16/04

Data Communication:

→ Data Communication Send & receive the data through some types of tramission medium.

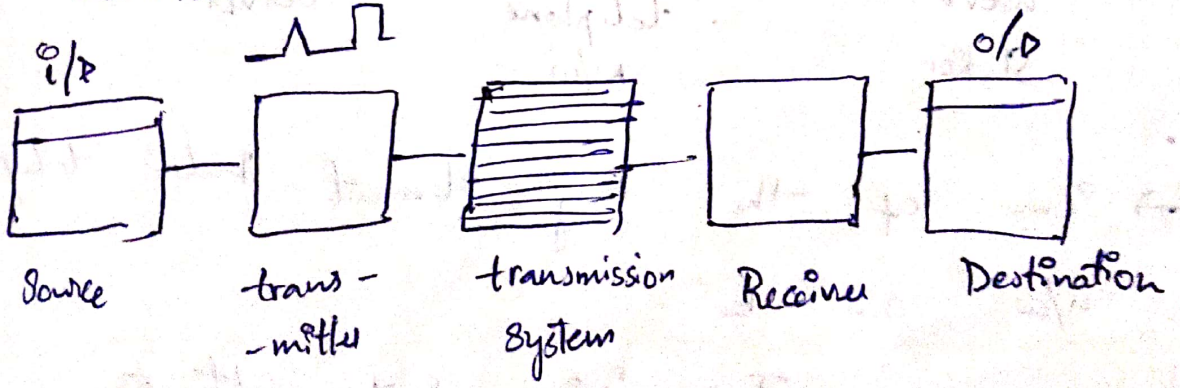
Types of Communication:

1) Simplex - One way communication (radio)
2) half Duplex - 2 way (at a time one Only) (walki-talkie)
3) full Duplex - 2 way (phone)

Data: raw fact & information

Communication Model:

1) Source
2) transmitter
3) transmitter s/m
4) Recievers
5) Destination



- Source (generate raw data
- transmitte:
  It transforms & encodes data into the Electromagnetic Signals.

3) transmission System

It is a line b/w Source & destination.

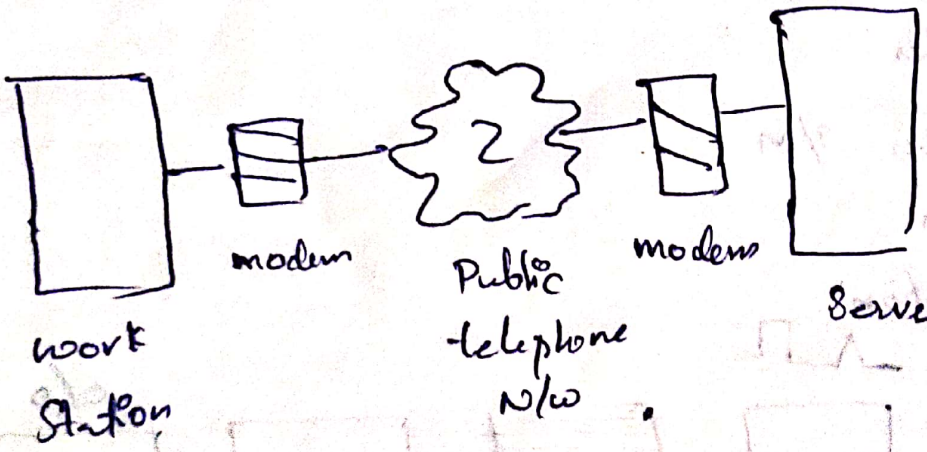
4) Receiver.

It decodes the Raw data a given by the transmitter.

5) Destination

It Receives the incoming data from the Reciever

Ex: Public telephone n/w



→ Some of the key element public telephone n/w can be

→ Transmission System, utilization

→ Signal generation

→ Synchronization.

→ Error detection & Controlling

→ and routing security.

Network :

1. WAN — Circuit switching, packet & frame relay
2. LAN — Bluetooth
3. MAN — wifi.

Protocal:

→ Set of rules that exchange info. the two system.

Key elements:

- Syntax (Block of code) (or) data block.
- Symantic (flow of control of data) error management.
- Time.

Simplex Mode	half duplex mode	full duplex mode
→ In Simplex mode the Communication is Unidirection	→ In half duplex mode the Communication is bidirection, but One at a time	→ In full duplex mode, the Communication is directional.
→ A device can Only Send the data but Can't receive it (or) It can Only receive the data but Can't Send it	→ Both the devices Can Send & receive the data but One at a time.	→ Both devices Can Send & receive the data Simultaneously
→ half duplex mode is better, when compared Ex: Radio, Keyboard	→ Full duplex mode is better. Ex: walkie talkie	→ Full duplex is best Ex: telephone network.

OSI Model: (Open System Interconnection) refence model

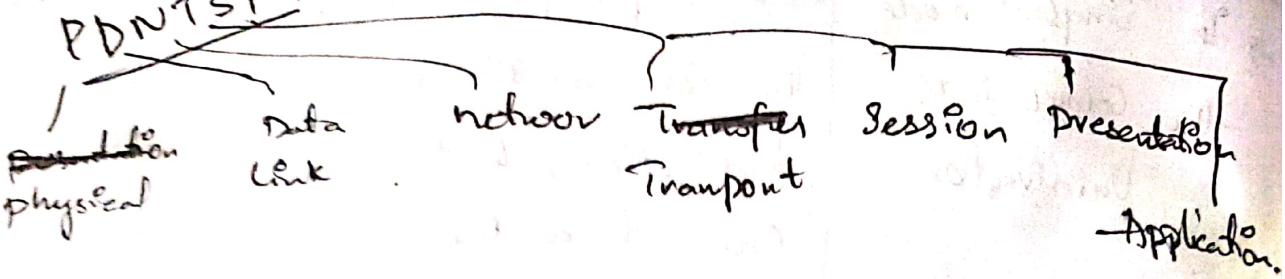
→ how Information from a Software application in One Computer moves through a physical medium to the Software application in another Computer.

→ 7 layers. (each layer is collection of protocals)

→ developed ISO (International Organization for Standardization in 1984)

→ architecural model for Intercomputer Communication,

→ ~~RDTSPTA~~ PDNTSPA - pls don't tell secret password to Anyone.



i) Application (L): Top most layer of OSI model (7 layer).

→ It provides service for network application.

→ network application which use network

Ex: chrome, firefox, out look, Skype etc.

FTP → File Transfer protocal.

web surfing :→ HTTPS / HTTPS

(Hyper text transfer protocal Secure)

mail: →

SMTP (Simple mail transfer Protocal)

Virtual terminal → Telnet.

ii) Presentation (L6): It receive data from application (L)

It performs operation like translation, Data Compression, encryption & decryption.

→ translation → Ex: ABCD → 1011011

→ Compression Ex: 1011001 → 1011

→ encryption Ex: 10111O → X10X111XO

→ decryption Ex: X10X111XO → 10111O.

SSL (Secure Sockets layer).

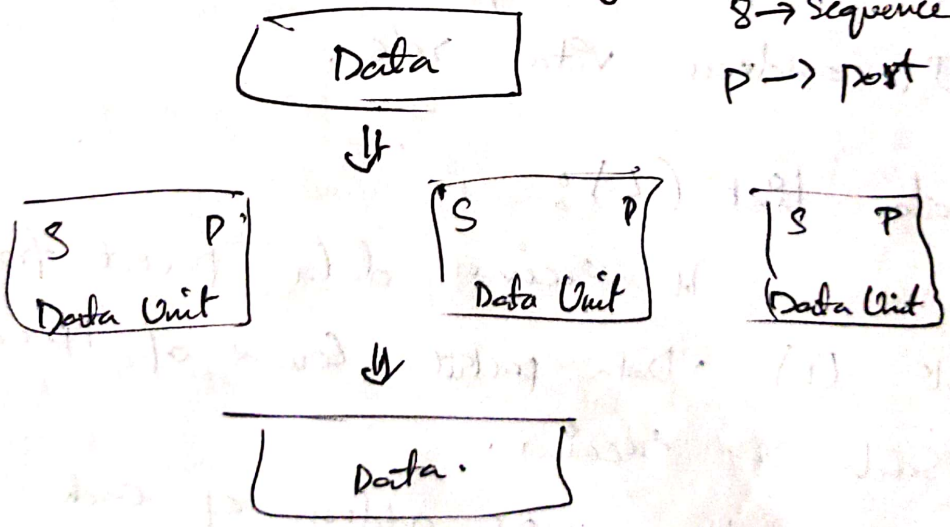
iii) Session (L): Session layer help in setting up & managing connection enabling sender & receiving of data & followed by termination of session once transfer done.

Before we start a session Authentication (who are you) is done.

Authentication: enter username & password if matched the session starts (connection established).

Authorization: different permission to access data (or) download it

iv) Transport (L): OSI model provides transparent transfer of data b/w end systems or host and is responsible for segmentation, flow control & error control & recovery.



Flow control: Constant flow b/w sender & receiver,

Error control: If any data unit did not reached the receiver then we use Automatic Repeat request is used.

TCP (Transmission Control protocal), UDP (User Datagram protocal)

All

→ Connection Oriented transmission

→ Connection less transmission.

→ TCP Slower

→ Provide feedback

→ lost data can be retracke

→ faster than TCP

→ nope

→ can't retrack.

v) Network (L):

It help the transfer of data received from transport layer in bw 2 (or) more systems.

Here data is divided into packets.

→ Router & Switching

→ IP address vital role.

vi) Data link (L):

It receives data packet from network (L). Data packet consist of IP address of sender & receiver.

Here mac addres of each system are assigned to Data packet to for frame (physical address).

MAC1	MAC2	IP1 IP2	Segment	Tail

MAC → 12 digit code

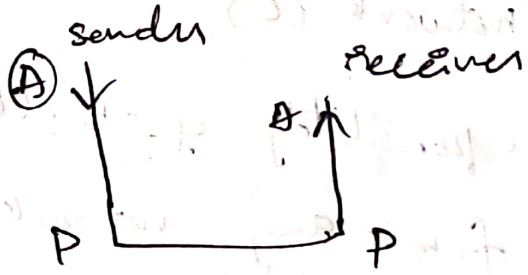
vii) Physical ~~Lay~~(L): Till now all data converted to bits. Now as pr medium the data is transffered form One System to another.

Copper wire ⇒ electrical signal

Optical → ligh

Air ⇒ radio, ~~mag~~ magnetic signal.

Note:



TCP/IP model (4 (L)):

→ Tramission Control protocal & internet (p).

→ Protocal are Set of rules which describe the movement of data b/w the source & destination on the internet

Application (L) ← Application, presentation, session

Transport (L)

Internet layer → network Lay

Network access (L) ← Data link (L), physical (L).

i) Network Access Layer : lowest (L) TCP/IP

physical + Data link = network (L)
(In OSI Model)

→ It defines how the data should be sent physical through the network

→ protocal like Ethernet, FDDI etc are used.

ii) Internet (L): second (L) TCP/IP

→ Internet (L) / network (L)

The main responsibility of this (L) is to send the packets from any network.

IP protocal: It is use to identify the User.

iii) Transport (L):

it is responsible for the reliability, flow control & Correction of data.

1) TCP
(Transmission control prol)

2) UDP
(User Datagram (P))

iv) Application (L): top most (L) in TCP/IP mo

→ This layer allow the user to interact with the application.

i) HTTP
ii) SNMP (Simple network managment protocal).
iii) SMTP
iv) FTP: file transfer protocal.
v) Telnet: It is an abbrivation of terminal network.
It establish connection blw: local Computer & remote Comp.
vi) DNS: Domain name system.

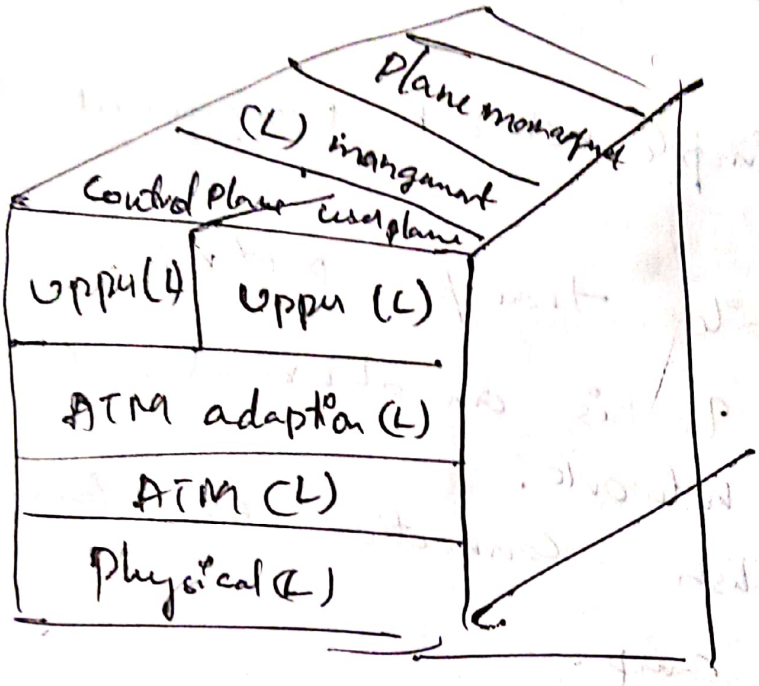
→ Domain name connect to IP address.

OSI	TCP/IP
→ 7 layer	→ 4 layer.
→ less Realiable	→ more Relaible
→ different session & presentation (L)	→ Use both Session & presentation (L) itself.

(ATM): Asynchronous Transfer mode.
It is switching techniques used by telecommunication network.

→ Data transfer is done in chunks.

→ It provides interface b/w user & network.



1) Physical (L): Involves Specification of transmission medium & signal encoding scheme Data.

2) ATM (L): Provides packet transfer

3) AAL (L): AAL map higher level information into ATM cells to be transported over an ATM network.

4) User plane: provides user information

5) Control (P): perform all control & Connection function.

6) Plane management: provides Coordination b/w all planes & layer management.

Data transmission :-

Data transmission is a mean, of transmitting digital (or) analog data over a communication medium to one or more devices.

i) Point to point : One device to another one device

ii) point to multipoint : One to many.

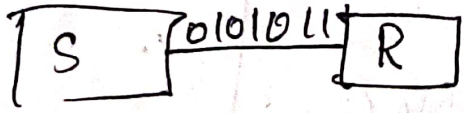
Data (T)

- Parallel (T)
- Serial (T)
  - Synchronous (T)
  - Asynchronous (T)

Parallel Transmission :

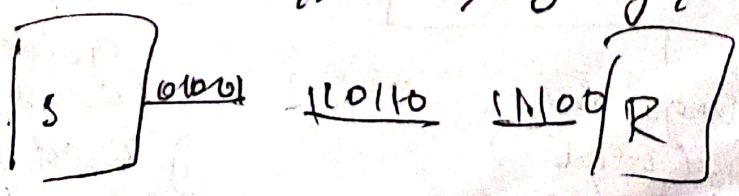
Here all the 8-bit of data is transfered from sender to receiver in a particular movement.

Serial (T) :



Synchronous (T) :

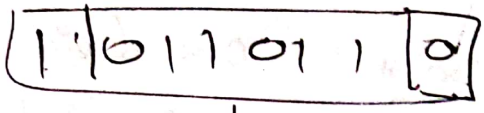
Sending bits one after another without start & stop bits or gaps.



Asynchronous (T):

Send one start bit at the beginning and one stop bit at the end of each byte.

→ cheap & effective.



Parallel Comm

→ 8 Data bits can be transfered at a time

→ transfer rate is high

→ Installatio cost more

→ Used for smaller distance

→ 9 lines are needed to Connecte

Serial data Comm.

→ Only One data bit can be transferred at a time

→ low

→ less

→ longer distance

→ 2 lines are need to Connect

Asynchronous com

→ Start & Stop bit are used

→ cheap & simple

→ less hardware

Synch

Transmission media:

guided media.
(wired)

i) Twisted pair cable:
ii) Shield/unshield
iii) Coaxial Cable

Unguided.
(wireless)

i) Radiowave
ii) Microwave
iii) Infrared wave (GPS)

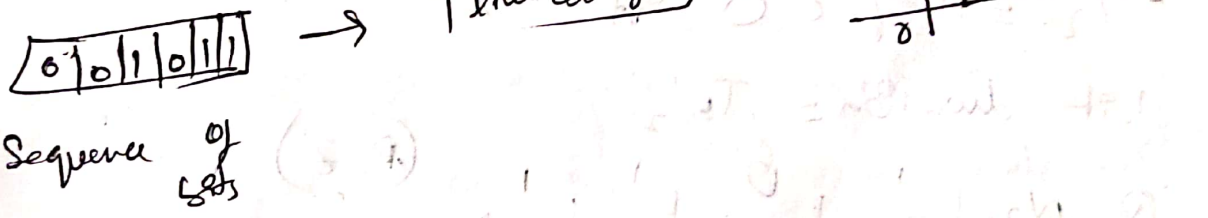
Coaxial cable

Base band (single sig) — Broadband (multiple signal)

iii) Optical fibre cable (light)

Digital data to digital signal :- (line coding)

It is a process of converting binary data, sequence of bit, digital data to a digital signal.



Sequence of bits

Classification of line code :

(±V, 0) (3)

Unipolar (2)(+A or 0) Polar (3)(±A/2, 0) Bipolar

RZ NRZ RZ NRZ manchester AMI

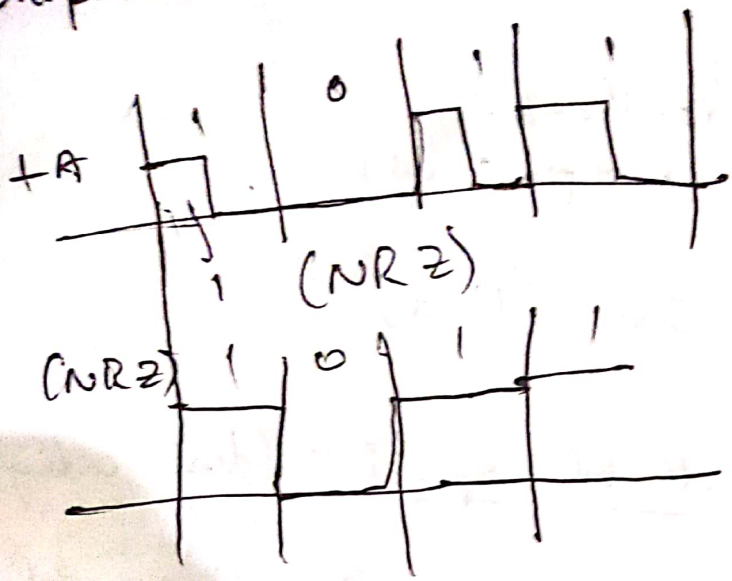
RZ - return to zero

NRZ - not return to zero

Prop :

→ power is efficient.
→ bandwidth used is reduced
→ Error reduced
→ Error detection & correction is possible.
→ cross talk b/w channels will be reduced.

