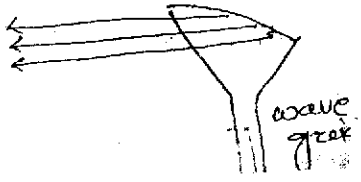


Unidirectional Antenna:

waves need unidirectional antenna that send out signal direction

Parabollic dish antenna	Horn antenna
on geometry of parabolla olic disk works like atching wide range of and directing them to a point.	- looks like a gigantic scoop.

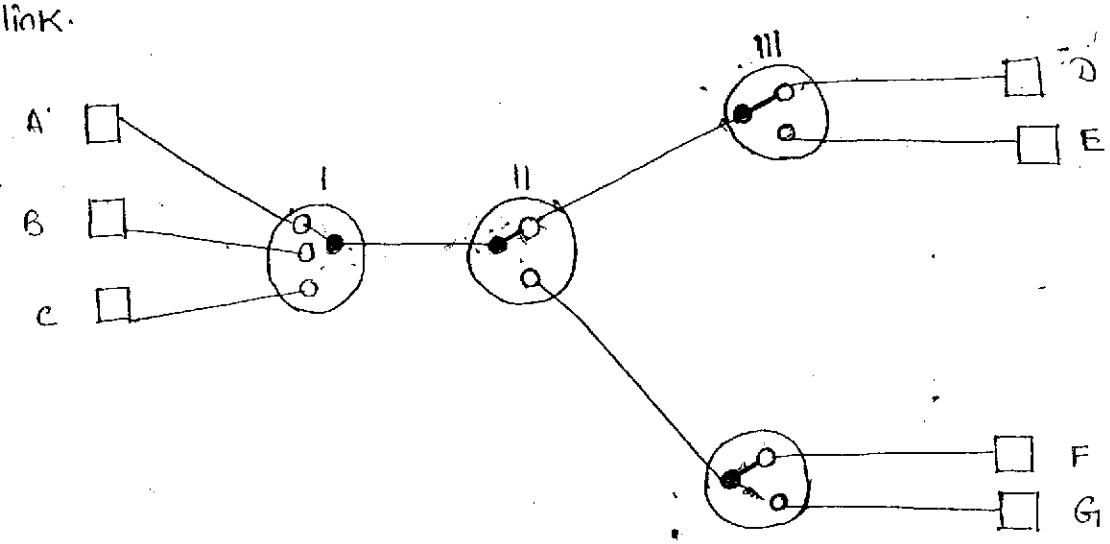




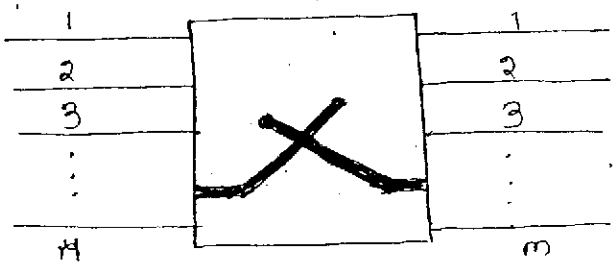
CIRCUIT SWITCHING AND TELEPHONE NETWORK:

CIRCUIT SWITCHING:

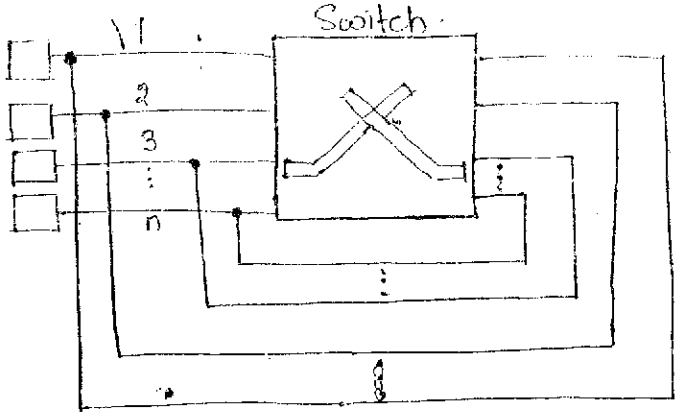
- Circuit switching creates a direct physical connection bet? two devices such as phones or computers.
- Following figure shows point-to point connections between 3 telephone A, B and C and ~~four~~ three telephones require 12 links. We can use four switches to reduce the no and total length of the link.



- Telephone A is connected to D through switch I, II, III.
- A circuit switch is a device with n i/p and m o/ps that creates a temporary connection between an i/p link and o/p link. The no. of i/p doesn't have to match the no. of o/p.



- A n by n folded switch can connect n lines in full duplex mode. i.e it can connect n telephones in such a way that each phone can be connected to every other phone.



Folded Switch

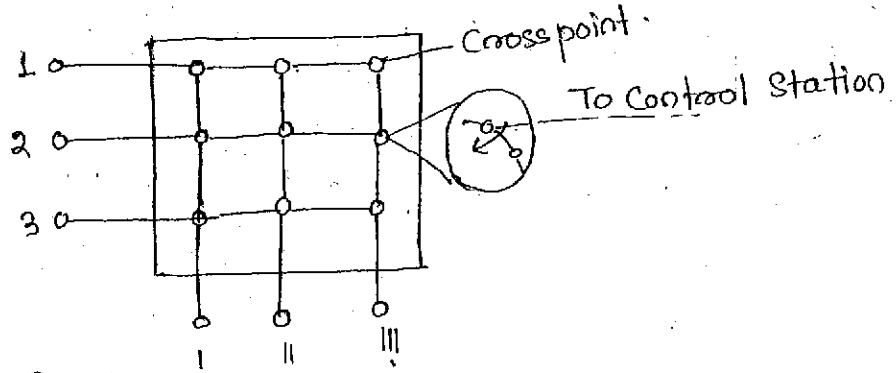
Circuit Switching is today can use either of two technologies
(i) Space-division switch
(ii) Time-division switch.

Space division Switch:

- In space division switch the paths in the circuit are separated from each other spatially. It is used in both analog and digital n/w.

Crossbar Switch:

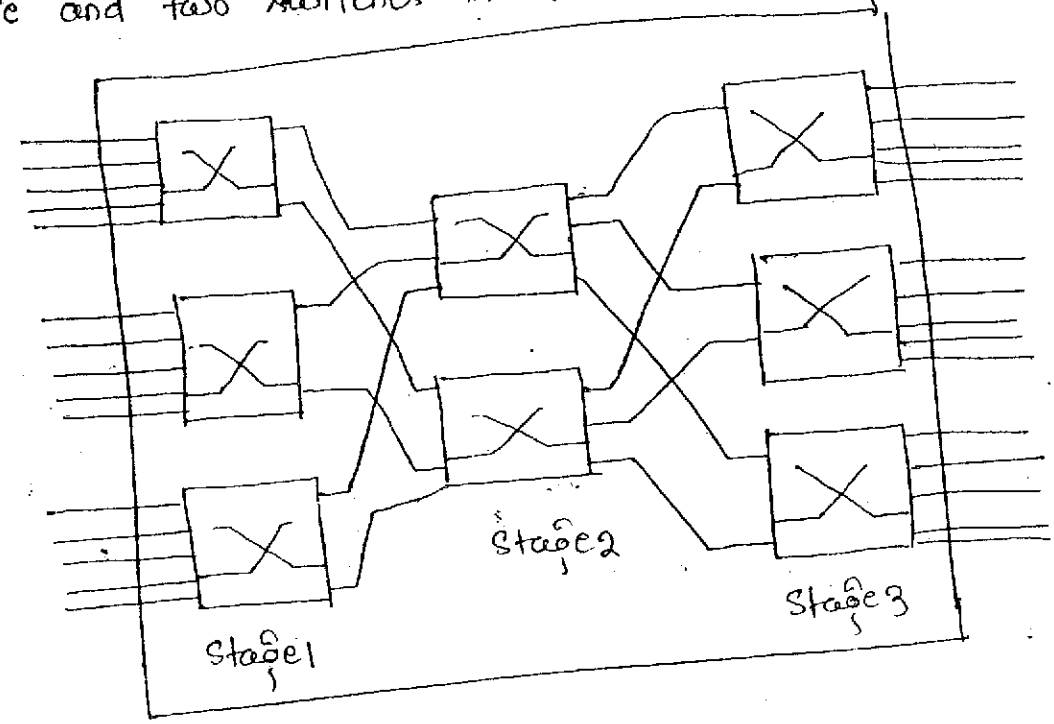
- A crossbar switch connects n i/ps to m o/ps in a grid, using electronic microswitches at each crosspoint.
- Limitation: No of crosspoints required.
- Connecting n i/p to m o/p using a crossbar switch requires n×m crosspoints.
- Suppose i/p = 1000
  o/p = 1000
  crosspoints = 1,000,000 which is impractical [only 25 percent of crosspoints are in use at a given time. The rest are idle]



Multistage Switch:-

- The sol^n to the above limitation is the multistage switch, which combines crossbar switch in several stages.

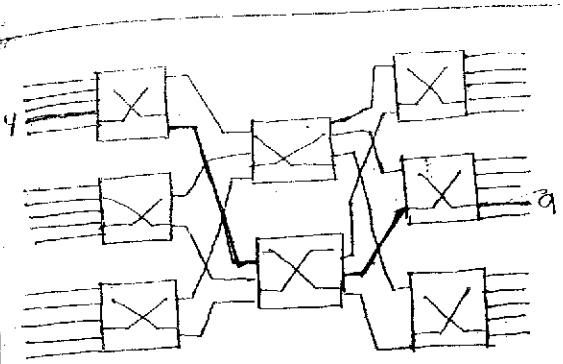
- In multistage switching device are linked to switches that in turn are linked to other switches.
- The design depends upon the no of stages and no. of switches required in each stage. Middle stage has fewer switch than first and last stage.
- e.g: In a three stage design three switches in the first and final stage and two switches in the middle stage.



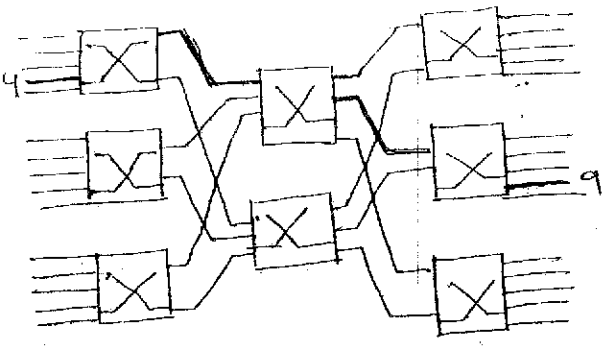
- Each of the first stage switch has i/ps from one third of the i/p device, giving them 5 i/p (5×3=15). Each of the first stage switch must have an o/p to each of the intermediate switches As two intermediate switch are there so first stage has two o/p. The intermediate switches must connect to all 3 stage switches. So they have (each) 3 i/ps and 3 o/ps.

Multiple Path

- It provides several options for connecting each pair of linked device.
- In the following figure a pathway is established between i/p line 4 and o/p line 9. First one uses the lower intermediate switch and switch's center o/p line to reach the last stage switch connected to line 9. Second one uses the upper intermediate switches.



First option



Second option

Blockings:

This savings comes at a cost. The reduction in the no. of crosspoints results in a phenomenon called blocking during periods of heavy traffic.

- Blockings refers to times when one i/p cannot be connected to an output because there is no path available between them, all the possible intermediate switches are occupied
- On single stage switch block doesn't occur, because every comb of i/p and o/p has its own crosspoint, so there is always a path.

Time division Switch:

- Time division switchings uses time-division multiplexing to achive switchings. Two methods used in time division switchings

(i) Time Slot interchange.

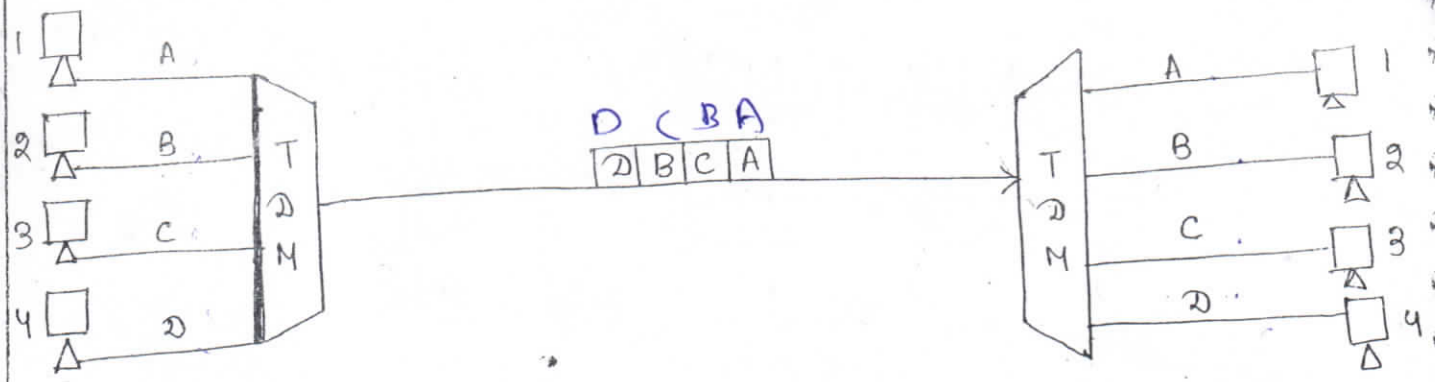
(ii) TDM Bus.

Time Slot Interchanges:

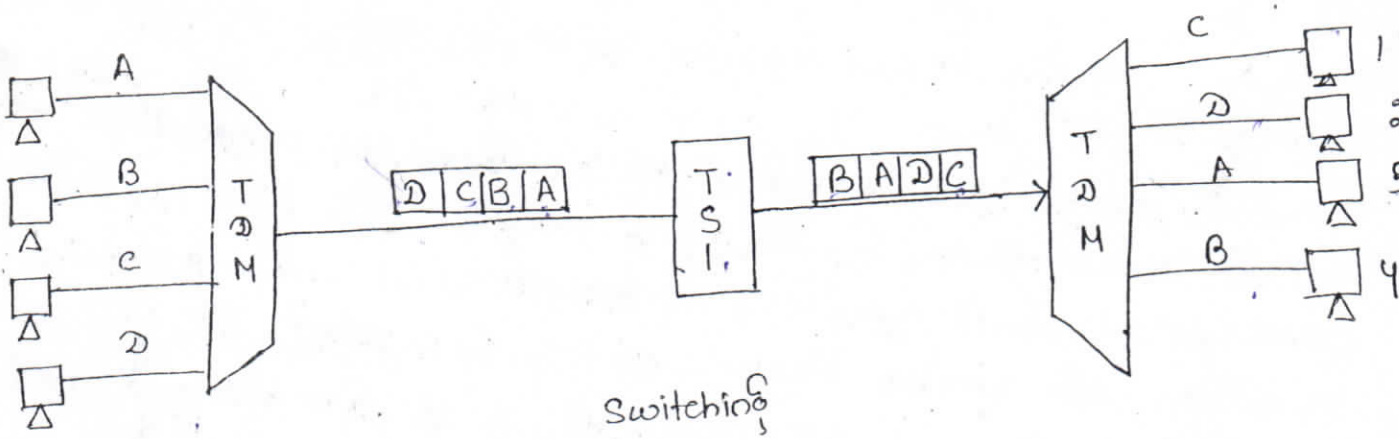
- Here the i/p line wants to send data to an o/p line acc. to the following pattern.

1 ⟶ 3 2 ⟶ 4 3 ⟶ 1 4 ⟶ 2

- Figure shows the ordinary time division multiplexings where the o/p is in same order as they are input data from 1 go to 1 2 to 2, 3 to 3 and 4 to 4.

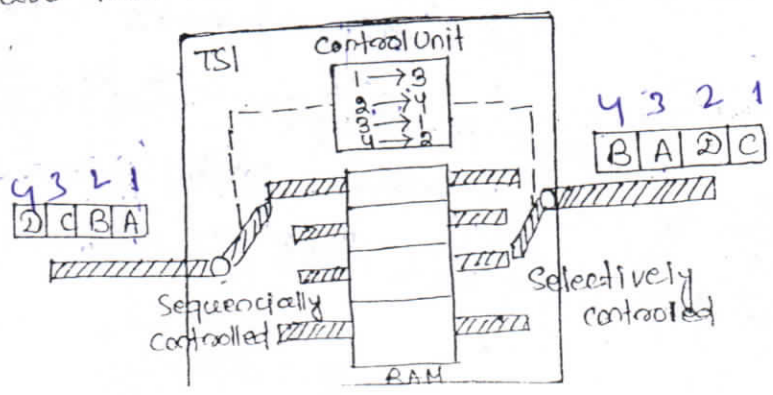


No Switching

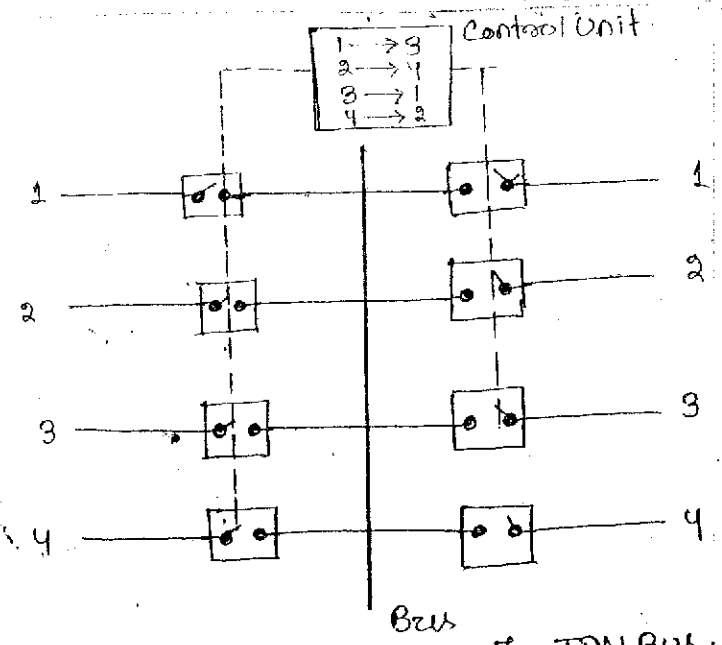


Switching

- We insert a device called a time slot interchange (TSI) into a link. The TSI changes the ordering of the slot based on desired connections. It changes the order of data from A, B C, D to C, D A, B. Now when the demultiplexor separates the slots, it passes them to proper o/p.
- TSI consist of random access memory (RAM) with several memory location. The size of each location is same as the size of single time slot. The no. of location is same as no. of i/p. The RAM fills up with incoming data from time slots in the order received. Slots are then sent in an order based on the decision of control unit.



TDM Bus:



- Figure shows a simplified version of TDM Bus. The i/o lines are connected to a high speed bus through i/o gates. Each i/p gate is closed during one of the four time slots.
- During the same time slot, only one o/p gate is also closed. This pair of buses allows a burst of data to be transmitted from one s/p i/p line to one s/p o/p line using the bus.
- The control unit opens and closes the gates according to switching need. At the first time slot i/p gate 1 and o/p gate 3 will be closed, during the second slot i/p gate 2 and o/p gate 4 will be closed.

Space and Time Division Switch Combinations:-

Advantage of Space division Switching:

It is instantaneous.

Disadvantage of Space division Switching:-

The no. of crosspoints required to make space division switching acceptable in terms of blocking.

Advantage of time division switching:-

It needs no cross-point.

Disadvantage of time division switching:-

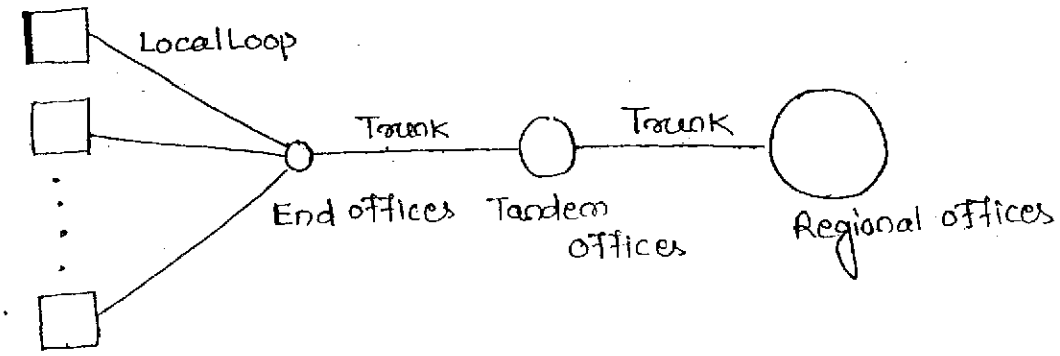
Processing each connection creates delays as each time slot must be sorted by RAM then retrived and passed on.

TELEPHONE NETWORK:

- Telephone network used to carry data as well as voice. The n/w is now analog as well as digital. Telephone network use circuit switching.

Major Components:

- The telephone network is made of three major components (i) local loops (ii) trunks (iii) switching offices.
- The telephone network has several levels of switching offices such as end offices, tandem offices and regional offices.



Local Loops:

- Local Loop is a twisted pair cable that connects the subscriber to the nearest end office or nearest local central office.
- The local loop when used for voice has bw of 4000hz.
- The first three digits of a local telephone number define the office and the next four digits define the local loop number.

Trunks:

- Trunks are the transmission media that handles the communication between between offices.
- A trunk handles hundreds and thousands of connection through multiplexing. Transmission is usually through optical fibers and satelite links.

Switching offices:

- To avoid having a permanent physical link between any two subscribers, the telephone company has switches located in a switching office. A switch connects several local loops or trunks and allows connection between different subscribers.

Making a Connection:

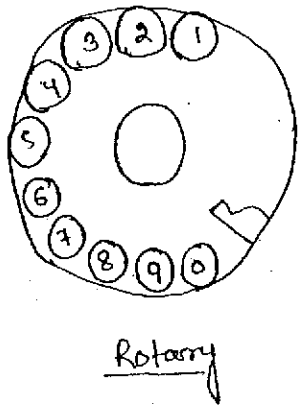
Subscriber telephones are connected through local loops to end offices.

Accessing the switching station at the end office is accomplished through dialing.

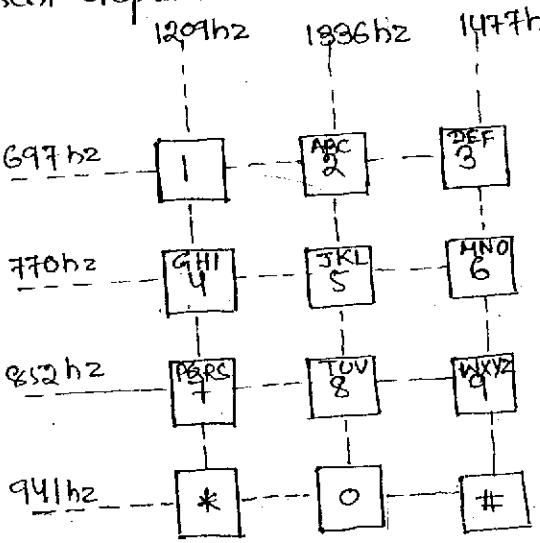
In the past, telephone featured rotary or pulse dialing, in which digital signal was send to the end office for each no. dialed. This type of dialing was prone to errors due to inconsistency of breaks during dialing process.

Today dialing is accomplished through touch-tone technique. Here instead of sending digital signal, the user send two small bursts of analog signals, called dual tone.

The frequency of the signal sent depend row and column of the pressed pad.



Rotary



Toneb-Tone

"Voice communication used analog signal in the past, but is now moving to digital signal. On the other hand dialing started with digital signal is now moving to digital signal"

Analog Service:

Telephone companies provided their subscribers with analog services.

Digital Service:

Today telephone companies provides digital service. These are less sensitive than analog services to noise and other form of interference.

Burst Error:

- A burst error means 2 or more bits in the data unit have changed. The length of burst error is measured from the first corrupted bit to the last corrupted bit. Some bits between them may not be corrupted.

- It is most likely to occur in a serial transmission.

DETECTION

- Error detection is simpler than error correction and is the first step in error correction process.

Redundancy:

- One error detection mechanism would be to send every dataunit twice.
- The receiving device would be able to do a bit-for-bit comparision.
- Any discrepancy would indicate an error, and an appropriate correction mechanism would be set in place.
- This system is completely accurate but it would be inexpportably slow.
- Here not only the transmission time double, but also the time it takes to compare every unit bit by bit must be added.
- Instead of repeating the entire data stream a shorter group of bit must be appended at the end of the unit because the eatra bits are redundant to the information. they are discarded as soon as accuracy of transmission has been determined.

DATA LINK LAYER

- Data link layer lies between network layer and physical layer in the internet model. It receives service from physical layer and provides service to network layer.
- It is responsible for carrying packet from one hop (computer for router) to the next hop.

Duties of data link layer:

Some of the duties of data link layer are:

(i) Packetizing
(ii) Address
(iii) Error Control
(iv) Flow Control
(v) Access Control.

ERROR DETECTION AND CORRECTION:

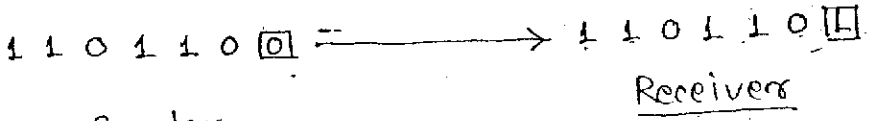
Data can be corrupted during transmission. For reliable communication errors must be detected and corrected.

TYPES OF ERRORS:

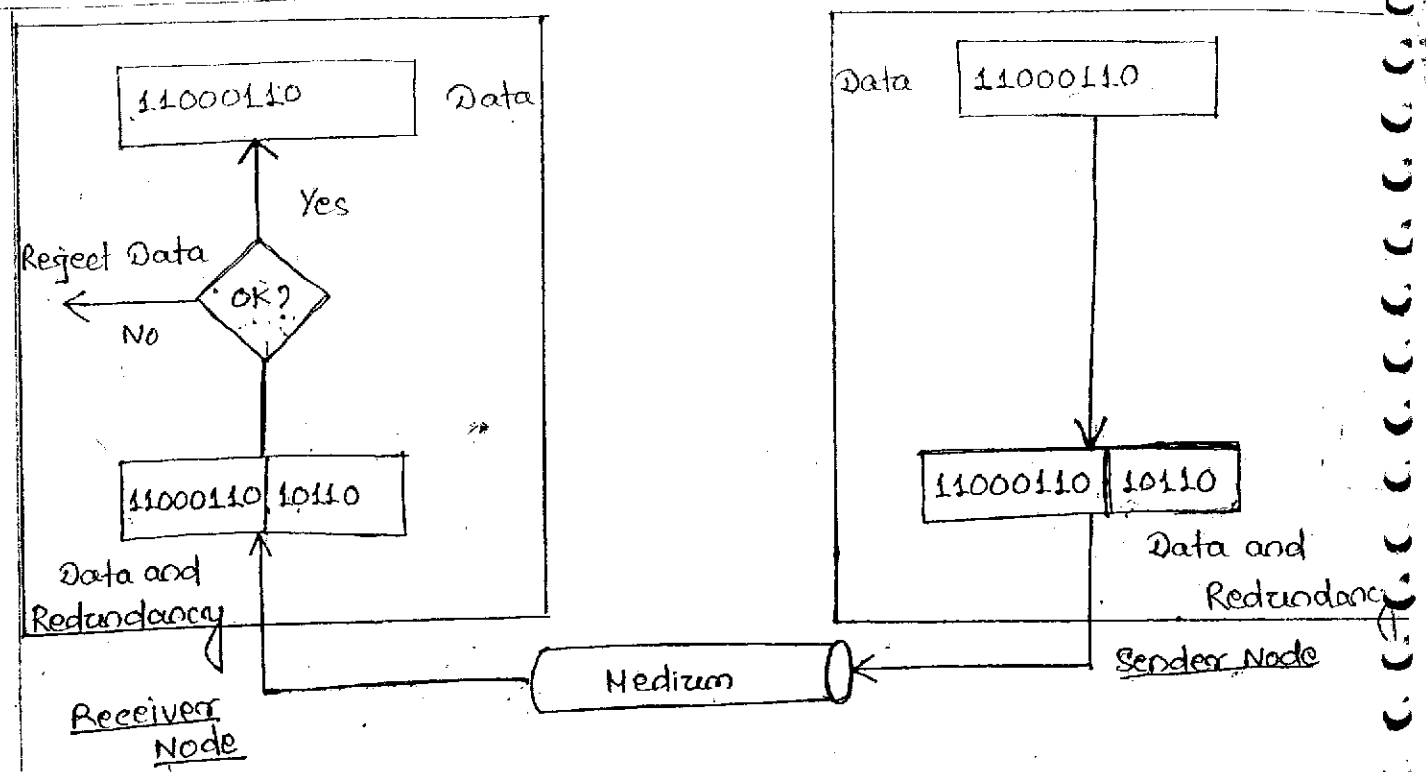
When bits flow from one point to another they are subjected to unpredictable changes because of interference.

Single-Bit Error

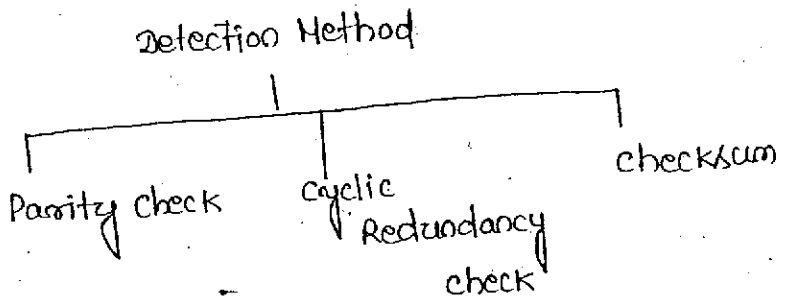
Single bit error means only one bit of a given data unit is changed i.e 1 to 0 or 0 to 1.



- Single bit errors are the least likely type of error in serial data transmission. It can happen if one are sending data using parallel transmission.



Once the data stream has been generated, it passes through a device analyzer it and adds an appropriately coded redundancy check. The data unit is now enlarged by several bits travel over a link to the receiver. The receiver puts the entire stream through a checking function. If the received bitstream passes the checking criteria, the data portion of the data unit is accepted and redundant bits are discarded.



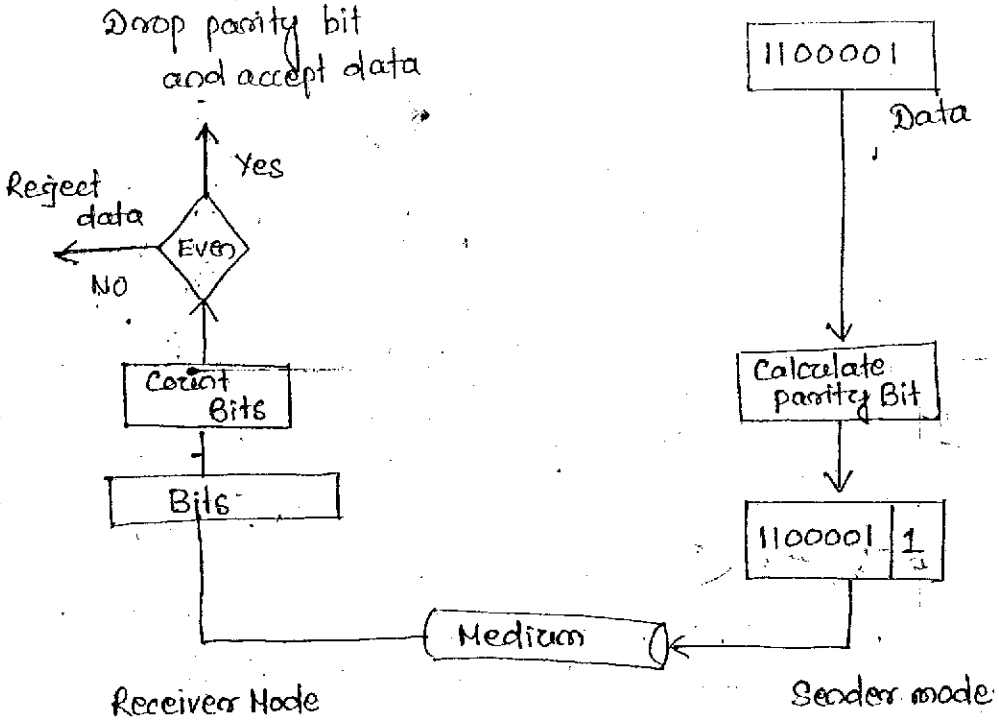
Parity Check:

- The most common and least expensive mechanism for error detection is the parity check.

parity check
- Simply parity check
- Two dimensional parity check.

Simple Parity Check:

- In this technique, a redundant bit called parity bit is added to every data unit so that the total no of 1s in the unit (including the parity bit becomes even. (or odd)

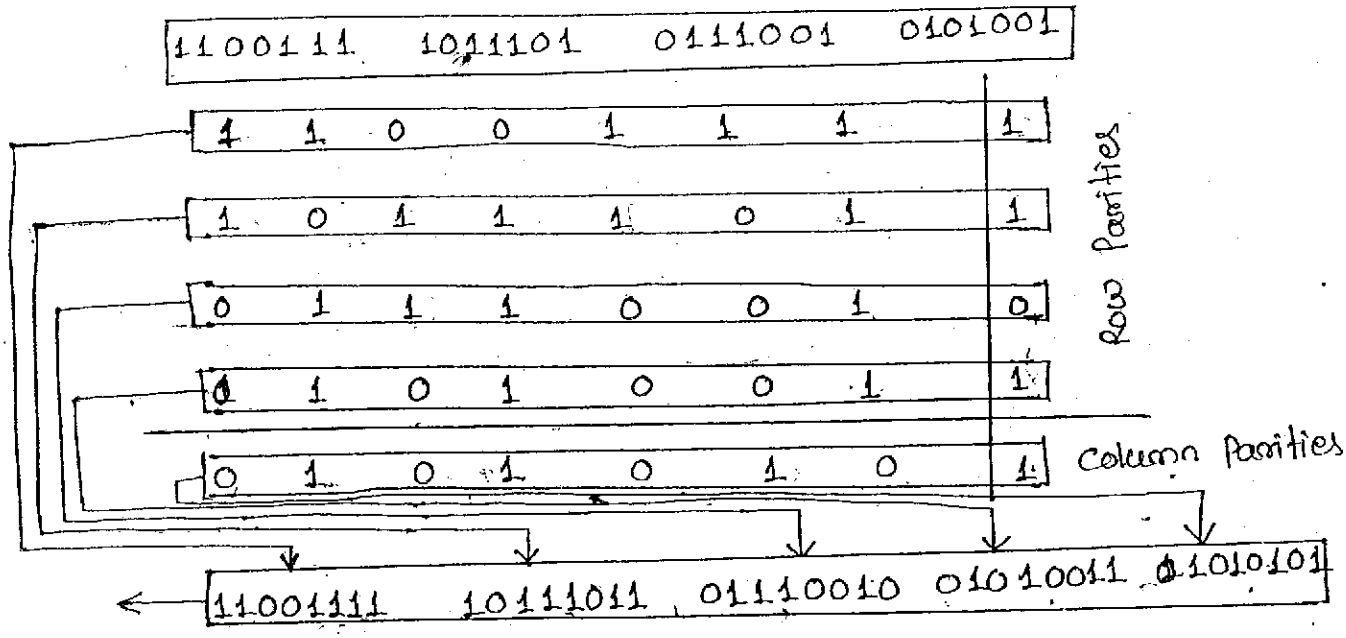


- When the no. of 1s are even it goes through a even-parity checking function. Some systems may use odd-parity checking where the no of 1s are odd.

performance:

Single parity check can detect all single bit errors. It can also detect burst errors as long as the total number of bits changed.

