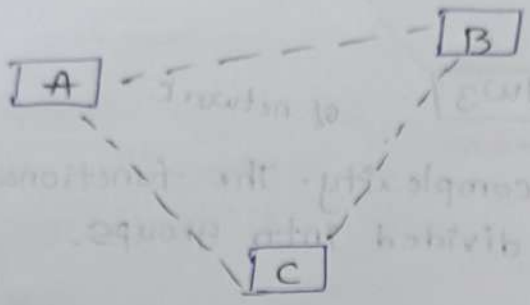
*Computer Networks:-

>> Exchange of information from one place to another

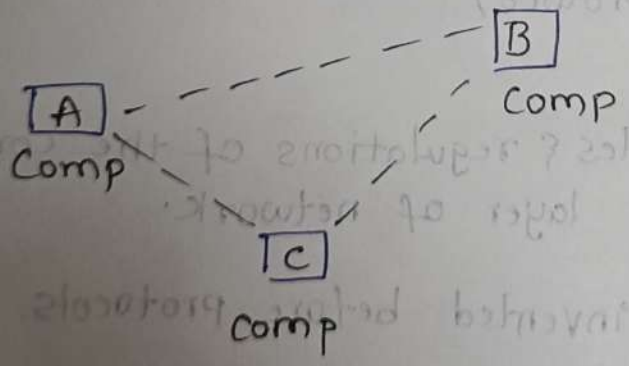
Network:-



1) A, B, C are Autonoums systems where there is no connectivity and no possibility to transmit the information
2) Now, the systems A, B, C are connected by wires/ cables inorder to transfer information
3) wires are called cables / carriers / Transmission cable

* connection of two (or) more autonomous systems is called "network"

* Autonoums systems means not depend on other systems

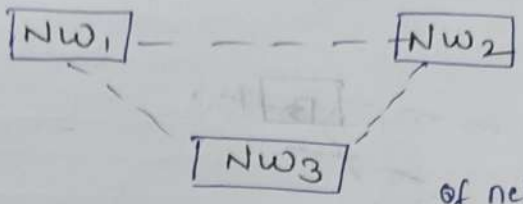


* computers are connected through wires inorder to exchange of information is called "computer network"

(or)

* connection of 2 (or) more autonoums systems

* optical fibres are used to transfer information
* Network connection is done with "internet"



of network

* To reduce the design complexity, the functionality of digital computer is divided into groups.
* The functionality of network is divided into different layers / modules.
* Different Network service providers are:-
  i) OSI reference model
  ii) TCP/IP reference model
  } Standard organisations that provides network

OSI → Open System interconnection

TCP → Transmission control protocol

IP → Internet protocol

Protocol → Set of rules & regulations of the corresponding/ Particular layer of network.

>>> OSI model was invented before protocols.

>>> TCP/IP model was designed after protocols are invented

>>> TCP model contains 5 layers

>>> OSI model contains 7 layers

>>> These standards are developed to reduce design complexity

1) ISO- OSI reference model:-

- Here, the network functionalities are divided into 7 layers :-

1) Physical layer
2) Data link layer → Dataflow
3) Network layer < Static / Dynamic
4) Transport layer
5) Session layer
6) Presentation layer
7) Application layer