Unipolar: (RZ)

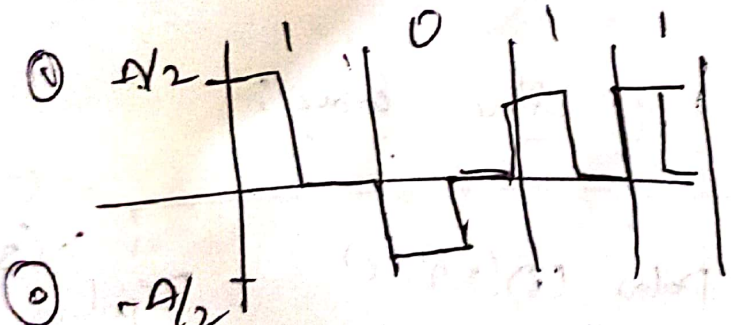


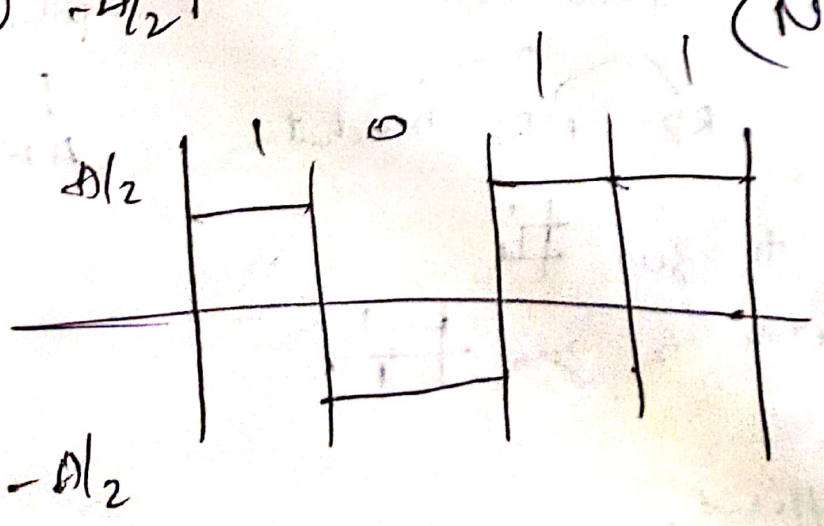
Polar (RZ)

$A/2$ = Logic 1 (on +ve)

$-A/2$ = Logic 0 (off -ve)

bit duration = $T_b/2$



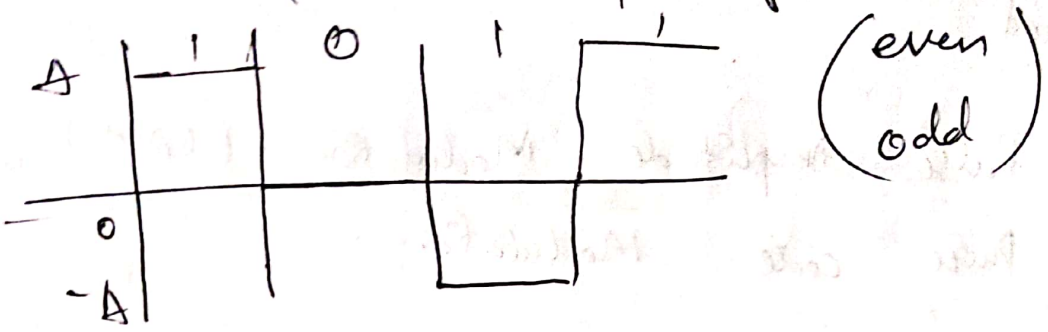


v) Bipolar NRZ format:-

0=0 (odd) +A = logic 1 (for 1st 1)

(even) -A = logic 1 (for 2nd 1)

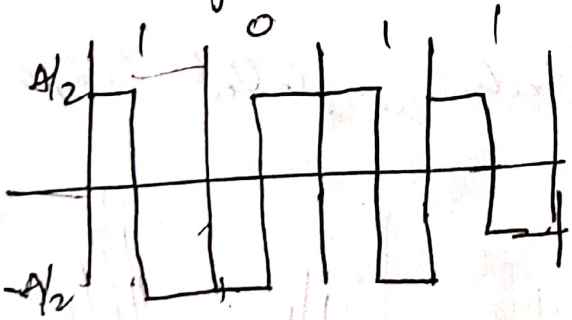
(alternative polarity).



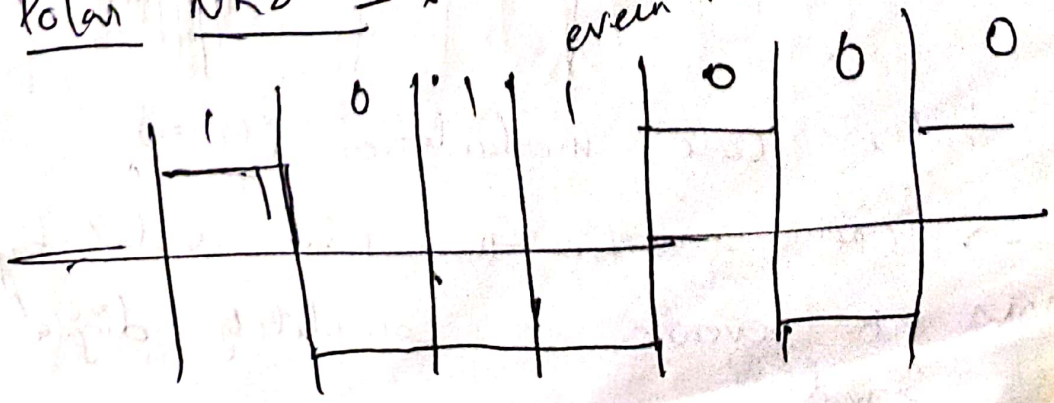
vi) Split phase Manchester format.

Symbol '1' = positive pulse of +A/2 amplitude for one half of symbol duration followed by negative pulse of -A/2 for remaining half duration.

Symbol '0' = reverse order.



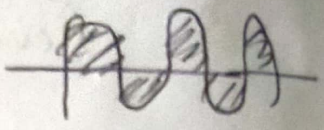
vii) Polar NRZ-I: odd ↑ even ✕ no change



Analog data to digital Signal Conversion:

→ ~~Encoding~~ we use decoder & encoder.

eg to record a song/voice



method

i) Pulse Amplitude Modulation - (PAM)

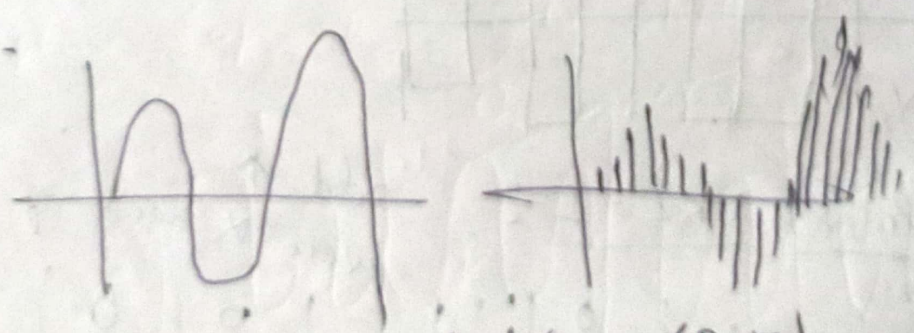
ii) Pulse code Modulation.

Pulse Amplitude Modulation:

→ Take analog signal sample it & generates a series of pulses based on the result of the sampling.

→ Sampling means measuring the amplitude of a signal to equal intervals.

→ PAM uses a technique called sample & hold.



II Pulse Code modulation (PCM)

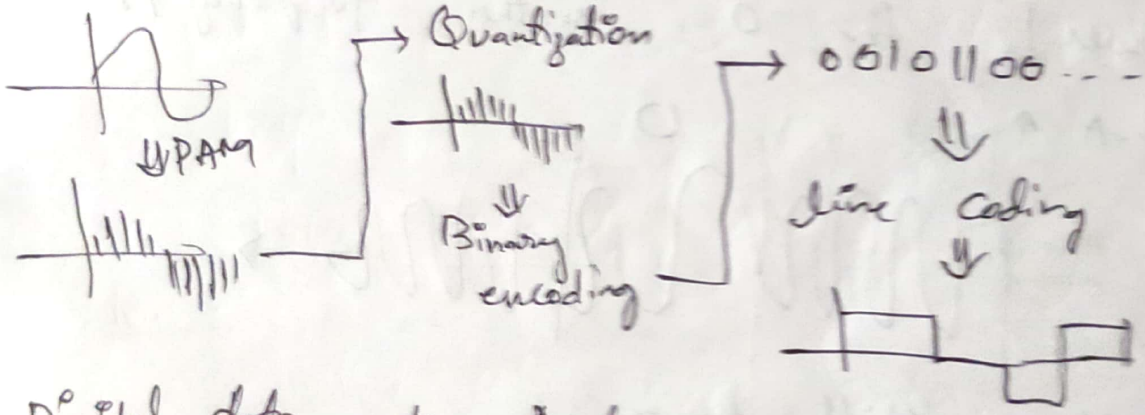
→ PCM modifies the pulse created by PAM to create a completely digital

→ Steps ⇒ Sampling
quantization
line-coding

a) Sampling: No of samples of the signal are taken at regular interval of a higher frequency of signal.

b) Quantization: the amplitude is written in binary format.

c) line-coding: Conversion to digital signal



Digital data to Analog signal:

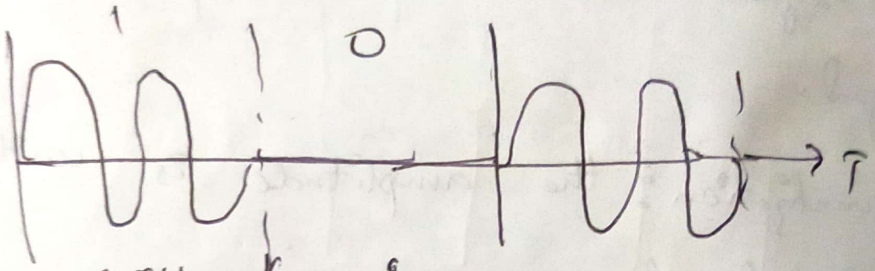
when data from one computer is send to another via some analog carrier, it is first converted into analog signal.

An analog signal is characterized by its amplitude, frequency & phase shifting key >.

i) Amplitude Shift Keying:

when binary data represents digit 1, the amplitude is held (high).

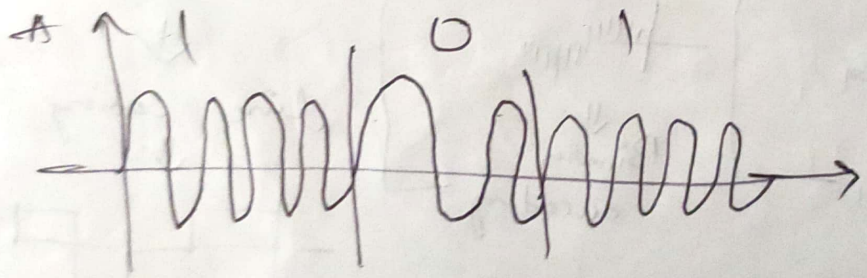
when binary data represent digit 0, the amplitude is 0(0)



ii) frequency Shift key:

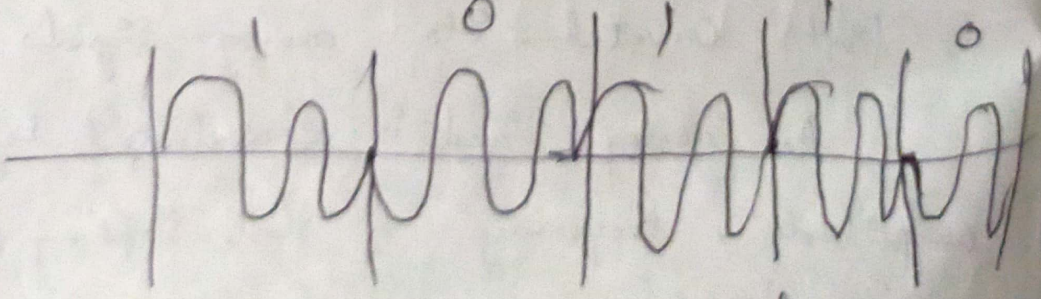
(higher) for 1 one frequency f_1

(lower) for 0 another frequency f_2



iii) Phase Shift keying:

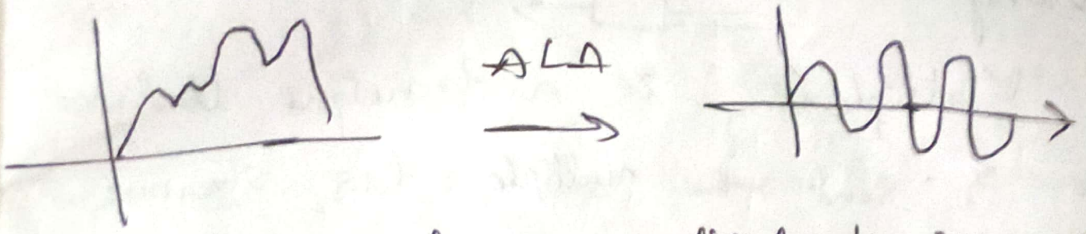
when a new binary symbol encounter the phase of the signal shift alternately.



Same direction

different direction.

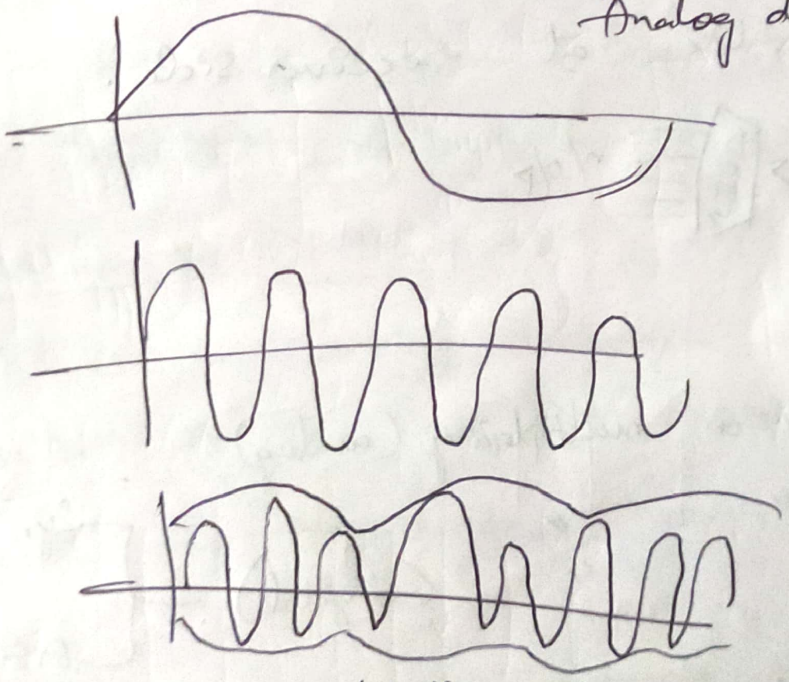
Analog data to Analog signal:



Analog signal are modified to represent analog data.

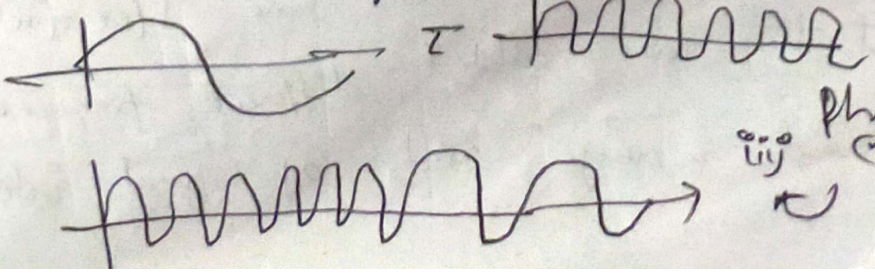
i) Amplitude Modulation:

In this modulation, the amplitude of the carrier signal is modified to reflect the analog data.



Amplitude modulation is implemented by using multiplexer.

ii) frequency (FM): It can be achived by making changes in the voltages level.



Unit-III

→ Multiplexing :-

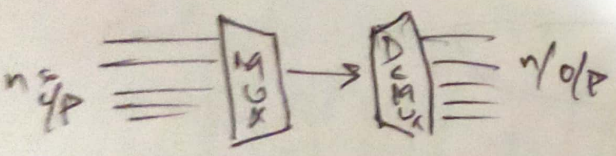
Multiplexing is a technique used to combine & send the multiple data streams over a single medium.

The process of combining the data streams is known as multiplexing.

→ MUX is used.

multiplexers that combine n input lines to generate a single output lines.

→ DEMUX is use at receiver side.



Types :

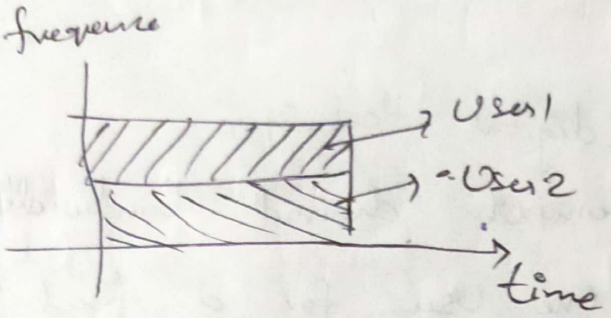
→ frequency division multiplexing (analog)
→ wavelength " " "
→ Time " " " (digital) → Syn TDM, Asy TDM

Frequency DIV :

→ It is an analog technique.
→ In FDM all users use the same common channel at the same time (for full time) but they are alloted different frequencies to prevent any kind of signal interfare.

→ So the bandwidth is divided among User not time.

→ There is possibility of cross talk in FDM since all signal are transmitted simultaneously.

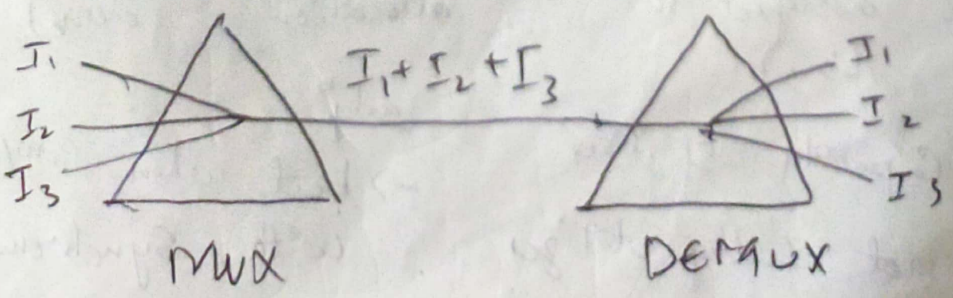


Adv → It is an analog signal
→ very simple & for full time

Dis → It suffers from cross talk
Ex: FM radio.

Wavelength DM

→ It is an analog technique.
→ WDM is same as FDM except that the optical signals are transmitted through the optic cable.
→ frequencies are very high.
→ high data transfer rate
→ at Sender mux at rec DEMUX is used.



→ light can be sent by different amount based on the angle of incident & wave-length of light.

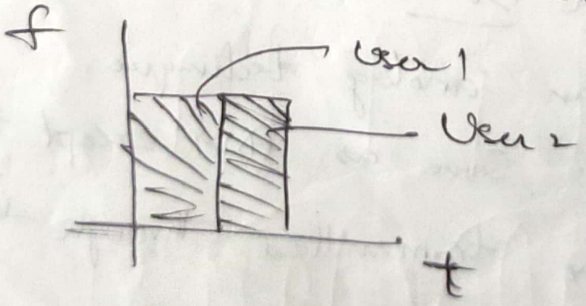
iii) Time DM:

→ It is a digital technique.