- In this method, a block of bits is organised in a table (rows and columns). First we calculate the parity bit for each data unit then organised in a table. Then we calculate the parity bit for each column and create a new row of 8 bits, they are parity bit for the whole block.



Data and Parity bits.

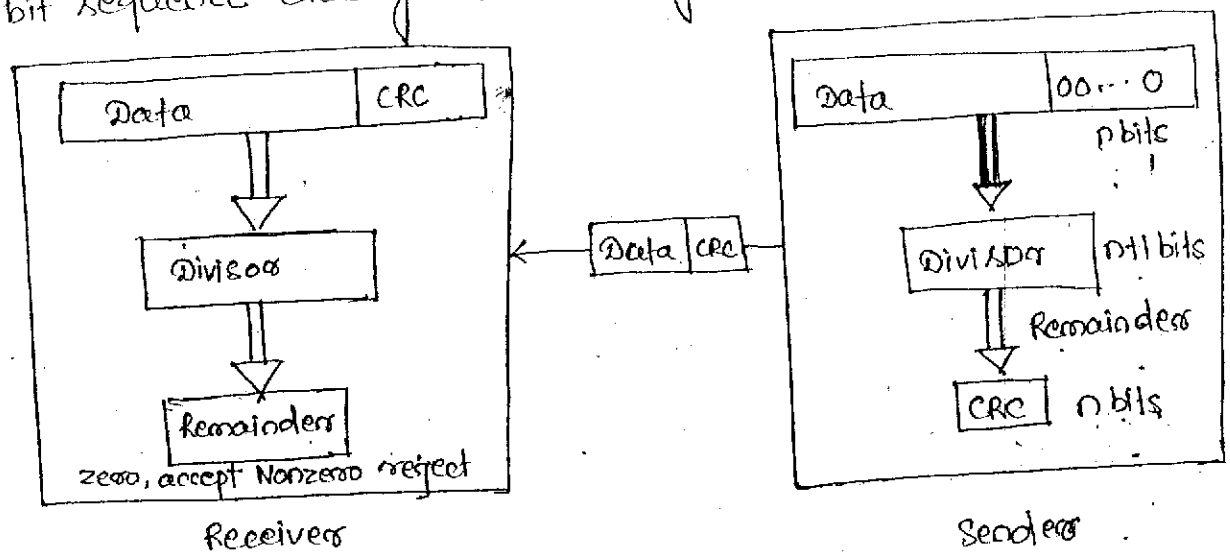
Performance:

2-D parity check increases the likelihood of detecting burst errors, but if 2 bit in one data unit are damaged and two bits in exactly same position in another data unit are also damaged, then the check will not detect an error.

Cyclic Redundancy check:-

- Unlike the parity check which is based on addition, CRC is based on binary division. In CRC instead of adding bits to achive a desired parity a sequence of redundant bits called the CRC or the CRC remainder is appended to the end of a data unit so that the resulting data unit becomes exactly devisible by a second predetermined

binary number. There is a predetermined divisor. The remainder is CRC. to be valid, CRC must have two qualities.
- It must have one less bit than the divisor and appending it to the end of the data string must make the resulting bit sequence exactly divisible by the divisor.

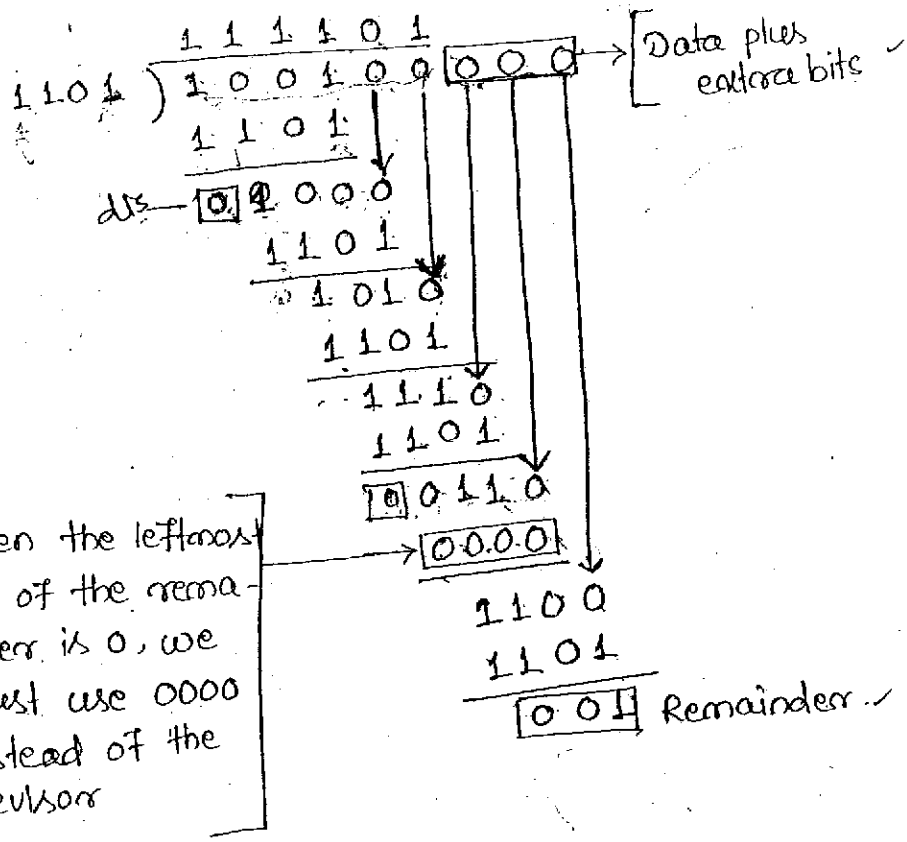


- First a string of n 0s is appended to the data unit. The number n is 1 less than the number of bits in the predetermined divisor, which is n+1 bits.
- Second the newly elongated data unit is devided by the divisor, using a process called binary division. The remainder resulting from this division is the CRC.
- Third the CRC of n bits derived in step 2 replaces the appended 0s at the end of the data unit. CRC may consist of all 0s.
- The data unit arrives at the receiver data first followed by the CRC. The receiver treats the whole string as a unit and devides it by the same devisor that was used to find the CRC remainder.
- If the string arrives without errors the CRC checker yeilds a remainder of zero and the data unit passes. If the string has been changed in transit, the division yeilds a non-zero remainder and the data unit does not pass.

CRC Generator:

A CRC generator uses modulo-2 division. In the first step the 4 bit devisor is subscripted from the first 4 bits of the divident. Each bit of the divisor is subtracted from the corresponding bit of the dividend, without disturbing the next higher bit.

example:



CRC Checker:

After receiving the data appended with the CRC, it does the same modulo-2 division. If the remainder is all 0s the CRC is dropped and the data are accepted otherwise the received stream of bits is discarded and the data are resent.

polynomial:

The devisor in the CRC generator is most often represented not often string of 1s and 0s but as an algabric polynomial, because

(i) It is short

(ii) It can be use to prove the concept mathematically

$x^7 + x^5 + x^2 + x + 1$

x^6 | $x^4 x^3$ | | |

1 0 1 0 1 1 1 = 10100111

Divisor

```
          1 1 1 1 1 0 1
      ---------------------
1 1 0 1 | 1 0 1 0 0 0 0 1
          1 1 0 1
          ---------
            1 0 0 0
            1 1 0 1
            ---------
              1 0 1 0
              1 1 0 1
              ---------
                1 1 1 0
                1 1 0 1
                ---------
                  0 1 1 0
                  0 0 0 0
                  ---------
                    1 1 0 1
                    1 1 0 1
                    ---------
                      0 0 0 0
```

performance:

CRC is very effective error detection method

- CRC can detect all burst errors that affect an odd no. of bits.
- CRC can detect all burst errors of length less than or equal to the degree of polynomial.
- CRC can detect with a very high probability burst errors of length generator than degree of polynomial.

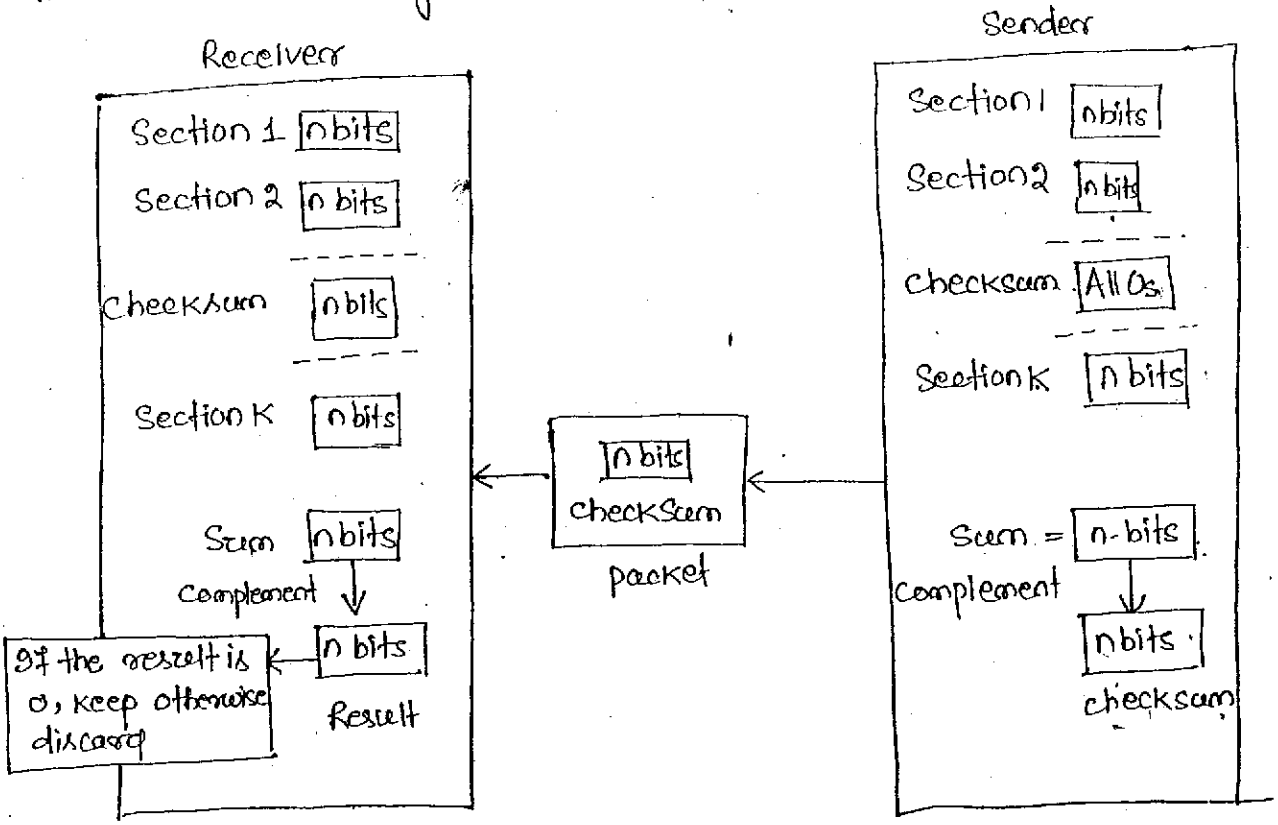
CHECKSUM

Like the parity check the CRC, the checksum is based on the concept of redundancy.

Checksum Generator:

- The checksum generator subdevides the data unit into equal segments of n bits, These segments are added using ones complement arithmatic, in such a way that total is also n bits

- The total is then complemented and appended to the end of original data unit as redundancy bit, called the checksum field.
- The extended data unit is transmitted across the network. So if the sum of data segment is T, the checksum will be −T.



Sender follows the following steps:

- The unit is divided into K sections, each of n bits.
- All sections are added using one complement to get the sum.
- The sum is complemented and becomes the checksum.
- The checksum is sent with the data.

Checksum checker:-

The receiver subdevides the data unit as above and adds all segments and components the result.

Receiver follows the following steps:-

- The unit is divided into K section, each of n bits.
- All sections are added using ones complement to get the sum.
- The sum is complemented.
- If the result is zero, the data are accepted, they are rejected.

Example:

Suppose the following block of 16 bits is to be sent using a checksum of 8 bits

10101001 00111001

Now deviding into n bits

```
  1 0 1 0 1 0 0 1
  0 0 1 1 1 0 0 1
-----------------
  1 1 1 0 0 0 1 0
```

Making Sum

checksum = 1's complement of sum =

```
  1 1 1 0 0 0 1 0
  | | | | | | | |
  0 0 0 1 1 1 0 1
```

Now the 16 bit data is sent along with checksum bits

So the data becomes

10101001 . 00111001 . 00011101.

Now receiver's step

```
  1 0 1 0 1 0 0 1
  0 0 1 1 1 0 0 1
  0 0 0 1 1 1 0 1
-----------------
  1 1 1 1 1 1 1 1
```

1's Complement = 0 0 0 0 0 0 0 0

If the complement of sum at receivers is 0's then accept the data otherwise reject it

Suppose there is a burst error of length 5 that affects 4 bit.

1010 1111 , 11111001, 00011101

Adding

```
  1 0 1 0 1 1 1 1
  1 1 1 1 1 0 0 1
  0 0 0 1 1 1 0 1
-----------------
  1 1 0 0 0 1 0 1
```

Result

```
                1
-----------------
  1 1 0 0 0 1 1 0
```

Carry

Sum

1's complement 0 0 1 1 1 0 0 1 means the data pattern is corrupted.

performance:-

The checksum detects all errors involving an odd number of bits as well as most errors involving an even no of bits.

ERROR CORRECTION

After error detection error correction is handled in many ways. The two most common methods are

(i) Error correction by retransmission
(ii) Forward error correction.

Error Correction by Transmission:-

In error correction by retransmission, when an error is discovered, the receiver can have the sender retransmit the entire data unit.

- This can be achived using flow and error control protocol.

Forward Error Correction:-

- In forward error correction, a receiver can use an error-correcting code which automatically corrects certain errors.
- Error correction codes however are sophisticated, then error detection codes and requires more redundancy bits.
- To calculate the no. of more redundancy bits r required to correct a given no. of data bits m, we must find a relationship between m and r.
- With m bits of data and r bits of redundancy added to them, the length of resulting code is m+r.
- If the total no. of bits in a transmission unit is 'm+r' than r must be able to indicate at least m+r+1 different states.

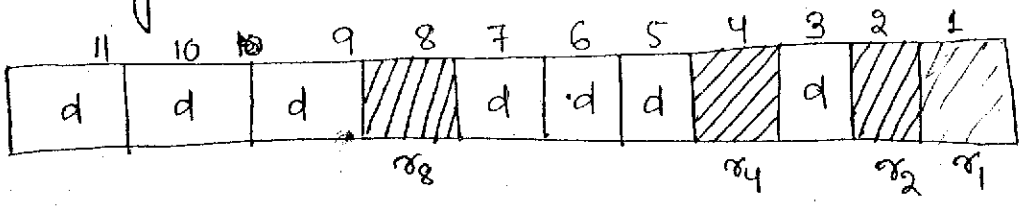
$$\therefore \quad 2^r >= m+r+1$$

- The value of r can be determined by plugging the value of m. If the value of m is 7, the smallest r value that can satisfy the eq is

$$2^4 = 7+4+1$$

Hamming Code:

Hamming code provides a practical solution. It can be applied to data units of any length and uses relationship between data and redundancy bits.



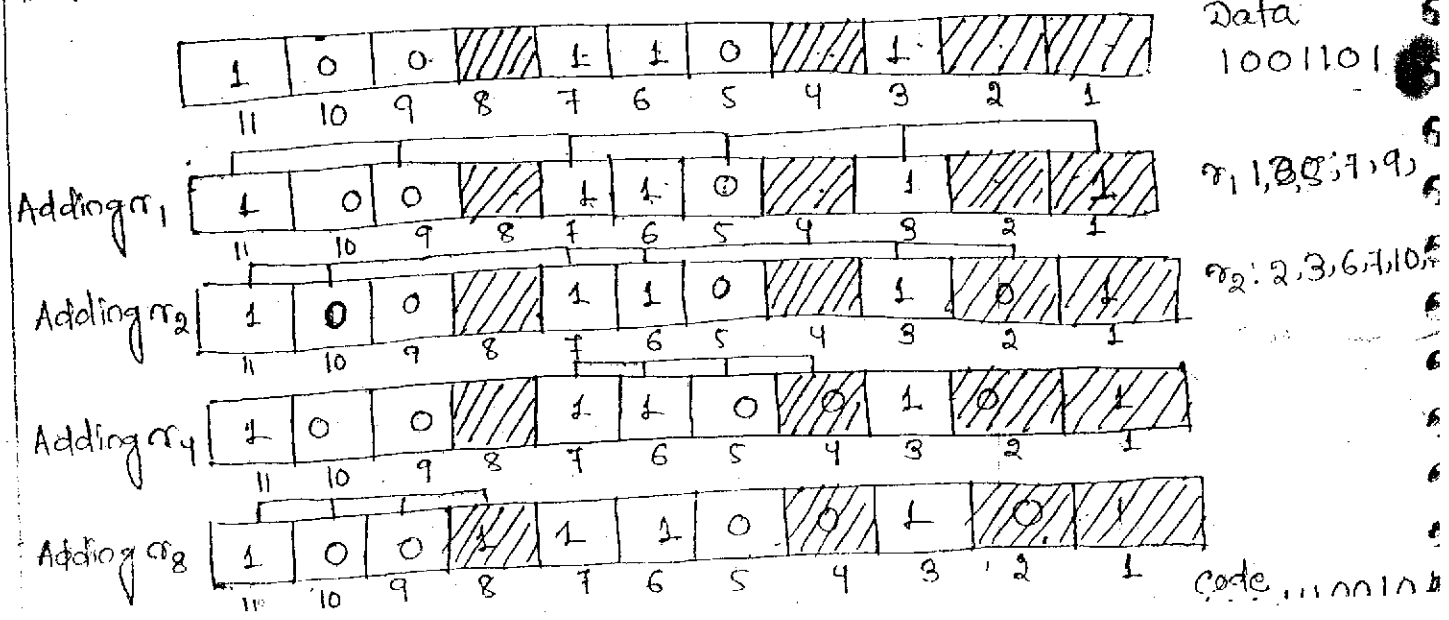
position of redundancy bit in hamming code

In hamming code each 'r' bit for one combination of for one combination of data bits as shown in fig.

r_1 : bits 1, 3, 5, 7, 9, 11
r_2 : bits 2, 3, 6, 7, 10, 11
r_4 : bits 4, 5, 6, 7
r_8 : bits 8, 9, 10, 11.

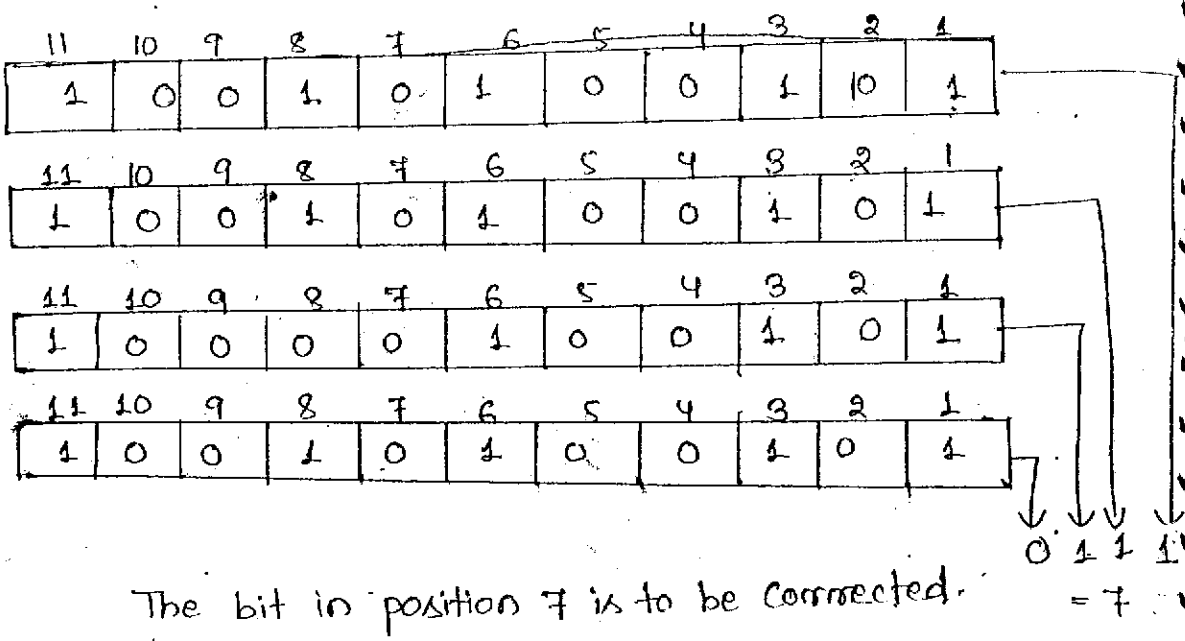
Calculating r values:-

The following figure shows a hamming code implementation for ASCII character. In the first step, we place each bit of the original character in its appropriate place in the 11-bit unit. In the subsequent steps, we calculate the even/odd parities for various bits component. The parity value for each comb^n is the value of the corresponding 'r' bit.



Error Detection and Correction:

Now suppose the 7th bit has been changed from 1 to 0. The receiver takes the transmission and recalculates 4 new parity bits.



The bit in position 7 is to be corrected.

DATA LINK CONTROL AND PROTOCOLS

Most important responsibility of the data link layer are flow control and error control. Collectively these function are known as data link control.

FLOW AND ERROR CONTROL

Flow Control:

- Flow control co-ordinates the amount of data that can be sent before receiving acknowledgement and is one of the most important duties of data link layer.
- On most protocols flow control is a set of procedures that how much data it can transmit before it must wait for an acknowledgement from the receiver.
- The receiving device must be able to inform the sending device before those limits are reached and to request that the transmiting device send fewer frames or stop temporarily.
- Incoming data must be checked and processed before they are used for this reason.
- Each receiving device has a flow of memory called buffer reserved for storing incoming data until they are processed
- If the buffer begins to fill up, the receiver must be able to tell the sender to halt transmision, until it is once again able to receive.

Error Control:

- Error control include both error detection and error correction
- It allows the receiver to inform the sender of any frame lost or damaged during transmision, and co-ordinates the retransmission of these frames by the sender.
- Anytime an error is detected an exchange specified frames are retransmitted. This process is called automatic repeat request.

Flow and Control Mechanism:

There are three common error and flow control mechanism.

(i) Stop- And- Wait ARQ
(ii) Go- Back - N ARQ
(iii) Selective- Repeat ARQ.

STOP- AND - WAIT ARQ:

- Stop-and- Wait is the simplest flow and error control mechanism.
- The sending device keep a copy of last frame transmitted until it receives an acknowledgement for that frame. Keeping a copy allows the sender to retransmit lost or damaged frame until they are received correctly.
- Both data frames and acknowledgement frames are numbered alternatively 0 and 1. A data 0 frame is acknowledged by an ACK1 frame, indicating that the receiver has received data frames 0 and now expecting data frame 1.
- If the receiver detects an error in the received frame, it simply discards the frame and sends no acknowledgement.
- The sender has a control variable, which we call S, that holds the no. of recently sent frame (0 or 1). The receiver has a control variable which we call R that holds the no. of next frame expected.
- The sender starts a timer when it sends a frame. If an acknowledgement is not received within a alloted time period the sender assumes that the frame was lost or damaged and resend it.
- The receiver sends only positive acknowledgement for frames received safe and sound. It is silent about the frames damaged or lost.
- If frame 0 is received, ACK 1 is sent, If frame 1 is received ACK 0 is sent.

Operation:

On the transmission of a frame, we have four situation

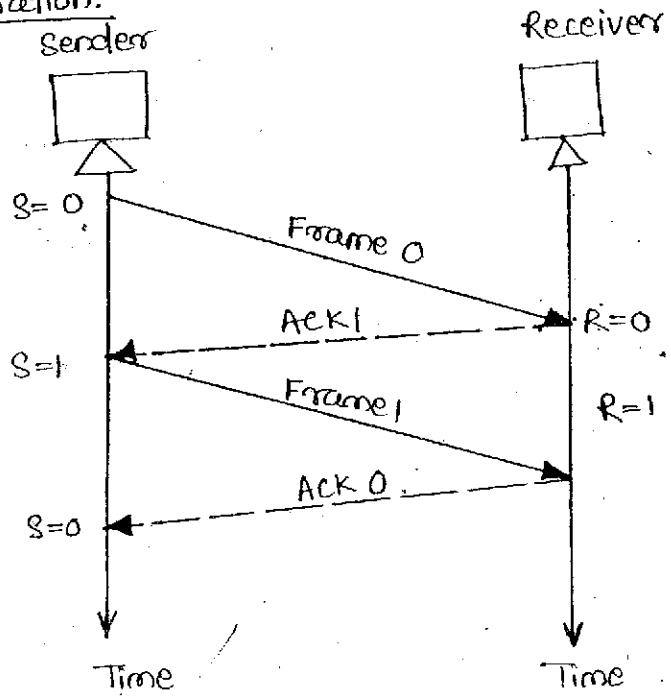
(i) Normal Operation

(ii) Frame is lost

(iii) Ack is lost

(iv) Ack is delayed.

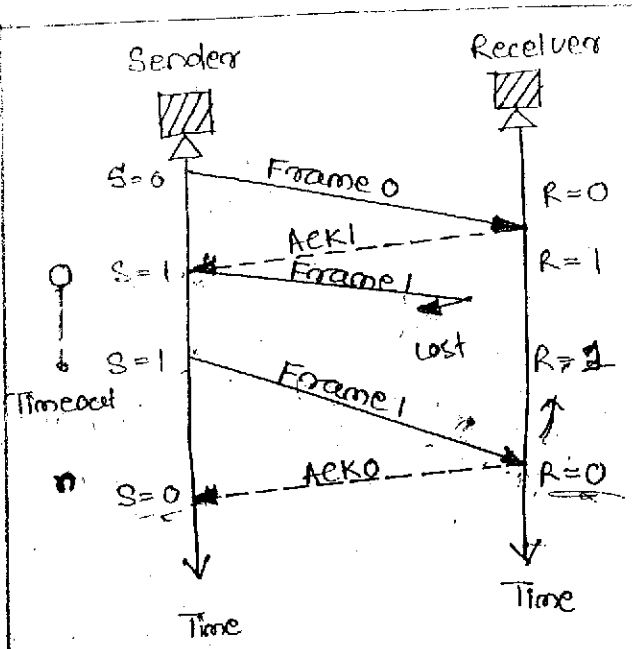
Normal Operation:



- On normal operation the sender sends frame 0 and waits to receive ACK 1. When ACK 1 is received, it sends frame 1 and then waits to receive ACK 0. The ACK must be received before the timer set for each frame expires.

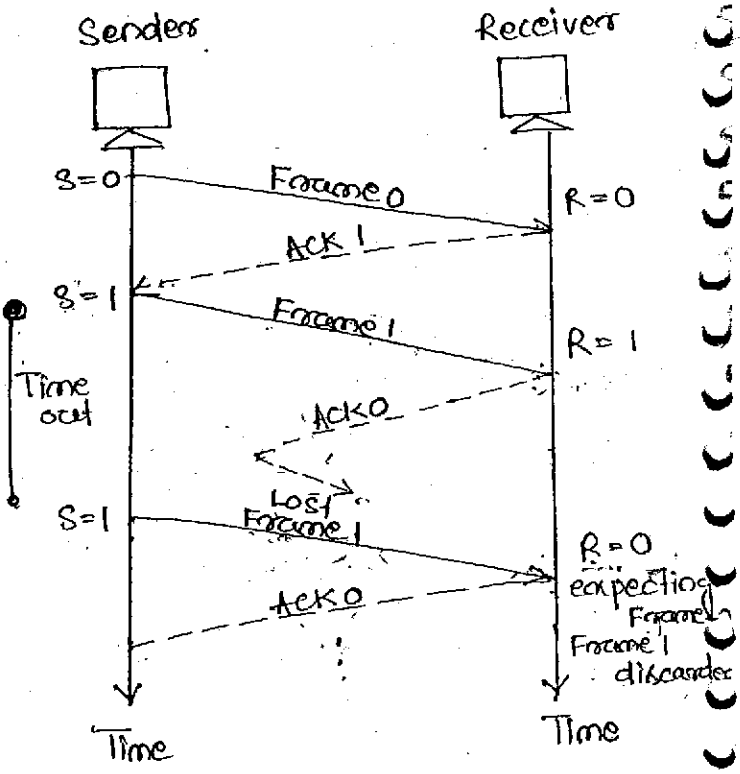
Lost or Damaged Frame:

- When receiver receives a damaged frame it discards it and remain silent which means frame is lost. After the timer at the sender side expires, another copy is sent.

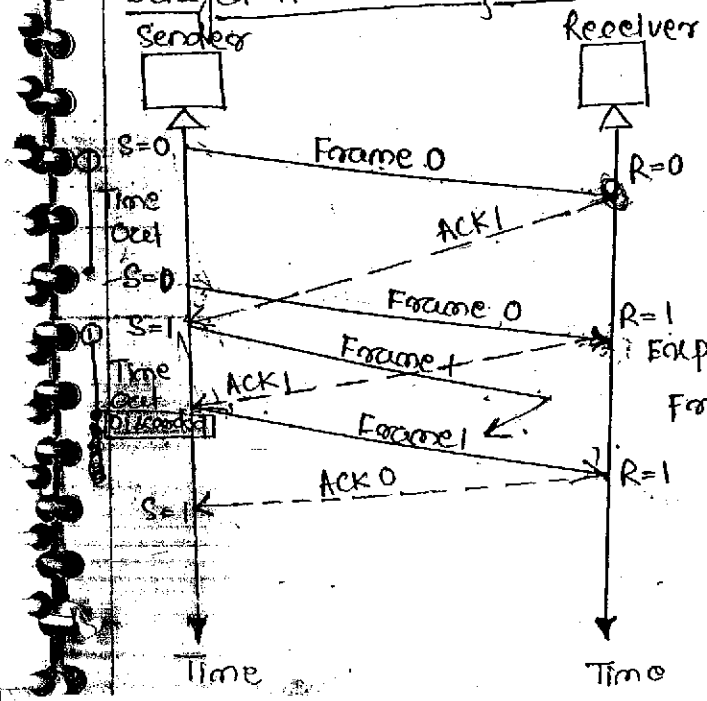


Lost Acknowledgement:

Here the waiting sender doesn't know if frame-1 has been received, when frame 1 expires the sender retransmits frame 1 which has already been received so Receivers discards the second copy.



Delayed Acknowledgement:



Expecting Frame 1
Frame 0 discarded

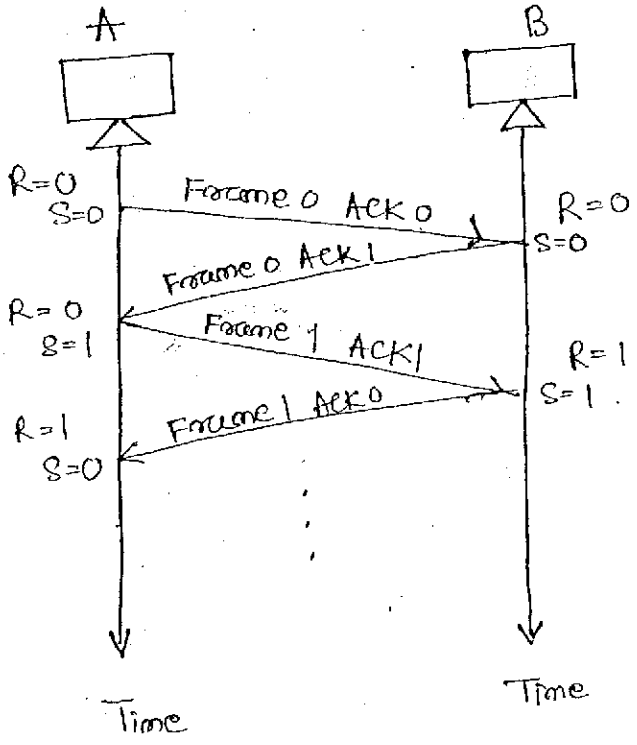
An acknowledgement can be delayed at the receiver, due to some problem with the link when the ack is delayed and the timer expires then the sender once again resends the frame which has already been received, so the second copy of the frame is discarded.

Bidirectional Transmission

We can have bidirectional transmission if the two parties have two separate channels for full duplex transmission or share channel for half-duplex transmission.

piggybacking:

It is a method of combining a data frame with an acknowledgement. Here station A and B have both data to send. Instead of sending separate data and Ack frames, station A sends a data frame that includes an Ack.