Network → Routing → Static Routing / Dynamic Routing
Network → IP address

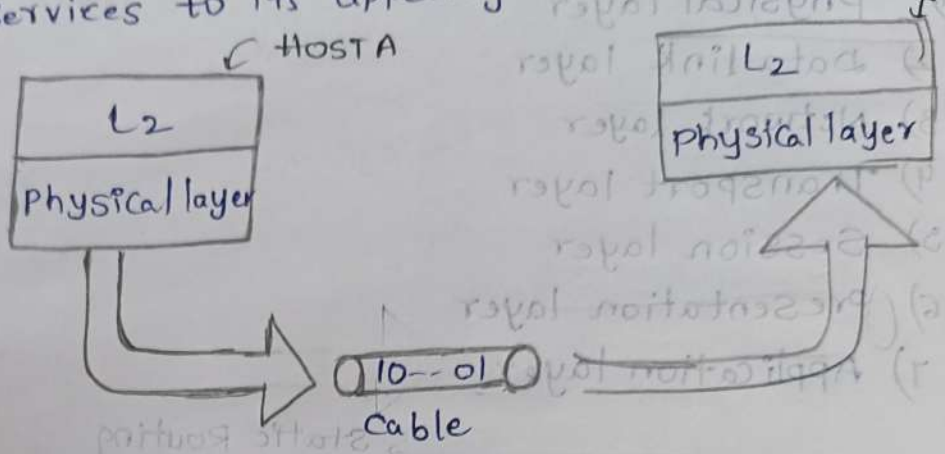
1) Network layer decides the route to travel
2) Transport layer transfers the data to the route that is decided in network layer
3) Session layer decides the time ie, login, logouts
4) presentation layer concentrates on syntax, Security by providing encoding & decoding.
5) Application layer provides services ie, for different applications

1) Physical layer:-

1) Select the type of the transimisson medium (Guided medium, unguided medium)

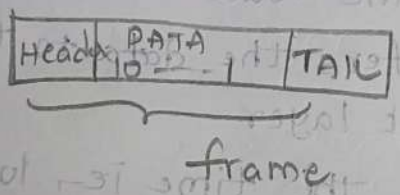
ex:- Copper wire, coaxial cable, twisted pair, optical fibre cable

2) Convert the data into 0's & 1's
3) Use the amplifier and Repeator to restrengthen the weak signal (Hardware)
4) Provide services to its upperlayer ie, datalink layer

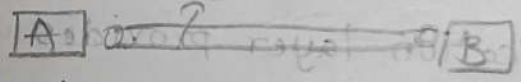


2) Data-link layer:-

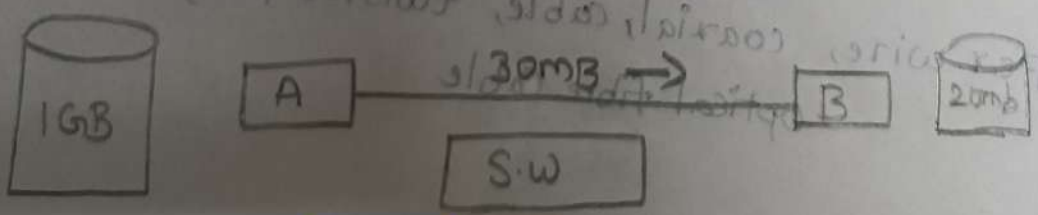
1) Framing:- group of bits received from physical layer



2) Header contains source details & destination details (48b
3) Tail is used to check the error in the data

2) End to end connection. 

3) Datalink layer decides which node to be connected to the cable
4) Error detection and collection.
5) Flow control:- control the dataflow between Fast Sender and Slow receiver.



S.W: ~~slidi~~ sliding window (Buffer)

→ Sender sends 30mb of data but receiver capacity is 20mb.

* The solution for the above problem is:-

i, use the sliding window protocols (Go back N)

ii, Select and Repeat sliding window protocol

6) It assigns the ~~Enter~~ Ethernet/ mac/ physical address to the nodes (48 bits)

7) use the ~~Bri~~ hardware as "Bridgers"

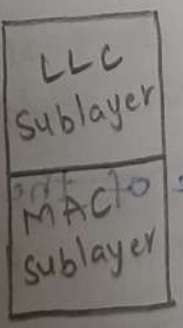
8) provide the services/ functionalities to its upper layer ie, Network layer.