→ In TDM complete channel bandwidth is allotted to one user for a fixed time slot.

→ It means each user can use the full bandwidth available but for a fixed (diff user time slot).

→ So the division is in time not in band width. Here no cross talk issue.



TDM

Synchronous TDM
(Time slots are pre assigned to user)

Asynchronous TDM
(Dynamical time slot allocation is done)

Dis:
→ Capacity of user is not fully utilized

adj
→ best when compare with Synchronous

Switching :

→ The technique of transferring the information from one computer network to another computer network is known as Switching.

→ Switching in a CN is achieved by using switches. {process of forwarding packet from sender to receiver}.

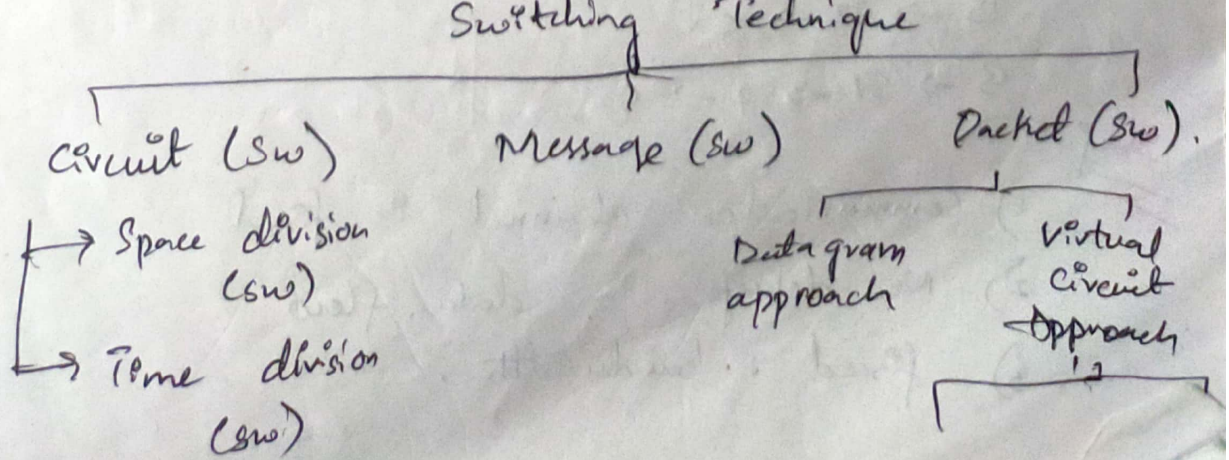
→ A switch is a small hardware device which is used to join multiple computers together with one local area network.

→ Switches operate at layer (2) in OSI model.

→ packet collision is minimum.

Switching techniques :

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

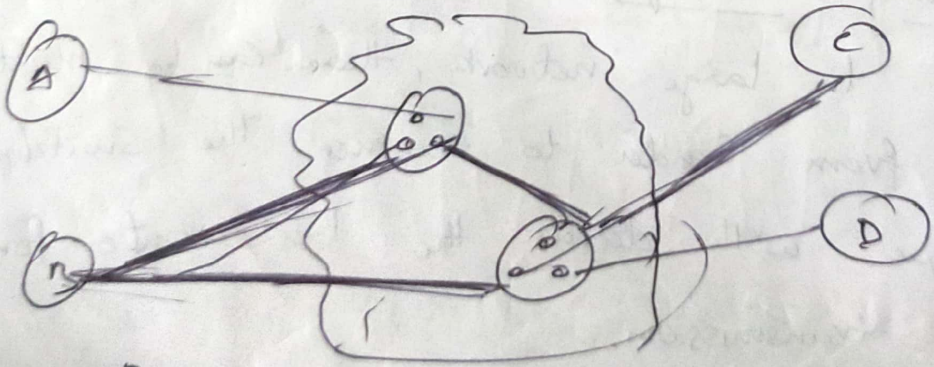


i) Circuit Switching : It is a transmission mode that involves setting up a dedicated end to end connection.

→ Commonly Used in Telephone System.
→ Connection Oriented
→ No delay in data flow.
→ Link of the connection cannot be used by any other data when it free.
→ More band width required.
→ Connection time is more.

3 phase

i) Circuit establishment
ii) Data transfer
iii) Circuit disconnect.



B → S2 → C

B → S1 → S2 → C

Adv

1) Communication channel is fixed
2) No delay in data flow
3) fixed bandwidth.

Dis Adv

→ Connection time is more.

→ when path is free other cannot use it.

ii) Message Switching: There is no dedicated path

Hw two communicating devices

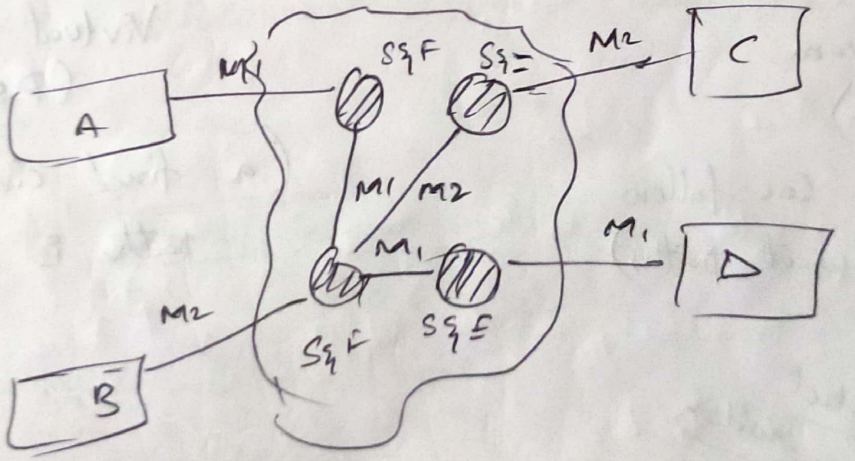
→ Each message is treated as an independent unit and includes its own destination & source address.

→ Also called as store & forward network.

→ Efficient traffic management

→ Some delay due to storing & forwarding.

→ Large storing capacity is required.



Adv efficient traffic management

Dis → Some delay due to storing & forwarding

ex: telegraph network.

forward only when next switch is enough empty.

Packet switching:

In this messages are broken up into packets.

Individual packets take different routes to reach the destination.

Adv → bandwidth reduces, efficient, cost efficient

→ In link failure different route can be chosen for remaining packet.

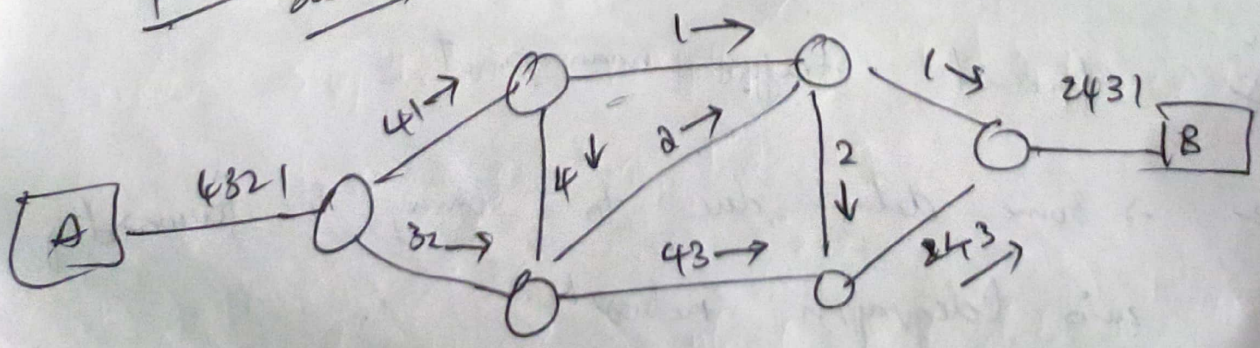
Dis

→ A bit complex, high usage of ram

Packet switching

- Data gram (PS) (packets can follow different paths)
- Virtual circuit (PS) (a fixed circuit path is followed)

Ex: Packet switch



Digital Subscriber line (DSL):-

→ It is a communication medium which is used to transfer internet through copper wire telecommunication line

→ when we get broadband from popular companies like BSNL, Airtel, when we take a plan with landline & internet then the connection they provide now is (DSL).

→ In previous years they use to give Dial-up connection which faced a problem (network disconnected when your in call).

→ It's removed in DSL

ph line	Internet line
30%.	70%.

Adv → No additional wiring

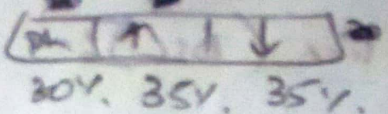
→ cost effecient

→ User can use both telephone & internet at the same time.

DSL

- Symmetric DSL
- Asymmetric DSL

Symmetric DSL



→ Here Splitting of upstream & downstream frequencies.

→ provides equal speed to both uploading & downloading data transfer.

→ This connection may provide 2 Mbps upstream & downstream.

(No found commonly)

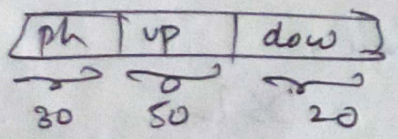
Adj → Equal upstream & down stream speed.

Disadv
→ mostly upstream speed is useless.
→ Not so efficient

Asymmetric DSL:

It provides a wide frequency range for down stream transfers, which offer several times faster than SDSL

→ upstream 20 Mbps & 1.5 mbps upstream.



→ As most users download most data than they upload.

Hence ADSL is widely used.

Adv → Both telephone & internet can be used at any point of time.

→ Better than all connections.

Dis

→ quality of the wire should be high.

→ depend on external factor distance 3km.

Characteristics of ADSL:

→ we can upload the data at a lower data speed rate.

→ we can download the data at a higher data speed rate.

→ Both telephonic & internet usage can done at any point of time.

Error Detection Techniques :-

Error : Due to noise or any external facta changes in binary bit are done i.e 0 to 1 (or) 1 to 0 is called error.

Types of errors

Single bit error

In this Only 1 bit in the data Unit has changed.

10110010 [sender]

10110000 [reciever]

Burst error

In this 2 (or) more bits in the data Unit changes.

10110010

10111001

→ Error detection is the detection of errors caused by noise or other impairments during transmission from the transmitter to the reciever.

→ Error detection & correction are Implemented at the data Link layer or the transport layer on an OSI model.

few error detection techniques:

→ Simple parity check
→ Two dimensional parity check
→ Check sum
→ Cyclic redundancy check.

1) Simple parity check: In this an extra bit (parity bit) is added to each word before transmitting.

→ Even parity: No. of 1's in given word including parity should be even.

→ Odd parity: No. of 1's in given word including parity should be odd.

1 0 0 1 0 1 1

Data

P | Data

Parity + D

even

0 1 0 0 1 0 1 1 (4)

0 1 1 0 1 0 1 1 error (5)

Odd

1 1 0 0 1 0 1 1 (3)

1 1 1 0 1 0 1 1 error (6)

limitation

→ not suitable for detection of multiple error
→ It can't do correction.

ii) Two dimensional parity check:

In this, the data word is organised in table (or) matrix.

Note: It checks and detect upto 3 errors.

Error affecting 4-bits may not be detected.

Ex:

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

⇓ Change 1 bit

								Old
0	1	0	0	1	1	1		1
1	0	0	1	1	0	1	0	1
0	1	1	1	0	0	1	0	0
0	1	0	1	0	0	1	1	1
0	1	1	1	0	1	0		
Old 0	1	0	1	0	1	0		

$\overline{0} = 1$ ✓

(iii) Check Sum: In this each word is added to the previous word & total sum (check sum) is calculated. Then check sum is transmitted along with the data.

(7, 11, 12, 0, 6)

w_1 w_2 w_3 w_4 w_5

$= 7+11+12+0+6 = 36$

| Data | C.S |

Sender → | Data | C.S | (receiver).

If (CS = CS1)

then no error (OR)

else error. Instead of C.S send Complement of C's

Sender - 36 → 36 + (C.S) = 0, (no error)

ex! Using one's complement

check sum = 7+11+12+0+6

= 36

↓ binary

100100 → as the no. of bit are > 4 Use wrapping

0100

10

0110 (6) → Inverse 1001

Data | Inverse c.s

7 + 11 + 12 + 0 + 6 + 7

= 45

↓ Binary

10 1101 (45)

↓ wrapping

1101

10

1111

↓ Inverse

0000 all zero no error.

iv) Cyclic Redundancy check (CRC):

It is based on the concept of binary Division.

→ CRC generator

i) Append string of n 0's to the data Unit

ii) Divide newly generated data Unit by the divisor.

iii) Remainder after ii) is n bit CRC

iv) The CRC will replace n 0's to get

CRC checked

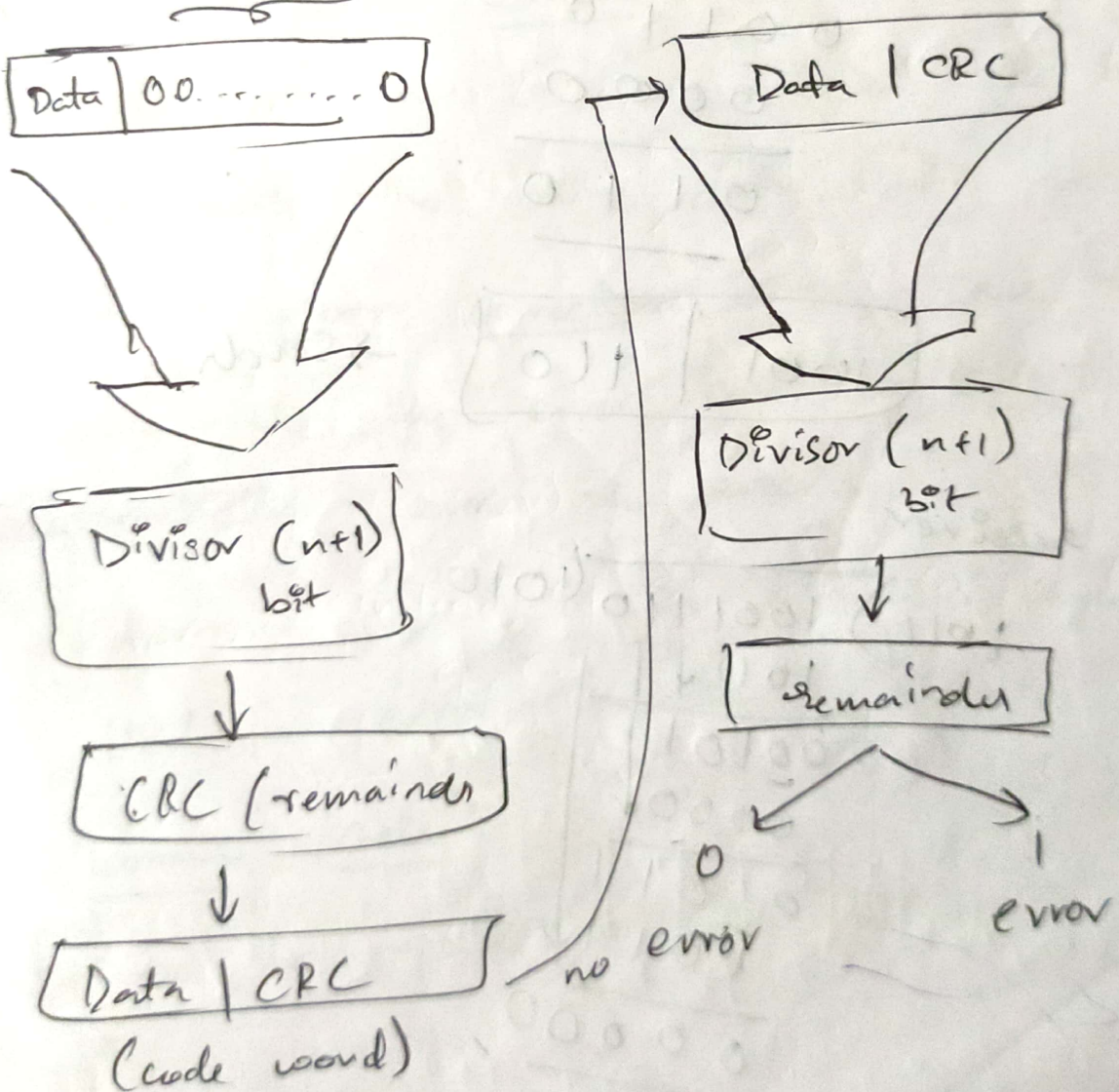
i) there the reciever recives the data &

CRC (code word)

ii) Divide it by divisor

iii) if remainder = 0 (Accept)

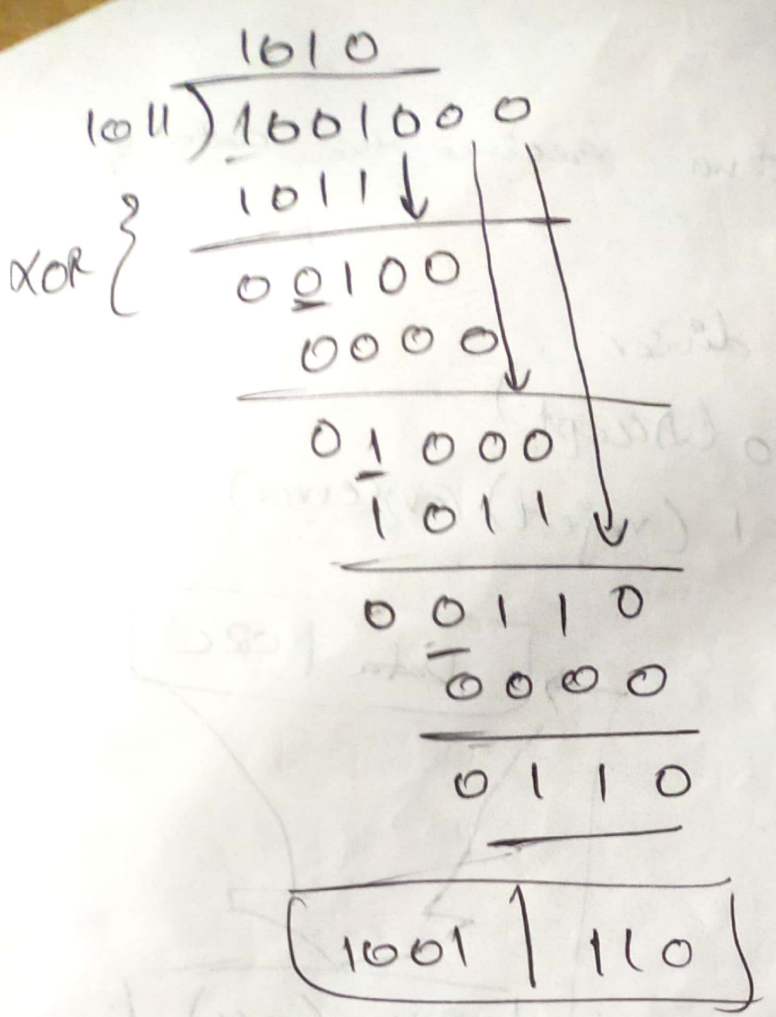
remainder = 1 (reject) (or) (error)



Eg: i) Data set = 1001, Divisor = 1011

Sol Data = 1001

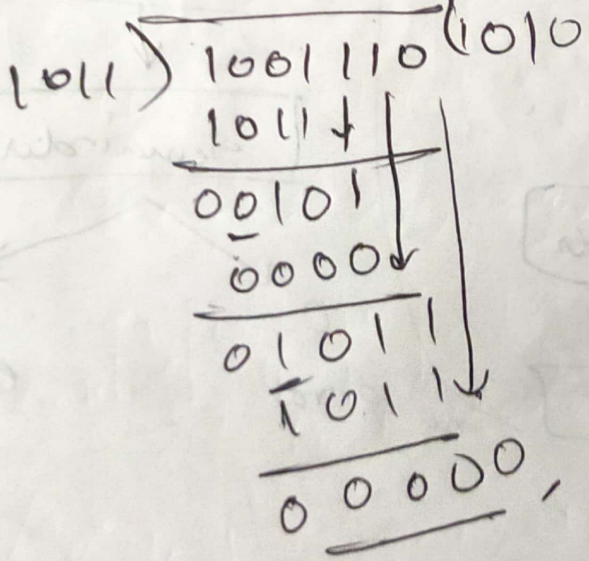
Divisor = 1011 (n+1 bits) ⇒ n=3



0^1 = 1

1^1 = 0

at receiver



remainder = 0

Hence no error

All the above 4 methods help in error detection.