GO-BACK-N ARQ:

Disadvantage of Stop-and-Wait ARQ:

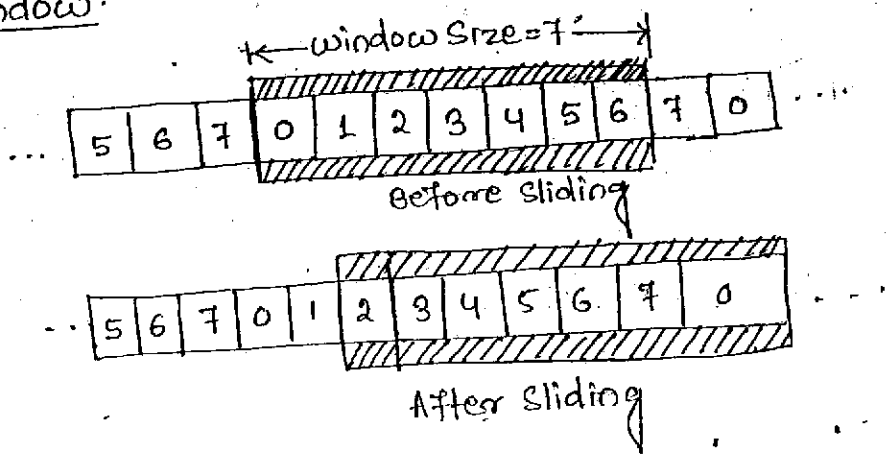
- Here at any point in time for a sender there is only one frame the outstanding frame, that is sent and waiting to be acknowledged
- To improve the efficiency and have a better use of transmission medium we need to let more than one frame be outstanding

Sequence Numbers:

- Frames from a sending station are numbered sequentially. If the header of the frame allow m bits for the sequence number, the sequence no. range from 0 to $2^m - 1$.
  e.g.: If m = 3 Sequence no are 0 to 7.

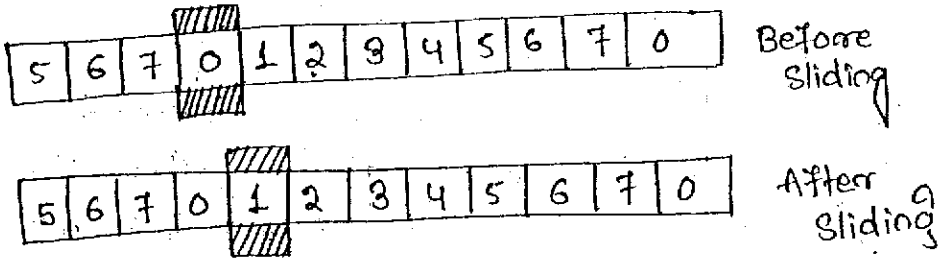
Sender Sliding window:

- At the sender side, to hold the outstanding frames, until they are acknowledged, we use the concept of window.
- We imagine that all frames are stored in a buffer. The outstanding frames are enclosed in a window.
- The frames to the left of the window are those that have already acknowledged. those to the right of the window can't be sent until the window slides over them.
- Size of the window is atmost $2^m - 1$.
- The window slides to include new unsent frames when the correct acknowledgement are received. The window is a sliding window.



Receiver Sliding Window:

- The size of the window at the receiver site in this protocol is always 1.
- The receiver is always looking for a specific frame to arrive in a specific order. Any frame arriving out of order is discarded



Control Variables:

- The Sender has three variables S, S_F, S_L

  S: holds the sequence no. of recently sent frame.

  S_F: holds the sequence no. of first frame in the window

  S_L: holds the sequence no. of last frame in the window

  $$W = S_L - S_F + 1$$

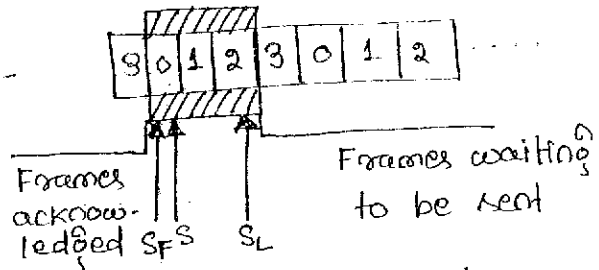
  where

  W: Size of window.

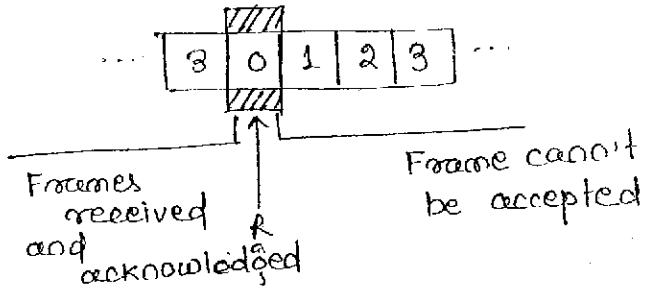
- The receiver has only one variable R

  R: holds the sequence no. of the frame it expects to receive.

- If the number of received frame is same as the value of R, the frame is accepted, if not, rejected.



a. Sender window



b. Receiver Window

Timers:

The sender set a timer for each frame sent and the receiver has no timers.

Acknowledgment:

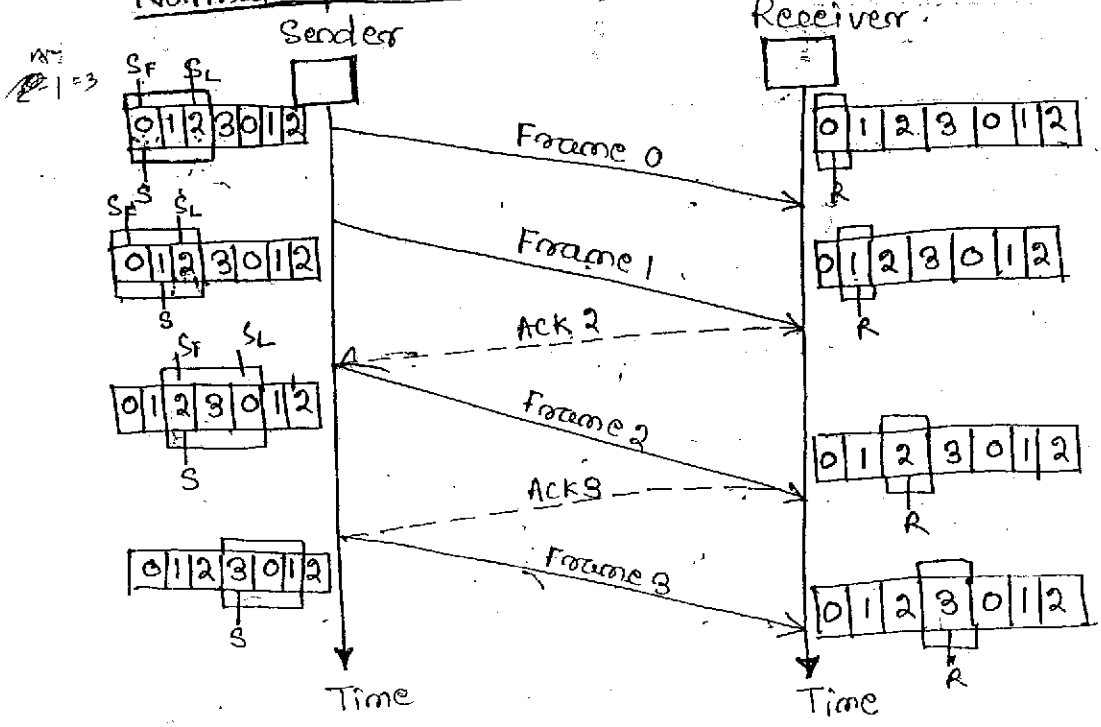
The receiver sent +ve acknowledgment if the frame has arrived safe and sound in order. If a frame is damaged or is received out of order the receiver will silent and will discard all subsequent frames until it receives the one it is expecting

Resending Frame:

When a frame is damaged, the sender goes back and sends a set of from the damaged one upto the last one sent.

Operation:

Normal operation:

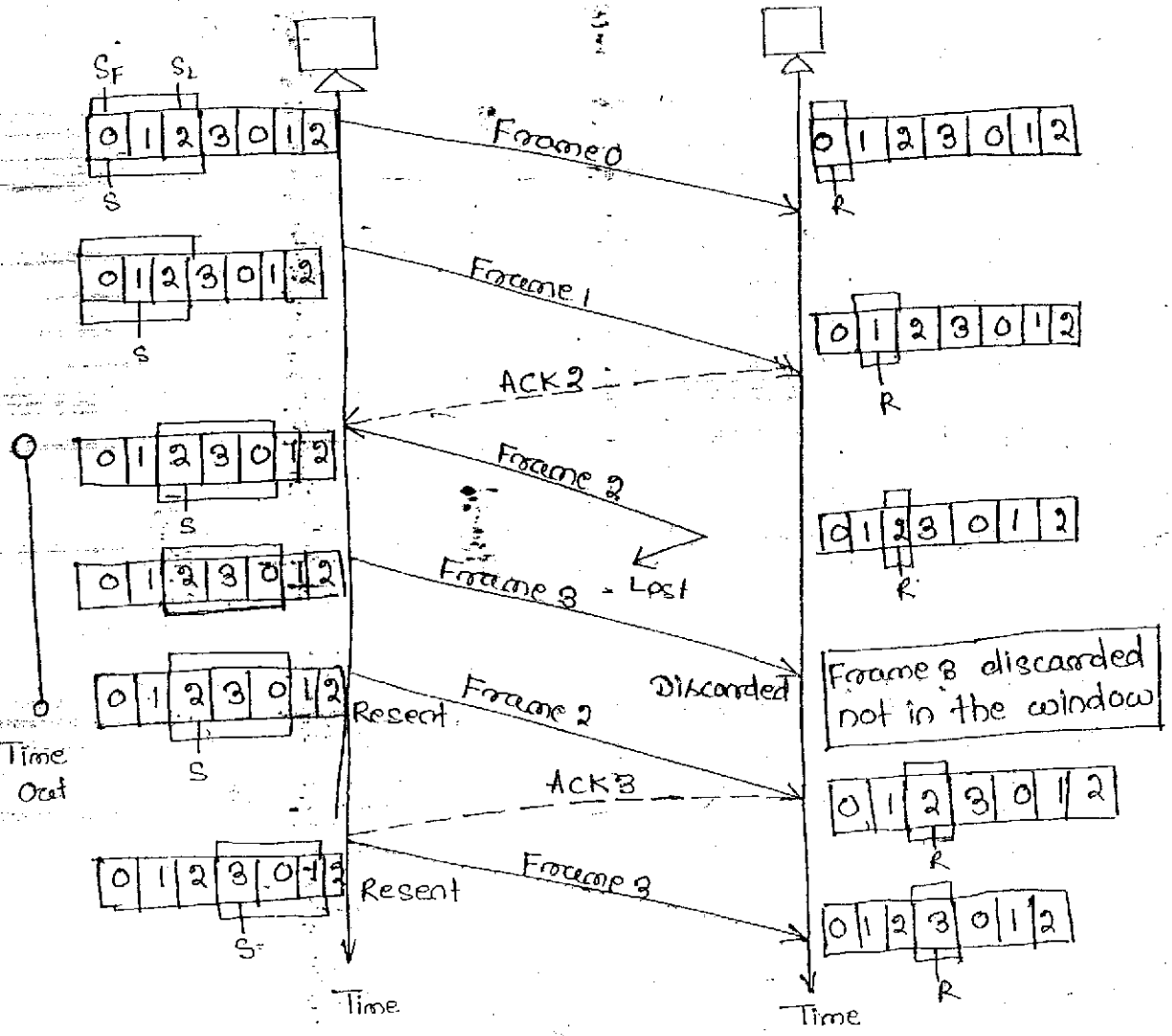


2 bit
0 00
1 01
2 10
3 11

$2^n - 1$
$= 2^2 - 1$
$= 4 - 1$
$= 3$

- Here the sender keeps track of the outstanding frames and updates the variables and windows as the acknowledgement arrive.

Damaged or Lost Frame:



Here frame 2 is lost, when receiver receives frame 3, it is discarded. After the timer for frame 2 expires at the sender side, the sender send frame 2 and 3.

Damaged or Lost Acknowledgement:-

- If an ACK is damaged or lost, we have two situations. If the next ACK arrives before the expiration of any timer, there is no need for retransmission of frames. If the next ack arrives after the time out, the frame and all the frames after that are resent.

Delayed Acknowledgment:

A delayed acknowledgment also triggers the resending of frames

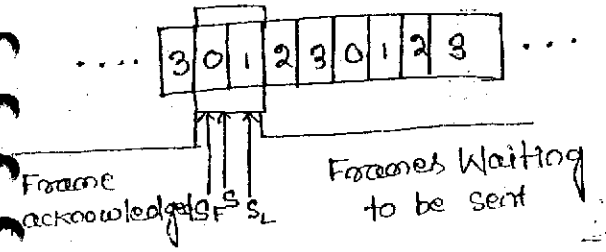
SELECTIVE REPEAT ARQ:

- For noisy links, there is another mechanism that doesn't send N frames only when one frame is damaged, only the damaged frame is resent
- This mechanism is called Selective Repeat ARQ.
- The processing at the receiver is more complex.

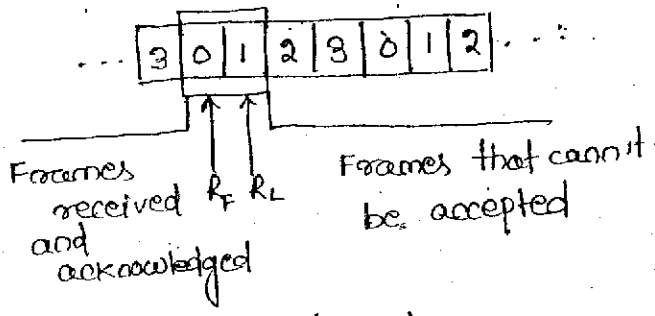
Sender and Receiver Windows:

At the sender side the size of the window is $\frac{2^m}{2}$, and also in receiver side.

Here the receiver is looking for a range of sequence nos. It has two control variables R_F and R_L to define the boundaries of the window.



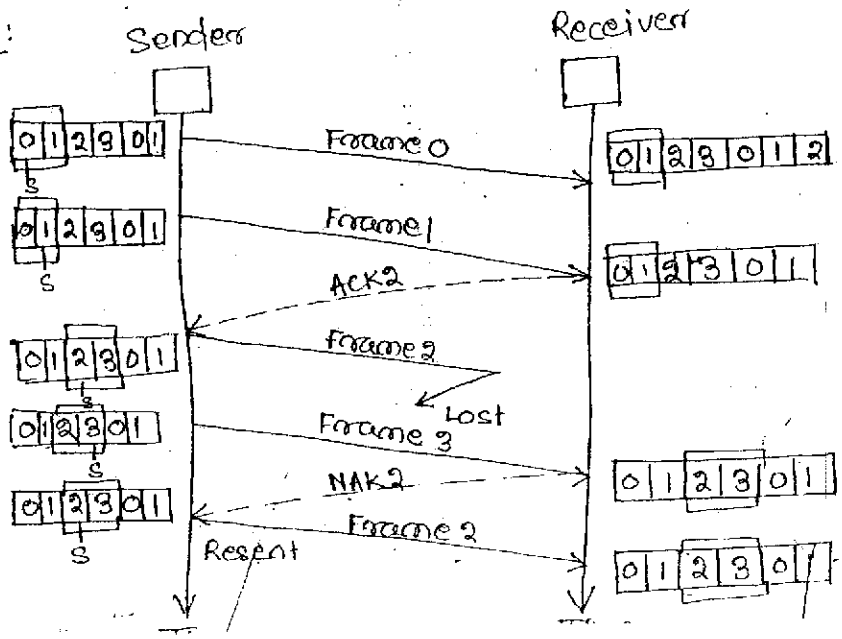
Sender Window



Receiver Window

- Selective Repeat ARQ defines a negative acknowledgment (NAK) that reports the sequence no. of a damaged frame before the timer expires.

operation:



- Frame 0 and 1 are accepted when received because they are in the range specified by the receiver window.
- When frame 3 is received it is also accepted however the receiver sends NAK2 to show that frame 2 has not been received.
- When the sender receives the NAK2, it resends only frame 2.

HDLC

- High-level Data Link Control is an actual protocol designed to support both half duplex and full duplex communication over point to point and multipoint links. It impliment all the ARQ mechanisms.

Transpher Mode:

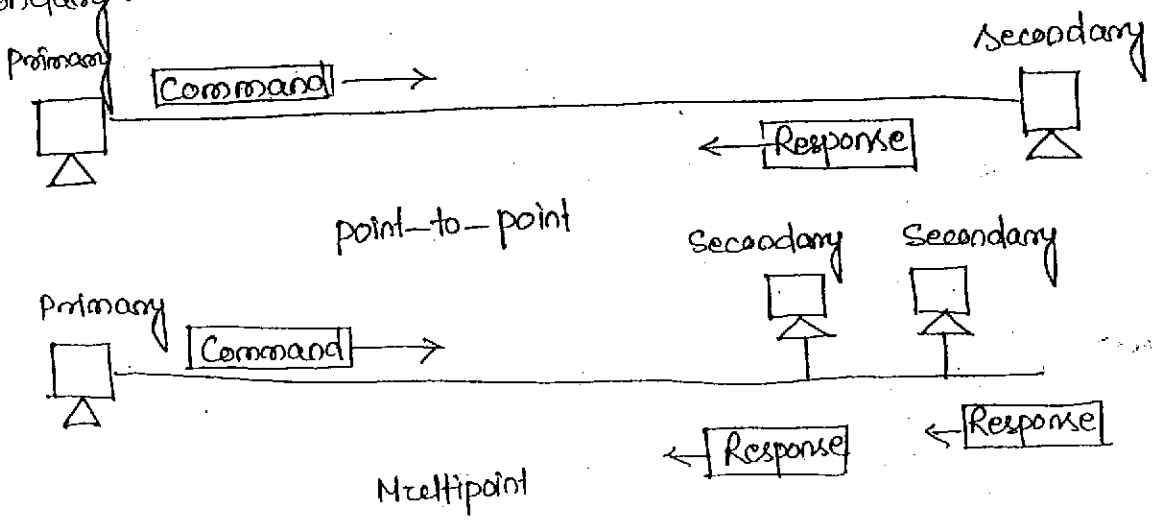
HDLC provides two common modes of transmission

NRM:

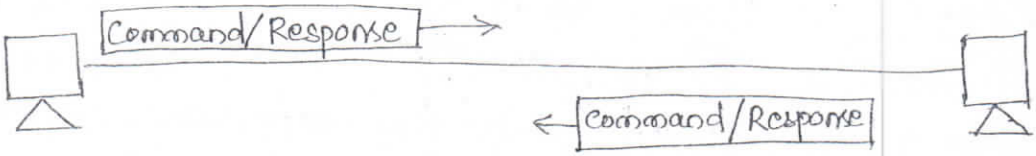
- In normal response mode the station configuration is unbalanced. We have one primary station and multiple secondary station
- A primary station can only send commands, a secondary station can only respond
- NRM used for both point-to-point and multipoint links.

ABM:

- In asynchronous balanced mode, the configuration is balanced, and each ~~function~~ station can function as primary or secondary.



NRM



ABM

Frames:

HDLC defines 3 types of frames

(a) I Frame: (Information frame):

Used to transport user data and control information relating to user data.

(b) S Frame (Supervisory frame):

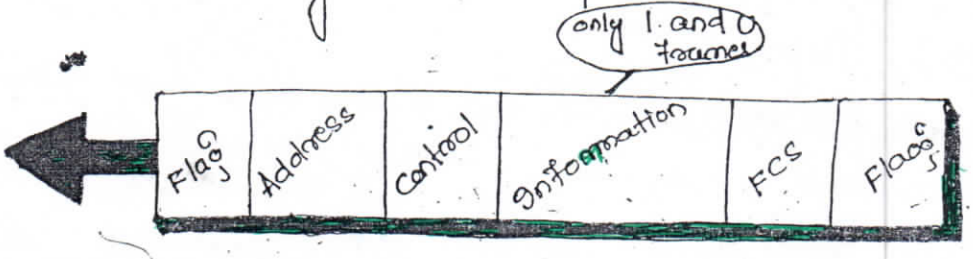
Used to transport control information.

(c) U Frame (Unnumbered frame):

Reserved for system Management.

Frame Format:

Each HDLC may contain upto Six fields.



Control field:-

It is a 1 or 2 byte segment of the frame used for flow or error control

Information field:-

It contains the user's data from the n/w layer or n/w management information.

FCS field:-

Frame check sequence is HDLC's error detection field using CRC.

Flag field:

8 bit sequence with a bit pattern 01111110 that identifies both beginning and end of a frame and serve as a synchronization pattern for the receiver.

Address Field:

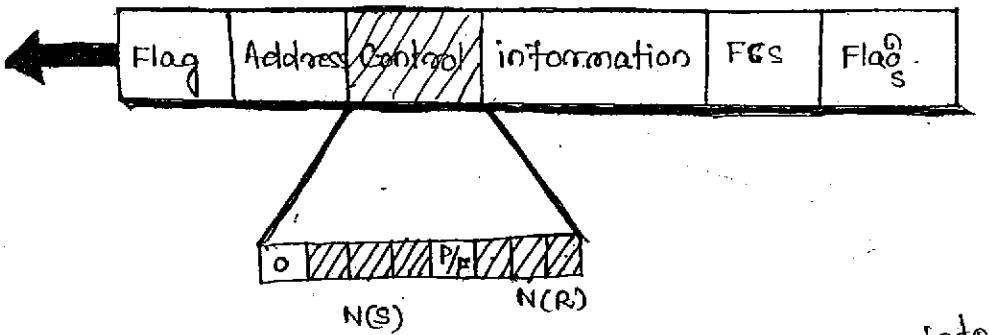
The second field of an HDLC frame contain the address of the secondary station that is either the originator or the destination of the frame. If a primary ~~key~~ station creates a frame it contains a "to address". If a secondary station creates a frame it contains a "from address". An address field can be 1 byte or several byte long. depending on the needs of the n/w, one byte can identify upto 128 stations.

If the address field is only 1 byte, the last bit is always a 1. If the address is more than 1 byte all bytes but the last bit is end with zero, only the last will end with 1. Ending each intermediate byte with zero indicates to the receiver that there are more address bytes to come.

FRAME TYPES:

I-Frame

- I frames are designed to carry user data from n/w layer. They can include flow and error control information.



The bits in the control field of the I-frame are interpreted as follows.

- If the first bit of the control field is zero, this means the frame is I-frame.
- Next 3 fields called N(S) defines the sequence no. of the frame in travel.

Flag field:

8 bit sequence with a bit pattern 01111110 that identifies both beginning and end of a frame and serve as a synchronization pattern for the receiver.

Address Field:

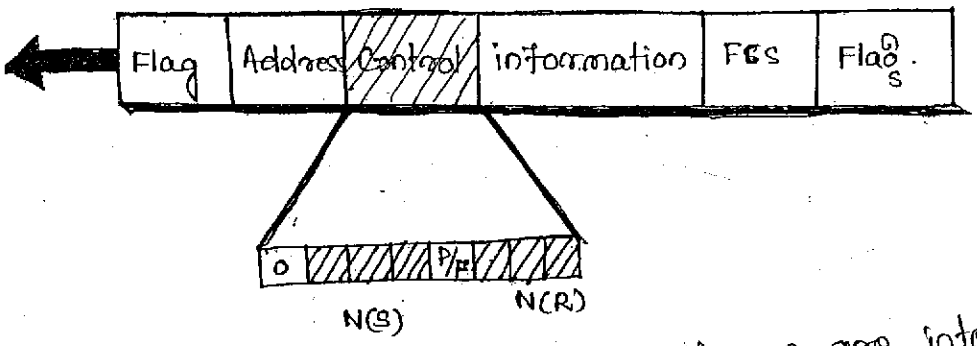
The second field of an HDLC frame contain the address of the secondary station that is either the originator or the destination of the frame. If a primary ~~key~~ station creates a frame it contains a "to address". If a secondary station creates a frame it contains a "from address". An address field can be 1 byte or several byte long. depending on the needs of the n/w, one byte can identify upto 128 stations.

If the address field is only 1 byte, the last bit is always a 1. If the address is more than 1 byte ~~(all but then)~~ all bytes but the last bit is end with zero, only the last will end with 1. Ending each intermediate byte with zero indicates to the receiver that there are more address bytes to come.

FRAME TYPES:

I-Frame

- I frames are designed to carry user data from n/w layer. They can include flow and error control information.



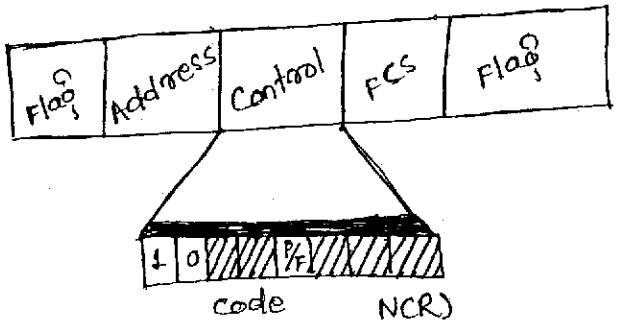
The bits in the control field of the I-frame are interpreted as follows.

- If the first ~~field~~ bit of the control field is zero, this means the frame is I-frame.
- Next 3 fields called N(S) defines the sequence no. of the frame in travel.

With 3 bits we can defines a sequence no from 0 to 7.
The P/F field is a single bit with dual purpose. Always set to 1 whenever it is either poll or final. poll when the frame is send by a primary station to a secondary. Final means when the frame is sent by a secondary to a primary station.
The next 3 bits called NCR) correspond to the value of ACK when piggybacking is used.

S-Frame:

Supervisory frames are used for flow and error control when piggybacking is either impossible or inappropriate.
S- Frame don't have information fields.



The bits in the control field are interpreted as follows.
If the first 2 bits of the control field are 10 ; this means the frame is S-frame.
Second two fields of the the frame is a code that defines the 4 types of S-Frames.

Receive Ready (RR)
Receive Not Ready (RNR)
Reject (REJ)
Selective Reject (SREJ)

Receive Ready:

If the value of the code- subfield is 00, it is an RR S-frame. This kind of frame acknowledges a safe and sound frame or group of frames.

Receive not Ready:

If the value of the code subfield is 10, it is an RNR S-frame. It acknowledges the receipt of a frame or group of frames and indicates that the receiver is busy and can't receive more frames. It acts like a congestion control mechanism by asking the sender to be slowdown.

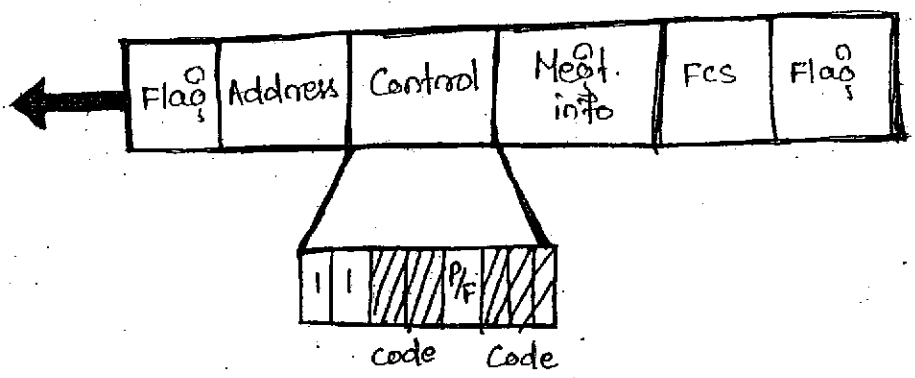
Reject:

If the value of the code subfield is 01, it is a REJ S-Frame. It is a NAK frame that can be used in Go-BACK-N-ARQ to improve the efficiency.

- Fifth bit in the control frame are P/F bit.
- The next 3-bit called NCR) correspond to the ACK and NAK value.

U Frame:

- It is used to exchange session management and control information between connected devices.
- It contain an information field, but used for system management information not user data.



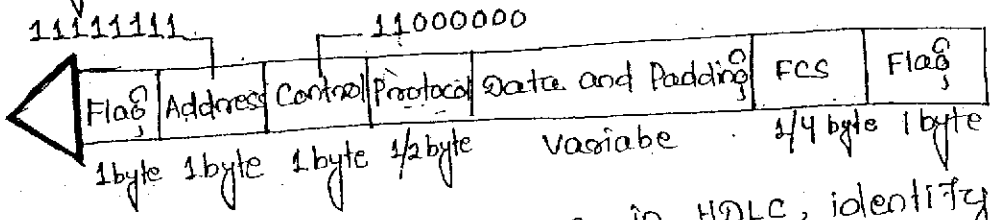
Point to Point Access - PPP

POINT TO POINT PROTOCOL:

- One of the most common protocol for point-to-point access is the point-to point protocol.
- Sevices provied by PPP are.
  - * It defines the format of the frame to be exchanged bet devices.
  - * It defines how two devices can negotiate the establishment of the link and the exchange of data
  - * It defines how the n/w layer data are encapsulated in the data link frame.
  - * It defines how two device are authenticate each other. (previously checked)

Frame Format:

PPP employs a version of HDLC



Flag field: The flag field like one in HDLC, identify the boundries of PPP frame 01111110.

Address field: It uses the broadcast addresses of HDLC, 11111111 to avoid data link address in the protocol.

Control field: Control field uses the format of U-frame in HDLC. The value is 11000000 show that the frame doesn't contain any sequence no. and that there is no flow or error control.

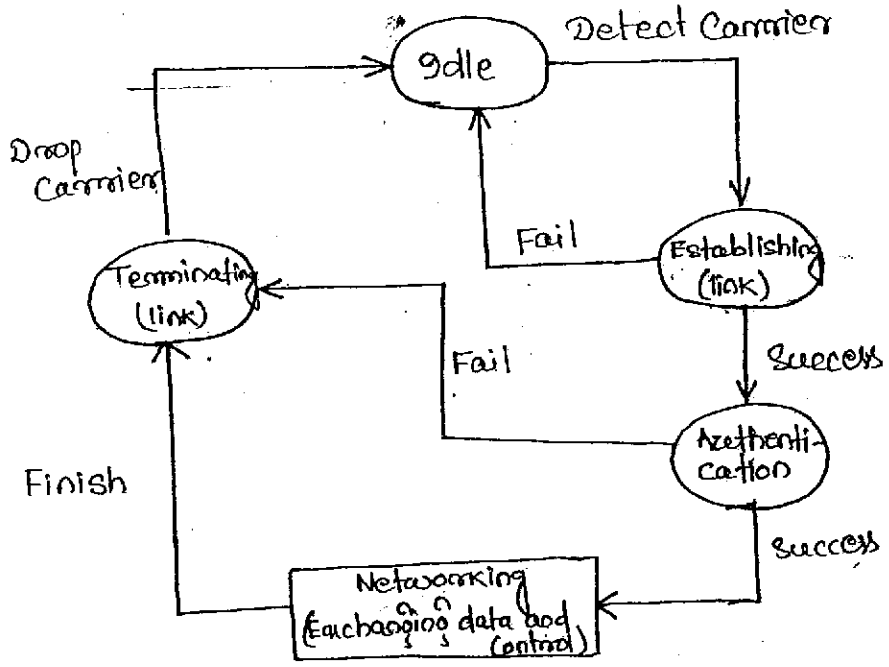
Protocol field: It defines what is being carried in the data field user data or other information

Data field: The field carries either user data or other information

Frame check sequence (FCS) field: It is a 2byte or 4 byte CRC.

Transition state:

A PPP connection goes through different phases shown in a transition state diagram.



Transition States

→ Ideal state: It means that link is not being used. There is no active carrier and line is quiet./Quite.

→ Establishing state: When one of the end point starts the communication the connection goes into establishing state. Here options are negotiated between the two parties. If the negotiation is successful the system goes to authenticating state or networking state. The link control protocol packets are used for this purpose.

→ Authenicating state: The authenticating state is optional. The two end points may decide, during the establishing state, not to go through this state. If they decide to proceed with authentication, they sent several authentication packets. If the result is successful, the connection goes to the networking state, otherwise go to terminating state.

Networking State: When a connection reaches this state, the exchange of user control and data packets can be started The connection remains in this state until one of the end-points wants to terminate the connection.

Terminating state: When the connection is in the terminating state several packets are exchanged between the two ends for house cleaning and closing the link.

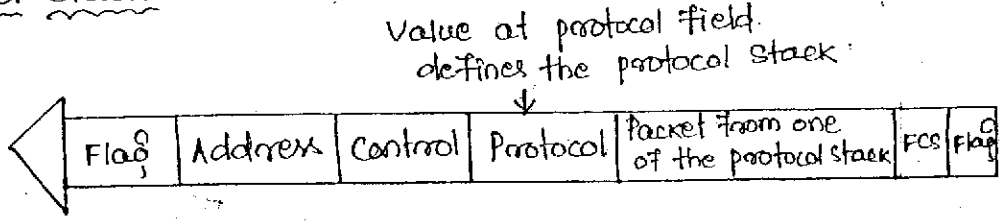
PPP STACK

PPP uses a stack of other protocols to establish the link, to authenticate the parties involved and carry the n/w layer data.

Three sets of protocols are defined to make PPP a powerful stack.

(i) Link control Protocol
(ii) Authentication Protocol
(iii) Network Control Protocol.

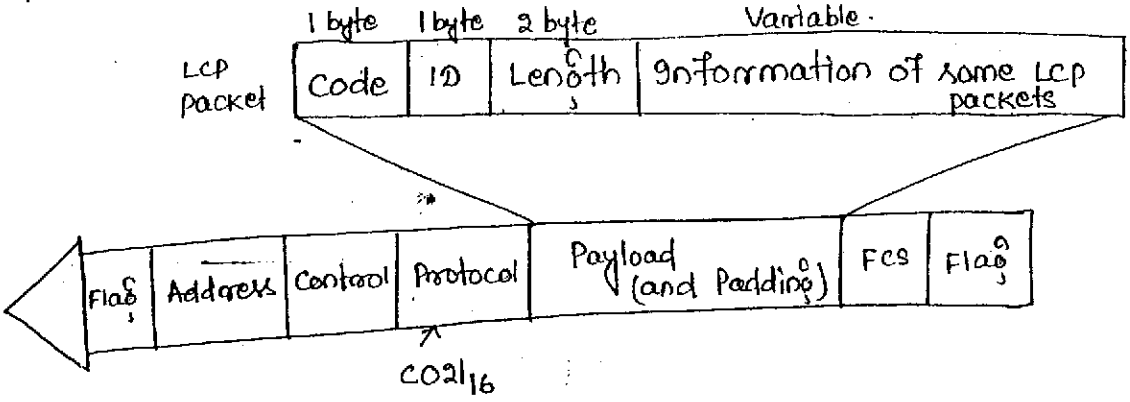
Protocol Stack



Link Control Protocol:

- It is responsible for establishing, maintaining, configuring and terminating links.
- It provides negotiation mechanisms to set options between the two end points.
- PPP carrying an LCP Packet is either in establishing state or terminating state.

- No user data is carried during these states.
- LCD packets are carried in the data field of PPP frame. LCP packet is the value of protocol field.



LCP packet encapsulated in a frame.

Description:

Code: The field defines the types of LCP packets.

ID: This field holds a value used to match a request with the reply. One endpoint inserts a value in this field which will be copied in the reply packet.

Length: Defines the length of entire LCP packet.

Information: It contains extra information needed for some LCP packet.

Configuration Packets:

Configuration Request: A end point that wishes to start a connection sends a configure-request with list of zero or more option to other endpoint.

Configure-ack: If all the options listed in the configure-request packet are accepted by the receiving end, it sends a configure-ack packet, which repeats all the options requested.

Configure-nak: If some options are needed to be omitted or revised, it sends configure-nak packet.

Configure Reject: If some options are not recognized by the receiver, it sends configure reject making those that are not recognised.

Link Termination Packets

Used to disconnect the link between two end-points.

Terminate-Request: Either party can terminate the link by sending a terminate request packet.

Terminate-ack: The party that receives the terminate request packet must answer with a terminate-ack packet.

Link Monitoring and Debugging Packet:

Used for monitoring and debugging the link.

Code Reject: If the endpoint receives a packet with an unrecognized in the packet, it sends a code-reject packet.

protocol Reject: If the endpoint receives a packet with an unrecognized protocol in the frame, it sends protocol reject packet.

Echo-Request: This packet is sent to monitor the link. Its purpose is to see if the link is functioning.

Echo-Reply: It is sent in response to an echo-request

Discard-Request: This is a kind of loop back test packet. It is used by the sender to check the internal condition. The receiver of the packet just discards it.

Authentication Protocol:

- It plays a very important role in PPP because PPP is designed for used over dial-up links, where varification of user identity is necessary.
- Authentication means validating the identify of a user who needs to access a set of resources.
- PPP has created two protocols for authentication.
  - (i) Password authentication protocol (PAP)
  - (ii) Challenge handshake authentication protocol (CHAP).
- During this state, no user data are exchanged, only the corresponding packets to authenticate the user.

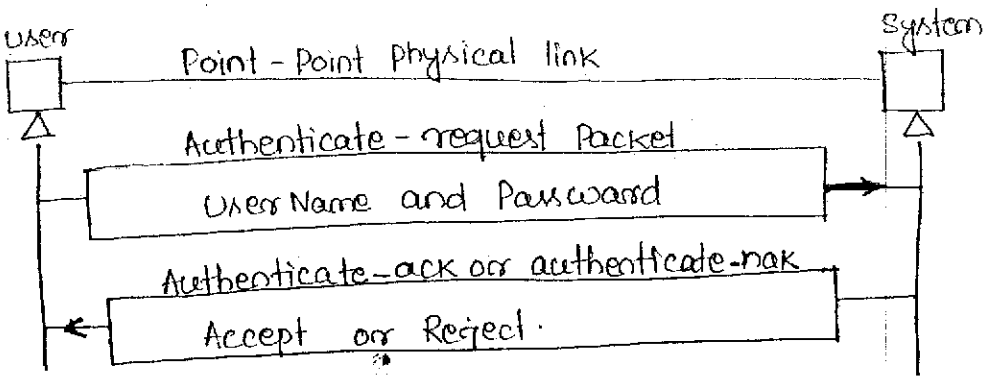
PAP

- A password Authentication Protocol is a simple authentication procedure of two steps.
  - (i) The user who wants to access a system sends an authenication identification (user name) and a password
  - (ii) The system checks the validity of the identification and password and either accepts or denies connection.

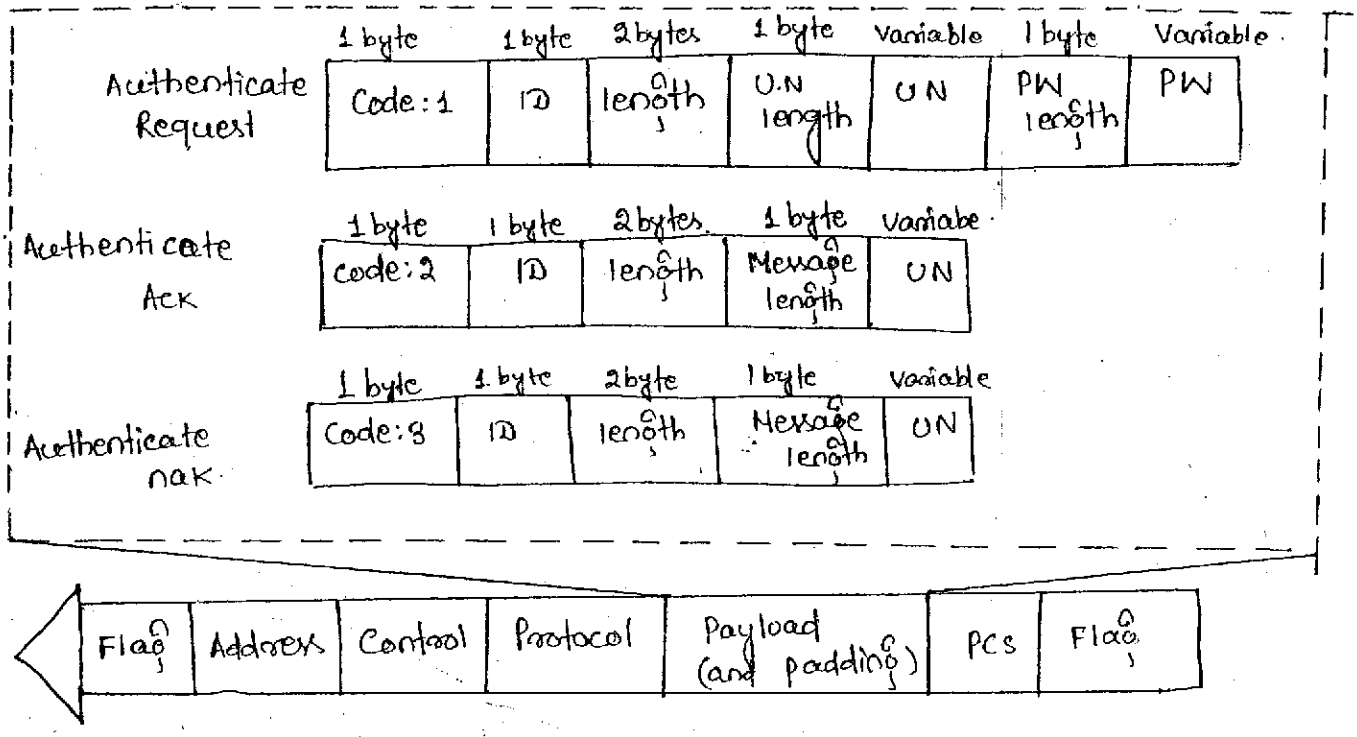
- Disadvantage:
  It is not secure, a third party with access to the link can easily pickup the password and access the system resources.

PAP Packets:
- PAP packets are encapsulated in a PAP frame. It is distinguished from other packets by the value of protocol field $C023_{16}$.
- There are 3 PAP packets
  - -> authenticate - request : used to send UN and PW
  - -> authenticate - ack : used to allow access
  - -> authenticate - nak : used to denay access.

PAP



PAP Packet:



CHAP

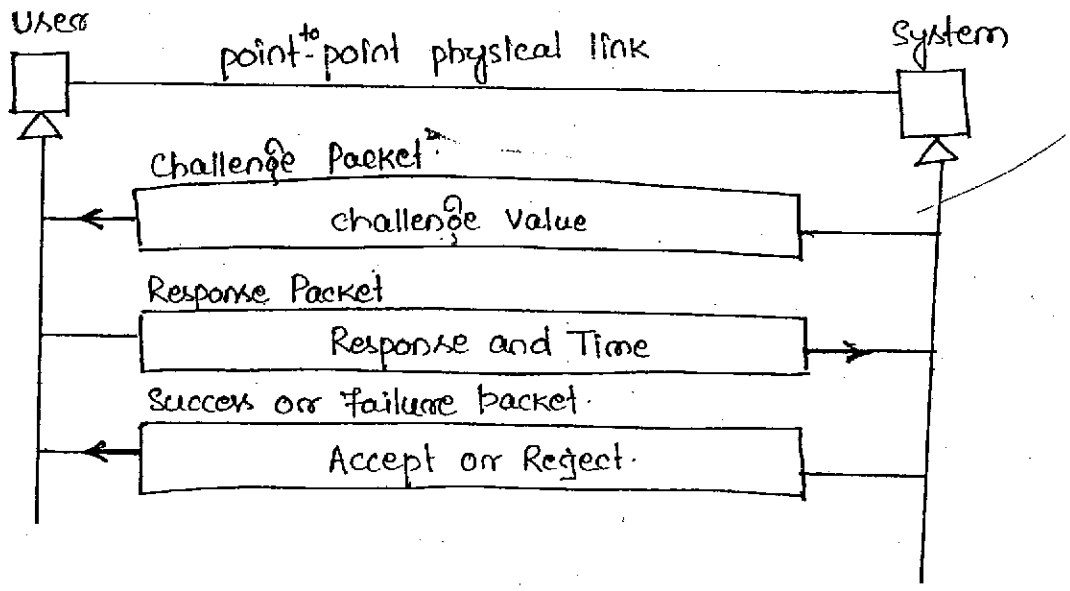
- It is a three way hand shaking authentication protocol that provides greater security than PAP.
- PW is kept is secret, it is never sent on-line.

- The system sends to the user a challenge packet containing a challenge value.
- The user applies a predefined function that takes the challenge value and user's own password and creates a result. The user ~~the~~ sends the result in the response packet to the system.

- The system does the same. It applies the same function to the PW of the user (known to the system) and the challenge value to create a result. If the result created is same as the result sent in the response packet, access is granted, otherwise it is denied.

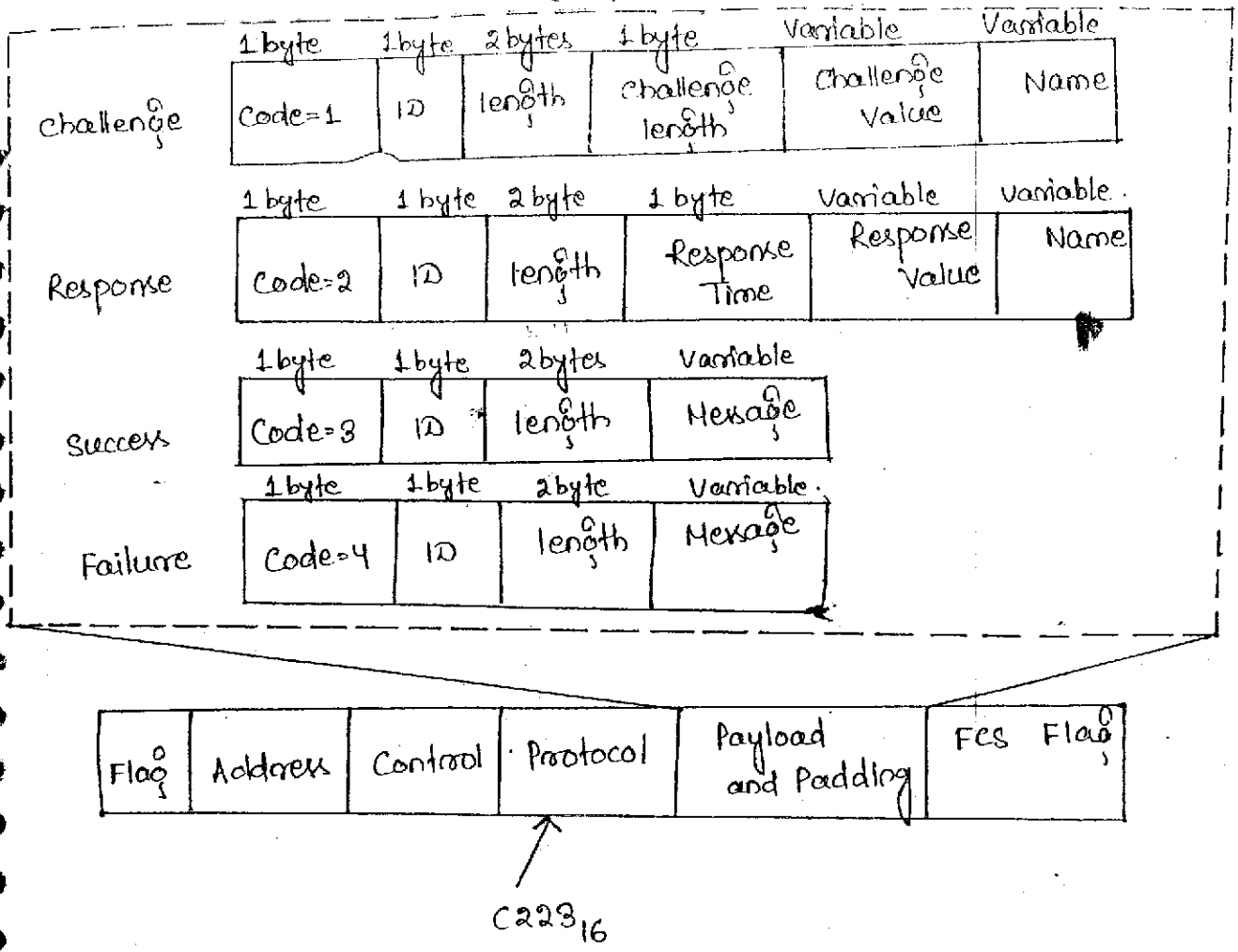
CHAP Packets:

- CHAP Packets are encapsulated in the PPP frame. A CHAP packet is distinguished from other packet by the protocol field.
- There are four CHAP Packets: challenge, Response, Success, Failure.



CHAP

- The first packet is used to send the challenge value.
- Second is used by the user to return the results of the calculation.
- The third is used by the system to allow access to the system.
- Fourth is used by the system to deny access to the system.



Network Control Protocol:

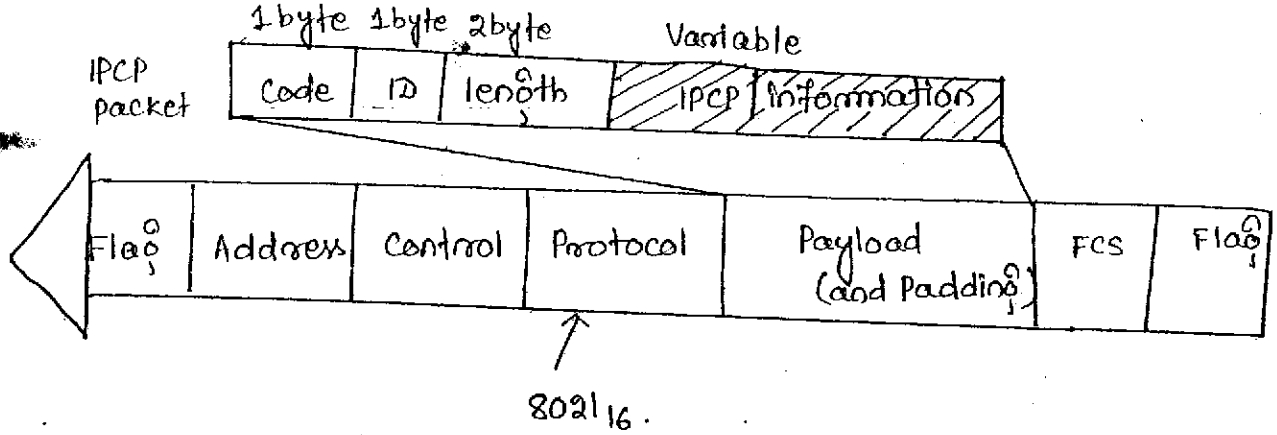
- After the link is established and authentication is successful the connection goes to the networking state.
- Here PPP uses NCP. It is a set of control protocols to allow the encapsulation of data coming from network layer protocol into PPP frame.

IPCP:

- PPP requires two parties to negotiate not only at the data link layer but also at the n/w layer
- Before user data can be sent a connection must be established at this level.

- The set of packets that establish and terminate a n/w layer connection for IP packets is called Internetwork Protocol Control Protocol (IPCP).

- The value of protocol field 8021_{16} defines the packet encapsulated in the protocol as an IPCP packet.



- Seven packets are defined for the IPCP distinguished by their code values as:

1. configure_request (01), 2. Configure-ack (02)
3. Configure_nak (03) 4. Configure-reject (04)
5. Terminate-request (05) 6. Terminate-ack (06)
7. Code-reject (07)

- A party uses configure-request packet to negotiate options with the other party.

- After configuration, the link is ready to carry IP data in the payload field of a PPP frame. (value of protocol field is 0021_{16}), to show that an IP data packet (not IPCP) is being across the link.

- After IP has sent all its packets, the IPCP can take control and use the terminate request and terminate-ack packets to end the n/w connection.

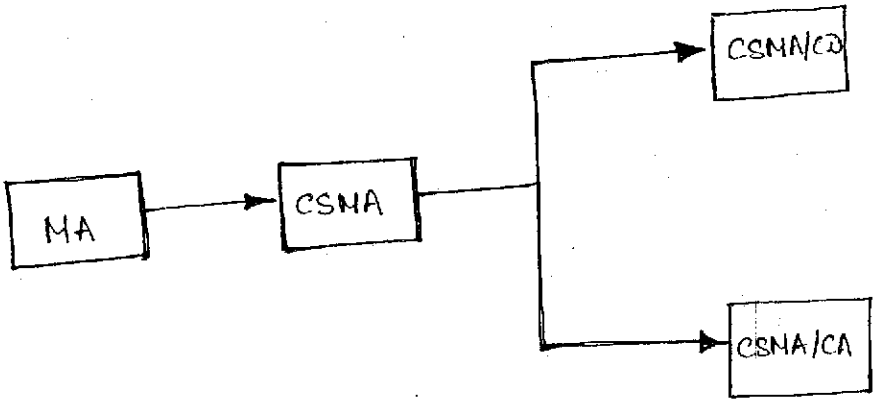
MULTIPLE ACCESS

When nodes or stations are connected to or use a common link called a multipoint or broadcast link, we need a multiple access process protocol to co-ordinate access to the link.

On a Multipoint network many formal protocols have been devised to handle access to the shared Link. They are categorised into 3 groups.

Random Access

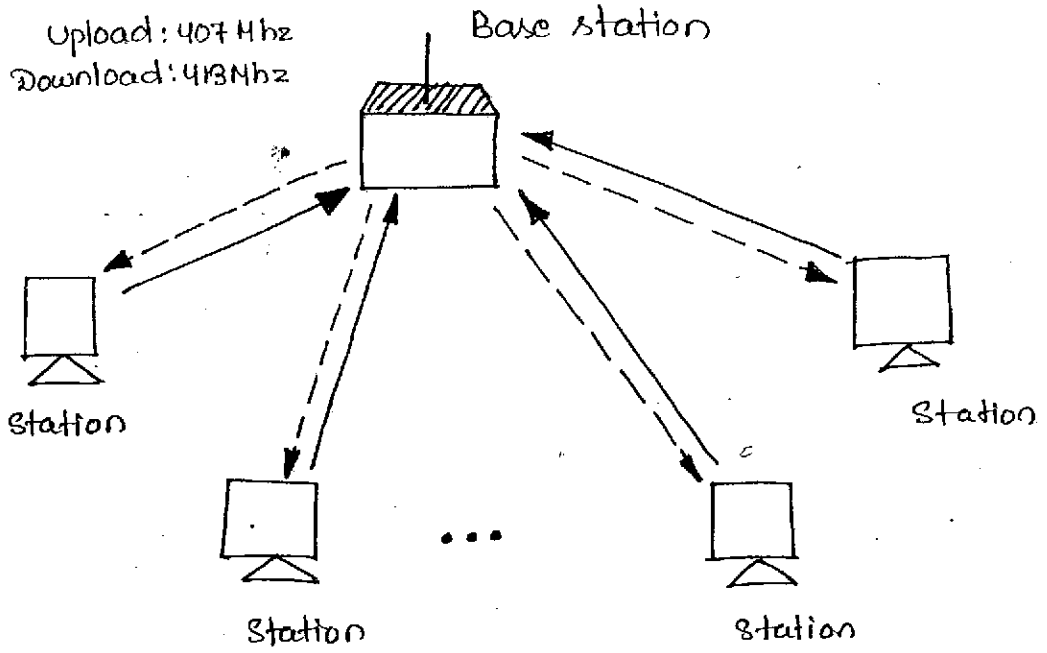
- On random access method each station has the right to the medium without being controlled by any other station. If more than one station tries to send there is an access conflict (collision) and the frames will be either destroyed or modified.



- A method known as ALOHA used a very simple procedure called multiple access. It is improved with a procedure that force the station to sense the medium before transmitting. This is called carrier sense multiple access CSMA. It again developed into CSMA/CA (collision avoidance) and CSMA/CD (collision detection).

Multiple Access:

- ALOHA, the earliest random access method was designed to be used on a radio (Wireless local area network) with a data rate 9600 bps.

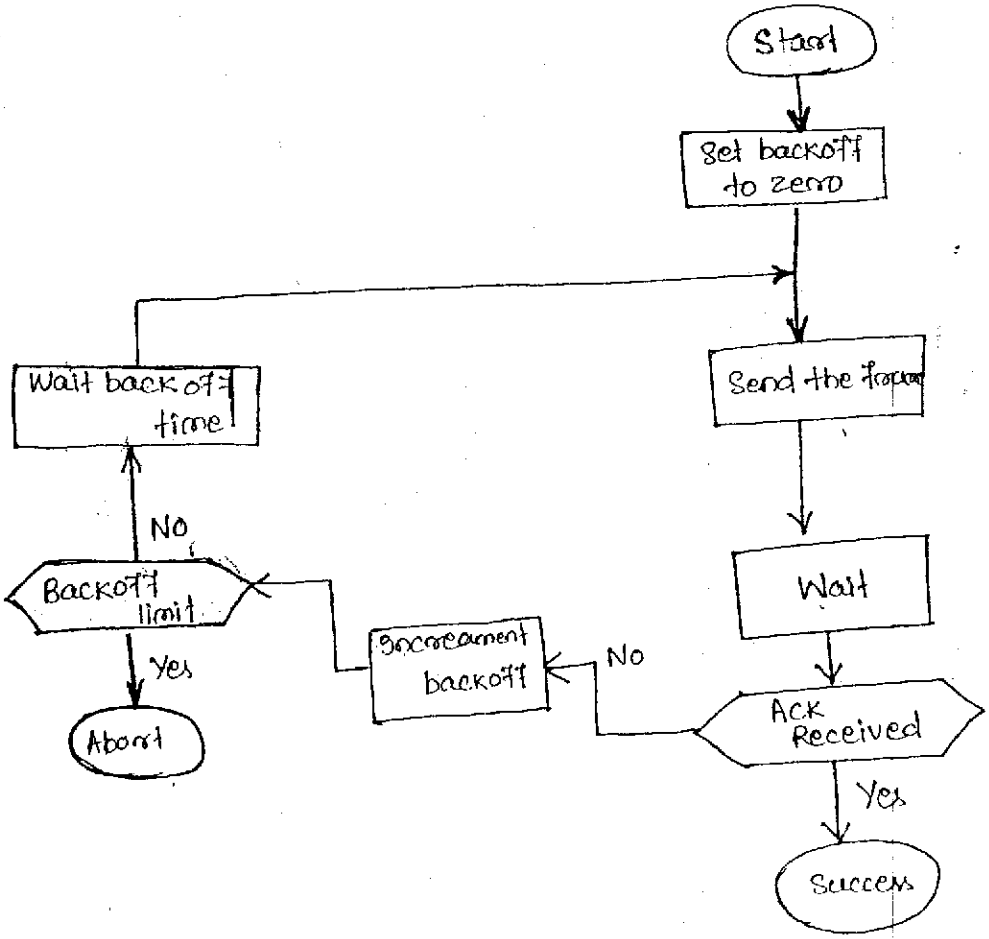


ALOHA Network.

- A base station is the central controller. Every station that needs to send a frame to another station first send it to the base station.
- The base station receives the frame and relays it to the intended destination.
- The BS acts as a hop
- The uploading transmission uses modulation 407Mhz and downloading transmission uses a carrier frequency of 413Mhz.
- When there is a collision ALOHA protocol works like the following rules:

- Multiple Access: Any station sends a frame when it has a frame to send.
- Acknowledgement: After sending the frame, the station waits for an acknowledgement. If it doesn't receive an acknowledgement during alloted time, which is two times the maximum propagation delay, it assumes that the frame is lost. It sends it again after a random amount of time.

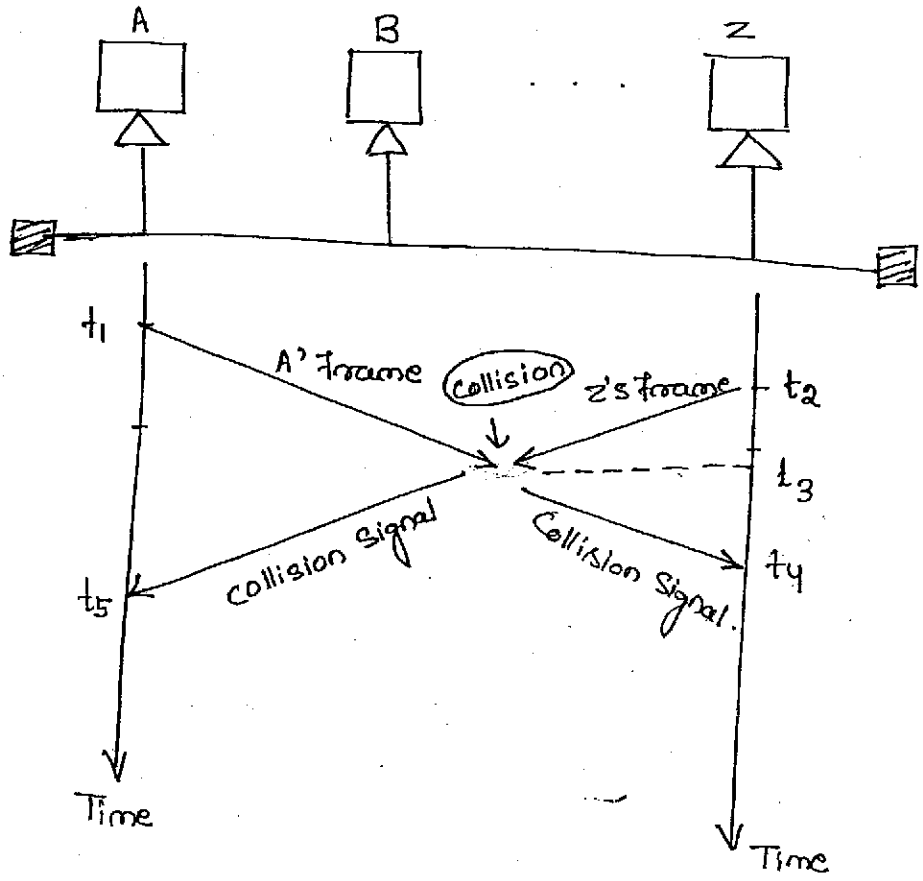
- After several tries, if there is no acknowledgement, the station gives up.



procedure of ALOHA protocol

Carrier Sense Multiple Access (CSMA):

- To minimize the chance of collision, the CSMA method was developed.
- It is based on the principle "sense before transmit" or "Listen before talk". It requires that each station first check the state of the medium.
- It can reduce the possibility of collision but it cannot eliminate it.
- The possibility of collision still exists because of the propagation delay when a station sends a frame, it takes a while for the first bit to reach every station to sense it.
- A station may sense the medium and find it idle, only because propagation by another station has not yet reached the station.



- At time t_1, station A at the end of the medium senses the medium, The medium is idle, so it sends a frame. At time t_2 ($t_2 > t_1$), station Z at the right end of the medium

senses the medium and finds it idle because, at this time, propagation from station A has not reached station z. Station z also send a frame. The two signals collide at time $t_3 (t_3 > t_2 > t_1)$ The result of collision is a garbel signal propagate in both direction which reaches station z at time $t_4 (t_4 > t_3 > t_2 > t_1)$ at station A at time $t_5 . (t_5 > t_4 > t_3 > t_2 > t_1)$.

Persistance Strategy:-

- It defines the procedure for a station that senses a medium.

Two substrategies have been devised

(i) Non persistent.

(ii) Persistent.

Non Persistent:

In a non persistent strategy, a station that has a frame to send senses the lines. If the line is idle the station sends immediately. If the line is not idle the station waits a random period of time and senses the line again

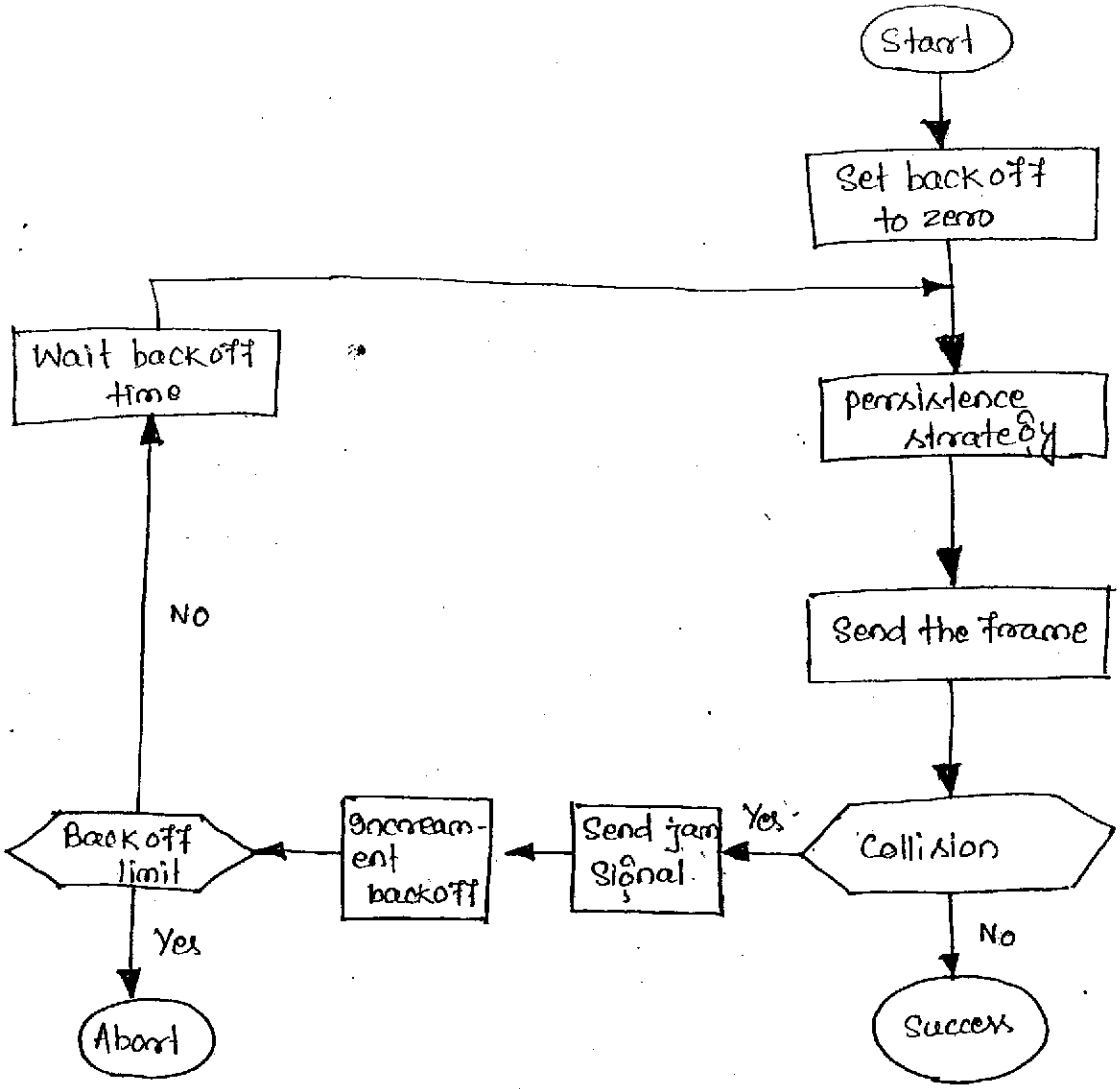
It reduces the collision bet two more stations wait for the same amount of time and then retry again simultaneously. It reduces the efficiency of the n/w when the medium is idle where stations have frames to send

Persistent:

Here a station senses the line. If the line is idle the station send a frame. This method has two variation 1-persistent and p-persistent.

In 1-persistent if the station finds the line idle, the station sends its frame immediately. This method increases the chances of collision.

In p-persistent method, if the station finds the line idle, the station may or may'nt send. It sends with and refrains from sending with probability 1-p



CSMA\CD procedure

- The station that has a frame to send, sets the backoff parameter N to zero.
- It then senses the line using one of the persistence strategies.
- After sending a frame if it doesn't hear a collision until the whole frame has been ~~sent~~ sent, the transmission is successful.
- However if the station hears a collision, it sends a jam signal to the line to inform that a collision has occurred.
- By this it informs other station about the ~~inform~~ situation

e.g: It sends with probability p (≤ 0.2) and refrains from sending with probability of 0.8. i.e each station after sensing an idle line sends a probability of 0.2 (20 percent of the time). The station generates a random no. If the random no. is (between 1 to 100) less than 20, the station will send otherwise the station refrains from sending.