→ Error Corrections:

Error Correction codes are used to detect & correct the error when data is transmitted from sender to the receiver

Two ways:

i) Backward error Correction: Once the error is discovered, the receiver requests the sender to retransmit the entire data Unit.

ii) forward error correction: In this case the receiver uses the error correcting code which automatically corrects the error.

* Hamming code is one of most popular & used for error correction & detects.

→ Hamming codes:

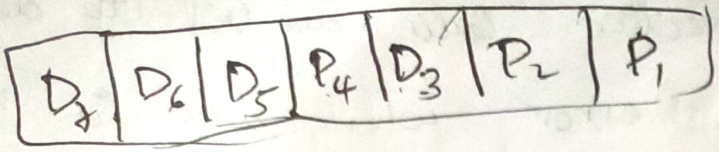
It can be applied to data Unit of any length.

It is used to detect & correct single bit errors.

→ Hamming code Structure:

All bit positions that are power of 2 are marked as parity bit (1, 2, 4, 8) other bits are for data.

* Commonly we use 7 bit hamming code



P - Parity
D - Data

$P_1 \rightarrow P_1\ D_3\ D_5\ D_7$

$P_2 \rightarrow P_2\ D_3\ D_6\ D_7$

$P_4 \rightarrow P_4\ D_5\ D_6\ D_7$

for P_1 check 1 bit, skip 1 bit

⇓

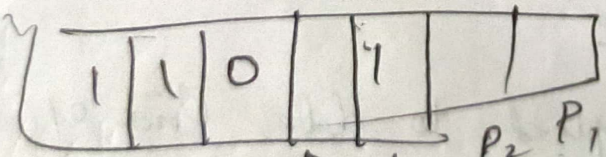
(1, 3, 5, 7, 9. ...)

for P_2 check 2 bit, skip 2 bit

(2, 3, 6, 7, 10, 11, ---)

for P_4 check 4 bit, skip 4 bit

(4, 5, 6, 7, 12, 13, 14, 15.)



$D_7\ D_6\ D_5\ P_4\ D_3\ P_2\ P_1$

→ P_1 101

⇓

0

→ P_2 111

⇓

1

P_4 011

⇓

0

1 1 0 0 1 1 0

Detecting error:

Consists 7 bit code

At receiver end, bit (1,3,5,7), (2,3,6,7) & (4,5,6,7) are checked

for even parity — then no error else error

check P_1 P_2 P_4 even parity

If not get correct values of P_1, P_2 P_4

Convert to decimal — then update

in the code.

$$\boxed{101} = 5$$

$$D5 = 1$$

Data link controls:

Data link control is the service provided by the Data link layer to provides reliable data transfer over the physical medium.

It is in the half duplex transmission mode, one device can only transmit the data at a time. If both the device transmit the data simultaneously, they will collide and leads to the loss of the information.

The Data link layer provides the Coordination among the devices so that no collision occurs.

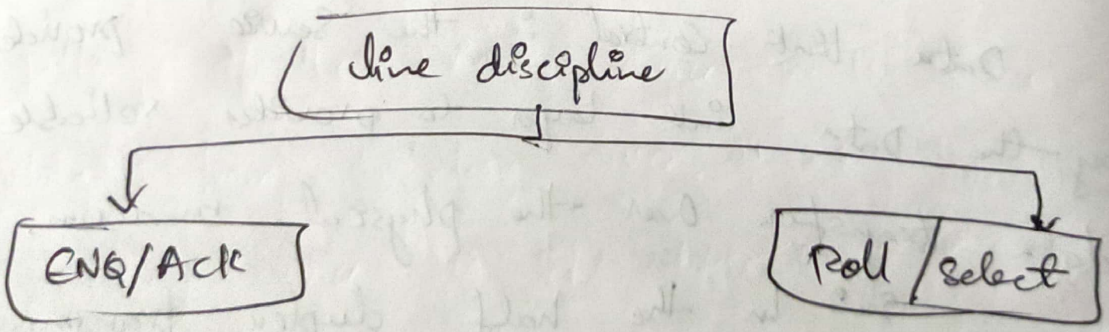
→ 3 Function

i) line discipline — who should send the data
ii) flow control — How much data should be sent
iii) Error control. — How can error be detected.

I) Line Discipline:

→ line Discipline is a functionality of the data link layer provides the co-ordination among the link system (among system).

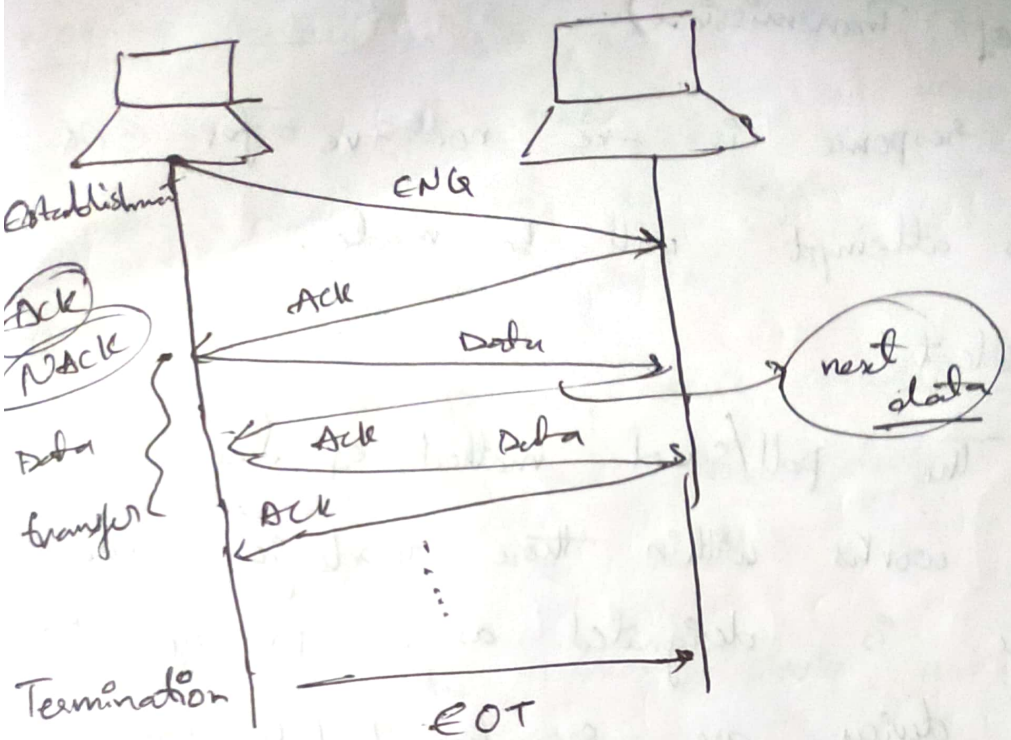
→ It determine which device can send and when it can send the data



i) ENQ/ACK

→ ENQ/ACK Stand for Enquire Acknowledgment

→ It take care that which device will start the transmission & wheather the recipient (receiver) is ready or not.



working:

→ Initially transmitter transmits the from called an Enquiry [ENQ] asking whether the receiver is available to receive the data (or) not.

→ The receiver responds either with positive acknowledgement (Ack) (or) with -ve (NACK) where +ve ACK means that the receiver is ready to receive the transmission & -ve ACK means that the receiver is not ready to accept the data.

→ If the response to the ENQ is +ve, the Send will transmit the data and Once all its data has been sent, the divice finishes its transmission with an EOT

(End of Transmission)

→ If the response is -ve nor +ve for ENQ then 3 attempt will be made.

ii) Poll/Select:

The poll/select method of line discipline works within those topologies where on device is designated as a primary station & other devices are secondary (1 to many types)

In this, the primary device & multiple secondary devices consists of a single transmission line and all the exchange are made through primary device even though the destination is a secondary device.

Polling: If the primary device wants to receive data from secondary device, it ask the secondary device to send data or vice versa this is polling.

Selecting: If the primary device wants to send some data to the secondary devices then it tells the target secondary device to get ready to receive the data, this process

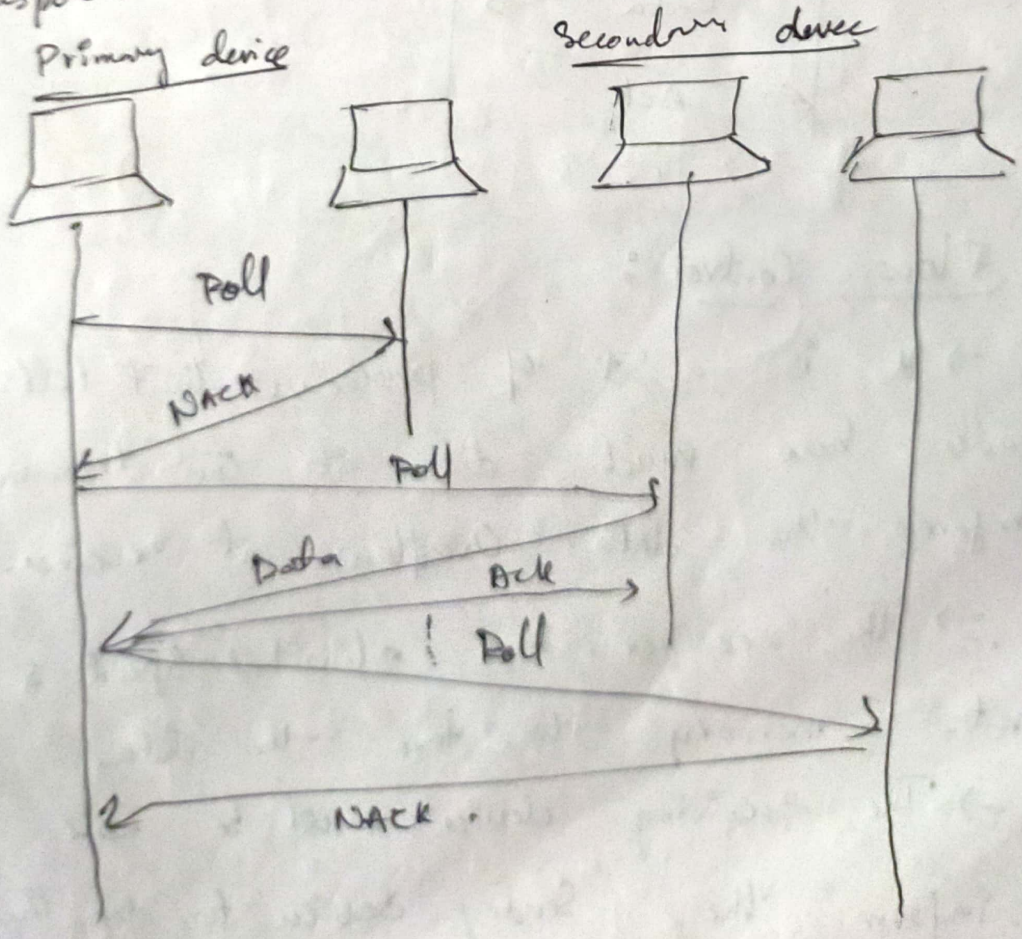
working of poll:

→ The poll mode is used when the primary device wants to receive some data from the secondary device.

→ when a primary device wants to receive the data, then it asks each device whether it has anything to send.

→ Initially, the primary device asks (poll) the first secondary device, if responds with NACK (means that it nothing to send

Now it approches 2nd secondary device, if it responds with ACK means that data is sent.

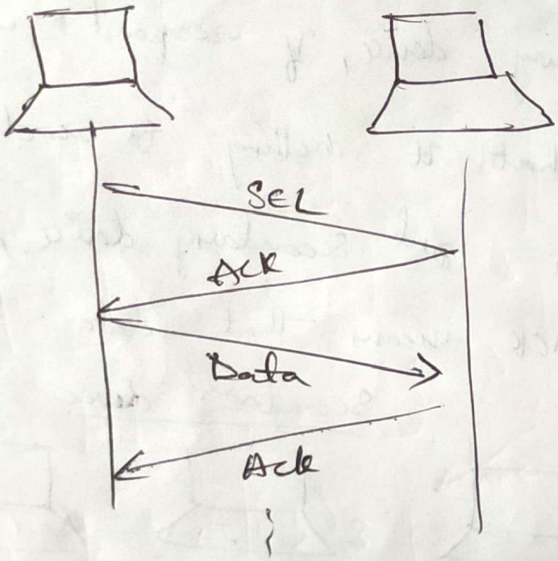


Working of Select:

→ The Select mode is Used when the primary devic has Something to Send.

→ when primary device wants to Send it Selects a device & Send SEL to that device.

→ If that device is ready it will Ack & from then data will be Sending.



II. Flow Control:

→ It is a Set of procedures that tells the Sender how much data it can transmit before the data Overflow at receiver.

→ The receiver has a limited Speed & limited memory to store the data.

→ The receiving device must be able to inform the Sending device to stop the

transmission temporarily before limits are reached.

Control flow

Stop & wait

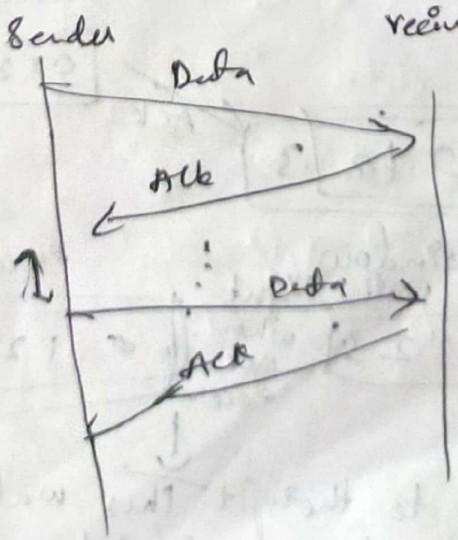
sliding window.

1) Stop & wait:

→ from the name we can say it stops & waits

→ Initially the data is sent from the Sender side to the receiver side & now sender waits for Ack & One Ack is received then it again sends data.

→ It continues till whole is transmitted at the end of the data after receiving Ack Sender send EOT

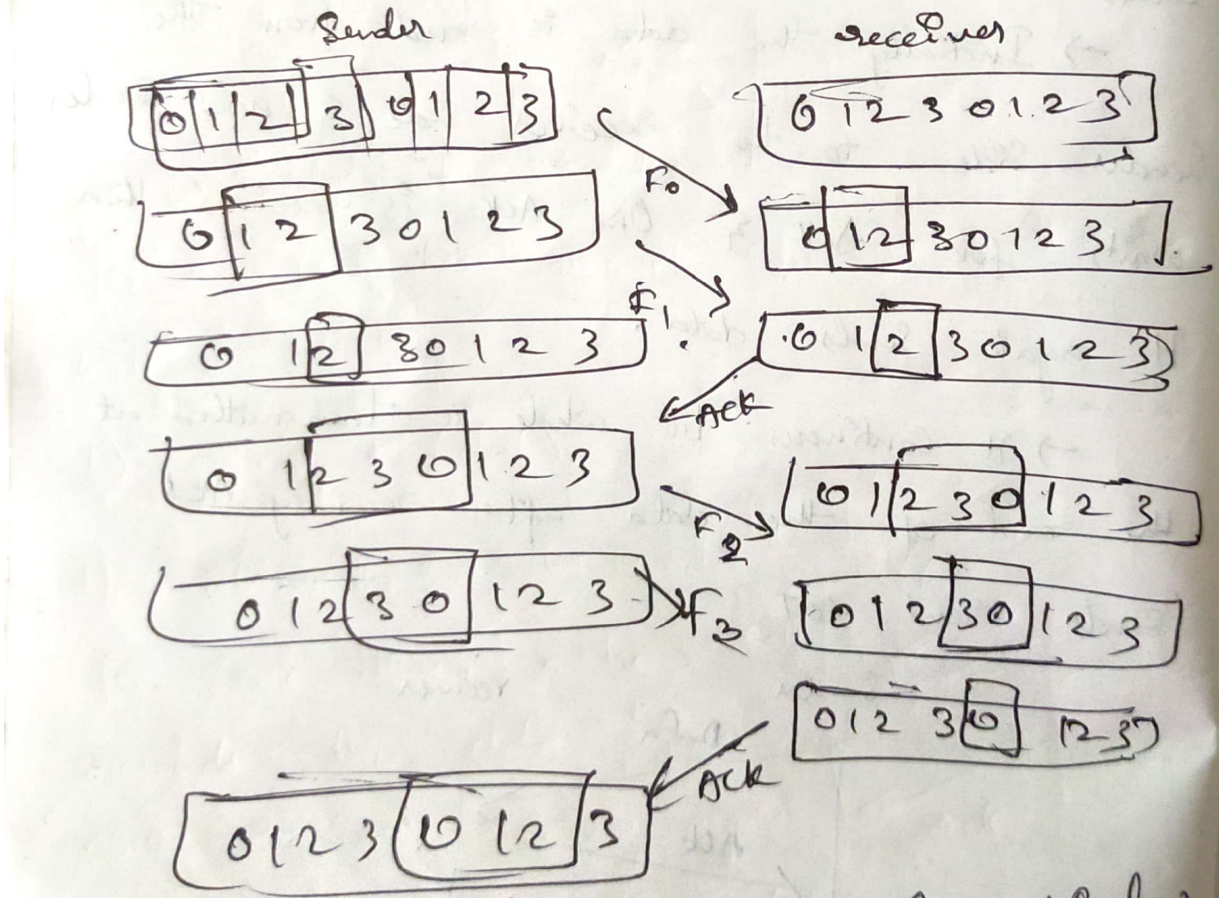


ss buffer

ii) Sliding window flow Control protocol:-

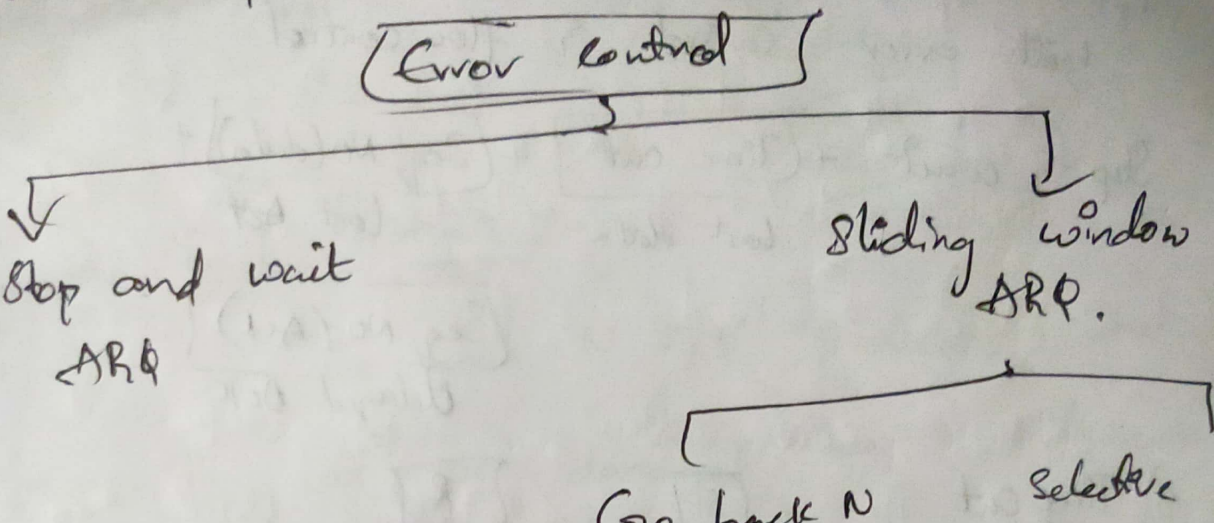
Sliding window is a dyamic window which allow the Sender to transmit a specified number of a data unit befor any ack is received

This is used to Overcome the problem of stop-and-wait protocal that transmit frame in just One direction and One frame at a time



Error Control

Error control is a technique of error detection & retransmission

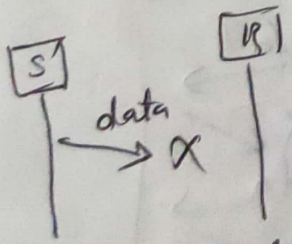


i) Stop and wait ARQ

The problem faced by stop & wait will be rectified using stop & ARQ.