It combines advantage of two strategies i.e 1. Reduces the chance of collision and improves the efficiency

CSMA/CD

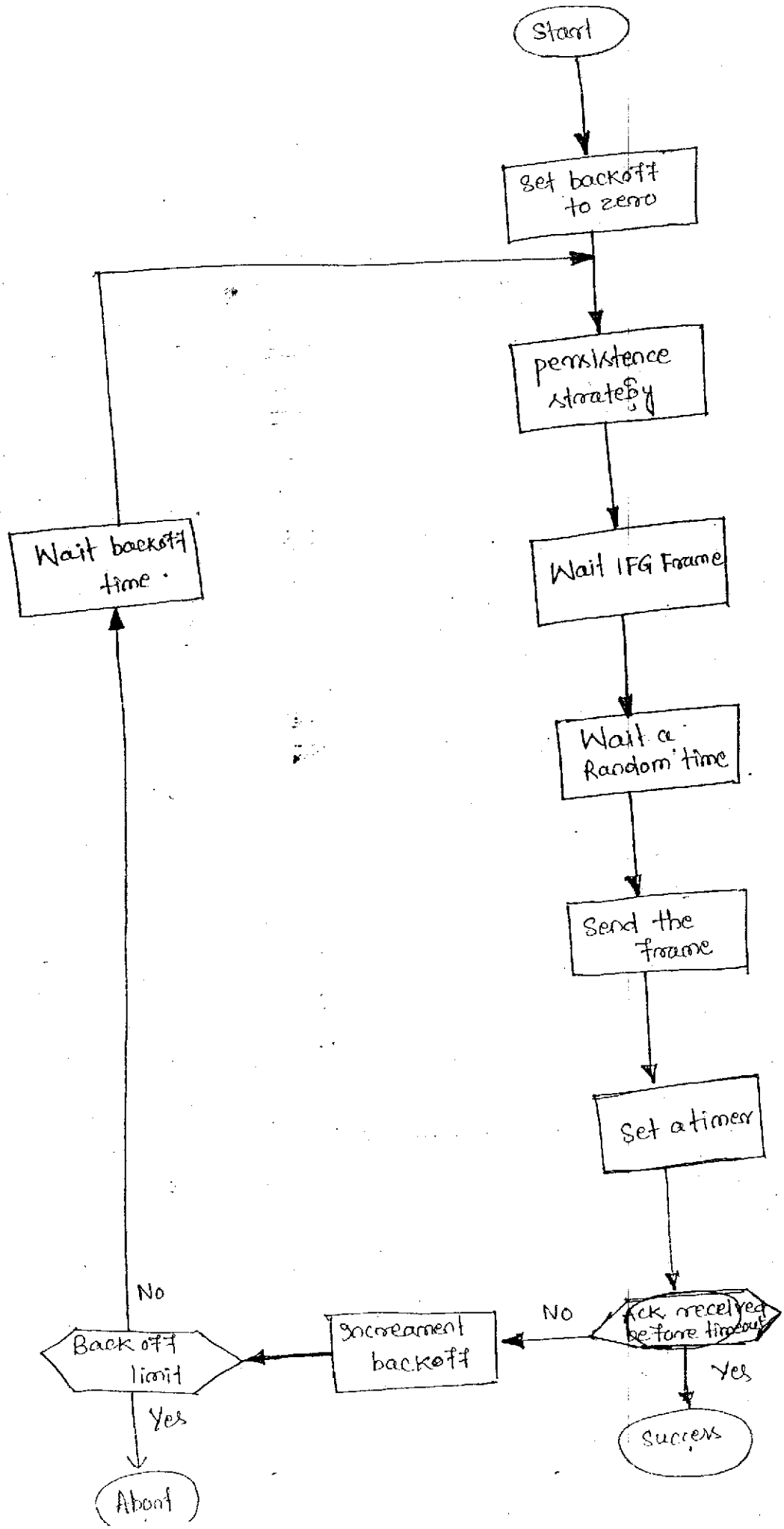
(Carrier sense multiple access with collision detection)

- It doesn't define the procedure for collision, it defines the procedure of handing collision.
- In this method any station can send a frame. The station then monitors the medium to see if transmission was successful and finished.
- If there was a collision, the frame need to be sent again To reduce the probability of collision the station waits needs to back off.
- In the exponential backoff method, the station waits an amount of time between 0 and $2^N \times$ maximum propagation time (time needed for a bit to reach at the end of n/w) where
  N → no. of attempted transmission.
- So it waits between
  0 and $2 \times$ (maximum_propagation_time) for first time
  0 and $2^2 \times$ (maximum-propagation-time) for second time
  so on.

- All station discard the part of the frame received.
- The station then increament the value of backoff parameter by
- It checks to see if the value of the parameter exceeds the limit (usually 15)
- If this value exceeds the limit, it means that the station has tried enough and should give up the attempt.
- If the value has not exceeded the limit, the station waits a random backoff time based on the current value of the backoff parameter and senses the line again.

CSMA/CA:

- In this method there is no collision. The procedure avoids collisi
- The station use one of the persistence strategies. After it finds the line is idle, the station waits an IFG (interface gap) amount of time.
- It then waits another amount of time, After that it sends the frame and sets a timer.
- The station waits for an acknowledgement from the receiver.
- If it receives the acknowledgment before the time expires, the transmission is successful.
- If the station doesn't receive an acknowledgment it knows that something is wrong (the frame is lost or the acknowledgement is lost).
- The station increament the value of backoff timer, waits for backoff amount of time, and resenses the line.
- It is used in wireless LANs.

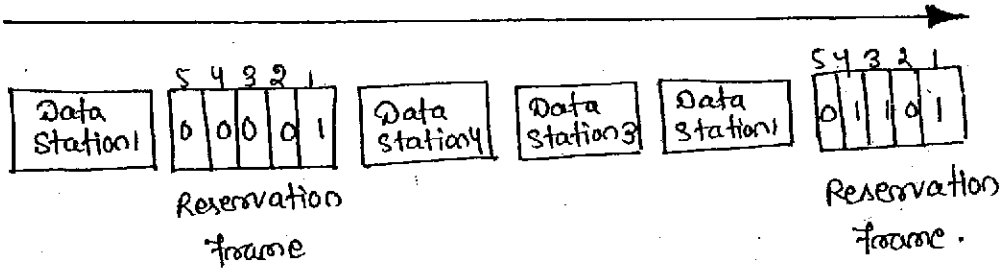

Start
Set backoff to zero
persistence strategy
Wait IFG Frame
Wait a Random time
Send the frame
Set a timer
Ack received before timeout
No
Yes
Success
Increament backoff
No
Back off limit
Yes
Abort
Wait backoff time

Controlled Access

- In controlled access, the station consult one another to find which station has the right to send.
- A station cannot send until it has been authorized by other station.
- There are three controlled access method.

(i) Reservation :

- In reservation access method, a station needs to make a reservation before sending a data frame.
- Time is divided into intervals, a reservation frame precedes the data frame send in that interval.
- If there are N station in the system, there are exactly N reservation minislots in the reservation frame
- Each minislot belong to a station.
- When a station needs to send a data frame, it makes a reservation can send their data frames after the reservation frame.

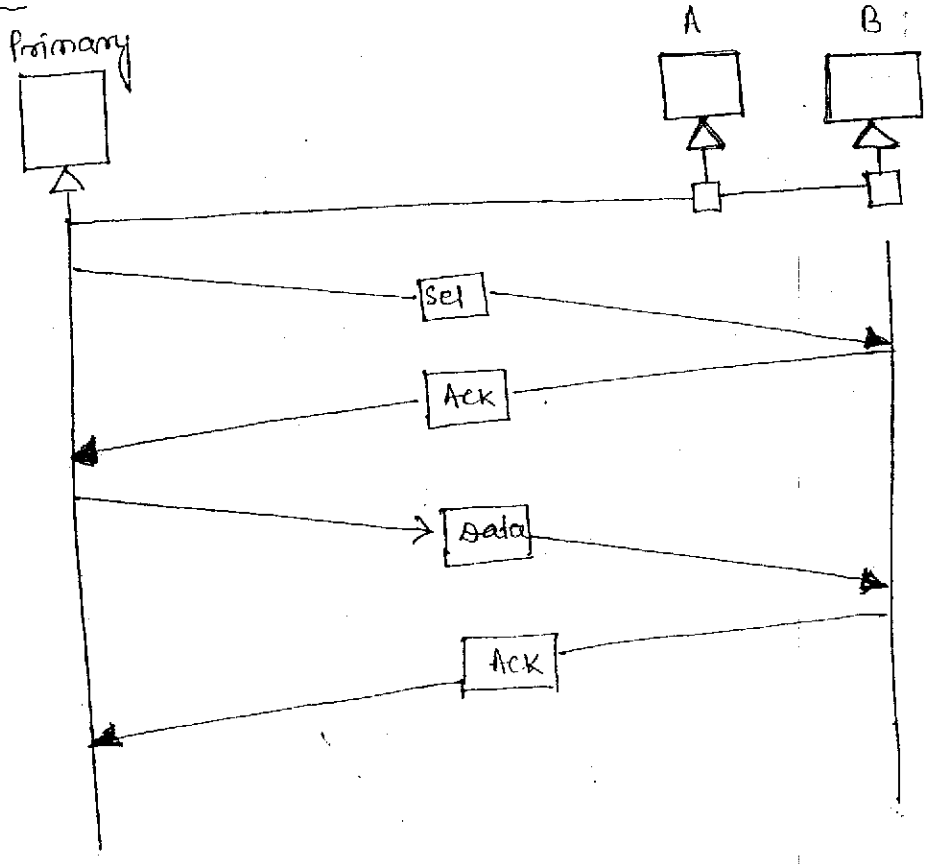


(ii) Polling :

Polling works with topologies in which one device is designed as a primary station and other devices are secondary station.

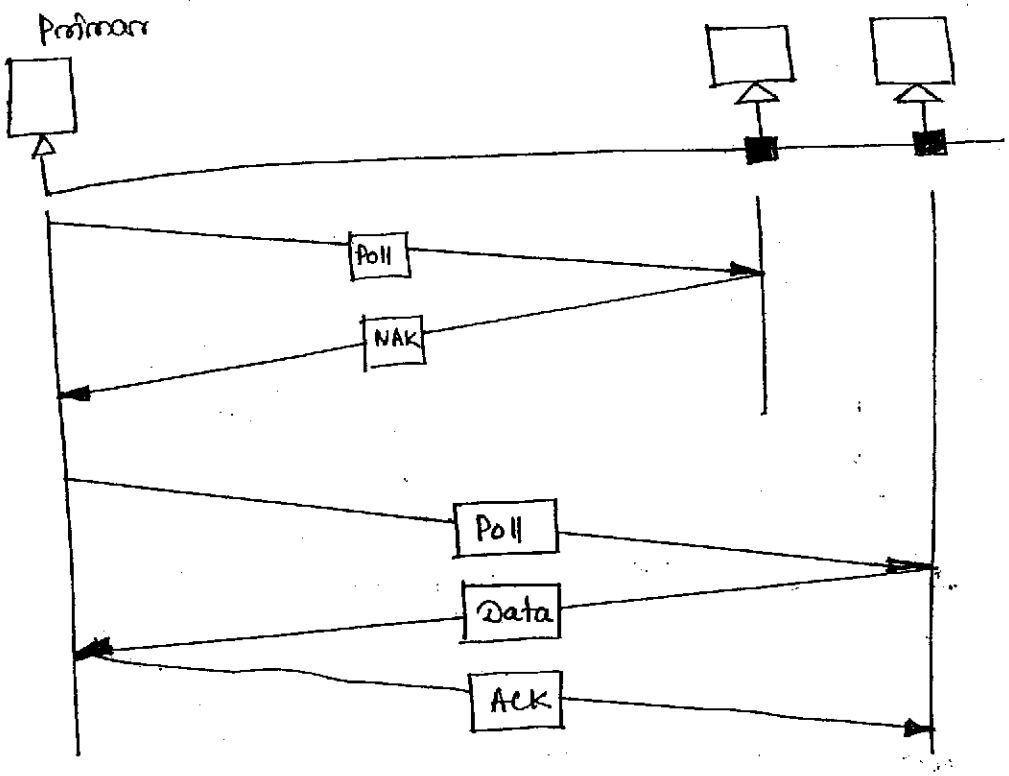
- All the data exchanges must be made through the primary device even when the ultimate station is a secondary device.
- Primary device controls the link, the secondary device follow its instruction.
- It is upto the primary device to determine which device is allowed to use the channel at a given time.
- The primary device, therefore is always the initiator of a session.
- If the primary wants to receive data, it asks the secondaries if they have anything to send; this function is called polling.
- If the primary device wants to send data, it tells the secondary target to get ready to receive, this function is called selecting.

Select:



- The select mode is used whenever the primary device has something to send.
- If the primary is neither sending or receiving data, it knows the link is available.
- If it has something to send, the primary device sends it.
- It doesn't know whether the receiving device is prepared to receive.
- So the primary must alert the secondary to the upcoming transmission and waits for an acknowledgment of the secondary ready status.
- Before sending data, the primary creates and transmit a select (SEL) frame, one field of which includes the address of the intended secondary.

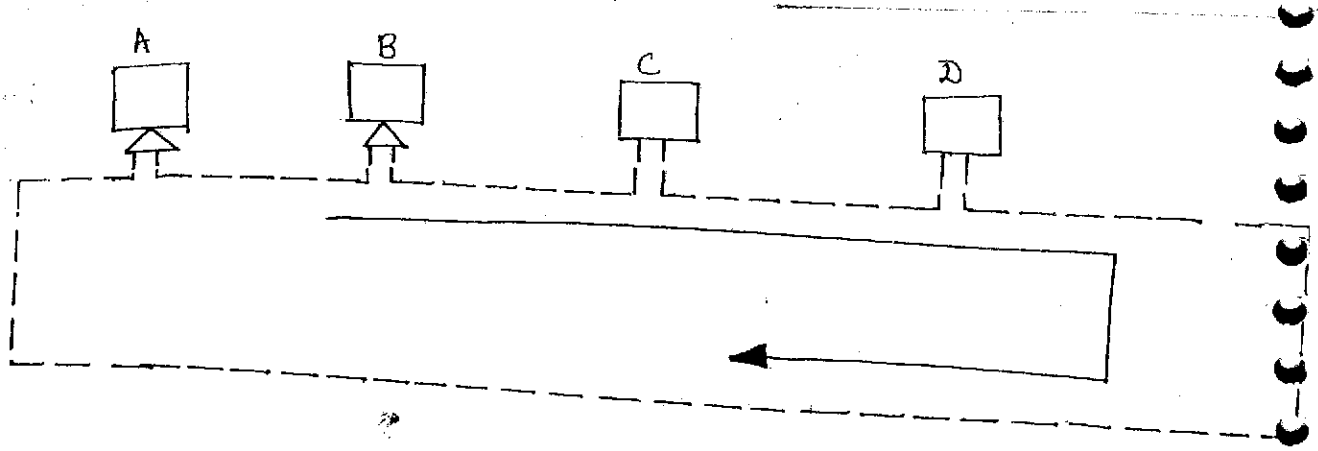
Poll:



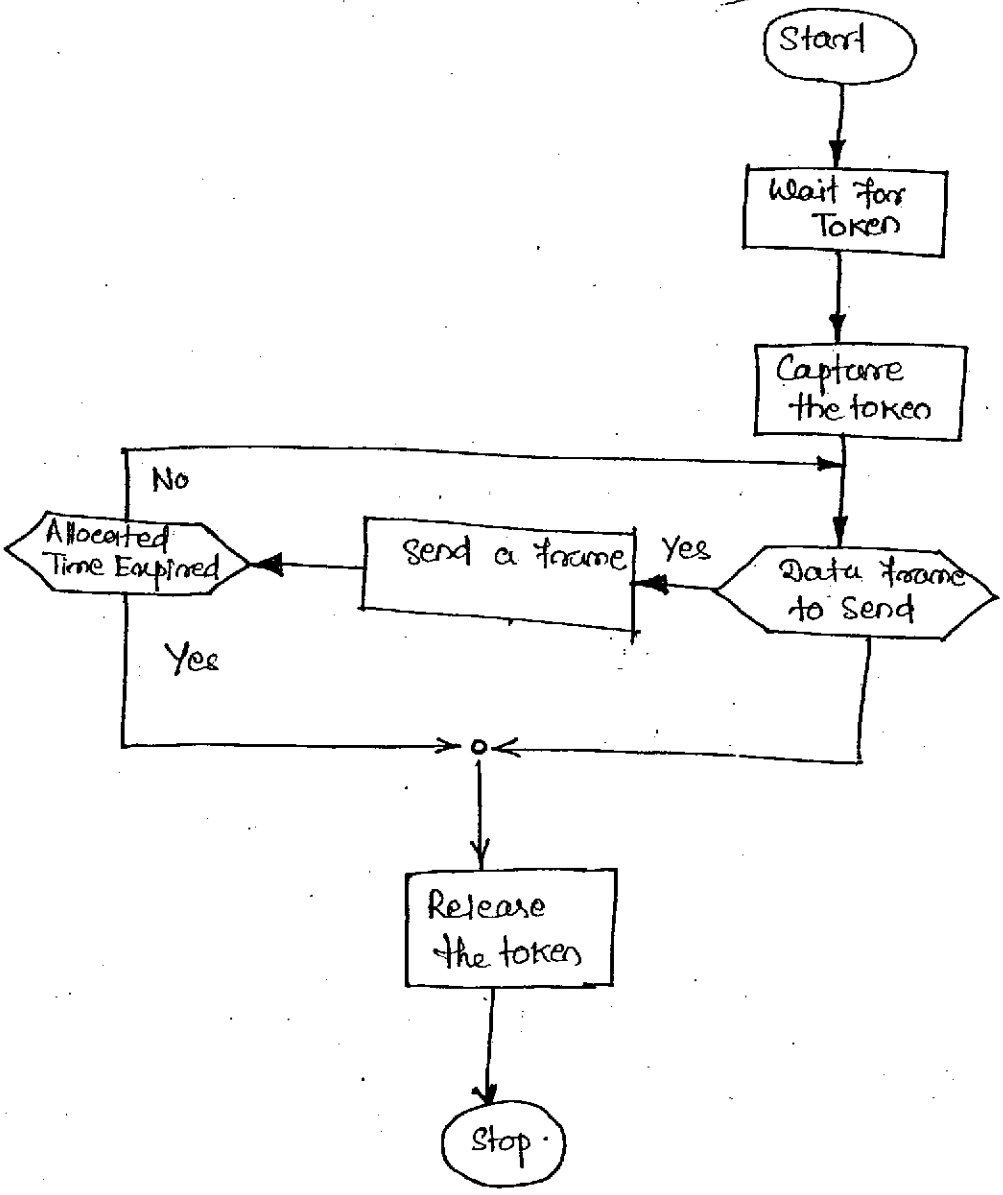
- The polling function is used by the primary device ~~has some-thing to send~~, to receive frame solicit transmission from the secondary device.
- When the primary is ready to receive data, it must ask (poll) each in turn if it has anything to send.
- When the first secondary is approached, it responds either with a NAK frame if it has noting to send or with data (in the form of a data frame) if it does.
- If the response is negative (a NAK frame), the primary the polls the next secondary in the same manner until it finds one with data to send.
- When the respose is +ve, the primary reads the frame and returns an acknowledgment (ACK frame) verifying its receipt.

(iii) Token Passing:-

- In the token passing method, a station is authorized to send data when it receives a special frame called a token.
- In this method stations are arranged around a ring.
- Each station has a predecessor and a successor.
- Frames are coming from the predecessor and going to the successor.
- When no data are being sent, a token circulates around the ring.
- If a station needs to send data, it waits for the token.
- The station captures the token and sends one or more frame, and finally it releases the token to be used by successor station. (next station on physical or logical ring)



Token Passing Network:



Token Passing Procedure

CHANNELIZATION

- Channelization is a multiple access method in which the available bw of a link is shared in time, frequency or through code.
- There are three channelization protocol
  (i) FDMA (ii) TDMA (iii) CDMA

FDMA:

- In frequency division multiple access, the available bw is shared by all stations.
- Each station use its allocated band to send the data. Each band is reserved for specific station.
- FDMA is a data link layer protocol that uses FDM at the physical layer.

TDMA

- In time division multiple access the entire bw is just one channel. The station share the capacity of the channel in time.
- Each station is allocated with a time slot during which it can send data.
- TDMA is a data link layer protocol that uses TDM at physical layer.

CDMA:

- Code division multiple access is based on coding theory. Each station is assigned with a code, which is a sequence of number called chips.
- Suppose we have four stations, each station has a sequence of chips.

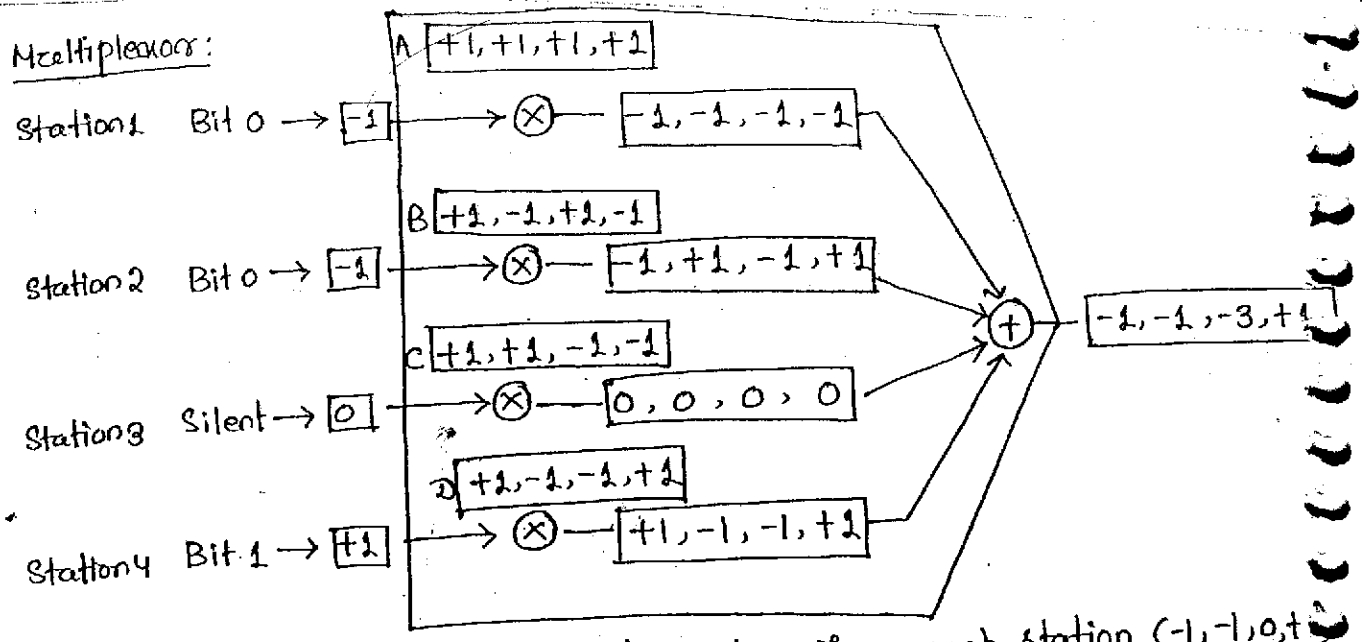
+1 +1 +1 +1	+1 −1 +1 −1	+1 +1 −1 −1	+1 −1 −1 +1

- Rules for encoding

  Station send 0 — Data bit 0 — −1
  Station send 1 — Data bit 1 — +1
  Station is idel — Silence — 0

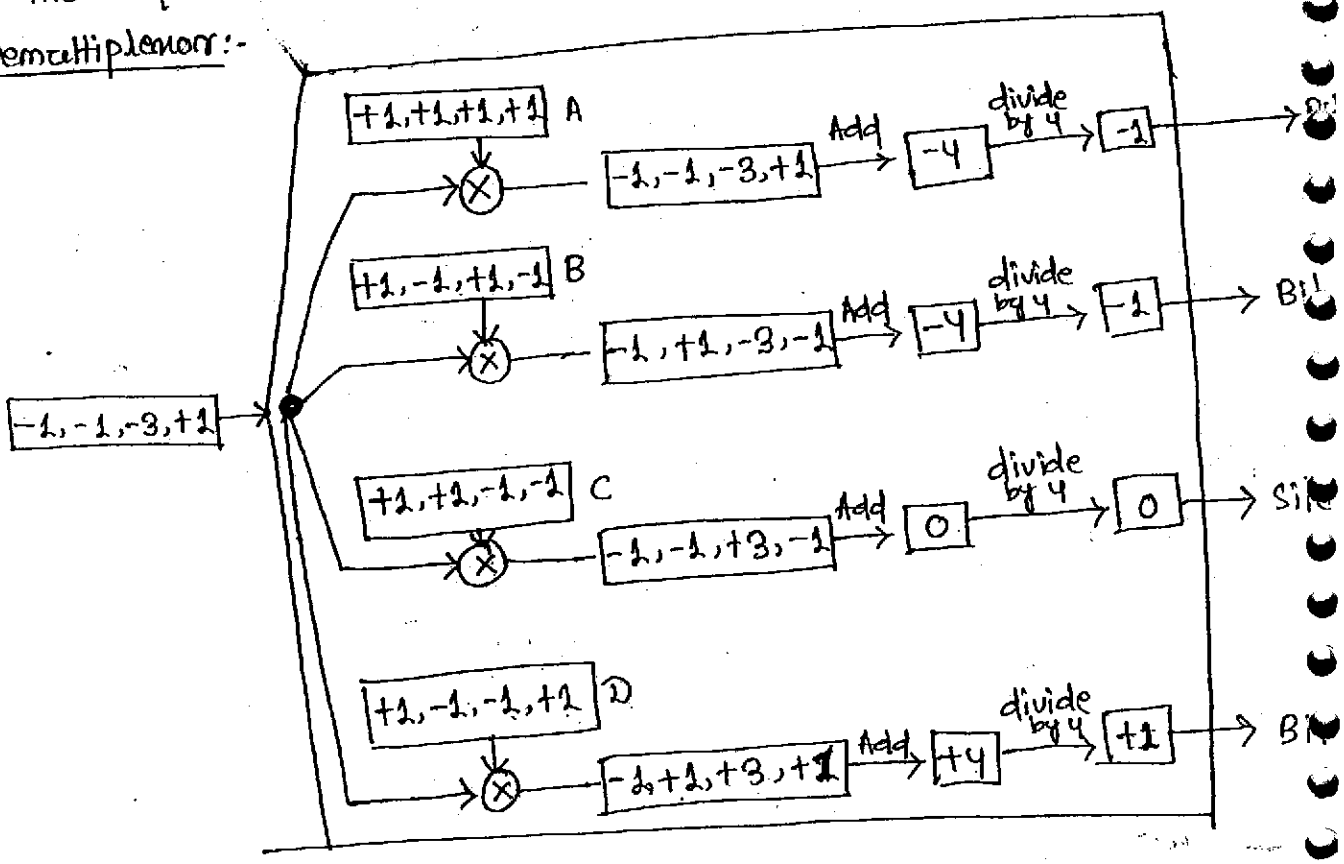
- We assume that station 1, 2 are sending 0 bit, ~~channel~~ station 4 is sending 1 bit and station 3 is silent.

Multiplexor:



i. Multiplexor receives one encoded number from each station (-1,-1,0,+1)
ii. The encoded no. sent by station 1 is multiplied by each chip in sequence A. A new sequence is the result (-1,-1,-1,-1). The same is true for the remaining stations.
iii. All chips are added. The result is one new sequence.
iv. The sequence is transmitted through the link.

Demultiplexor:-



i. The demultiplexer receives the sequence sent across the link.
ii. It multiplies the sequce by the code for each receiver. The multiplication is done chip by chip.
iii. The chips in sequence are added. The result is always +4, -4, 0
iv. The result of step 3 is divided by 4 to get -1, +1, 0
v. The number in step 4 I decoded to 0, 1 or silence by the receiver.

Orthogonal Sequence:-

The sequence of the stations are carefully selected, called as orthogonal sequence.

Sequence Generation

- To generate a sequence we use a walsh table, a 2-D table with a equal no. of rows and columns.
- Each row is a sequence of chips.
- Acc. to walsh if we know the table for N sequence, we can create the table for 2N sequence W_{2N} $(N = 2^m)$
- The walsh table W_1 for one chip sequence has one row and one column. We can chose -1 or +1 (here we choose +1)

$$W_1 = [+1]$$

$$W_{2N} = W_2 2^m = W_{2\,2^0} = W_2 = \begin{bmatrix} W_1 & W_1 \\ W_1 & \overline{W_1} \end{bmatrix}$$

As W_{2N} so 2 row and 2 columns

$$= \begin{bmatrix} +1 & +1 \\ +1 & -1 \end{bmatrix}$$

$$W_4 = \begin{bmatrix} W_2 & W_2 \\ W_2 & \overline{W_2} \end{bmatrix} = \begin{bmatrix} +1 & +1 & +1 & +1 \\ +2 & -1 & +1 & -1 \\ +2 & +1 & -2 & -1 \\ +1 & -1 & -2 & +2 \end{bmatrix}$$

LOCAL AREA NETWORKS

Ethernet

Traditional Ethernet:

- Traditional ethernet was designed to operate at 10Mbps. Acc to the n/w by a device is through a contention method (CSMA/CD). The media are shared between all stations.

MAC Sublayer:

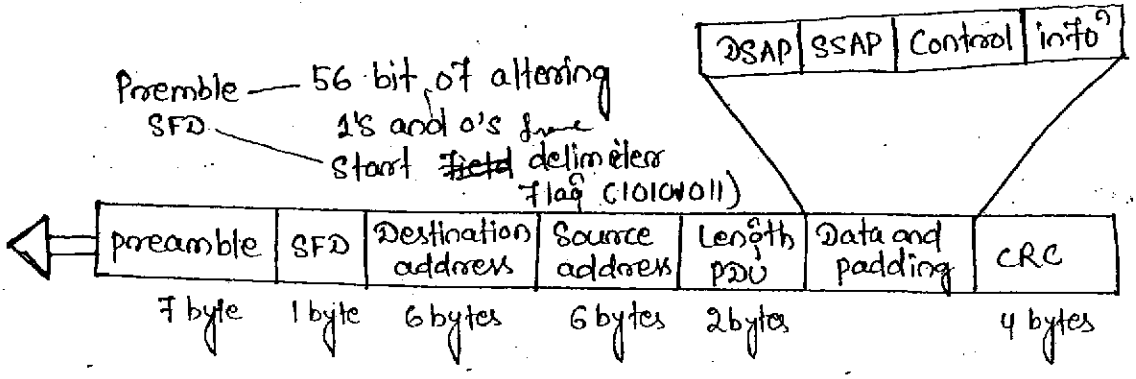
- It governs the operation of the access method. It also frames data received from the upper layer and passes them to PSS sublayer for encoding.

Access Method: CSMA/CD:

- Traditional ethernet uses 1-persistent CSMA/CD as the access method.

Frame:

- Ethernet frame contain 7 fields: preamble, SFD, DA, SA, length and type of protocol data unit (PDU), upper layer data, and the CRC.
- It doesn't provide any mechanism for acknowledging received frames, making it as an unreliable medium.
- Acknowledgement must be implemented at higher layers.



802.3 MAC frame

• Preamble:-
→ It contains 7 bytes of alternating 0s and 1s, that alert the receiving system to the coming frame and enable it to synchronize its input timing.
→ The pattern provides only an alert and a timing pulse.
→ The preamble is actually added at the physical layer and is not a part of the frame.

• Start frame delimiter (SFD):-
→ The second field (1 byte: 10101011) signals the beginning of the frame.
→ It tells the station that they have the last chance for synchronization.
→ The last two bit 11 and alert the receiver that the next field is the destination address.

• Destination Address (DA):-
→ DA field is 6 byte and contain the physical address of destination station or stations to receive the packet.

• Source address (SA):
→ SA field is also 6 byte and contain the physical address of the sender of the packet.

• Length/Type:
→ The field is defined as length or type. field.
→ If the value of the field is less than 1518, it is a length field and defines the length of data field as follows.
→ If the value of the field is greater than 1536, it defines the type of PDU packet that is encapsulated in the frame.

Data:-
→ The field carries data encapsulated from the upper layer protocol.

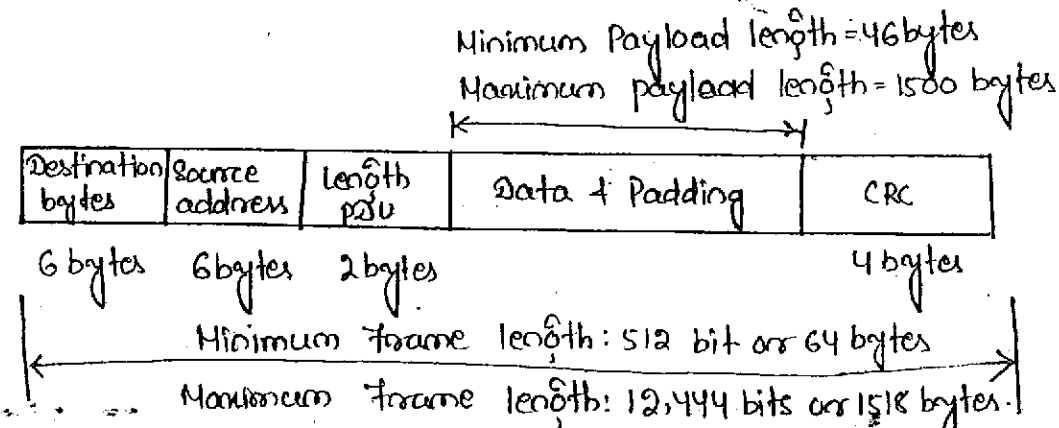
→ It is minimum of 46 and maximum of 1500 bytes.

• CRC:-

→ The last field contains the error detection information. (CRC-3)

Frame Length:

Ethernet has imposed restrictions on both the minimum and maximum length of a frame.



- Minimum length restriction is required for the correction of CSMA/CD.
- If there is a collision before the physical layer sends a frame out of a station, it must be heard by all station.
- If the entire frame is sent out before a collision is detected, it is too late.
- MAC layer has already discarded the frame, thinking that the frame has reached the station/destination.
- This situation is aggravated as the frame length diminishes in size since smaller frames are send out faster.
- The standard has therefore defined the smallest frame length for every 10 Mbps, ethernet LAN as 512 bits or 64 bytes.
- Part of this length is the header and the tailer (6 byte source address, 6 bytes destination address, 2 bytes length/type, and 4 bytes CRC) = 18 bytes
- Then the minimum length of data from the upper layer 64-18 = 46 bytes.

- If the upper layer packet is less than 46 bytes, padding is added to make up the difference.
- The standard defines the maximum length of a frame as 1518 bytes.
- If we subtract the 18 bytes of header and tailer, the maximum length of payload is 1500 bytes.

Addressing:-

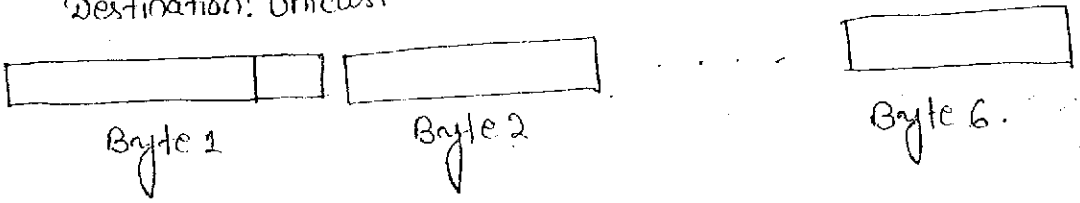
- Each station on an ethernet network has its own NIC (network interface card).
- The NIC fits inside the station and provids the station with a 6 byte physical address.
- The ethernet address is 6 bytes that is normally written in hexadecimal notation, using a hypen to separate bytes from each other.

06-01-02-01-2C-2B

Unicast, Multicast and Broadcast Address:

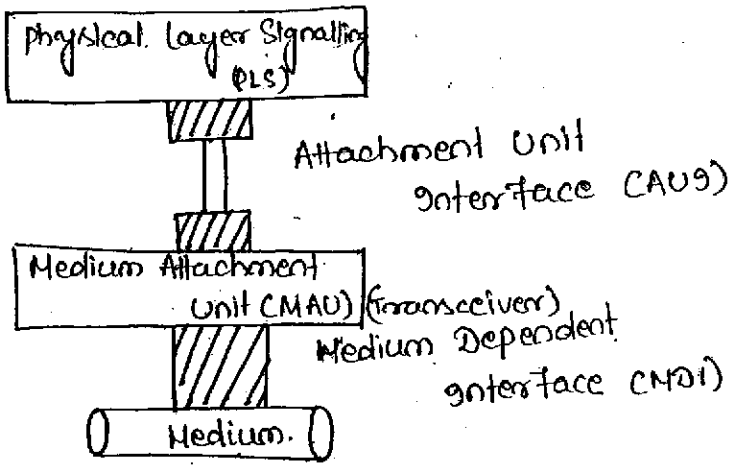
- A source address is always a unicast address - the frame comes from only one station.
- The destination address however can be unicast, multicast, broadcast.

Source: always 0
Destination: Unicast 0, multicast 1



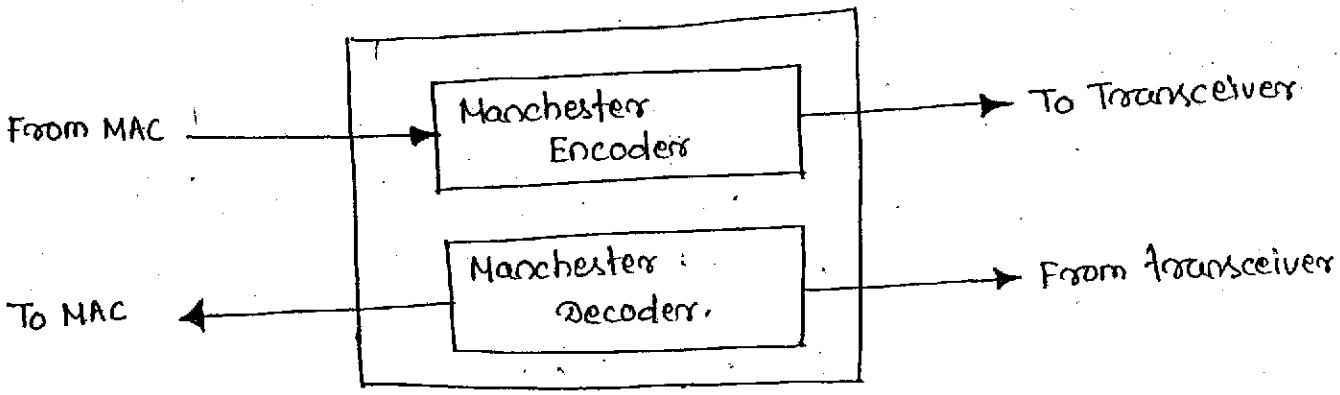
- A unicast destination address defines only one recipient: the relationship between the sender and receiver is one-to-one.
- A multicast destination address defines a group of address. The relationship bet^n the sender and receiver is one-to-many.
- The broadcast address is a special case of multicast address: the recipients are all the stations on the network.

Physical Layer:-



PLS: (Physical Layer Signaling)

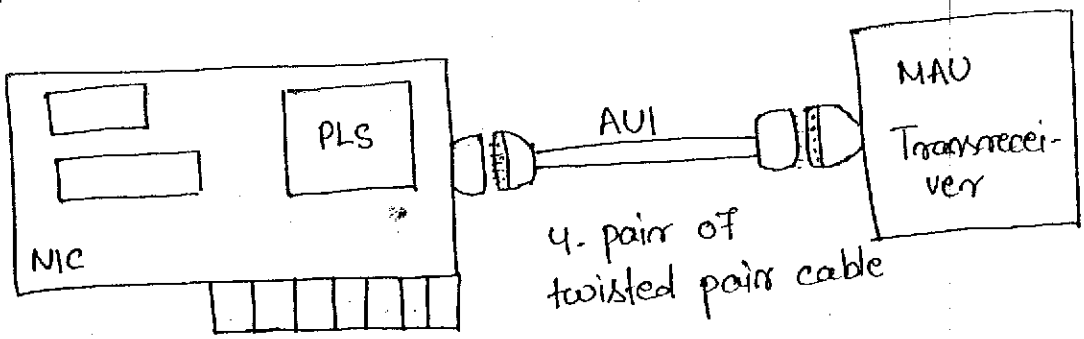
PLS sublayer encodes and decodes data, Traditional Ethernet uses Manchester encoding with data rate 10Mbps. For this data rate a bw of 10baud is needed.



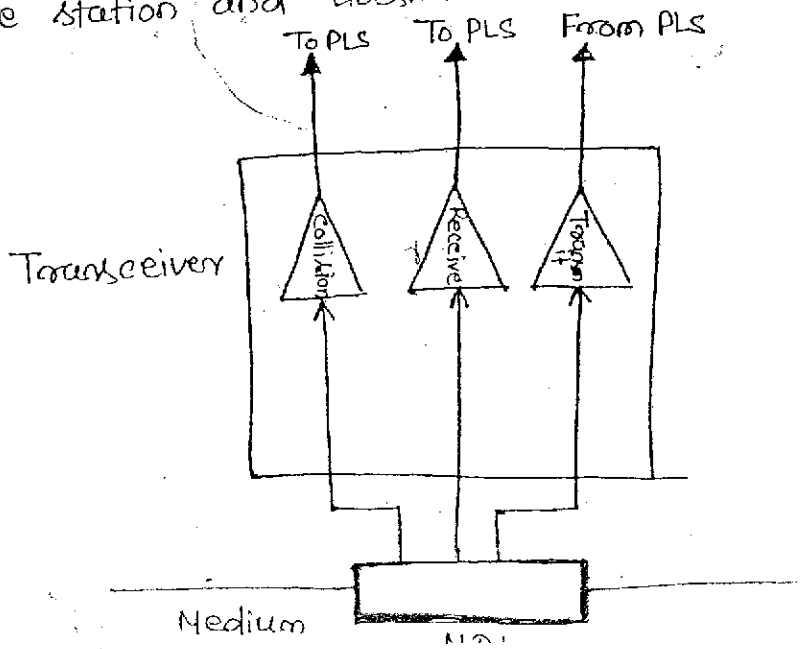
AUI: (Attachment Unit Interface)

The attachment Unit Interface is a specification that defines the interface between the PLS and MAU. AUI was ~~created~~ developed to create a kind of medium independent

interface between PLS and MAU.
Designed for the first implementation of ethernet which used thick co-axial cable.



MAU Transceiver:-
The medium attachment unit or transsceiver is medium dependent it creates the appropriate signal for each particular medium. There is a MAU for each type of medium used in 10Mbps ethernet.
A co-axial cable needs its own type of MAU, the twisted pair needs a twisted pair MAU and a fiber optic cable needs a fiber optic MAU.
The transreceiver is a transmitter and a receiver. It transmits signal over the medium, and receives signals over the medium it detects collision.
A transreceiver can be external or internal. An external transreceiver is installed close to the media and is connected via AUI to the station. An internal transreceiver installed inside the station and doesn't need an AUI cable.



MDI:

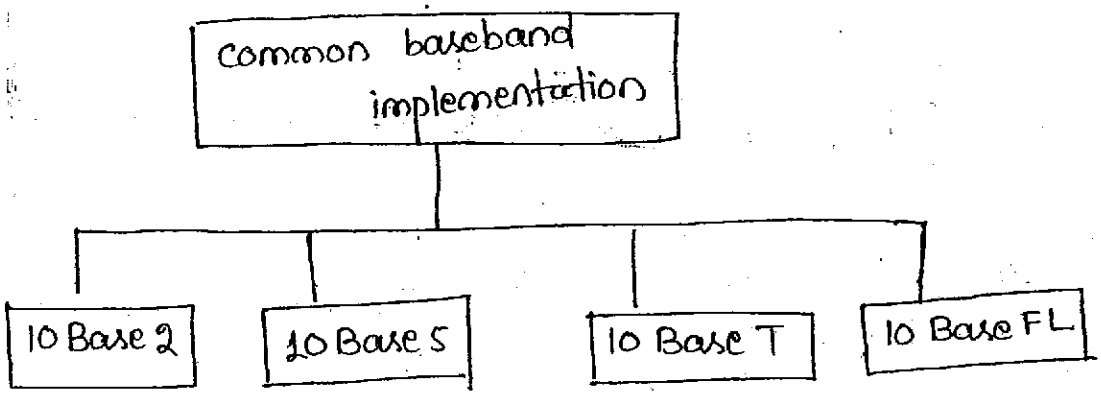
To connect the transciver (internal or external) to the medium we need a medium dependent interface (MDI). The MDI is just a piece of h/w for connecting a transceiver to the medium.

For external transceiver, it can be a tap or tee connector. For internal transceiver, it can be a jack.

physical Layer Implementation:-

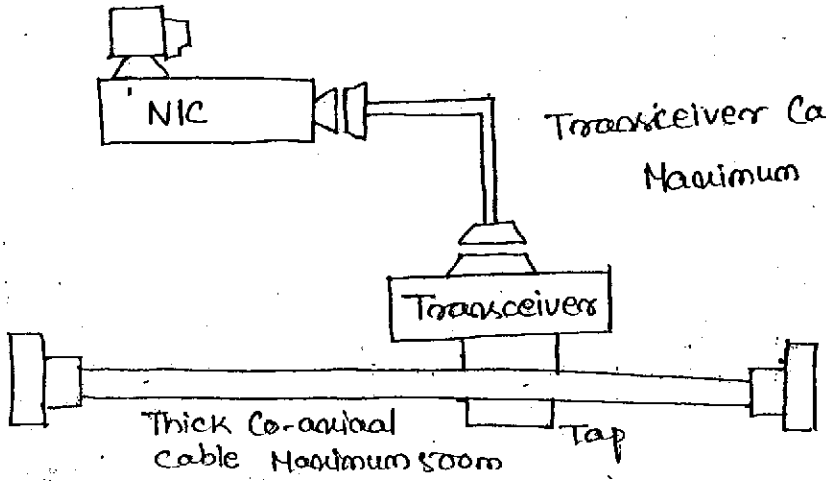
The standard defines four different implementions for baseband 10-Mbps ethernet.

Categories of traditional ethernet:-



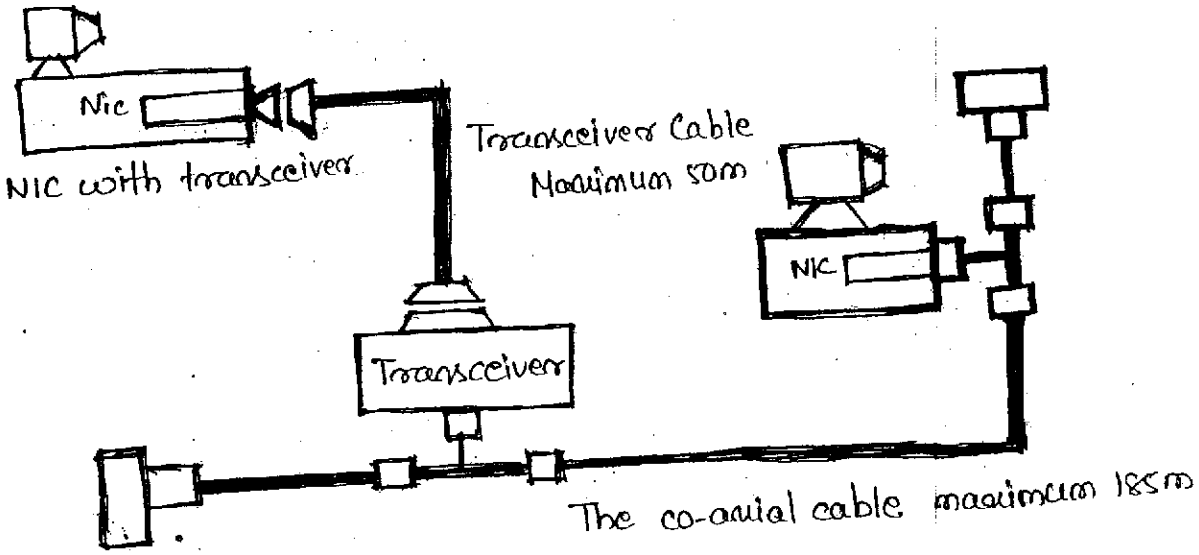
10-Base-5 (Thick Ethernet)

- The first implementation is called 10Base5, Thick ethernet or Thicknet.
- 10Base5 uses a bus topology with an external transceiver connected via a tap to a thick co-axial cable.



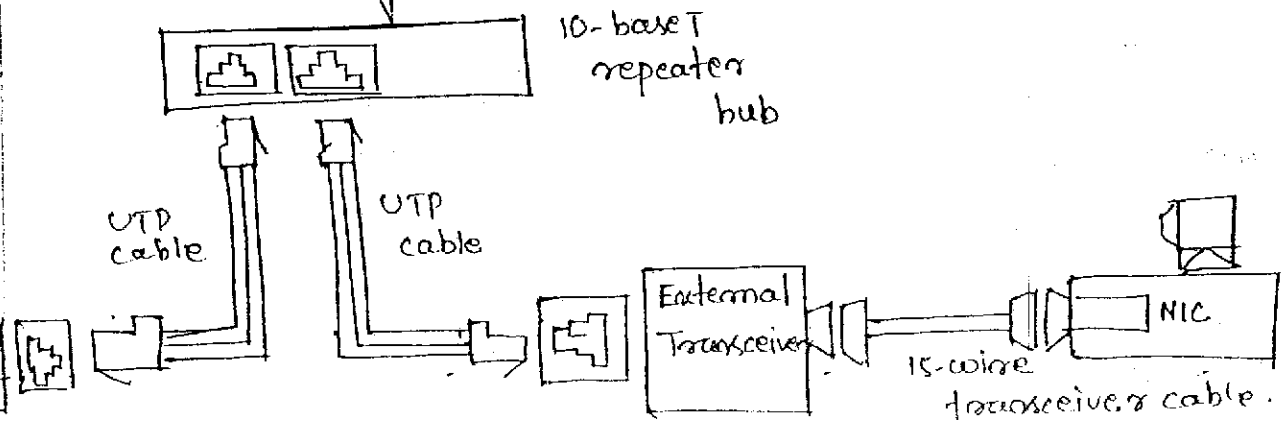
10Base-2 : Thin Ethernet :-

- The second implementation is 10Base2, thin ethernet or chipernet.
- 10 Base-2 uses a bus topology with an internal transceiver or point to point connection, with an external transceiver.
- If the station use internal transceiver, there is no need for an AUI cable doesn't
- If the station uses an internal transceiver, then external transceiver can be used in conjuction with the AUI.



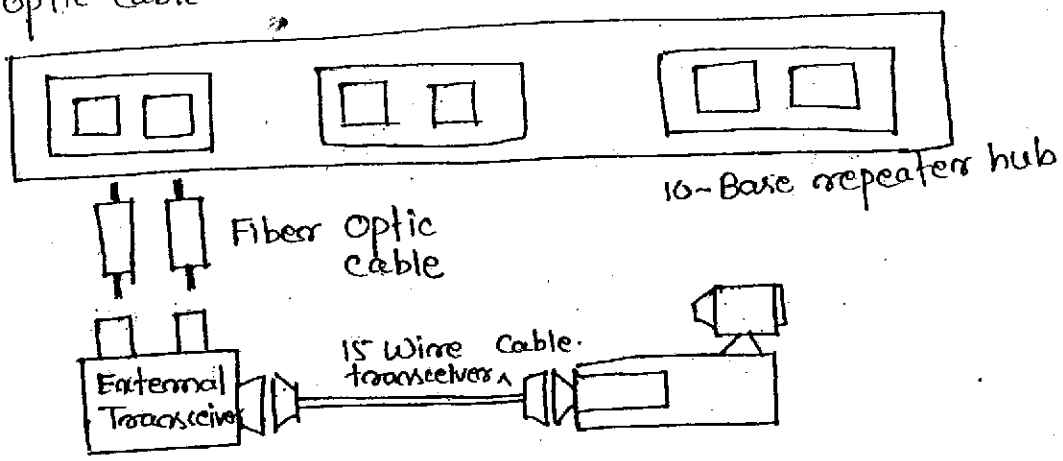
10 Base T : Twisted-Pair Ethernet :-

- Third implementaion is called 10-BaseT or twisted pair ethernet.
- It uses a physical star-topology.
- The stations are connected to the hub with an external transceiver or internal transceiver.
- When an internal transceiver is used, there is no need for an AUI cable, the interface card is directly connected ~~through~~ an AUI to the medium connector.
- When an external transceiver is used, the transceiver is connected through an AUI cable to the interface.



10BaseFL - Fiber Link Ethernet

- It uses a star topology.
- The standard is normally implemented using an external transceiver called fiber optic MAU.
- The station is connected to the external transceiver by an AUI cable.
- The transceiver is connected to the hub by using two pair of fiber optic cable.

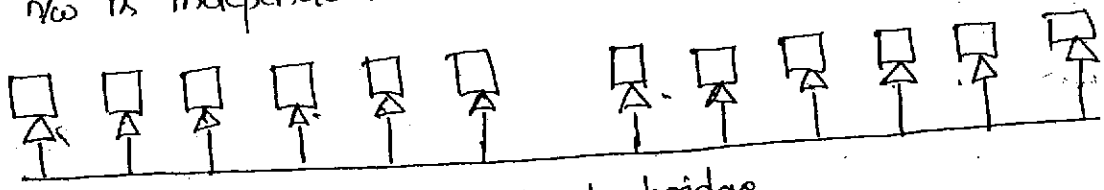


BRIDGED ETHERNET

- The first step in the ethernet evalution was the division of a LAN by bridges.
- Bridges have two effects on ethernet LAN
  - (i) Raise the Bandwidth
  - (ii) Separate collision domain.

Raising the Bandwidth:-

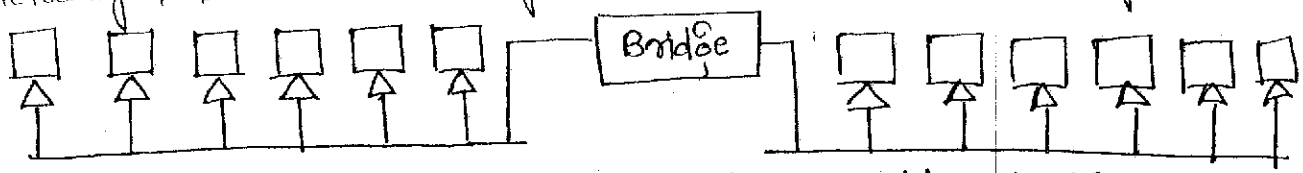
- Here the station share the bw of the n/w. If more than one station needs to use the n/w, the capacity is shared.
- If the datarate is 10Mbps. and there are two stations in the n/w then each will share a capacity of 5Mbps.
- A bridge devides a n/w into two or more n/ws where bw raise each n/w is independent.



without bridge

each station theoritically offered 10/12 Mbps

(Actually, because the bridge acts as a station in each segment).

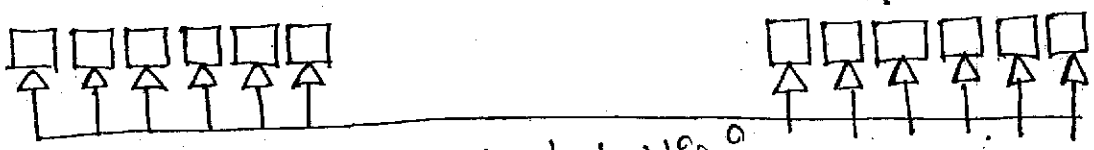


Each station theoritically offered 10/6 Mbps.

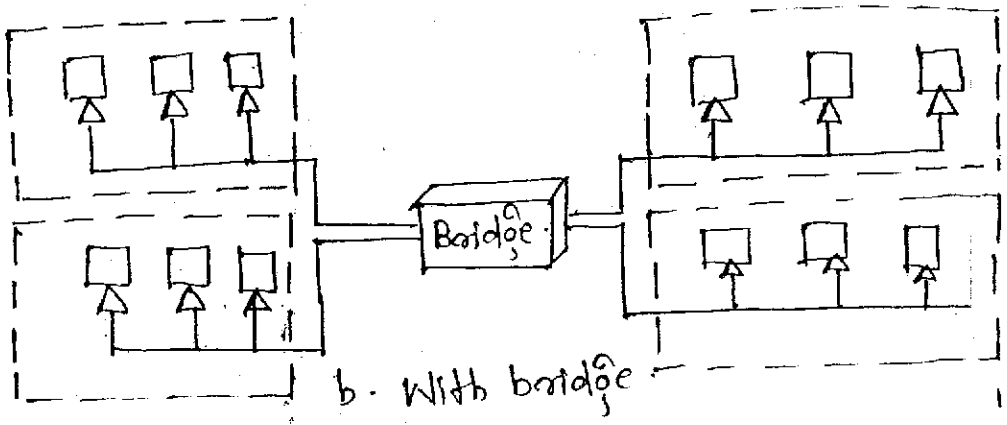
It is obvious that if we further divide the network, we can gain more bw for each segment. If we use a four-port bridge, each station is now offered 10/8 Mbps, which is 4 times more than a nonbridged network.

Separating Collision Domains:-

The collision domain becomes much smaller and the probability of collision is reduced tremendously. Without bridging 12 stations contend for access to the medium; with bridging only stations contend for access to the medium.



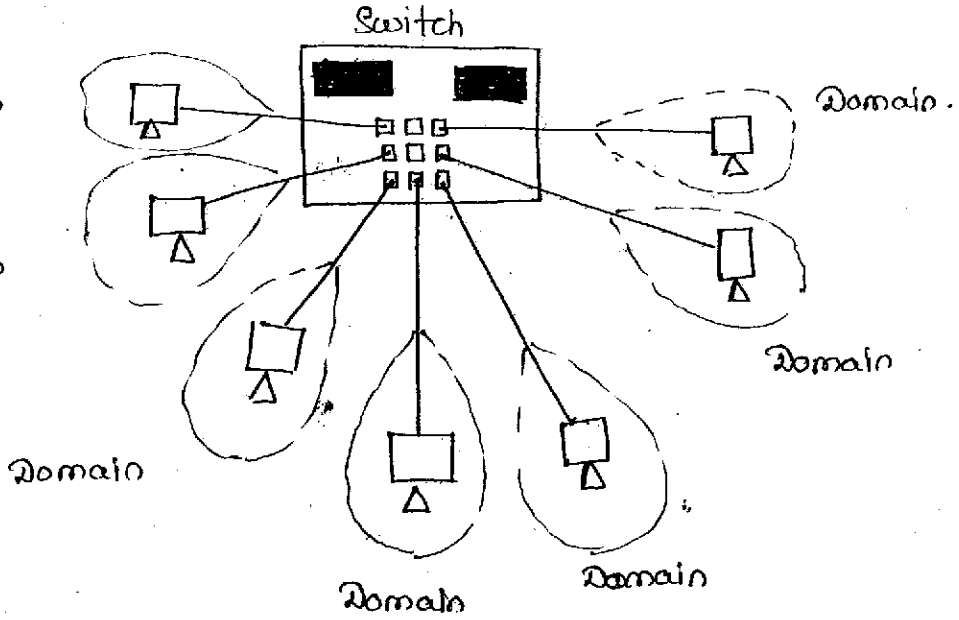
a. Without bridging



b. With bridge

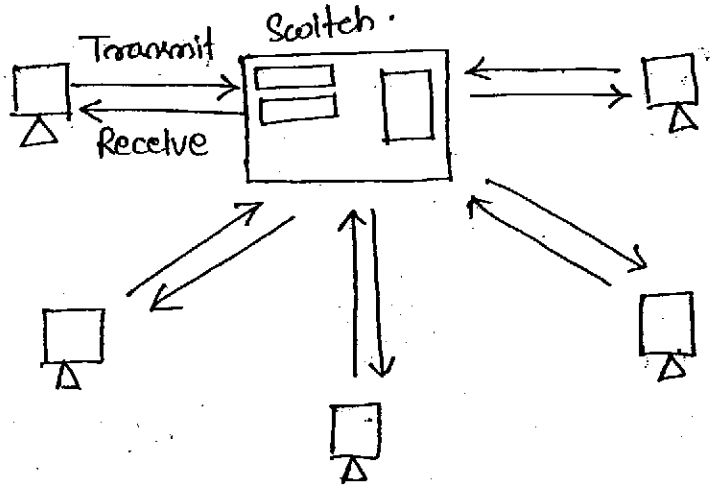
SWITCHED ETHERNET

- Uses a switched LAN instead of two to four networks, we have N networks, where N is the number of stations on the LAN.
- Here we have an N-port Switch.
- Here the bandwidth is only shared bet° the station and the bridge.
- A Layer 2 switch is an N-port bridge with additional sophistication that allows faster handling of the packets.



FULL DUPLEX ETERNET:

- One of the limitation of 10Base5 and 10Base2 is that communication is half duplex (a station can either send or receive) but not at the same time)
- Full duplex increases the capacity of each station from 10 to 20 Mbps.
- Instead of using one link between the station and the switch, the configuration uses two link one two transmit and one to receive.



Full duplex Switched Ethernet

Need for CSMA/CD:-

...ere each station is connected to the switch via two separate ...nks. Each station can send or receive without worrying ...bout collision. Each station or switch can ~~send~~ have a ...t-to-point dedicated path between the station and the ...itch. The job of MAC layer becomes much easier.

MAC:

Traditional Ethernet was designed as a connectionless protocol at the MAC sublayer. There is no explicit flow control and error control to inform the sender that the frame has arrived at the destination without error. When the receiver receives the frame it doesn't send any positive or negative acknowledgment.

To provide flow and Error control in full duplex switched Ethernet, a new sublayer called MAC control is added betn the LLC sublayer and MAC sublayer.

FAST ETHERNET

The need for a higher data rate resulted in the design of "Fast Ethernet" protocol (100 Mbps)

MAC Sublayer:-

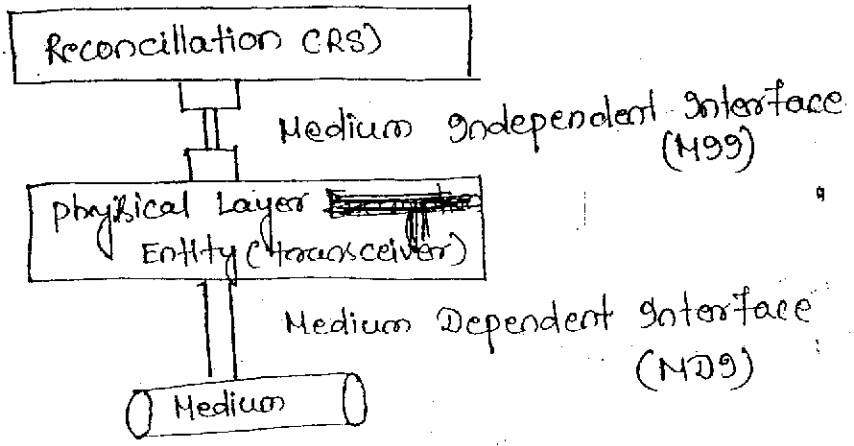
It remains untouched. The access method is CSMA/CD. It is backward compactible with traditional ethernet.

Autonegotiation:-

It allows a station or a hub a range of capabilities. It allows devices to negotiate the mode or data rate of operation. Its characteristics are:-

* To allow incompatible devices to connect one another.
* To allow one device to have multiple capabilities.
* To allow a station to check hubs capabilities.

physical layer:-



Reconcillation Sublayer:-

It replaces the PLS sublayer Encoding and decoding which were performed by PLS, are moved to the PHY sublayer (transceiver because encoding in fast-ethernet is medium dependent. RS is responsible for whatever is left over, specially passing of data to MII.

Medium Independent Interface:-

- It is an improved interface and is backward compatible with the AUI
- It features a parallel data path between "PHY" sublayer and "RS".
- Management functions are added.

PHY (TRANSCEIVER):-

The transceiver in fast ethernet is called PHY sublayer. It is responsible for encoding and decoding. A transceiver can be external or internal. An external transceiver is installed close to the medium and is connected via an MII cable. An internal transceive is installed inside the station (on the NIC card) and does not need an MII cable.

Medium Dependent Interface:-

MDI is just a piece of hardware that is implementation specific. To connect the transceiver (internally or externally) we need MDI.

PHYSICAL LAYER IMPLEMENTATION:-

100-Base TX:-

It uses two pairs of twisted-pair cable (either category 5 UTP or STP) in a star topology. It allows either an external transceiver (with an MII cable) or an internal transceiver.

100-BASE-FX

It uses two pair of fiber optic cables in star topology; it allows either an external transceiver (with an MII cable) or an internal transceiver.

100-Base-T4

It use fourer pairs of UTP for transmitting 100 Mbps and

and uses category 3 or higher UTP.

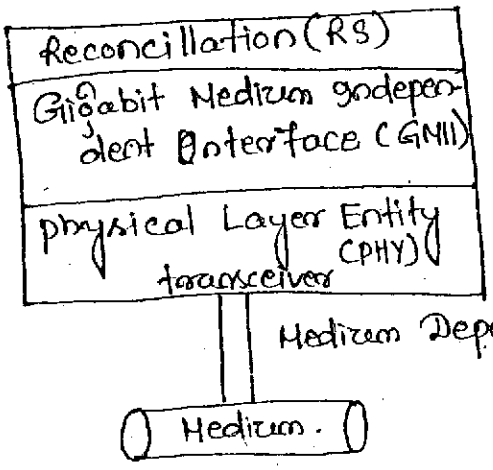
GIGABIT ETHERNET

Recent need for even higher data rate 1000 Mbps resulted in the of Gigabit Ethernet Protocol.

MAC Sublayer:-

It remain unstouched, its access method is CSMA/CD. Almost all implementation of Gigabit Ethernet follow full-duplex approach.

physical Layer:-



Reconcillation

The RS sublayer sends 8-bit parallel data to the PHY sublayer via GMII interface

Gigabit Medium independent (GMII) →

It is a specification that defines how the reconcillation sublayer is to be connected to the PHY sublayer (transceiver) its features are:-

- It can operate at 10, 100, and 1000 Mbps.
- It specifies a parallel data path (8 bit at a time) between RS sublayer and transceiver.
- Management function are included.
- No GMII cable and no GMII connector.

WIRELESS LANs

Wireless LAN is the fastest growing technology, found on college campuses, office buildings and public areas.

IEEE 802.11

IEEE has defined the specification for a wireless LAN, called IEEE.802.11, which covers the physical and datalink layers.

Architecture

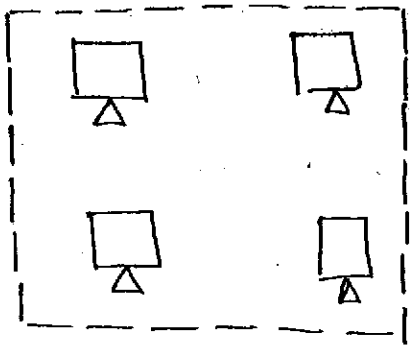
Standard defines two kinds of services

(i) Basic service set (BSS)

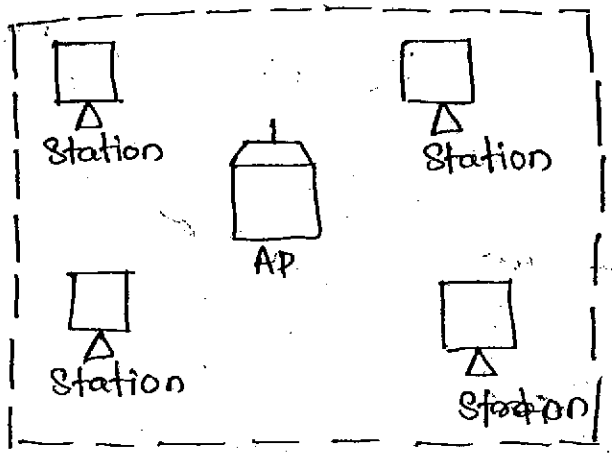
(ii) Extended Service Set (ESS).

Basic Service Set:-

- IEEE 802.11 defines the BSS as the building block of a wireless LAN.
- A basic service set is made of stationary or mobile ~~service~~ wireless stations and a possible central base station known as the access point (AP).
- A BSS without AP is a stand-alone n/w and cannot send data to other BSS. It is called an adhoc network.
- In this ~~station~~ architecture, station can form a n/w without the need of an AP, they can locate each other agree to be a part BSS.

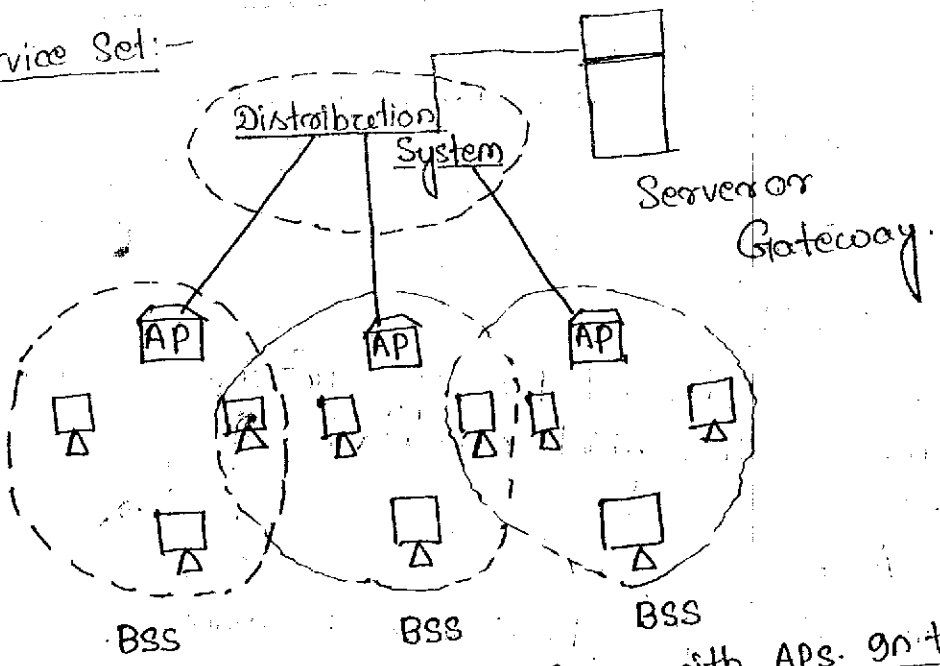


BSS without AP.