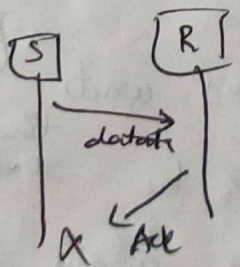
Problem faced by Stop and wait

1) Lost data



Sender wait for ack & receiver wait for data infinite amt of time

2) Lost Ack



Sender wait for Ack for infinite amt of time

3) delayed Act/data after time out on Sender side a long delayed ack might be wrongly considered as act of some other packet

to rectify above problem, we use

Stop and wait ARQ

⇓

both error control & flow control

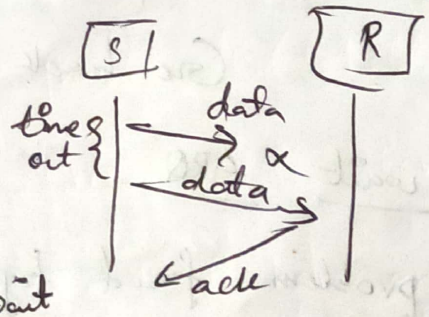
Stop & wait + Time out + Seq No (data) +

Time out → lost data

Seq No (data) → lost Act

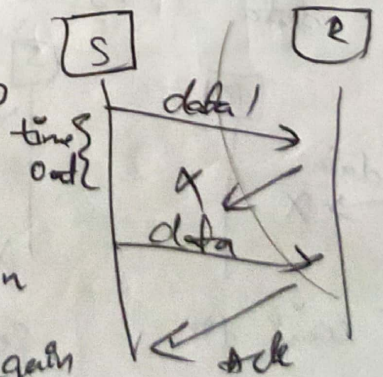
Seq No (Act) → delayed Act

a) Time Out



Here in this situation the Sender will wait for a particular amount of time & then he will resend data.

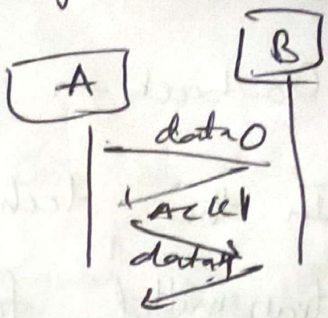
b) Sequence no (data):



Here also the Sender wait for some time & he resends the data again now receiver receive again & this data will discarded as he already has it.

c) delayed Ack :

this is resolved by introducing Seq no for ack also.



ii) Go Back n ARQ :-

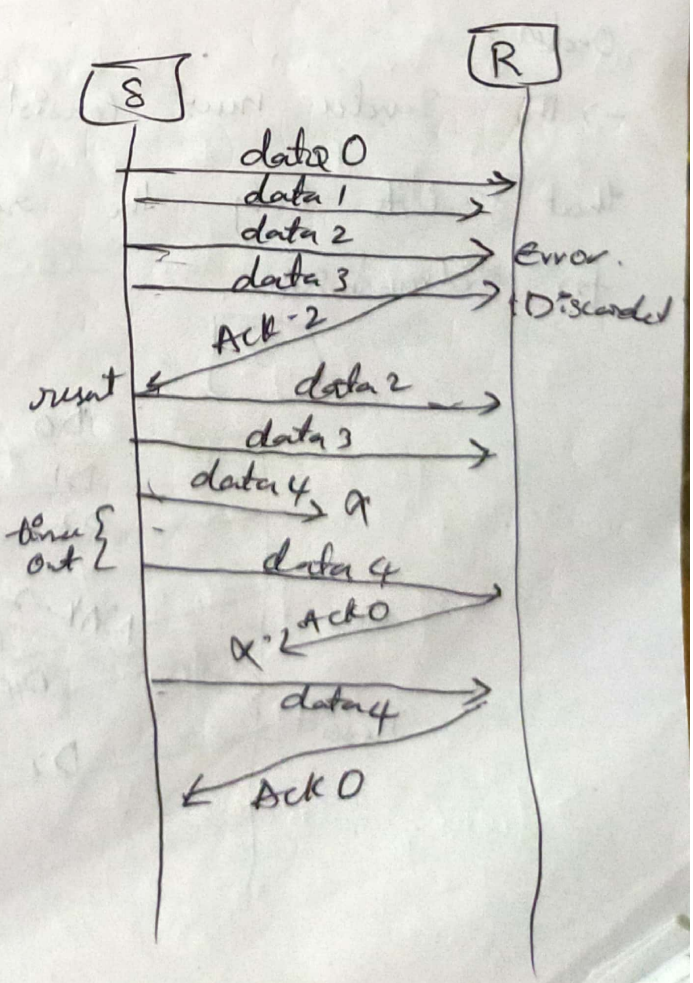
In Go back N ARQ protocal, if one frame is lost or damaged, then it retransmit all the frames after which it does not receive the positive ACK

In the same 3 case the retransmission is done

i) Damaged frame

ii) lost Data frame

iii) lost Ack



iii) Selective reject ARQ:

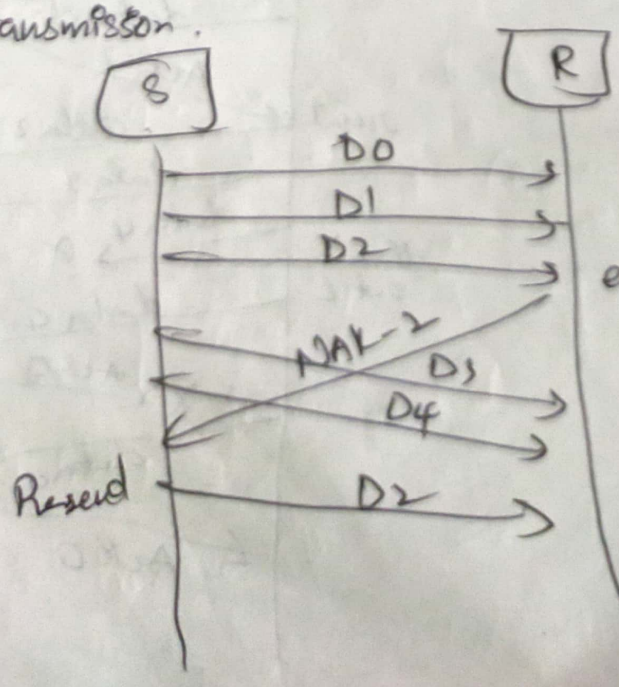
→ In this technique is more efficient than Go-back-n ARQ.

→ In this technique only those frame are retransmitted for which negative ack (NAK) has been received.

→ The receiver storage buffer keeps all the damaged frame on holding until the frame in error is correctly received.

→ The receiver must have an appropriate logic for reinserting the frame in a correct order.

→ The sender must consist of a search mechanism that selects only the requested frame for retransmission.



High level Data link Control: [HDLC]

→ The high level data link protocal (HDLC) developed by ISO.

→ HDLC is a bit-Oriented data link protocal, and it is designed to satisfy many of data control requirements.

→ HDLC protocal has three station

i) Primary station (sender)

ii) Secondary station (receiver)

iii) Combined station (Both sender & reciver)

→ Modes of operation are

i) Normal Response mode (NRM):

This mode is suitable for point to point as well as point to multipoint configuration

ii) Asynchronous Response mode (ARM):

This mode is used for communication b/w primary & secondary stations.

iii) Asynchronous Balance mode

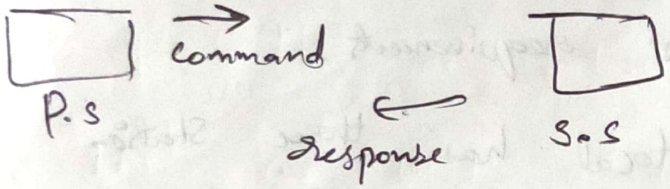
This mode is applicable to point to point communication between combined station.

NRM: 1) One primary station can send commands

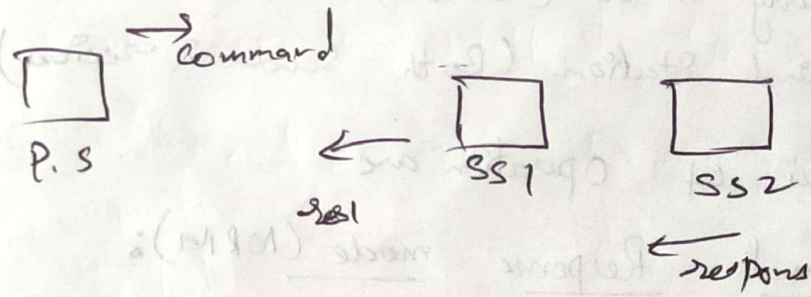
2) Multiple secondary station can send response

3) point to point & point to multipoint

Point to point (NRM)



Point to multipoint (NRM)

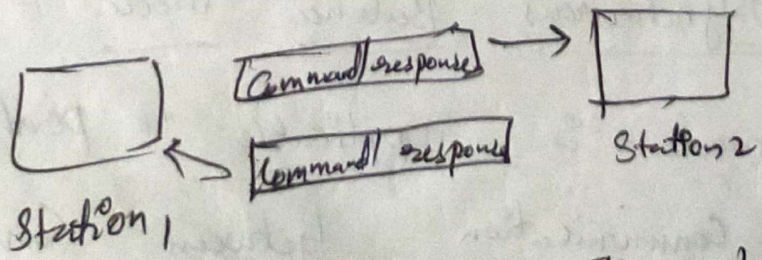


ii) Asynchronous Balanced mode (ABM)

Only point to point

→ Each station can function as primary & secondary.

→ point to point (ABM)



→ frame Structures There are three types of frame supported by HDLC

i) Information frame : Transport → user data, control info

flag	Address	control	User info	FCS	flag

ii) Supervisory (s) frame : Transport only control info.

flag	Add	control	FCS	Flag

iii) Unnumbered (u) frame : Reserved for system mang

flag	Add	control	Managmt	FCS	flag

a) flag : to identify begining & end of the frame.

b) Address : Contain the address of the secondary station.

c) Control : Used for error & flow control.

d) Information : User data (or) management info

e) FCFS → frame check sequence error detection field.

Network : A collection of computers, servers, main frames, network or peripheral device or other device connected to one another to allow sharing of data

Ex : Internet.

Unit-4

Types of networks:

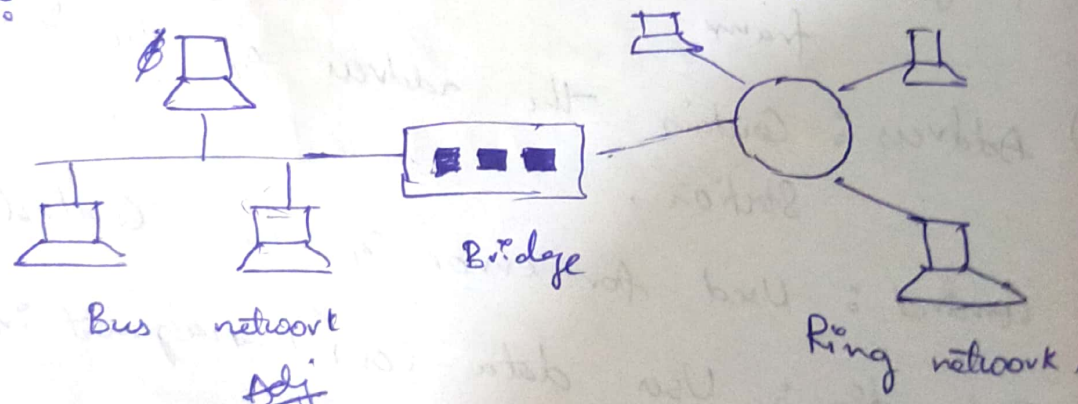
i) local Area Network (LAN):

It is also called as LAN & designed for small physical area such as an office, group of building or factory.

LAN's are used widely as it is easy to design & trouble shoot.

we can use different types of topologies through lan, these are star, ring, bus, tree etc.

Ex:



~~Adj~~

→ private Network

→ high Speed.

ii) Metropolitan Area Network (MAN):-

→ It was developed in 1980's

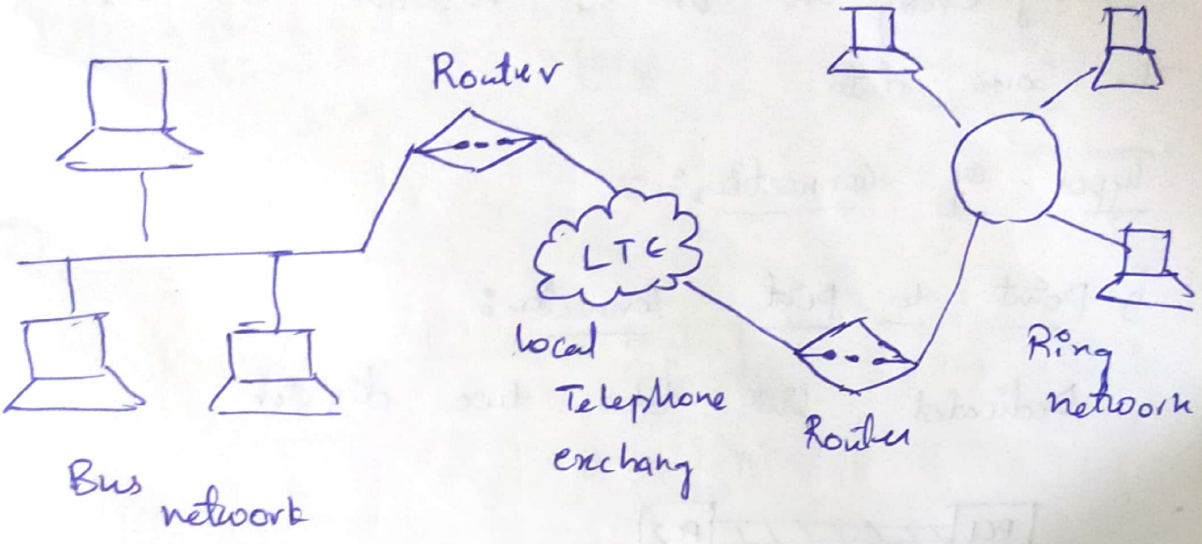
→ Its basically a biggest version of LAN

→ It is also called MAN and it, the similar technology as LAN.

→ It is designed to extend over the entire city.

→ Both ~~pairs~~ & private or public Company

Ex: different branches of clg's, company.



→ 50 km range.

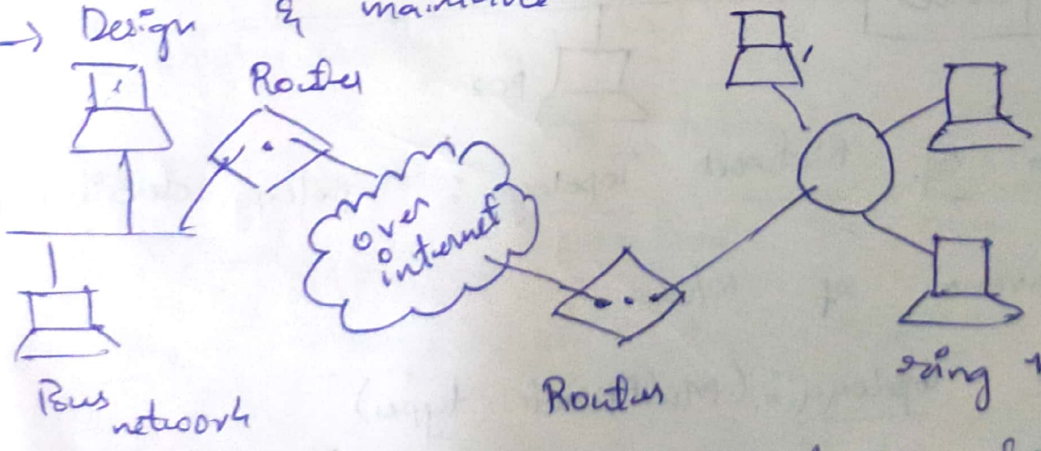
→ optical fibes are used.

iii) Wide Are Network (WAN):

→ long distance such as Country/State.

→ It can be public or private network.

→ Design & maintance is complex.



→ Communication medium used are Satellite, public telephone network which are connected by router.

→ Expensive

→ Security is real issue here

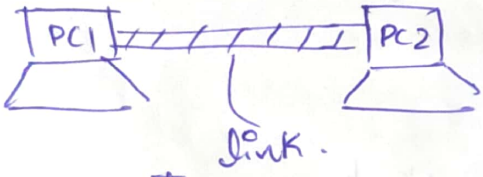
→ Setting up a network can be expensive

→ ~~Every~~ Every One on the network can use the same data.

Types of Connection:-

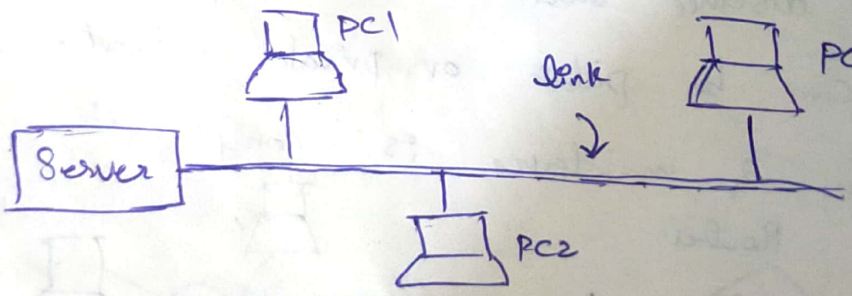
i) Point to point Connection:

Dedicated link b/w two division



ii) Multi~~point~~ port Connection:

More than two devices share a single link.



→ Types of Network Topology: Topology describes appearance of n/w.

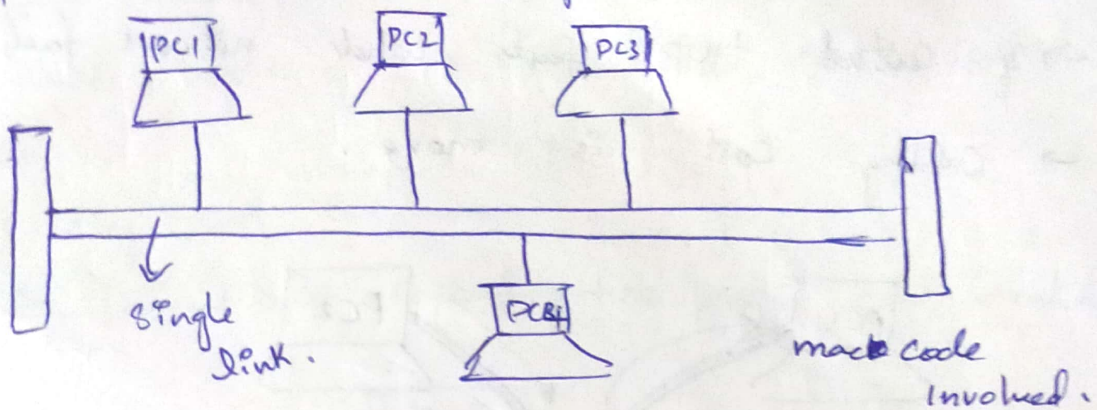
i) Bus Topology: (Multipoint types)

→ Easy to install, use for small network

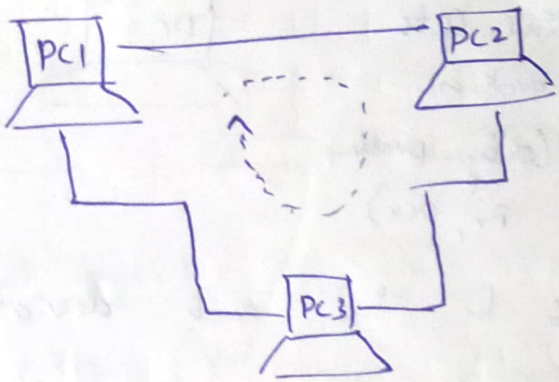
→ Cheap → Easy to expand

→ Slow speed as only one system can transmit at a time.

→ failure in Cable bring down whole n/w



ii) Ring Topology



In this each computer is connected to the next computer with the last one connected to the first.

- Multipoint data Connection.
- Token passing is used.

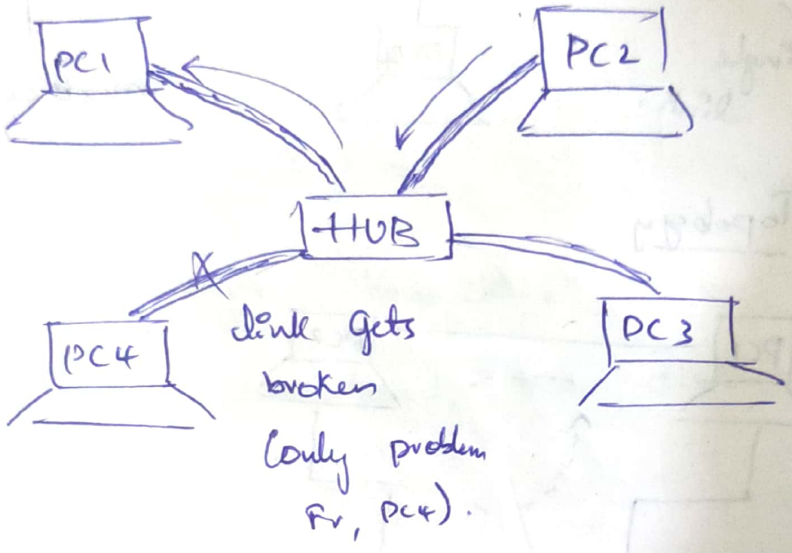
dis
- fault in any link bring down entire n/w.
- Difficult to troubleshoot the ring.

iii) Star topology:- All wires from the Computers go to a central location having a device called HUB.

→ All communication goes through HUB

→ If central HUB fails, whole network fails.

→ Cabling cost is more.



iv) Mesh topology: In this each device has a dedicated point-to-point link to every other device.

→ due to dedicated link, there is no traffic problem.

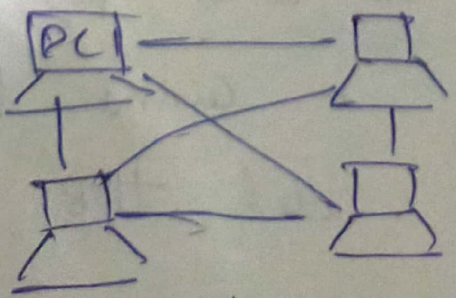
→ failure of one link doesn't affect entire n/w.

→ Expensive due to high cabling cost

→ More Secure & private

→ Easy fault diagnosis (point to point).

→ If we have n device => $(n(n-1)/2)$ link are needed.



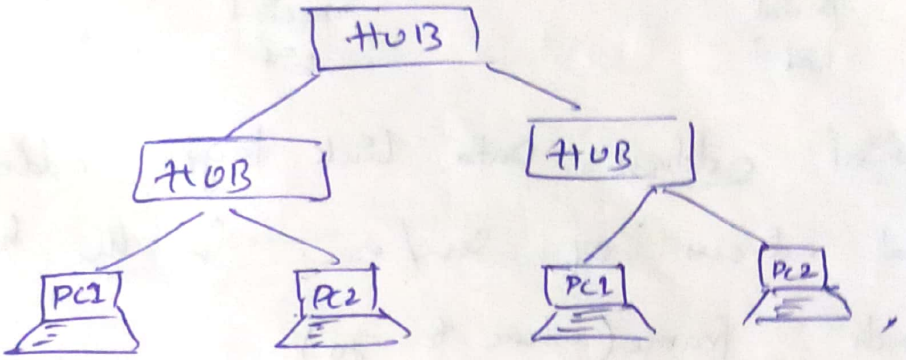
Mesh topology

v) Tree topology: Variation of Star topologies.

-> Node in a tree are linked to a central hub.

-> Cabling cost is more.

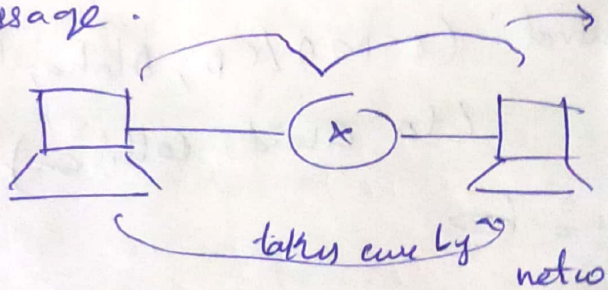
-> On failure of central HUB entire n/w breakdown



Data link layer:

-> It is the 2nd layer from the bottom. OSI

-> It is responsible for node to node delivery of message.



-> Error Correction will be done.

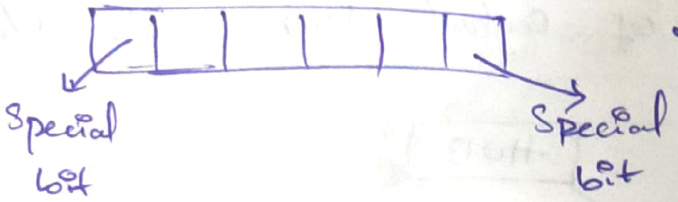
-> The packets are received from network layer then are divided into frames.

-> when the next node frame buffer is full it stops sending.

-> They use switches & hubs.

Function of Data link layer:

→ framing: packets received from the network layer are divided into frame.



like start & end.

→ physical address: Data link layer adds physical adress of sen/rec. in the header of each frame (where to go)

→ Error Control: (CRC, checksum, parity)

→ flow Control: Once buffer is full then stop sending.

→ Access control: (CSMA/CD, Aloha, Token ring) (to avoid collision).

MAC Sublayer:

→ The medium Access Control (MAC) is a sublayer of the data link layer of the Open System interconnection (OSI) reference model for data transmission.

Application layer

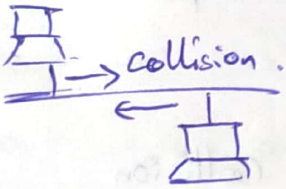
↓

-> To avoid collision of data we go for MAC.

-> Collision may occur when the data shared by 2 (or) more in a shareable link then collision occurs.

-> If it occur the data will be lost.

-> Commonly observed in bus (T)



-> MAC is responsible for the flow control & multiplexing for transmission medium.

-> It control transmission of data packet via remotely shared channels.

-> Ex: Broadcasting (Shared medium)
Ex: video call, audio call etc.

Protocals

- Random Access protocal
  - Aloha
  - CSMA
  - CSMA/CD
  - CSMA/CA
- Control Access
  - Polling
  - Token ring
- Channalisation protocal)
  - FDM
  - TDM.

I) Random Access protocol :-

No priority based they send (message) acc to their wish (no priority).

Aloha

(Pure Aloha) (Slotted Aloha)

a) Pure Aloha : Here Once data is ready to send the system starts sendings. No checking or anything is done here.

-> high chance of collision

-> Here concept of Ack. is also included (once data is sent succesivefully Ack is returned back to sender).

-> If a system which sended data did not receive ack then it will understand that collision occured & it sendes data after some random time

-> LAN based protocol.

Slotted Aloha :

-> Here time is divided into slots (i.e transission time).

-> Here at a time all system Connot send data.

-> Transmission would also start when its time slot starts.

→ Here also collision is possible.

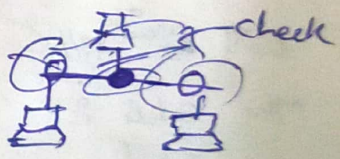
→ If many stations start sending data at exact movement of time then collision occur.

ii) CSMA : Carrier Sensor Multiple Access :

It removed the drawback of Aloha & CSMA was developed that sensed the channel before initiating in order to achieve greater efficiency.

i.e each of the device that are connected to the network are able to examine the state of channel (only their front) before sending info. transmission take place only, if communication channel is idle.

(not entire channel)



CSMA

1 persistant

data is sent once it notices its starting is free high chance of collision & it check again again when its free

0 persistant

Here again & again checking is not done it check for a random time Even here their is collision chance but less than 1 persistant

p persistant

Combination of 1 persistant & 0 persistant it depends on p value probability.

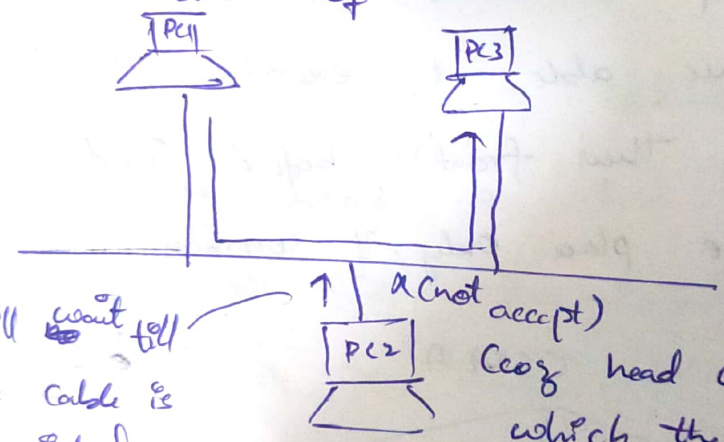
CSMA (wired) - CD

→ Carrier - Sense multiple Access with Collision Detection.

→ The drawback CSMA/CD is a advanced version of CSMA. here collision is also detected.

→ It's also used Under ethernet in lan technology

→ Here we dont Use any concept of Ack, coz it ↑ chance of collision



→ Let we assume a case if PC1 sending data to PC3 & at that exact moment only PC2 is sending data to PC3

→ Then could be a chance of collision.

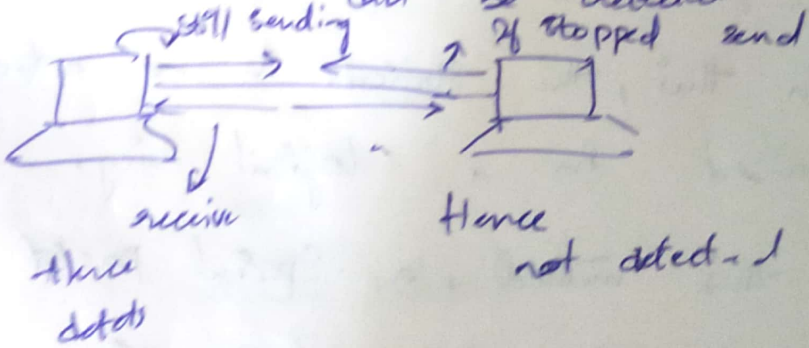
→ Collision Detection can be done when collision occurs the signal from collision (after collision the signal will be sent to the station. If PC1 is sending data, if recieved the collision signal it will understand that it

data was collided.

(Note at the movement when the System received collision signal it should at send data else it can't detected

ex

Now collision signal will sent & if at that movement also if the System is sending data then it can be detected.



CSMA/CA : Used wireless & used Acc.

I Controlled Access: In this technique, all the station consult one another to find which station has the right to send.

a) polling: works with topologies. In this one device is designated as primary station and the devices are Secondary Station.

- All data exchange must be made through the primary device.

2-function: Primary wants to send data.

Select: To select a particular station to send data (for sending)

Polling: Individually asking when it needs data (for receiving)

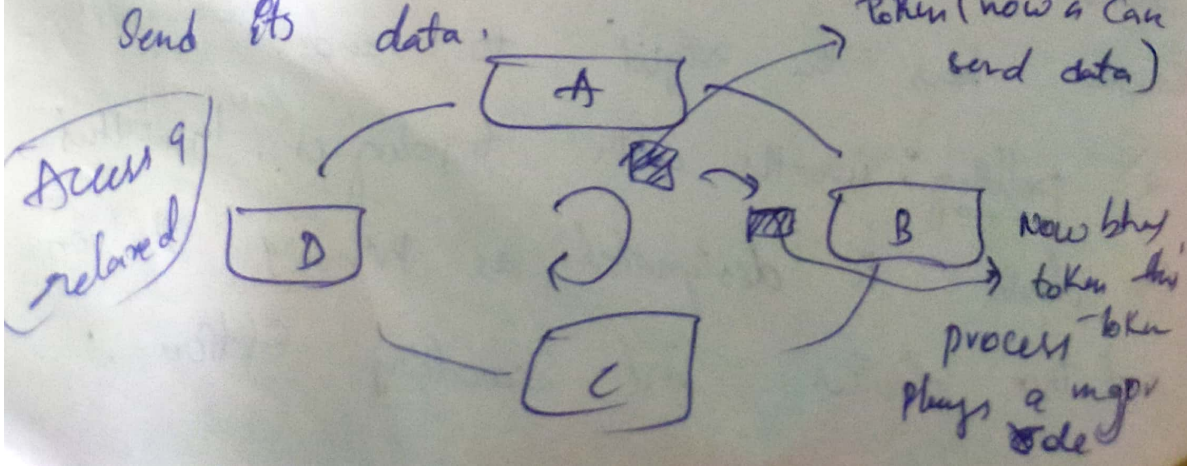
→ primary wants to recieve data

b) Token passing method:

In this, the stations in a network are organised in a logical ring.

In this method, a special packet called a token circulates through the ring.

The possession of the token gives the station right to access the channel & send its data.



IEEE Standard (802)'s

Institute of Electrical & electronics Engineer.

→ 802.1 to 802.20

Standard	Name	explanation
802.1	Management & Internet working	Covers routing, bridging & inter network communication
802.2	Logical link Control	Cover error control & flow control over data frames.
802.3	Ethernet LAN	covers all forms of ethernets (10 MBps to 10 GBps).
802.4	Token Bus LAN	"
802.5	Token Ring LAN	
802.6	MAN	
802.11	wireless network	
802.12	High speed network	

802.2 Logical Control

802.1 Management.	802.3 ethernet lan	802.4 Token bus	802.5 Token ring	802.6 MAN	8029 Data n/w	811 wireless lan	12 high Speed lan

IEEE 802.3

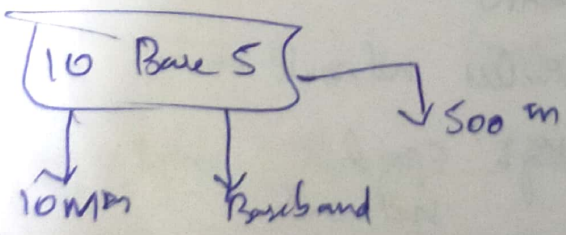
→ currently widely known Standards are the Ethernet (IEEE 802.3)

Types of Ethernet

- Std Ethernet → further divided
- fast ethernet
- gigabit ethernet
- Ten gigabit ethernet

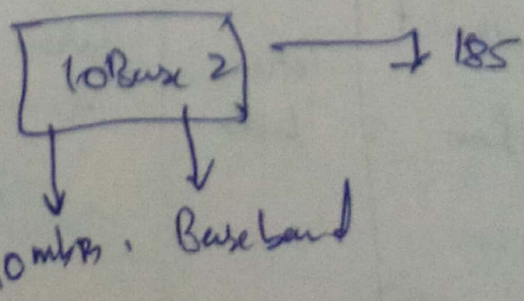
i) 10BASE5 (or) Thick ethernet

→ Here we Use coaxial Cable
→ max length of transmission can be 500m
→ max no. of stations 100
→ topology Used is bus.



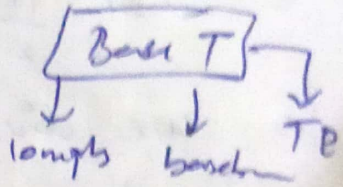
ii) 10 Base 2 or Thin ethernet

→ Coaxial Cable
→ 185m
→ 30
→ bus



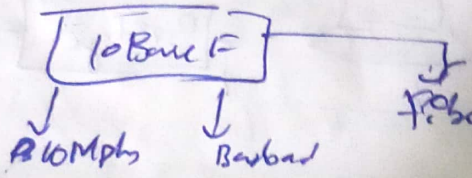
iii) 10 Base T or twisted pair ethernet:

→ Here we use twisted pair
→ max length of transmission can be 100m.
→ max no. of station 1024
→ topology used is star



iv) 10 Base F or fiber ethernet:

→ Here we use fiber optic
→ max length of " " " 2000m
→ max " " " 1024
→ t- " " "



Bridged ethernet: (variant)

Bridge is a device which is inserted in std ethernet lan to raise bandwidth & separate collisions.