BSS with AP

Extended Service Set:-



- An ESS is made up of two or more BSSs with APs. In this case the BSS are connected through a distribution system, which is usually a wired LAN.
- The distributed system connects the APs in the BSSs.
- ESS uses two types of station
  i) mobile ii) stationary
- Mobile stations are normal stations inside a BSS. The stations are AP stations that are part of a wired LAN.
- When BSSs are connected, we have what is called an Infrastructure network, on this n/w the stations within reach of one another can communicate the use of an APs.

Station Types:-

IEEE 802.11 defines 3 types of stations based on their mobility in a wireless LAN.

(i) No Transition Mobility:- A station with no transition mobility is either stationary only moving only inside a BSS.

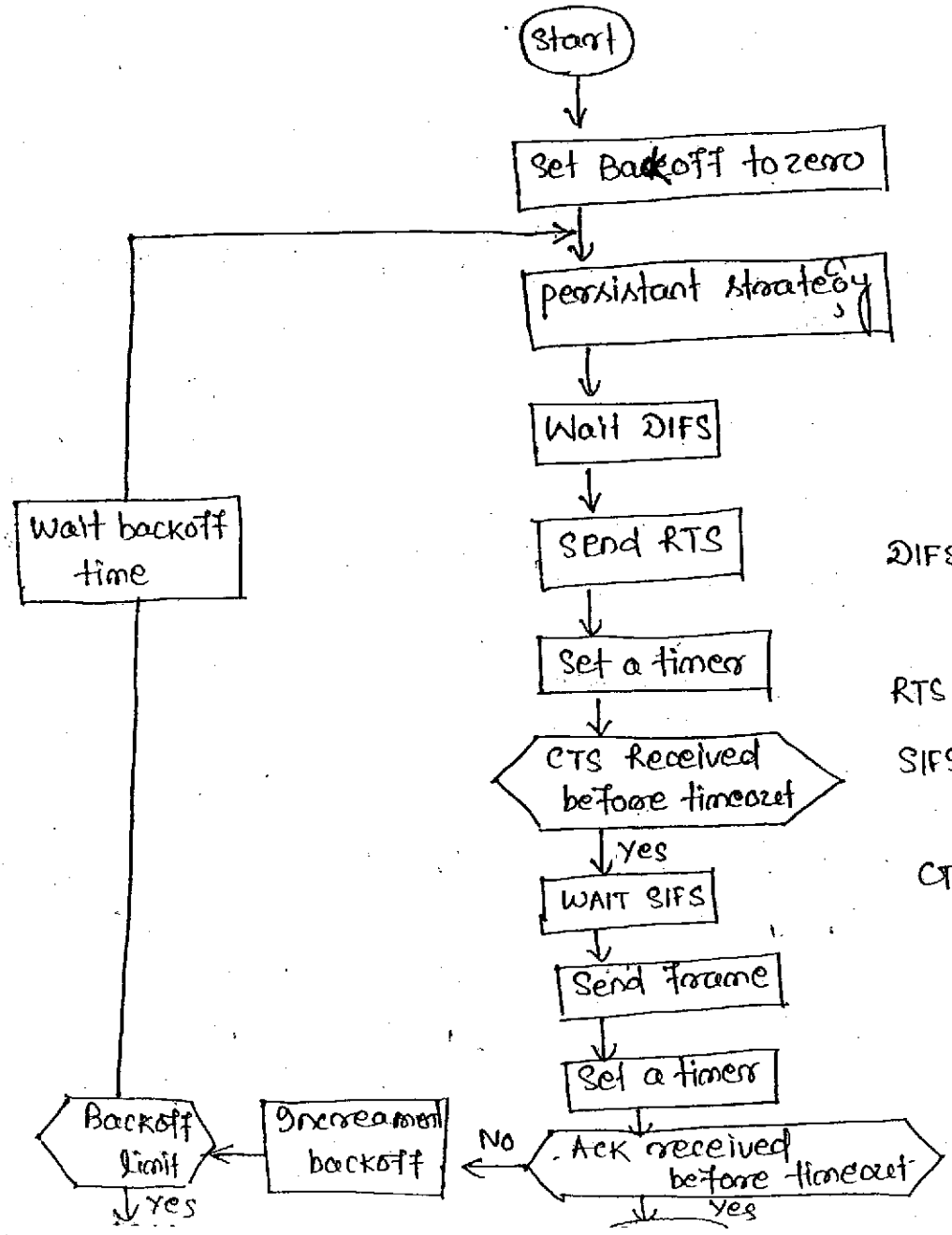
(ii) BSS Transition Mobility:- A station with BSS-transition mobility can move from one BSS to another but the movement is confined inside one ESS.

(iii) ESS Transition Mobility:- A station with ESS-transition mobility can move from one ESS to another.

CSMA/CA

Wireless LAN can't implement CSMA/CD for three reasons.

- Collision detection implies that the station must be able to send data and receive collision signal at the same time. This implies costlier station and increase bw.
- Collision may not be detected because of hidden terminal problems. A terminal may be hidden from another in wireless environment (due to natural abstaction). This doesn't happen in wired LAN because all stations are connected by wire.
- The distance between stations in w-LAN can be great. Signal fading could prevent a station at one end from hearing collision at other end



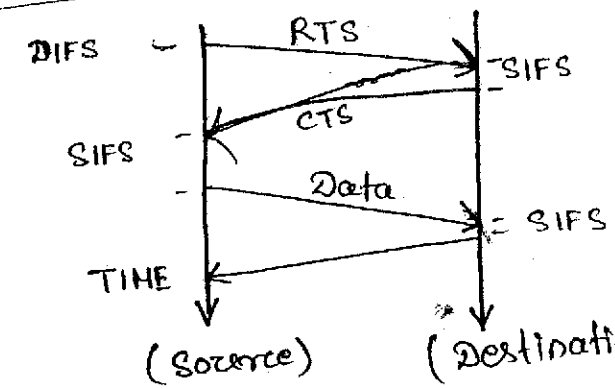
DIFS: Distributed interframe space

RTS: Request to Send

SIFS: Short interframe space

CTS: Clear to Send

Frame Exchange Time Line:-



- Before sending a frame, the source station senses the medium by checking the energy level at the carrier frequency.
  - The channel uses a persistent strategy with backoff until the channel is idle.
  - After the channel is found idle, the station waits for a period of time called DIFS, then station sends a control frame called RTS.
- After receiving RTS and waiting for a short period of time called SIFS, the destination station sends a control frame indicating that that the destination station is ready to receive data.
- The source station sends data after waiting an amount of time equal to SIFS.
- The destination station, after waiting for an amount of time equal to SIFS sends an ACK, to show that frame has been received.

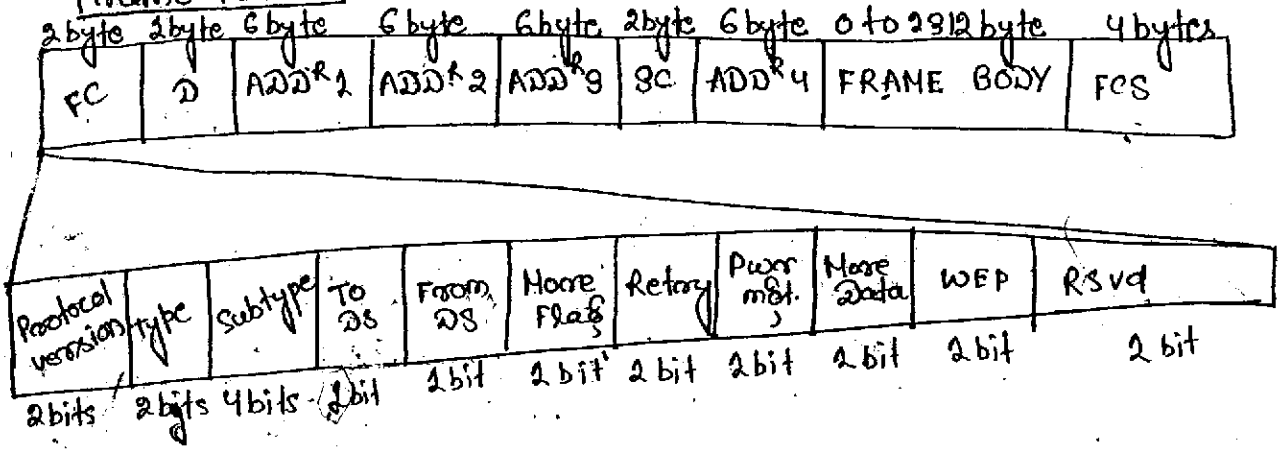
Network Allocation Vector

When a station sends an RTS frame, it includes the duration of the time that it needs to occupy the channel. The station that are affected by this transmission create a timer called "NAV" (Network Allocation Vector) that shows how much time must pass before these station are allowed to check the channel for idleness. Each time a station access the system and sends RTS frame, other station starts their NAV.

COLLISION DURING HANDSHAKING :

Two or more stations may try to send RTS frames at the same time. These control frames may collide. However, because there is no mechanism for collision detection, the sender assumes that there has been a collision if it has not received a CTS frame from the receiver. The backoff strategy is employed and the sender tries again.

Frame Format :-



Frame Control :-

FC field is 2 byte long and defines the type of frame and some control information

- protocol version → Current version is 0.
- Type → Management (0,0), Control (01), Data (10).
- More flag → When set to 1, means more fragments.
- Retry :→ When set to 1, means retransmitted frame.
- Pwr mgt :→ When set to 1 means station is in power mgt mode.
- More data → When set to 1, means station has more data to send.
- WEP → (Wired equivalent privacy). When set to 1 means encryption
- RSVd → Reserved.

D:-
This fields defines the duration of transmission that is used to set value of NAV. It defines ID of the frame.

ADDRESS:-
The meaning of each address field depends upon the value of the "TODS" and "FROM DS".

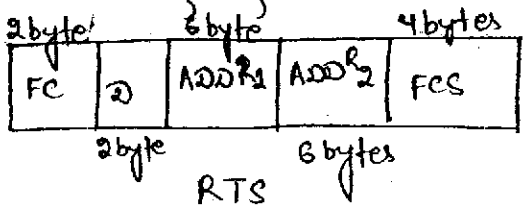
Sequence Control:-
It defines the sequence no. of the frame to be used in flow control.

FCS:-
CRC error detection

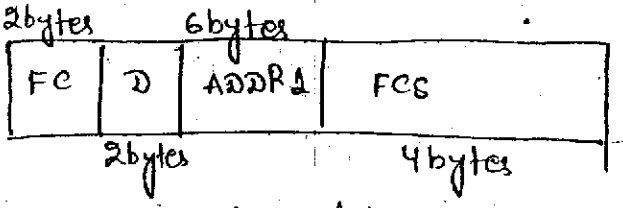
Frame types:-
Three categories of frames.

1. Management frame:- It is used for initial communication between stations and access point.

2. Control frame:- It is used for accessing the channel and acknowledging frame



RTS



CTS or Ack

1011 → RTS
1100 → CTS
1101 → Ack

3. Data Frame:- It is used for carrying data and control information.

To	From	ADDR1	ADDR2	ADDR3	ADDR4
0	0 → Dest. Station	Source St.	BSSID	N/A	
0	1 → "	Sending AP	Source St.	N/A	
1	0 → Receiving AP	Source St.	Dest. St.	N/A	
1	1 → "	Sending AP	Dest. St.	Source Destination	

BLUETOOTH

Bluetooth is a wireless LAN technology designed to connect devices of different function such as telephones, computers. A Bluetooth LAN is an adhoc network, which means that the n/w is formed spontaneously, the devices sometimes called gadgets, find each other and make a n/w called "piconet.

Architecture:-

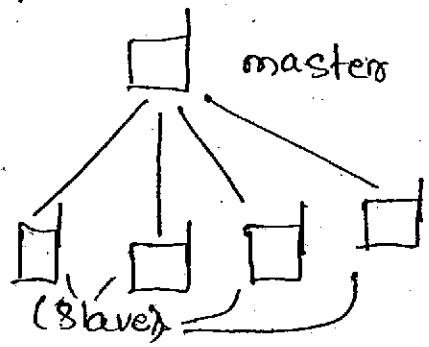
Bluetooth defines two types of n/w

(i) Piconet

(ii) Scatternet.

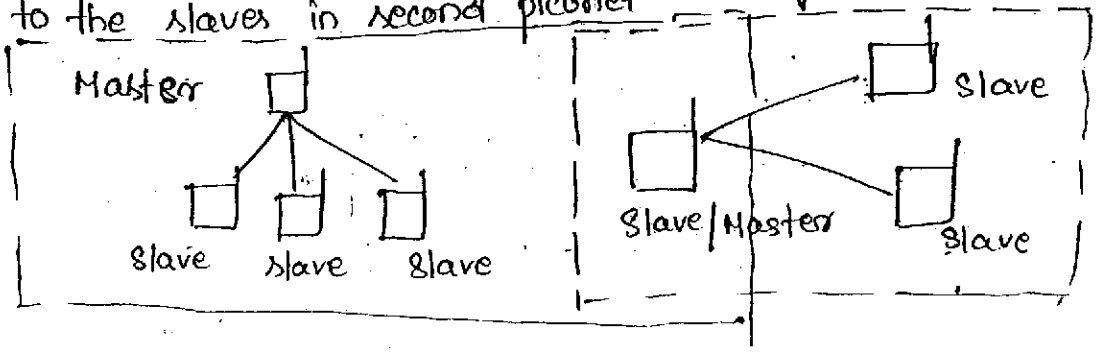
PICONET:-

Piconet otherwise called smallnet. A piconet can have upto 8 stations, one of which is called master and the rest are called slaves. All slave stations syncronizes their clocks and hopping sequence with the master slaves. The communication bet^n master and slave is one-to-one or one-to-many.

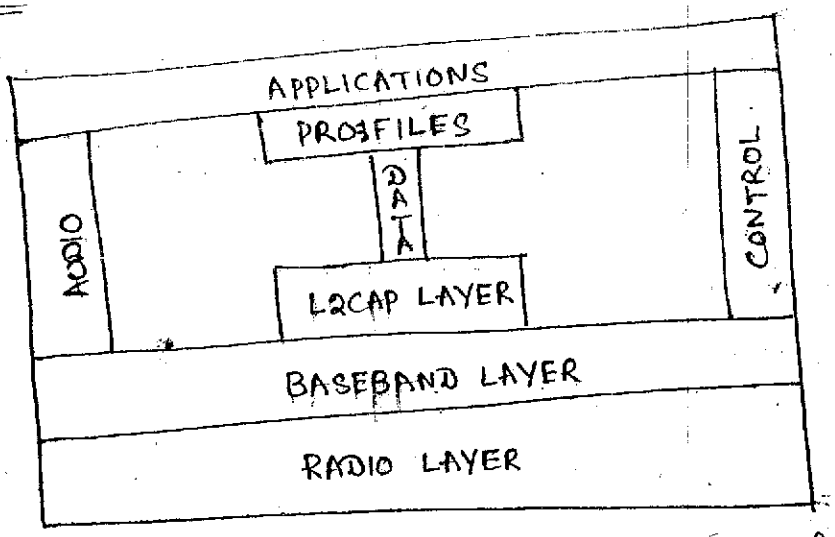


SCATTERNET

Piconets can be combined to form what is called scatternet. A slave station in one piconet can become the master of another piconet. This station can receive messages from the master (in the first piconet) and acting as a master delver it to the slaves in second piconet.



Bluetooth Layers:-

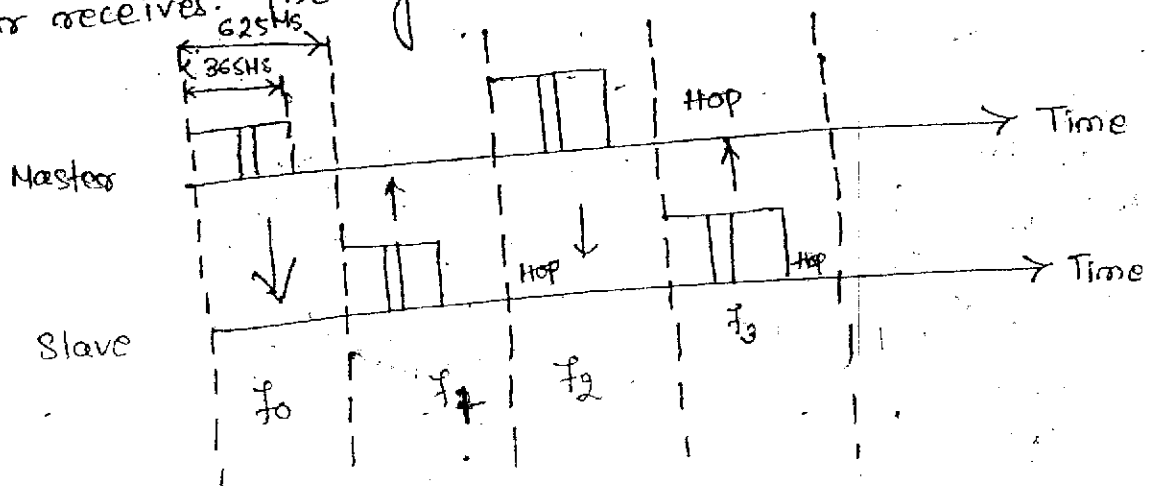


Radio Layer:-
It is roughly equivalent to the physical layer of the internet model. Bluetooth devices are low power and have a range of 10m.

Baseband Layer:-
It is roughly equivalent to the MAC (medium access control) sublayer in LANs. The access method is TDMA. The master and slave communicate with each other using time slots. This means that during the the time that are frequently is used, a sender sends a frame to a slave or a slave sends a frame to the master.

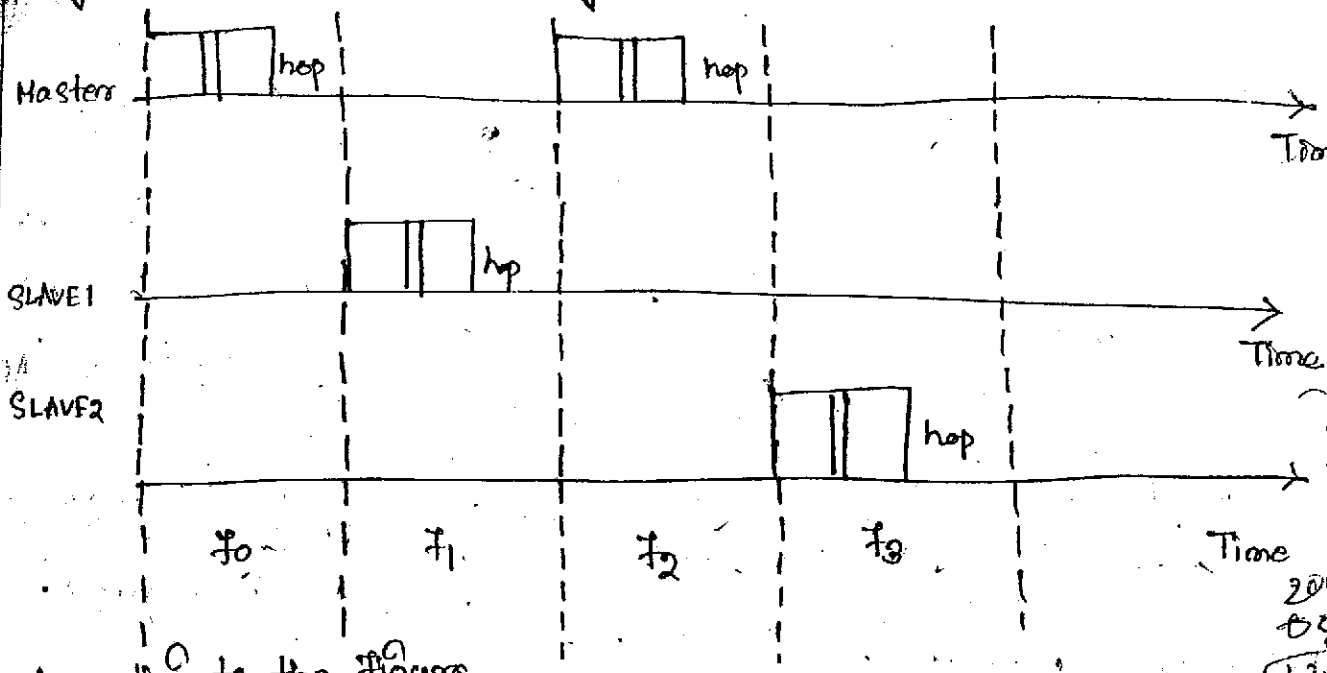
Single Slave Communication

If the piconet has only one slave, the TDMA operation is very simple. The time is divided into slots of 625 MS. The master uses even-numbered slots (0, 2, 4 ....) and slaves uses odd-numbered slots (1, 3, 5 ....) In slot 0, the master sends and the slave receives; in slot-2 the slave sends and the master receives. The cycle is repeated.



Multiple Slave Communication:-

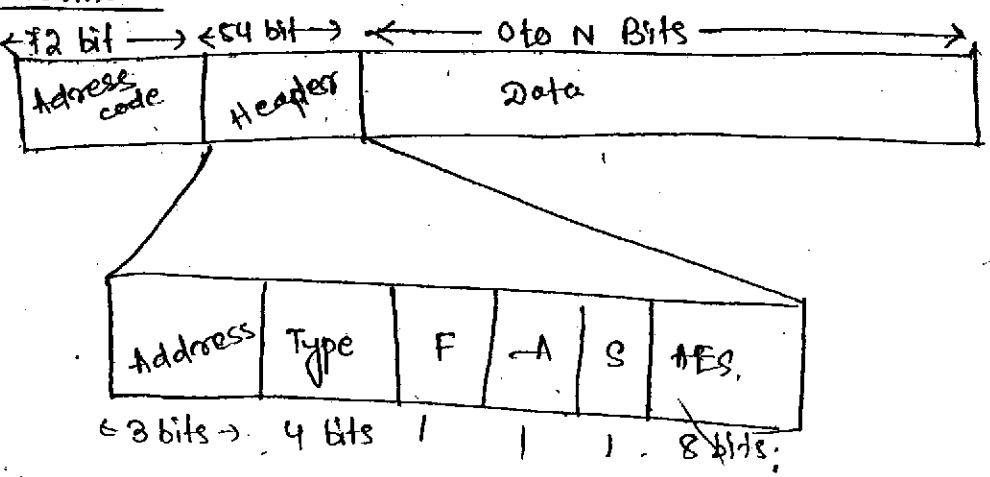
The process is a little more complex if there is more than one slave in the piconet. All slaves listen on even-numbered slots, but only one slave sends in any odd-numbered slot



According to the figure

2. On slot 0, the master sends a frame for slave 1.
2. On slot 1, slave 1 sends a frame to the master because the previous frame was addressed to slave 1; other slaves are silent.
3. On slot 2, the master sends for slave 2.
4. On slot 3, only slave 2 sends a frame to the master because the previous frame was addressed to slave 2; other slaves are silent.
5. The cycle continues.

Frame Format



Access Code:- It contains synchronization bits and the identifier of the to distinguish the frame from one piconet to another.

Header: 54 bit field is a repeated 18 bit pattern

Address:- It defines upto seven slaves (1 to 7). If address is zero, it is used for broadcast communication from master to all slaves.

Type:- It defines the type of data coming from upper layer.

F:- Used for flowchart. When set to (1) it indicates that is device is unable to receive more frames.

S:- Holds sequence number. Uses stop. wait. 2 bits is for ack

A: Ack

HEC:- Error correction uses checksum to detect errors.

Data:- It contains data as content coming from upper layers.

(15)

CLIENT SERVER MODEL

The purpose of a n/w is to provide services to users. A computer runs a program either to request a service from another computer or to provide service to another computer. This means that two computers connected by an Internet, must each run a program, one to provide a service and the other to request a service. In Internet, the application programs are entities that communicate with each other, not computers or users.

CLIENT: A client is a program running on the local machine requesting a service from the server. A client program is started by the user and terminates when the service is complete. A client opens the communication channel using the IP address of the remote host and well-known port address of the specific server program running on that machine. This is called active open. After a channel of communication is opened the client sends its request and receives a response. The whole process is finite and eventually comes to an end. At that moment, the client closes the communication channel with an active close.

SERVER: A server is a program running on the remote machine and providing service to the clients. When it starts, it opens the door for incoming requests from clients, but it never initiates a service until it is requested to do so. This is called a "passive open".

A server program is an infinite program. When it starts, it runs infinitely unless problem arises. It waits for incoming requests from clients. When a request arrives, it responds to the request, either iteratively or concurrently.

CONCURRENCY

Both clients and servers can run in concurrent mode.

CONCURRENCY IN CLIENTS ⟹

clients can run on machine either iteratively or concurrently. Running clients iteratively means running them one by one i.e. one client must start, run and terminate before the machine can start another client.

But, now-a-days we allow concurrent clients i.e. two or more clients can run at same time.

CONCURRENCY IN SERVERS ⟹

An iterative server can process only one request at a time i.e. it receives a request processes it and sends the response to the request before it handles another request.

A concurrent server can process many requests at the same time and thus can share its time between many requests.

Servers can use either UDP (Universal datagram protocol) a connectionless transport layer protocol or TCP (Transmission Control protocol) a connection-oriented protocol.

4 types of servers are there :-

* Connectionless iterative
* Connectionless concurrent
* Connection oriented iterative
* Connection oriented concurrent

Connectionless Iterative server ⇒ The servers that use UDP are normally iterative which means that the server processes one request at a time. Here, the server uses one single port for this purpose, the well known port. All the packets arriving at this port wait in line to be served.

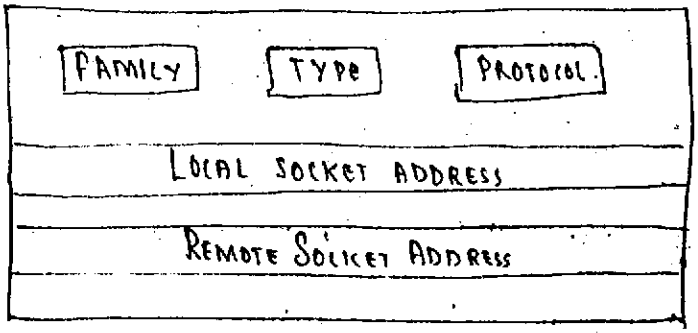
Connection Oriented Concurrent Server ⇒ The servers that use TCP are normally concurrent. This means that the server can serve many clients at the same time. A connection is established between the server and each client and this connection remains open until the entire stream is processed and the connection is terminated.

Socket Interface.

Sockets ⇒

The communication structure that we need in socket programming is a socket. A socket acts as an endpoint. Two processes need a socket at each end to communicate with each other.

A socket is defined in the operating system as a structure.



(Socket Structure)

* Family :- It defines the protocol group i.e. IPv6, IPv4, Unix protocols.
* Type :- It defines the type of socket :-
  - Stream socket
  - Packet socket
  - Raw socket.

* PROTOCOL :- This field is usually set to zero for TCP & UDP.

* LOCAL SOCKET ADDRESS :- It defines a combination of the local IP address and port address of the local application program.

* REMOTE SOCKET ADDRESS :- It defines a combination of remote IP address and port address of the remote application program.

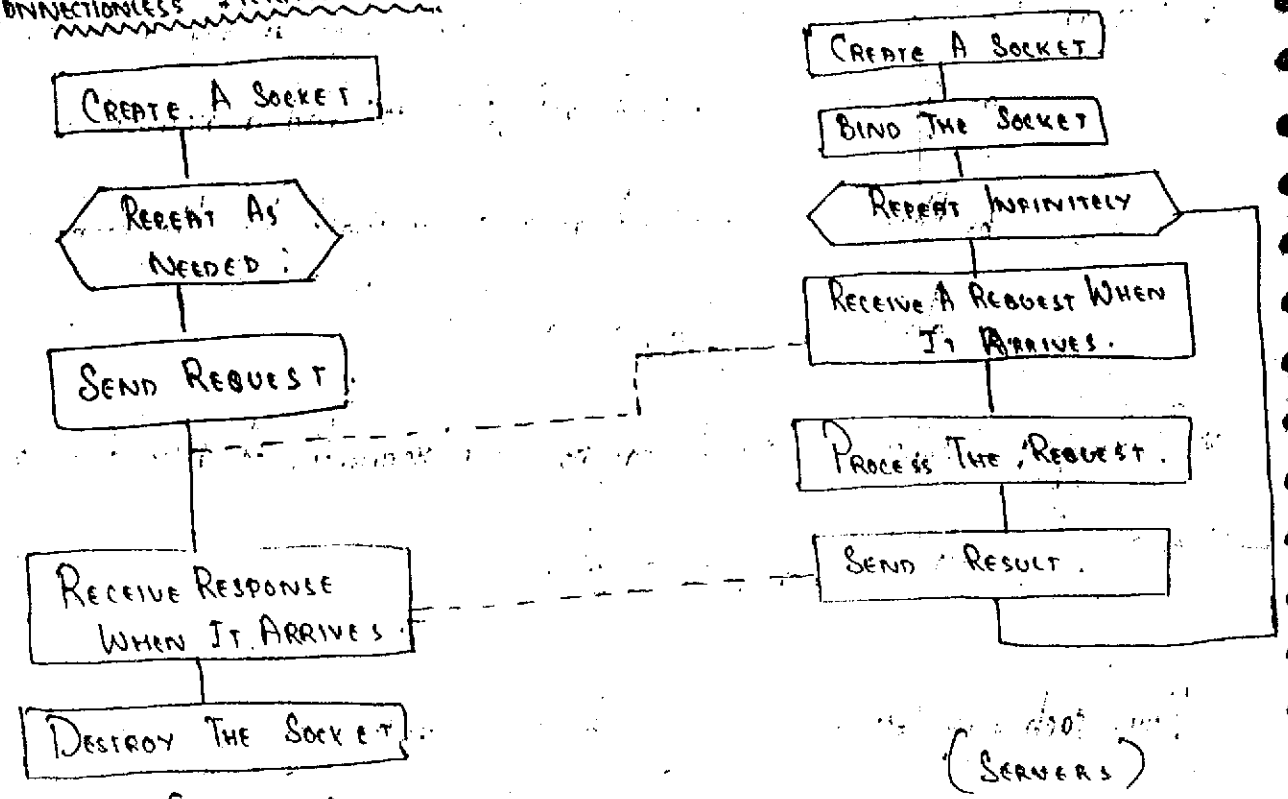
SOCKET TYPES.

* STREAM SOCKET :- It is designed to be used with a connection oriented protocol such as TCP. TCP uses a pair of stream sockets to connect one application program to another across the Internet.

* DATAGRAM SOCKET :- It is designed to be used with a connectionless protocol such as UDP. UDP uses a pair of datagram sockets to send a message from one application program to another across the Internet.

* RAW SOCKET :- Some protocols that use the services of IP and use neither stream sockets nor datagram sockets.

CONNECTIONLESS ITERATIVE SERVER.



SERVER ~~>

* Create a socket :- The server asks the operating system to create a socket.

* Bind :- The server asks the operating system to enter information in the socket related to the server. This is called binding the server socket.

* Repeat :- The server repeats the following steps infinitely :-

  a) Receive a request :- The server asks the operating system to wait for a request destined for this socket and to receive it.

  b) Process :- The request is processed by the server.

  c) Send :- The response is sent to the client.

CLIENT ~~>

* Create a socket :- The client asks the OS to create a socket. Here, no binding is done since the OS fills the information in the socket normally.

* Repeat :- The client repeats the following steps as long as it has requests :-

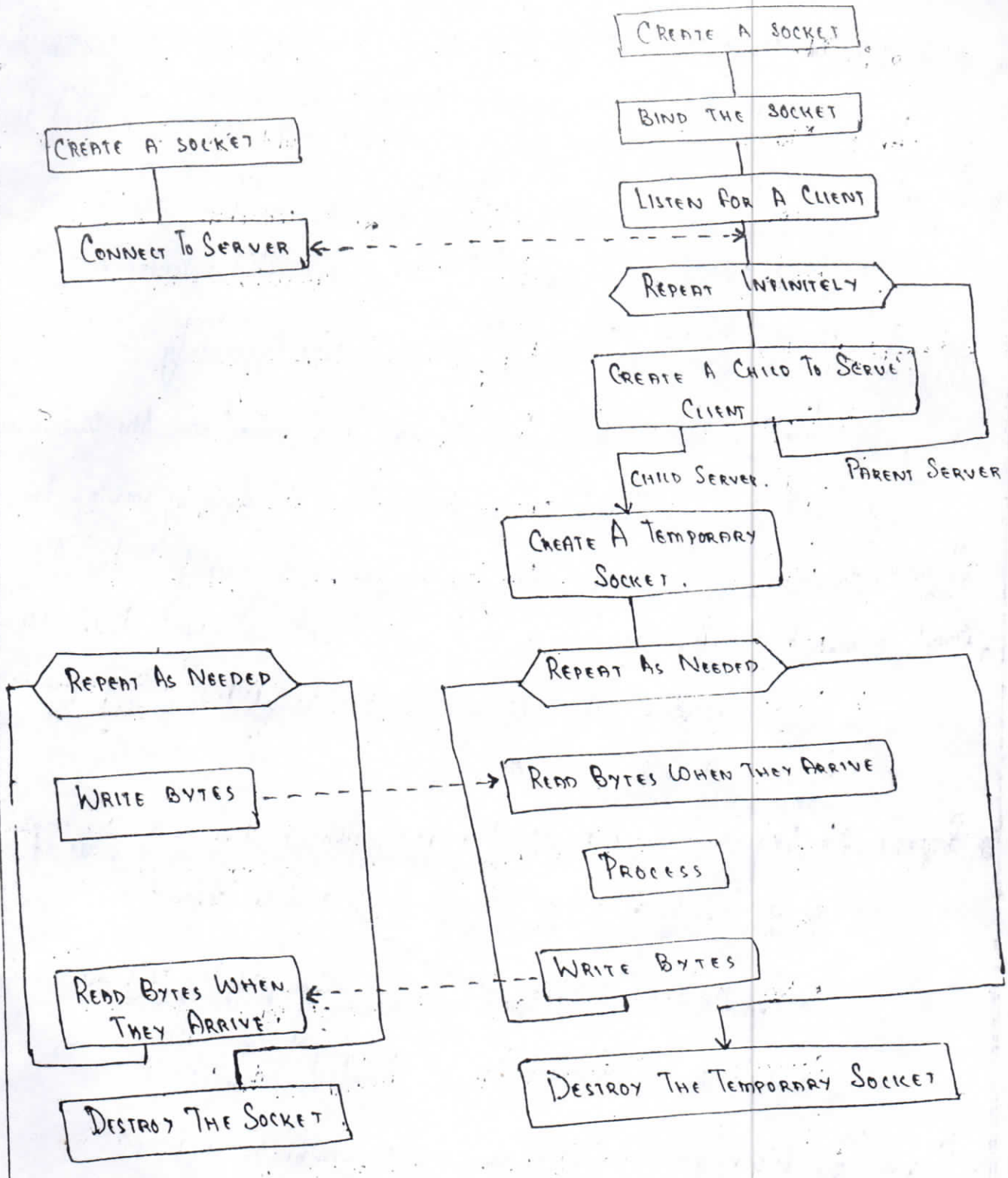
  a) Send :- The client asks OS to send a request.

  b) Receive :- The client asks OS to wait for the response and deliver it when it has arrived.