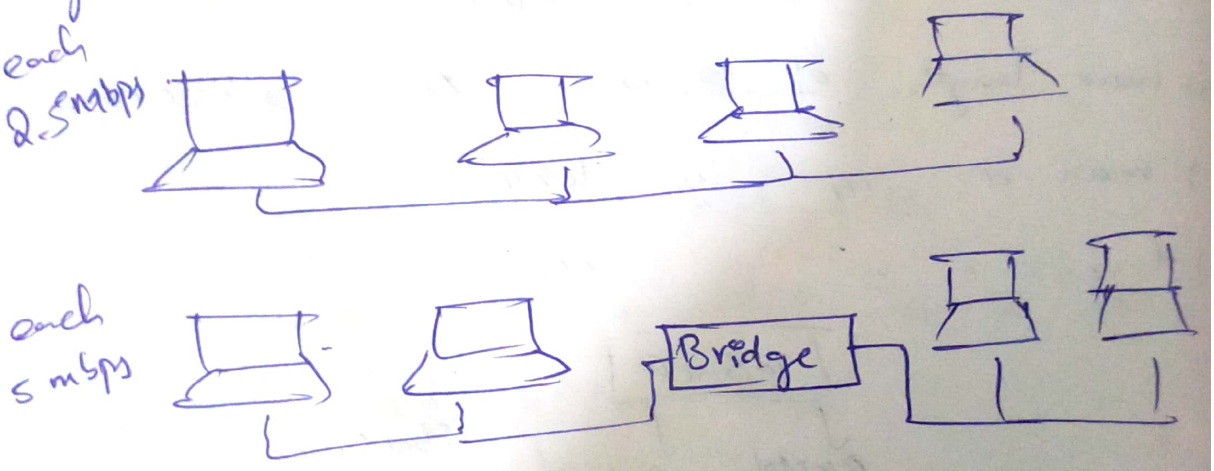
→ In Unbridged ethernet, 10 mbps is shared among all stations.
→ A bridge divides the n/w into two or more networks (raising the bandwidth)

→ So if without bridge if one device is this it can have 10Mbps but when we increase the no. of devices like 2 devices

$$\Rightarrow \frac{10}{2} = 5\text{Mbps}$$

→ So we divide devices with bridge.

This concept helps a lot when we many system



→ reduce the chance of collision.

→ If 100 system are connected collision chance is high.

→ If we divide it 4-part the collisi rat

Here we can bridge for our adj

Switched ethernet :

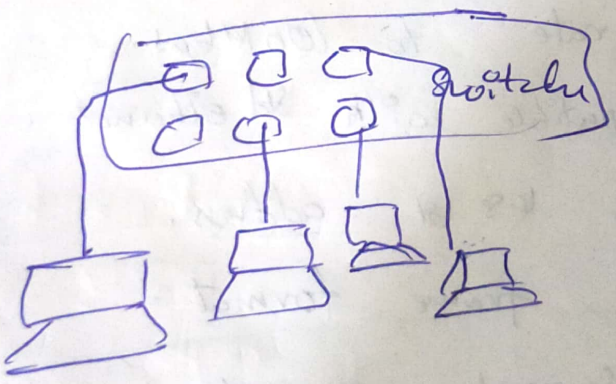
→ Same idea as bridged LAN the extension of it is switched ethernet.

→ Here we use switches to connect ethernet LAN to host computer.

→ Here we can connect n no. of station.

→ Acc to the no. of ports on the switch we can connect

→ Here here for each network we can reach 10Mbps & the collision also reduce.



Full Duplex ethernets (two wired)

→ One limitation of 10Base 5 & 10Base 2 is that communication is half duplex. (Single wired)

→ This mode increase the speed from 10mbps to 20 Mbps.

→ Instead of using one link like station & switch we use 2 link here

→ One transmit & another receive.

→ Hence no chance of collision.

→ Hence no need of CSMA/CD - to detect collision

→ Hence a station send & receive data independently.

→ No chance of collision.

Fast ethernet:

→ Transmit data 10 times faster at a rate of 100Mbps.

→ goal of fast ethernet

→ Upgrade data rate to 100Mbps.

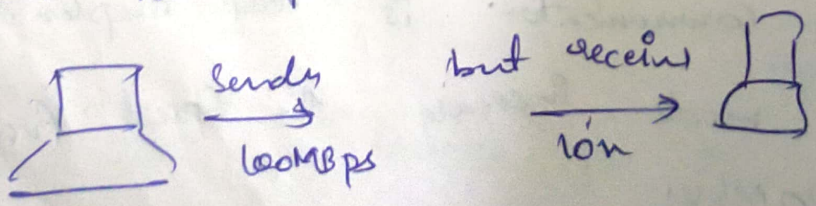
→ Make it compatible with Std ethernet.

→ Keep the same 48 bit address.

→ Keep the same frame format.

→ Here only support star topology.

Autonegotiation: Combination b/w station able to data rate speed.



there sender slow down to 10MBps

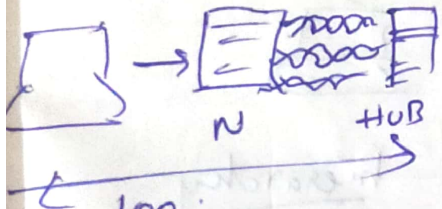
→ Fast ethernet may be point to point or star

fast ethernet

100 Base TX
(two wire
Category
5 UTP)
Unshielded
twisted
pair
100 m
2 type 5 UTP
NRZ
encoding

100 Base FX
(Two wire
fiber)
Optical fiber
2000m
2 Optical
Cable
8 bit or 6 bit
Ternary encoding

100 Base T4
(four wire
Category 3
UTP)
twisted pair wire
100m
4 Type 3 UTP
8-bit or 6 bit
Ternary en



100
2

2

4 wired

Gigabit Ethernet :

→ upgrade data rate to 1 Gbps
→ Compatible with fast & std ethernet.
→ Uses same 48 bit address
→ Use the same frame format
→ Support autonegotia also
→ In full duplex mode, there is no collision & max length of the cable is determined by the signal.

CSMA/CD

→ In half duplex mode we use (~~CSMA/~~CD)

3 methods

traditional, as in std ethernet

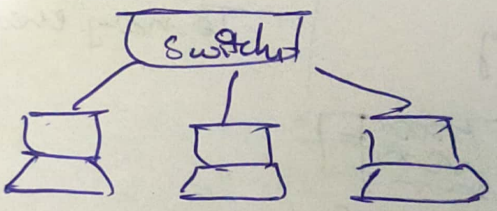
Carrier extension increase the length

frame bursting multiple types of frame are sent.

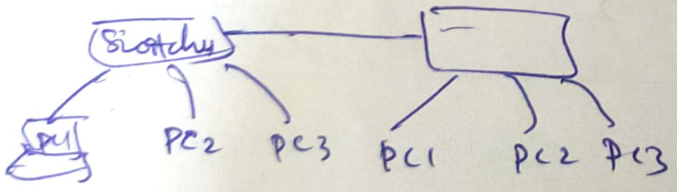
We can implement gigabit ethn in 4 way

point to point

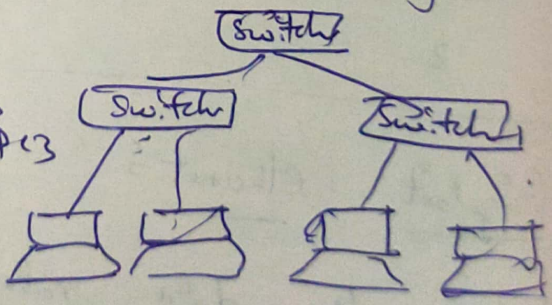
star



Two star



star hierarchy



Gigabit (E)

1000Base SX (2 wire Short wave fiber)

1000Base LX (two wire long wave fiber)

1000Base CX (2 wire copper)

1000Base T (4 wired UTP)

550m	500	25	100
no. pairs 2	2	2	4
NRZ encoding	NRZ	NRZ	NRZ

10 gigabit (E):

-> Upgrade data to 10 Gbps
-> make it compatible with 8d fast & gigabit (E)
-> Use full duplex
-> Use the same frame format
-> Interconnect LANs to MAN or WAN.

3 types

10 GBase S	10 G Base L	10G Base E
Short wave 850nm multimode 300m	long wave 1310 nm Single mode 10 km	extended 1550 nm / Single mode 40 km

Fiber Channel:

A fiber channel is a high speed n/w techn used to connect Servers to data storage area network.

It handle high performance disk storage for applications in many corporate n/w & it supports data backups & provide speed - faster distance - longer flexibility T.

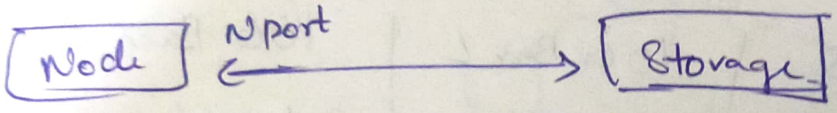
Topologies :

→ point to point topology
→ fibre channel Arbitrated loop
→ Switched fabric topology (✓)

i) point to point :

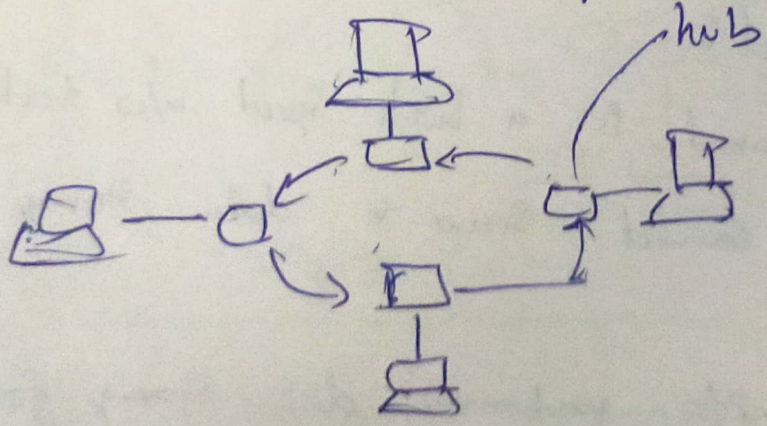
This is the simplest of all topologies & here a single link connects only two ports.

→ less expensive because no hubs
→ 10Km (if multiple 500m)



ii) Fibre channel Arbitrated loop :

→ similar to ring



→ Here arbitrated signals are sent to check channel is free or not before sending data.

→ It Can Conned 127 device

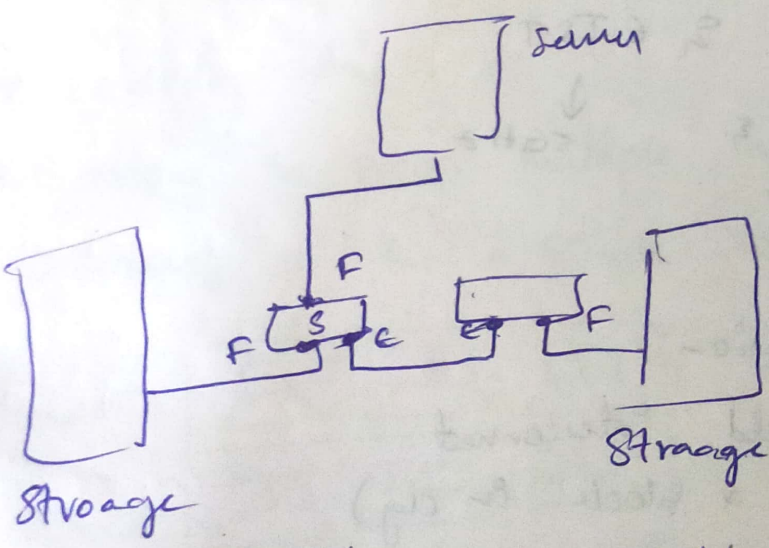
→ No data Security (which travelling anyone can read it!

→ If one device fails the msg or data can't to passed (to recover it we use Hubs)

iii) Switched fabric topology:

→ Most Used now a days.

→ network of switches in a fibre channel.



2 layer & 3 layer switching

Unit - 5

Wireless LAN:

WLAN

→ ~~other~~, a wireless local area network, it is used to establish a wireless connection b/w 2 or more devices.

→ we can use a wireless distribution method within a limited area such as in school or office etc.

→ popular std Organization support WLAN's are IEEE & ETSI

↓ ↓

2.4 GHz & 5GHz 5GHz

→ Application

→ lan extension

→ cross build interconnect (b/w a block in city)

→ Ad-hoc networking.

→ nomatic access (OTG via autions (Dress vehicles).

Features

→ flexibility, easy to add more devices

→ No problem with external conditions like floods, rain etc.

→ Increased mobility & collaboration

User can move within the environment without loosing connection

→ no wiring difficulties.

Disadv

→ transmission quality is low

→ wireless equipment is costly

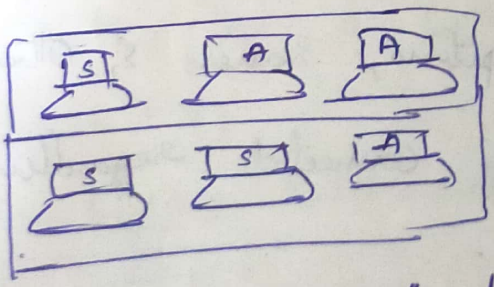
→ less Safety & security (Cracking is possible).

VLAN: Virtual LAN

→ It is a custom network created from one or more existing lan's.

→ It allow to group multiple networks (both wired & wireless) to the a single logical n/w.

Eg



Here the system are mixed hence.

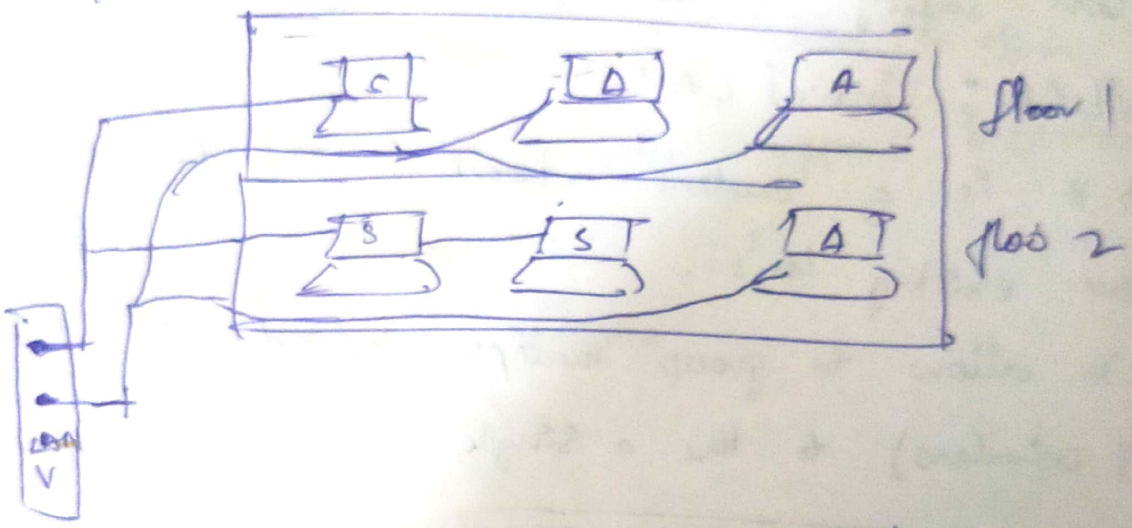
If they are connected normally then this will be issue that the Accounting info is also sent to shipping & shipping data is sent to accounting which is of no use

If you want to rearrange them we need to shift shipping dep machine to the floor1 & move Acc mach. to the floor.

which a hectic work as all wires Cables & every need to the moved & changed.

→ Instead of doing this we use VLAN

→ Using VLAN we can create a virtual network & separate traffic.



→ VLAN the computers, Servers & other network devices are logically connected regardless of their physical location.

Adj → Improve Security

→ Traffic management

→ make a network Simpler.

IEEE 802.11 (wifi) / Architecture:

→ It provides 2 types of services

i) BSS

ii) ESS

→ Basic Service Set (Station & AP (Access point) with same radio coverage)

Extended Service Set (Collection of BSS is ESS) Connected through AP.

→ Station (STA) - mobile nodes

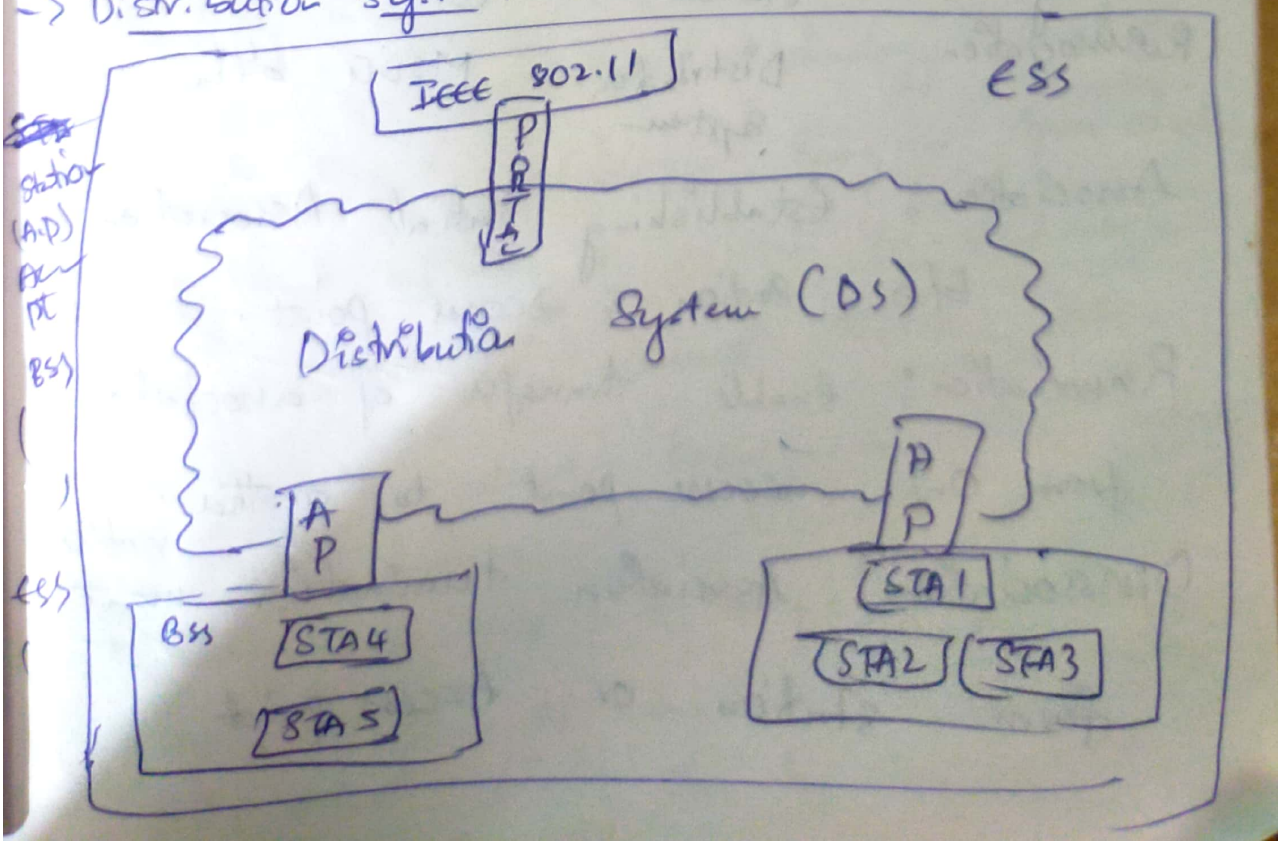
It can be any device or can be a mobile device.

→ Access point (AP): Stations are connected to access point.

Every station is communicate with the help of Access point then ~~to~~ BSS

→ portal: Acts as a bridge to other wired network.