* Destroy :- When the client has no more requests, it asks the OS to destroy the socket.

Here, each server serves many clients but handles one request at a time.

CONNECTION - ORIENTED CONCURRENT SERVER



SERVER ~~~>

* Create a Socket :- The server asks OS to create a socket.

* Bind :- The server asks the OS to enter information in the socket created.

* Listen :- The server asks the OS to be passive and listen to the client that needs to be connected to this server. A connection needs to be made for data transfer (TCP — connection oriented).

* Repeat :- The server repeats the following steps infinitely :-

a) Create a child :- When a child requests a connection, the OS creates a temporary child process and assigns the duty of serving the client to the child. The parent process is free to listen for new clients.

b) Create a new socket :- A new socket is created to be used by the child process.

c) Repeating :- The child repeats the following steps as long as it has requests from the client :-

- Read :- The child reads a stream of bytes from the connection. (TCP is a byte-oriented protocol).
- Process :- The child processess the stream of bytes.
- Write :- The child writes the results as a stream of bytes to the connection.

d) Destroy Socket :- After the client has been served, the child process asks the OS to destroy the temporary socket.

CLIENT ⟹.

* Create a Socket :- The client asks the OS to create a socket.
* Connect :- The client asks the OS to make a connection.
* Repeat :- The client repeats the following steps as long as it has data to send.
  a) Read :- The client receives a stream of bytes from the server.
  b) Write :- The client sends a stream of bytes to be sent to the server.
* Destroy :- After the client has finished, it asks OS to destroy the socket. The connection is also closed.

DOMAIN NAME SYSTEM. (CH-25).

To be unambiguous, the names assigned to machines must be carefully selected from a name space with complete control over the binding between the names and IP addresses. The names must be unique because the addresses are unique.

FLAT NAME SPACE ⟹.

In flat name space, a name is assigned to an address. A name in this space is a sequence of characters without structure. The names may or may not have a common section and if they do it has no meaning. The main disadvantage of this is that it cannot be used in large system such as Internet because it must be centrally controlled to avoid duplication.

HIERARCHIAL NAME SPACE ⟹.

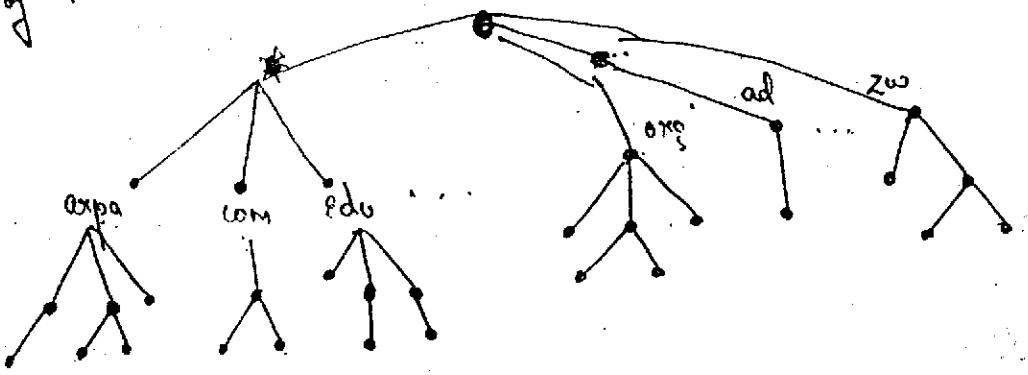
In hierarchial name space, each name is made up of several parts. The first part can define the nature of the organisation, the second part can define the name. the third part defines the departments and so on. A central authority can assign the part of the name that defines the nature of the organisation.

Domain Name Space

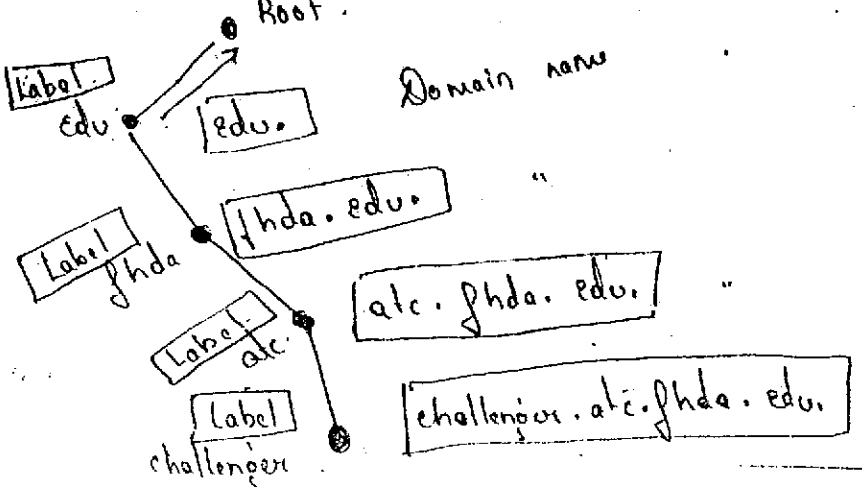
To match domain name with IP addr

In this design, the names are defined in an inverted-tree structure with the root at the top. The tree can have only 128 levels; level 0 (root) to level 127.

Label :-
Each node in the tree has a label which is a string with a maximum of 63 characters. The root label is a null string (empty string). DNS requires that children of a node have different labels which guarantees the uniqueness of the domain names.



Domain Name :-
A full domain name is a sequence of labels separated by dots (.). The domain names are always read from the node up to the root. The last label is the label of the root (null). This means that a full domain name always ends in a null label, which means the last character is a dot because the null string is nothing.



FULLY QUALIFIED DOMAIN NAME (FQDN) ⟹

If a label is terminated by a null string, it is called FQDN. An FQDN is a domain name that contains the full name of a host. It contains all labels, from the most specific to the most general, that uniquely defines the name of the host.

Eg: challenger.atc.fhda.edu.

PARTIALLY QUALIFIED DOMAIN NAME (PQDN) ⟹

A PQDN starts from a node, but it does not reach the root. It is used when the name to be resolved belongs to the same site as the client. Here, the resolver can supply the missing part called suffix to create an FQDN.

Eg: If a user at fhda.edu. site wants to get the IP address of the challenger computer, he or she can define the partial name.

challenger.

DOMAIN

A domain is a subtree of the domain name space. The name of the domain is the domain name of the node at the top of the subtree. Domain may itself be divided into domains, or subdomains.

DNS IN THE INTERNET

DNS is a protocol that can be used in different platforms. DNS is divided into three sections:-

a) Generic Domains.

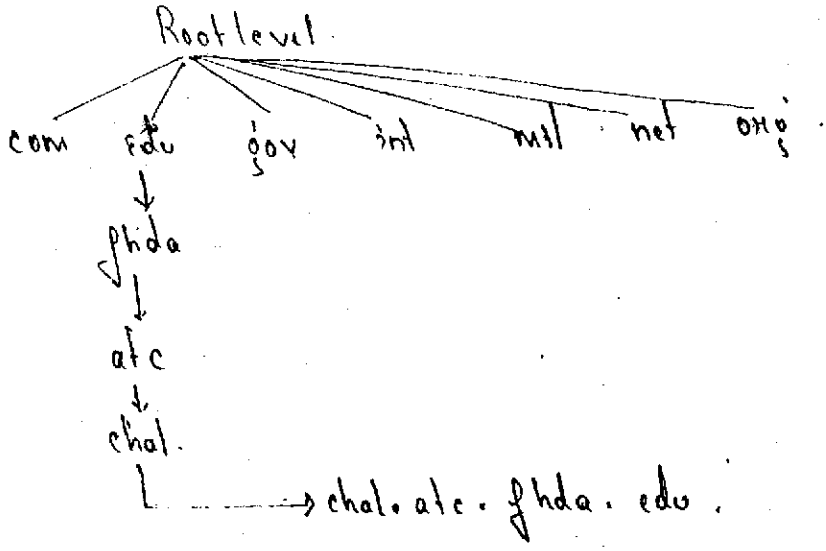
b) Country Domains.

c) Inverse Domains.

P.T.O.

Generic Domains

The generic domains defines registered hosts according to their generic behaviour. Each node in the tree defines a domain, which is an index to the domain name space database.



Generic Domain Labels

com → Commercial organisations.

edu → Educational institutions.

gov → Government institutions.

int → International organizations.

mil → Military groups.

net → Network support centers.

org → Non profit organisations.

New Generic Domain Labels.

aero → Airlines & aerospace companies.

biz → Bussiness or firms.

coop → Cooperative

info → Information service providers.

Museum → Museums.

name → Personal name.

pro → professional individuals.

Country Domains

The country domain section follows the same format as the generic domains but uses two character country abbreviations (Eg: ind for India)

Suppose balasore in India : bls.ind.
Orissa : bls.ors.ind.
Suppose Balasore College of Engg and Tech in bls in India :

(beet.bls.ors.ind.).

Inverse Domains

The inverse domains is used to map an address to a name. The server has a file that contains a list of authorized clients, the server lists only the IP address of the client (extracted from the received IP packet). To determine if the client is on the authorized list, the server can send a query to the inverse DNS server and ask for a mapping of address to name.

DNS Messages

DNS has two types of messages :-

* Query messages consists of a header and the question records.
* Response messages consists of header, question records, answer records, authoritative records and additional records.

Header

Both query and response messages have the same header format with fields set to zero for query messages.

i) Identification is used by the client to match the response with the query. The client uses a different identification number each time it sends a query. The server duplicates this number in the corresponding response.

ii) Flags is a collection of subfields that define the type of messages, the type of answers requested, the type of desired resolution (i.e. recursive or iterative).

iii) No. of question records contains the number of queries in the question section of the messages.

iv) No. of answer records contains the number of answer records in the answer section of the response messages. Its value is zero in the query messages.

v) No. of authoritative records contains the number of authoritative records in the authoritative section of a response messages. Its value is zero in the query messages.

vi) No. of additional records contains the number of additional records in the additional section of a response messages. Its value is zero in the query messages.

Question Section :-

It consists of one or more question records. It is present on both query and response messages.

Answer Section :-

This is a section consisting of one or more resource records. It is present only on response messages. It includes answer from server to client.

Authoritative Section :

This is a section consisting of one or more resource records. It is present only on resp messages. This section gives information (domain name) about one or more authoritative servers for the query.

Additional Information Section :

This is a section consisting of one or more resource records. It is present only on response messages. This section provides additional information that may help the resolver.

Cryptography (CH 31)

Cryptography means "secret writing". It means transforming messages to make them secure and immune to attacks.

* The original messages, before being transformed is called plain text. After the message is transformed it is called "ciphertext".
* An encryption algorithm transforms the plaintext to ciphertext.
* A decryption algorithm transforms the ciphertext back to plaintext.
* A key is a number (value) that the cipher as an algorithm operates on.

To encrypt a message, we need an encryption algorithm, an encryption key and the plaintext. These create the ciphertext.

To decrypt a messages we need a decryption algorithm a decryption key and the ciphertext. These reveal the original plaintext.

* The encryption and decryption algorithms are public i.e. anyone can access them.
* The keys are secret i.e. they need to be protected.

Symmetric Key Cryptography

In symmetric key cryptography, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data.

K. Pattanaik

In symmetric key cryptography, the algorithm used for decryption is the inverse of the algorithm used for encryption. This means that if the encryption algorithm uses a combination of addition and multiplication, the decryption algorithm uses a combination of division and subtraction.

Symmetric-Key algorithms are efficient; it takes less time to encrypt a message using a symmetric-key algorithm than it takes to encrypt using a public key algorithm. The reason is that the key is usually smaller. For this reason, symmetric key algorithms are used to encrypt and decrypt long messages.

A symmetric-key algorithm has two major disadvantages. Each pair of users must have a unique symmetric key.

This means if 'N' people want to use this method there needs to be

$N(N-1)/2$ symmetric keys.

Traditional Ciphers

A character was the unit of data to be encrypted. These traditional ciphers involved either substitution or transposition.

Substitution Cipher

A cipher using the substitution method substitutes one symbol with another. If the symbols in the plaintext are alphabetic characters, we replace one character with another:

eg We replace A with D, T with W.

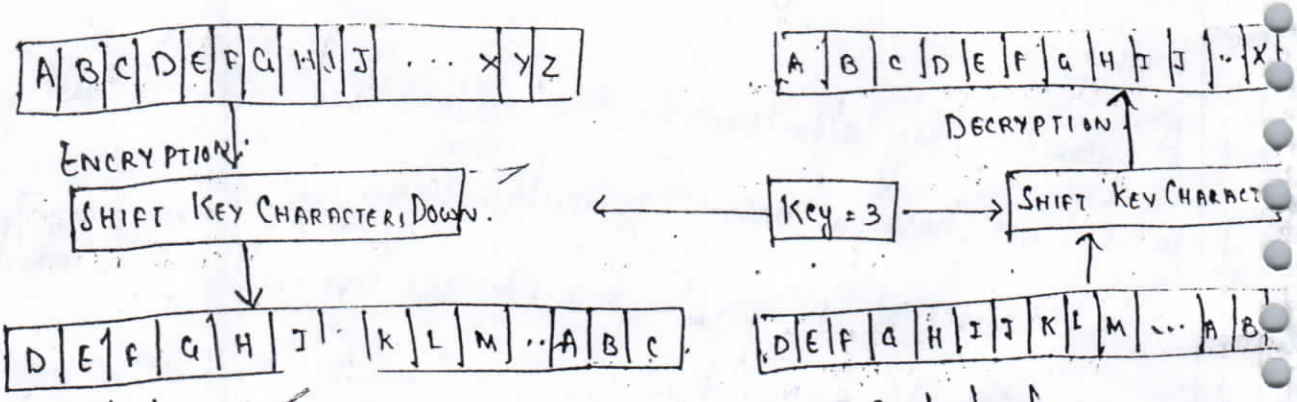
Suppose digits then 3 with 7, 2 with 6.

Substitution can be categorized as either monoalphabetic & polyalphabetic.

MONOALPHABETIC SUBSTITUTION :-

In monoalphabetic substitution, a character in the plaintext is always changed to the same character in the ciphertext regardless of its position in the text.

For example :- if the algorithm says that character 'A' in the plaintext must be changed to 'D'; every character 'A' is changed to character 'D' regardless of its position in the text. The first recorded ciphertext shifts each character down by three.



Monoal.

is very simple, but the code can be attacke

In

rance of a character can have a
ween a character in the plainte

ivision of the position
the shift value.
lly than created
difficult.

and m

Here,

K. Padmanabhi

Transpositional Cipher

In a transpositional cipher, the characters retain their plaintext form but change their positions to create the ciphertext. The text is organised into a 2-D table and the columns are interchanged according to a key.

1	2	3	4	5	6	7	8
A		G	O	O	D		
F	R	I	E	N	D		
I	S		A				
T	R	E	A	S	U	R	E

(PLAINTEXT)

Encryption ↓ / ↑ Decryption

1	2	3	4	5	6	7	8
3	6	4	1	2	8	5	7

1	2	3	4	5	6	7	8
		A	G				D
O	O						
E	N	F	I		R		D
A		I			S		
A	S	T	E	R	R	E	U

(CIPHERTEXT)

The key defines which columns should be swapped. This is not very secure either.

Block Cipher

Traditional ciphers used a character or symbol as the unit of encryption / decryption. Modern ciphers on the other hand, use a block of bits as the unit of encryption / decryption.

P-Box

A P-box (P for permutation) performs a transposition at the bit level; it transposes bits. The key and the encryption / decryption algorithm

are normally embedded in hardware. It can be implemented in software, but hardware is faster. Both the plaintext and ciphertext have same number of 1's and 0's.

S-Box

An S-box (S for substitution) performs substitution at the bit level; it transposes permutted bits. The S-box substitutes one decimal digit with another. The S-box has three components: an encoder, a decoder and a P-box. The decoder changes an i/p of 'n' bits to an output of 2^n bits. This o/p has one single '1' (the rest are 0's).

Product Blocks

The P-boxes and S-boxes can be combined to get a more complex cipher block

Data Encryption Standard (DES)

DES is a complex block cipher. Here, the algorithm encrypts a 64 bit plaintext using a 56 bit key. The text is put through 19 different and complex procedures to create a 64 bit ciphertext. DES has two transposition blocks, one swapping block and 16 complex blocks called iteration blocks.

Although the 16 iteration blocks are conceptually the same, each uses a different key derived from the original key.

In each block, the previous right 32 bits become the next left 32 bits (swapping). The whole DES cipher block is a substitution block that changes a 64-bit plaintext to a 64-bit ciphertext.

Public Key Cryptography

In public key cryptography, there are two keys :-

a) Private Key : It is kept to the receiver.

b) Public Key : It is announced to the public.

eg:- When sender sends a message to the receiver it uses public key to encrypt the message whereas the receiver uses private key to decrypt message.

In public-key encryption/decryption, the public key i.e. used for encryption is different from the private key that is used for decryption. The public key is available to the public; the private key is available only to an individual.

Public-key encryption/decryption has two advantages :-

* It removes the restriction of a shared symmetric key between two entities. Here, each entity creates a pair of keys; the private one is kept and the public one is distributed.
* The number of keys is reduced.

Public-key encryption/decryption has two disadvantages :-

* Algorithm is very complex.
* The second disadvantage of the public key method is that the association between an entity and its public key must be verified.

RSA

The most common public key algorithm is called RSA method after its inventors (Rivest, Shamir, Adleman). The private key here is a pair of numbers (N, d); the public key is also a pair of numbers (N, e).

'N' is common to private and public keys!

The sender uses the following algorithm to encrypt the message

$$C = P^e \bmod N$$

P ⟶ plaintext which is represented as a number.

C ⟶ number that represents ciphertext.

e ⟶ power.

Mod ⟶ indicates that the remainder is sent as ciphertext.

The receiver uses the following algorithm to decrypt the message:

$$P = C^d \bmod N$$

d, N ⟶ components of the private key.

Eg Private key is the pair $(\overset{N}{119}, \overset{d}{77})$.

Public key is the pair $(\overset{N}{119}, \overset{e}{5})$.

Suppose the sender wants to send character 'f' (6th alphabet).

∴ Encryption Algorithm ⇒ $C = P^e \bmod N$.

$= 6^5 \bmod 119 = 41$.

41 is the number sent as ciphertext.

Receiver uses:-

∴ Decryption Algorithm ⇒ $P = C^d \bmod N$.

$= 41^{77} \bmod 119 = 6$

∴ 6th alphabet is 'f'.

CH-30

Message Security

Message security provides 4 services. They are :-

a) privacy (confidential)

b) Message authentication.

c) Message integrity.

d) Non repudiation.

Privacy

It means that the sender and receiver expect confidentiality. The transmitted message must make sense to only the intended receiver and to all others, the message must be unintelligible. The message must be encrypted.

Privacy with Symmetric Key Cryptography

Privacy can be achieved using symmetric key cryptography in which a single key is shared between sender and receiver. This is very common for achieving privacy.

Privacy with Public Key Cryptography

Privacy can be achieved using public key cryptography in which there are two keys: a private key which is kept with the receiver and a public key which is announced to the public. The main problem with public key encryption is its owner must be verified.

Message Authentication

Message authentication means that the receiver needs to be sure of the senders identity and that no imposter has sent the message.

Digital signature can provide message authentication.

Integrity

Integrity means that the data must arrive at the receiver ~~needs to be sure of the sender's identity and that an imposter has not sent the message~~ exactly as they were sent. There must be no changes during the transmission i.e. may be accidentally.

Nonrepudiation

Nonrepudiation means that a receiver must be able to prove that a received message came from a specific sender. The burden of proof falls on the receiver.

eg:- A customer sends a message to transfer money from one account to another, the bank must have a proof that the customer actually requested this transaction.

Digital Signature

Digital signature's idea is similar to the signing of a document. When we send a document electronically we can either sign the entire document or we can sign a condensed version of the document.

Signing The Whole Document

Public key encryption can be used to sign a document. However, the roles of public and private keys are different here. The sender uses her private key to encrypt (sign) the message just as a person uses her signature to sign a paper document. The receiver on the other hand uses the public key of the sender to decrypt

the message just as a person verifies from memory another person's signature. In the digital signature, the private key is used for encryption and the public key for decryption.

Digital signatures can provide integrity, authentication and non repudiation.

Signing The Digest

Here, the sender creates a miniature version or digest of the document and signs it; the receiver then checks the signature on the miniature.

To create a digest of the message, we use a hash function. The hash function creates a fixed size digest from a variable length message.

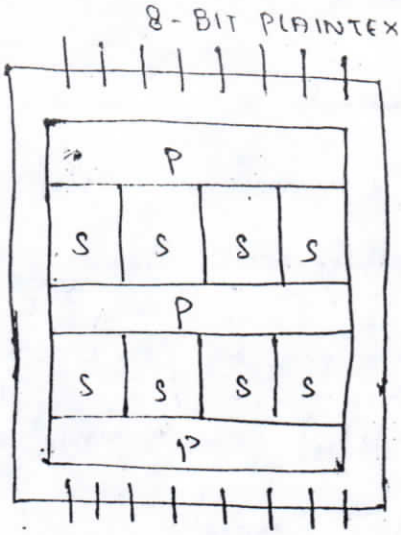
Hash function has two properties :-

* The digest can only be created from the message, i.e. hashing is one-way.
* Hashing is one-to-one function i.e. there is little probability that two messages will create the same digest.

After the digest has been created, it is encrypted using sender's private key. The encrypted digest is attached to the original message and sent to the receiver. The receiver receives the original message and the encrypted digest. He separates the two. He applies the same hash function to the message to create a second digest. He also decrypts the received digest using public key of the sender. If the two digests are same, all three security measures are preserved.

DATA ENCRYPTION STANDARD (DES)

'P' box and 'S' box are combined to get a more complex cipher block. This is called a product block.



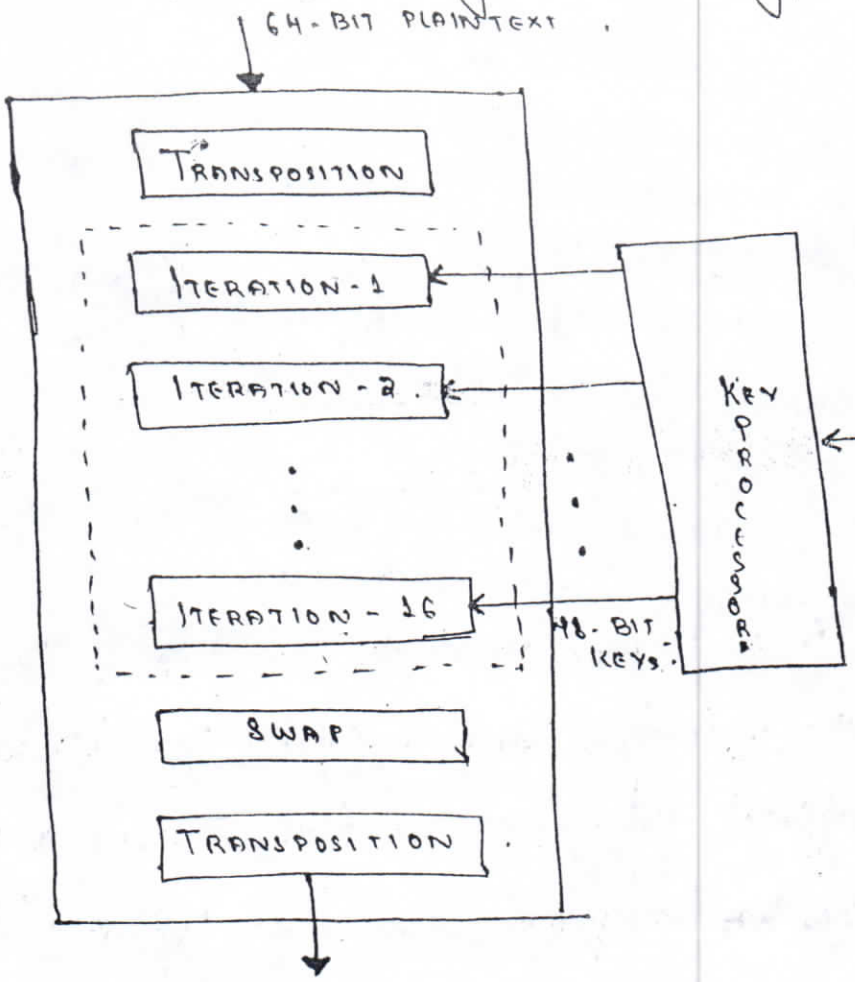
PRODUCT.

DES is an example of complex block cipher. The algorithm encrypts a 64-bit plaintext using a 56-bit key. The text is put through 19 different and complex procedures to create a 64-bit ciphertext. DES has two transposition blocks, one swapping block, and 16 complex blocks called iteration blocks.

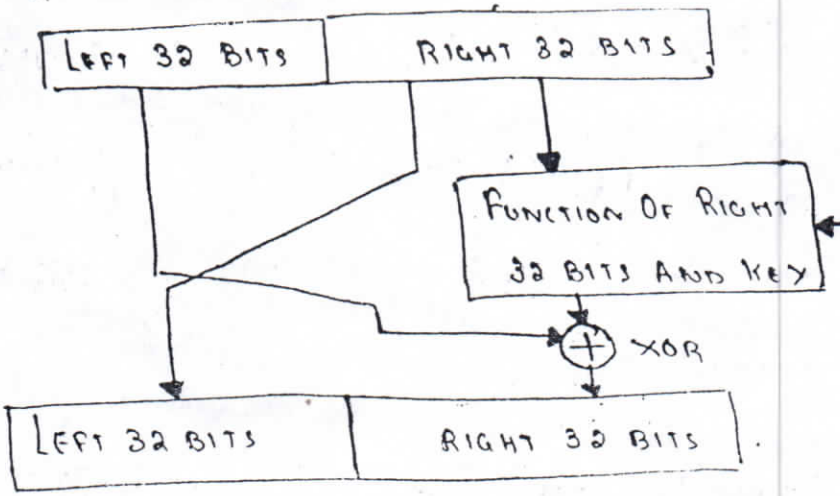
In each block, the previous right 32 bits becomes the new left 32 bits (swapping). The next right 32 bits, however, come from first applying an "operation" (a function) on the previous right 32 bits and then XORing the result with the left 32 bits.

The whole DES cipher block is a substitution block

that changes a 64-bit plaintext to a 64-bit ciphertext. In other words instead of substituting one character at a time, it substitutes 8 characters (bytes) at a time, using complex encryption and decryption algorithms.



General Scheme Of DES.



Iteration Block.

0 0 1
1 1 1
1 0 0
0 1 0

SMTP

There are two popular application of exchanging information

(i) Electronic mail exchange information between people.

(ii) File transpher exchange files between computers.

Electronic Mail:-

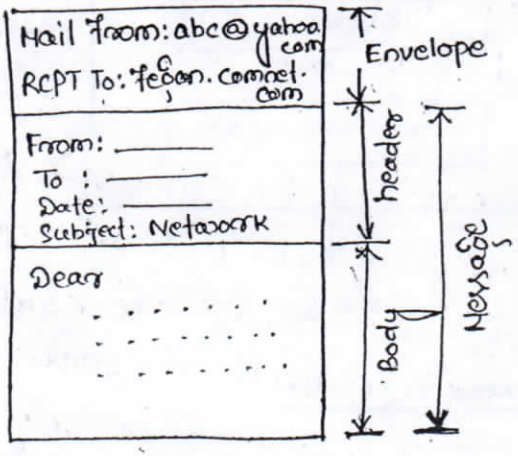
- One of the most popular n/w service is e-mail. It is used for se single message that that includes text, voice, video, graphics t one or more recipients.

Simple Mail Transpher Protocol (SMTP) is the standard mech for electronic mail in the internet.

Sending mail:-

To send mail the user creates mail that looks very similar to postal mail. It has an

(i) envelope (ii) message.



Envelope:-

The envelope usually contains the sender address, the address and other information.

Message:-

The message contain the header and the body. The heade the message define the sender, the receiver, the subject of message. The body of the message contains the actual informatio be read by the recepient.

Receiving Mail:-

The email system periodically checks the mailboxes

a user has mail, it informs the user with a notice of the user is ready to read the mail. a list is displayed in which each line contains a summery of the information about a particular message in the mailbox. The summery usually includes the sender mail-address, the subject and the time the mail was sent or received. The user can select any message and display its contains on screen.

Address:-

To deliver mail, a mail handling system must use an addressing system with unique address. The addressing system used by SMTP consist of two parts.

(i) local part

(ii) domain name

local part	@	domain name

Local part

Local part defines the name of a special file called the user mailbox, where all the mail received for a user a stored for retrival by the user agent.

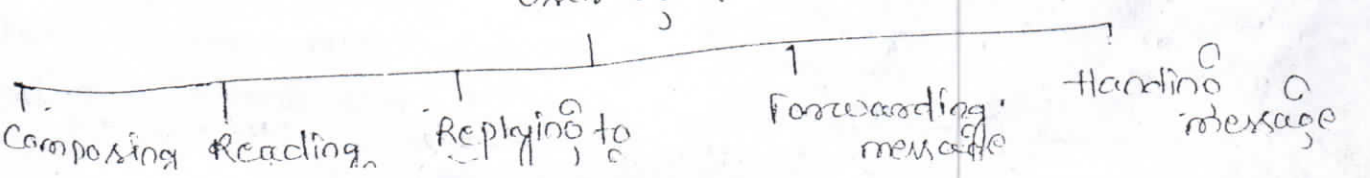
Domain Name

The second part of the address is the domain name. An organization usually selects one or more hosts to receive and send mail. they are sometimes called the mail exchanger. The domain name are assigned to each mail exchanger either comes from the DNS database or is a logical name. (the name of the organization.

User Agent

- The first component of an mail is the user agent. A user agent is sometimes called mail reader.

Services provided by a user agent:-



208

Composing Message:-

- A user agent is responsible for composing the email message to be sent out.
- Most user agents provide a template on the screen to be filled in by the user.
- Some have built in editor (spell checking, grammar checking)
- A user can create his/her own text editor and can import it into user agent.

Reading Message:-

- When a user invokes a user agent, it first checks the mail in the incoming mail box.
- Most user agent show one-line summery of each received mail which contains
  - A number field
  - A flag field, if the mail is new, already read but not replaied, read and replaied so on.
  - Size of message.
  - The sender
  - The subject field if the subject line in the message is not empty.

Replying in message:-

- After reading, the user agent to reply a message.
- A user agent allows the user to reply to the original sender or to all recipients
- The reply message originally contain the original message and message.

Forwarding Message:-

- Replying is defined as sending a message to the sender or recipient of the copy.
- Forwarding means to send the message to a third party.

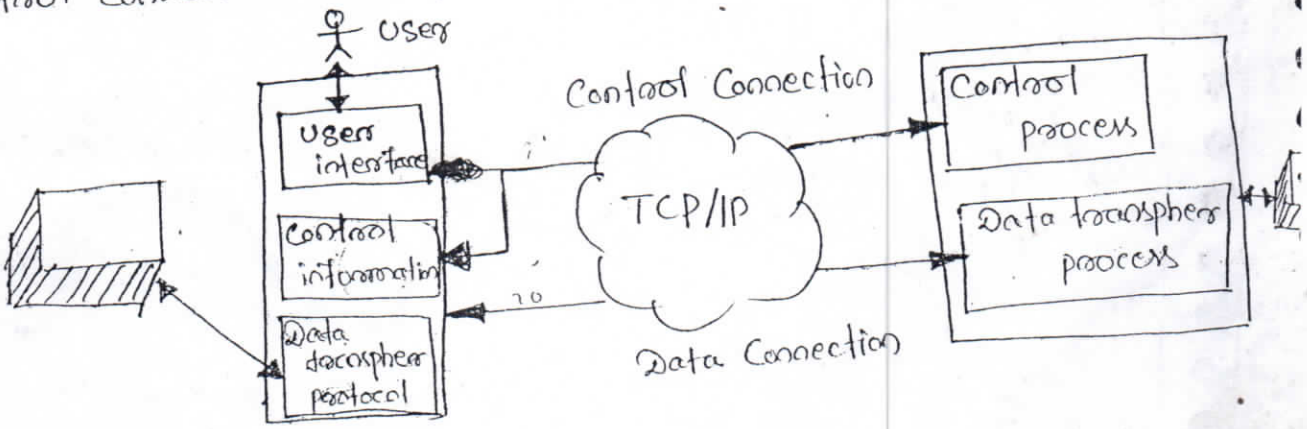
Handling Messaging:-

- A user agent normally creates two mailbox: inbox and outbox. Each box is a file with special format that can be handled by user agent.

- The inbox keeps all the received email until they are detected by the user. The outbox keeps all the sent emails until the user detects them.

File transpher Protocol :-

- File transpher protocol is the standard mechanism provided by the internet for copying a file one host to another.
- Problems while transpherring.
  * Two ~~files~~ systems may use different file name conventions.
  * Two systems may have different way to represent text and data.
- FTP differs from other client server application in that it establishes two connection between the client and the server.
- One connection for data transpher, the other for control information (commands and responses.
- Separation of ~~FTP~~ commands and data transpher make FTP more efficient.
- The control connection uses very simple rules of communication. We need to transpher only one line of command or a line of response at a time.
- Data communication on the other hand needs more variety of rules due to of data types transpher are of variety types.
- FTP uses two well known TCP ports : port 21 is used for control connection and port 20 is used for data communication.



- Client has three components
  (i) User interface (ii) Client Control Process (iii) Client Server data transpher process
- Server has two components
  (i) Server Control Process (ii) Server data transpher process
- The control connection is made between the control process.
- The data connection is made between the data transpher processes.
- The control connection is maintained during the entire FTP session. The data connection is opened and then closed for each file connection. It open each time commands that involpe transpher files are used, and closed when file is transphered.