→ Distribution System interconnection two several BSS.



IEEE 802.11 Services:

IEEE 802.11 define nine Services that need to be provided by the wireless LAN to provide functionality equivalent to that which is inherent to wired LANS.

2A3D IMPR

Service	Provider	Used to Support:
Association	Distribution System	MSDU delivery
Authentication	Station	LAN access & Security.
Deauthentication	Station	LAN " &
Dissociation	Distribution System.	MSDU Delivery
Distribution		MSDU
Integration	"	LAN
MSDU Sr	Station	LAN
Privacy	Station	LAN
Reassociation	Distribution System	MSDU deli

Association: Establishing Initial Association s/w Station & Access point.

Reassociation: Enable transfer of association from One access point to another.

Disassociation: Association termination note ~~note~~ from Station or Access point

Authentication: Established lan access & security connection.

Deauthentication: terminates lan access & security connection

Privacy: Prevents msg contents from be read by Unitened recipient

Distribution: A station Uses the distribution service every time it sends MAC frames across a distribution system.

Integration: the integration service enables the delivery of MAC frames through a portal to a distribution system & 802.11.

Bluetooth:

→ It is a wireless technology based on mobile computing technology. Being an Open wireless technology std, it is used to send or receive data to connect device.

→ It is also known as IEEE 802.15 std.

→ Bluetooth 2.4 to 2.485 GHz (range) (bandwidth)

→ The range of bluetooth technology over which data can be exchange is

less than 10mtrs but the latest version of bluetooth 5.0 can exchange data in a range 40-400 mtrs (@ 1mbps)

Application → speaker, headphones, headset
→ Data transfer app

Adv → wireless technology
→ very simple to form piconet
→ cheap technology
→ Robust. → low energy consumption.

Dis
→ low in bandwidth
→ data transmission range is constant as it is very less.

Architecture:
→ An Arc of bluetooth is called piconet
→ piconet offer the technology with the help of which data transmission occurs based on the node Master & Slave nodes
↓ sender ↓ receiver.
→ A master node is a node from which data is being sent & Slave node in which the data is received.

→ Ultra high frequency & short wavelength radio wave through which data transmission occur.

Types

i) piconet

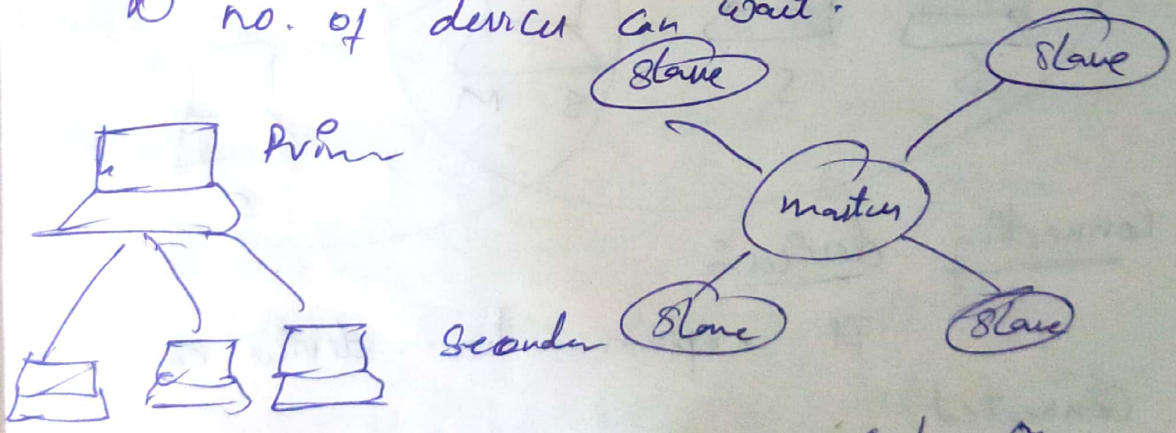
ii) Scatternet

piconet : It is a bluetooth n/w that consists of 1 primary (master) node & 7 active secondary (slaves) nodes.

∴ max no. of nodes in piconet → 8

max no. of devices = $2^8 - 1 = 255$

no. of devices can wait.



→ Here data transmission can only occur b/w master & slaves. and not b/w slave & slave.

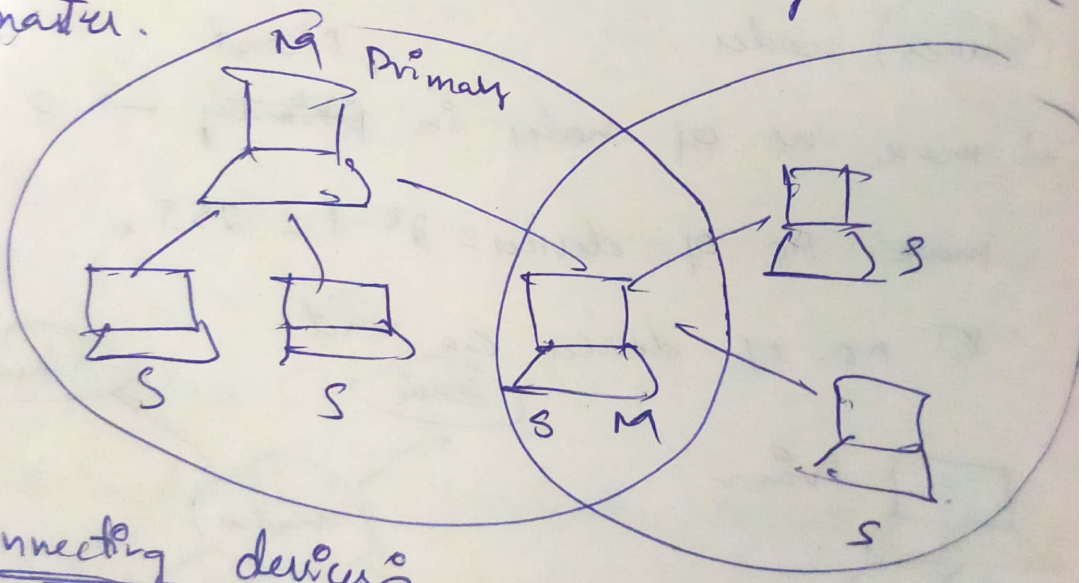
→ If the connection from master node gets disconnected the whole piconet is ~~follow~~ get disconnected.

ii) Scatter net :

→ It is formed by combination of piconet

→ A slave in one piconet can act as a master or primary in other piconet.

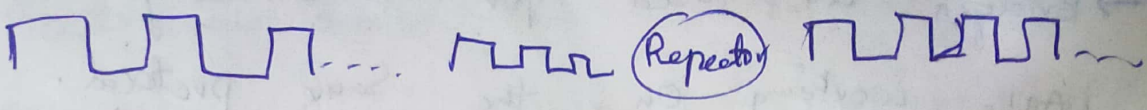
→ Such a station or node can receive msg from the master in the first piconet and deliver the msg to its slave in other piconet who it acting like a master.



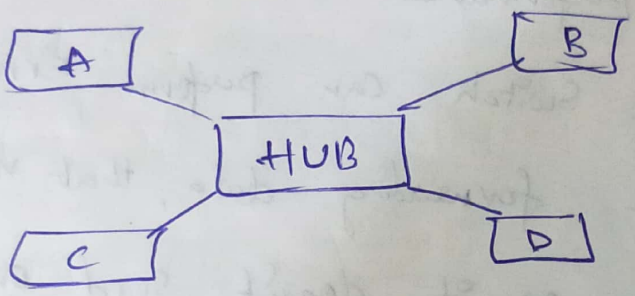
Connecting devices :

It explain how devices can be connected.

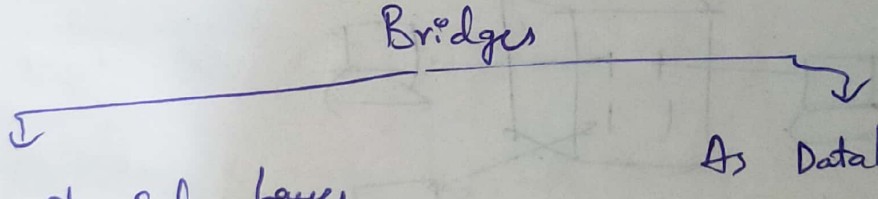
i) ~~Hoop~~ Repeater : A repeater operates at the the physical layer. Its job is to regenerate the signal over the same n/w before the signal become too week or corrupted so it can be transmitted over the same network



ii) HUB: A hub is a multiport repeator. A hub connects multiple wires coming from different branches (like star topology!)



iii) Bridges :- This device operates in both physical & data link layer.

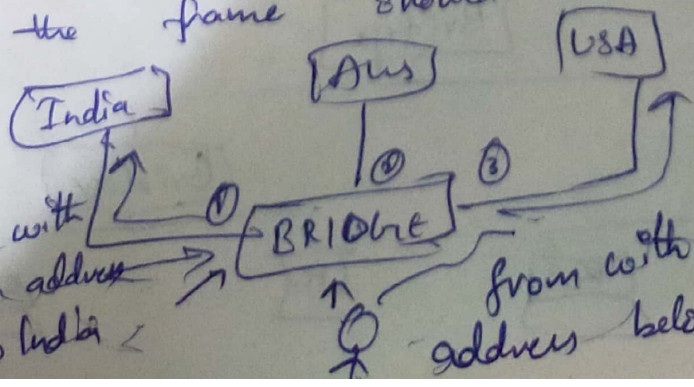


-> It regenerates the signal

-> checks mac Address of the frame

Note: A Bridge has filtering capacity.

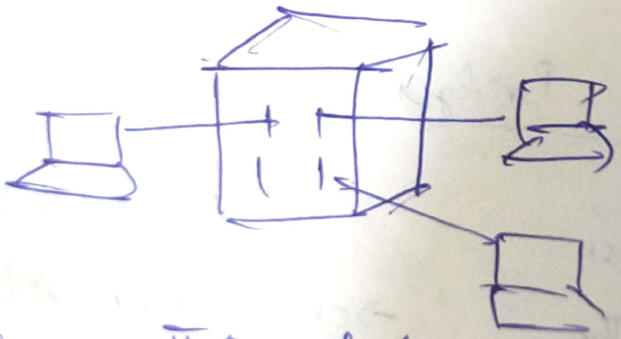
-> Bridge check the destination address of a frame and can decide from which outgoing port the frame should be sent.



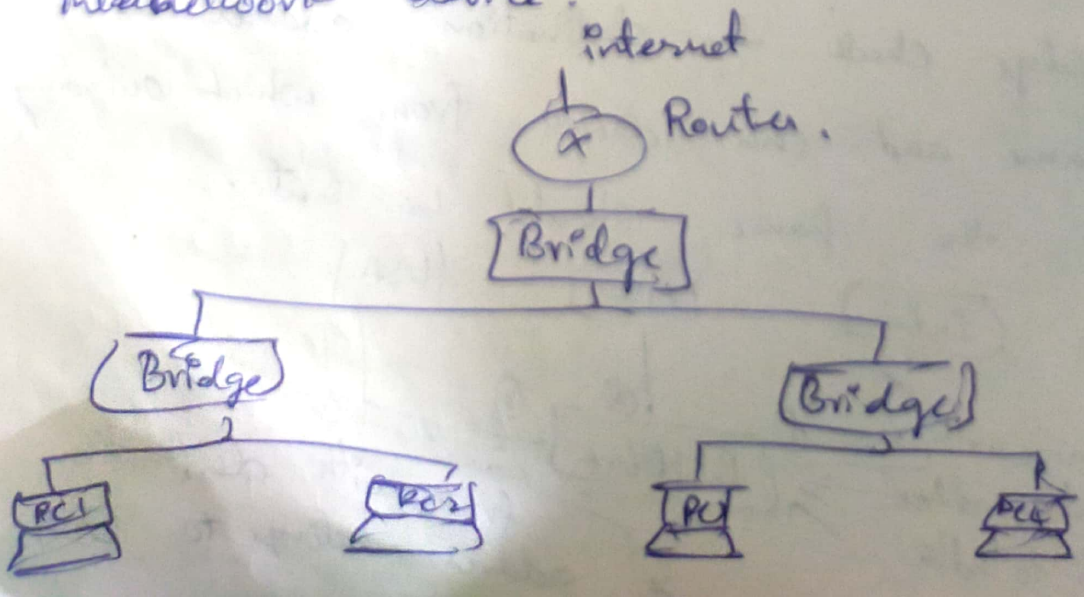
→ Bridges are used for interconnecting two LANs, working on the same protocal.

iv) Switches: A Switch is a multiport bridge with a buffer & is designed to boost the efficiency & performance.

The Switch can perform error checking before forwarding data, that make it very efficient as it doesn't send or forward packet that have errors.



v) Routers: This device operates in physical, data link layer & network layer. It is an interactwork device.

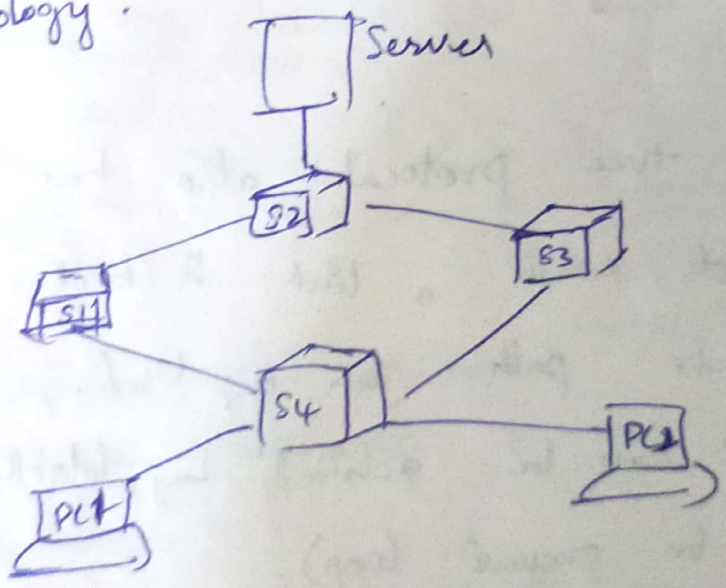


→ Router are device that Connect two or more network. They have both hardware & soft-ware.

vi) Gateway: when the networks that must be Connected are Using Completely different protocals from each other, a powerful device called gateway is Used.

Spanning tree bridge:

Spanning tree bridge protocal is Used b/w switches to ensure that loop is created in a topology.



normally

If PC1 sends a packet to S4 then it sends to all S_1, S_3 & PC_2 from their it Spread Out like

PC1 → S4

S4 → PC2, S1, S3

S1 → S4, S2

S3 → S4, S2

S3, S2 → Server

Server → S2

⋮ ⋮ This Continue, to break this we need remove a Connection.

But its not an efficient way so we use Spanning Tree protocals to achive by finding shortest path & remove loops.

→ Spanning tree protocal also has ability to detect when a link is broken so that an alternate path can be used.

(It can be achived by blocking 1 bridge to prevent loop).

So question is which to block.

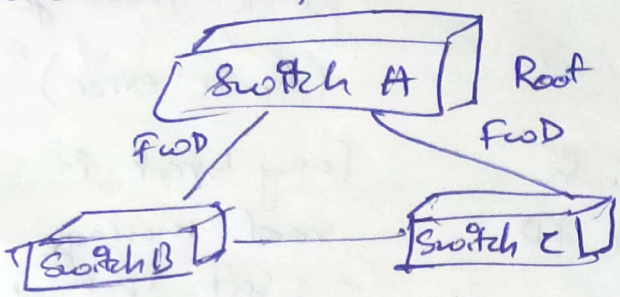
i) Elect a Root-Bridge

ii) Place rod interface into a forward State (FWD).

iii) each non root switch selects its Root Port.

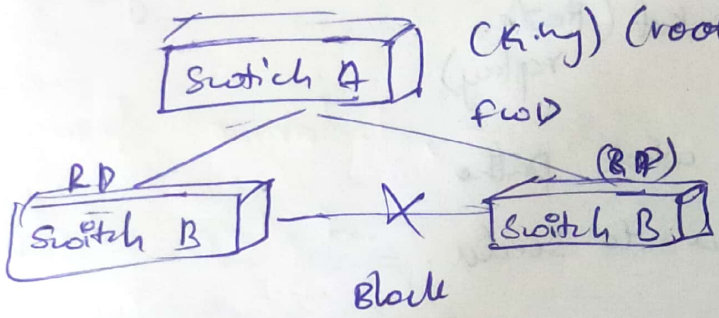
iv) Remaining disk choose a Destination port.

v) All other ports are put into a Block State



A → BC
B → AC
C → AB
: :

to rectify



Dynamic Source Routing Protocal:

→ Discovers the route blw Source & destination when required.

→ Operation is based on Source Routing Sender knows to complete path.

→ Intermediate nodes do not maintain routing information to route the packet to destination.

→ Less Network overhead as the no. of msg exchanges blw nodes is very low.

phases of DSR protocal

Route Discovery

Route maintenance

Route Discovery

↳ RREQ packet

Root request

Source Node ID

Destination node ID

Route maintain

↳ RERR message (Route error)

[any break in root message sent to near by node]

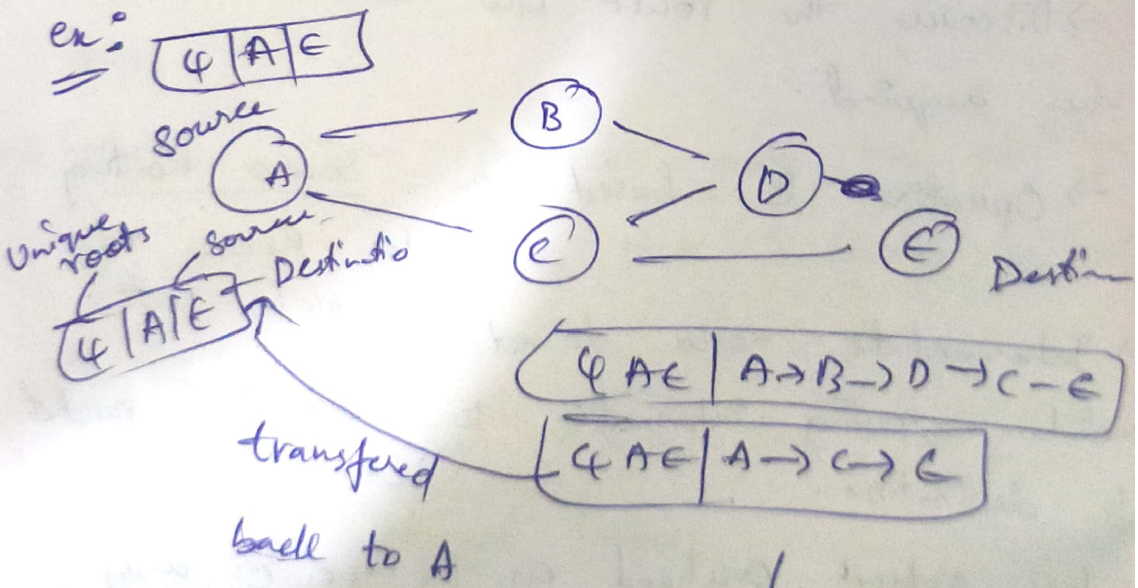
↳ RREP Packet (Route replay)

↳ sends the whole path from receiver to sender.

Route cache :

stores the path follows.

ex:



↓

Shortest Q A E is selected.

So