Note:-

The functionalities of datalink layer are divided into 2 sublayers:-

1) logical link control sublayer

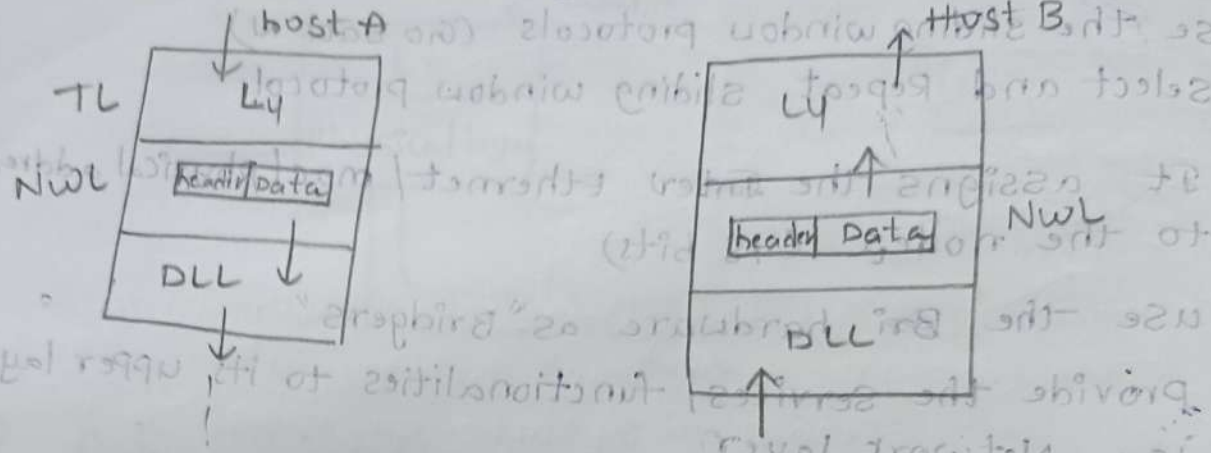
2) MAC sublayer (medium access control)



9) Topology:- The way of the nodes are connected in the network.

3) Network layer:

1) Packetisation:
The network layer receives the data from datalink layer and converts it into packets.



Note: The functionalities of Network are divided based on destination. Thats why the bottom layers offer their services to upper layer

2) Assign Ip address to the nodes in the Internet
Ip - Internet protocol

IPV4	IPV6
- 32 bits	- 128 bits

3) Routing: It decides the route of the path

⇒ Routing is of 2 types:-

i) Static Routing (Fixed)
ii) Dynamic Routing (Dynamic)

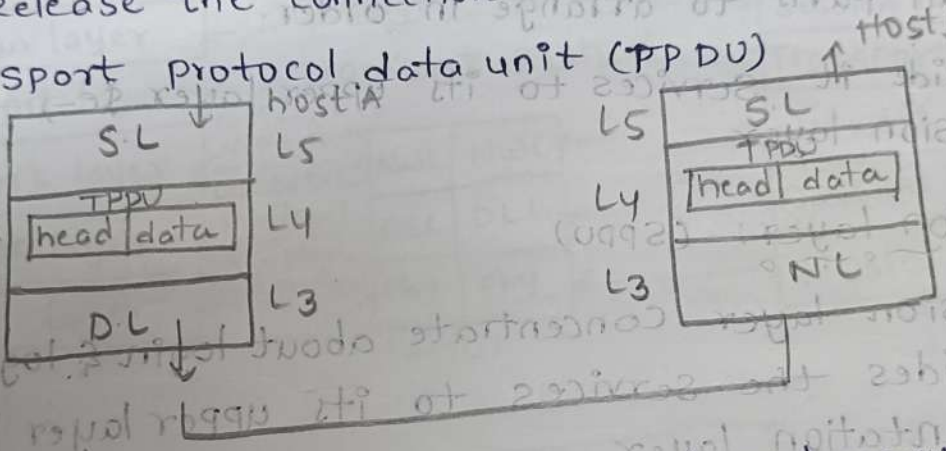
4) conjunction:- Too many packets in the network So, traffic occurs that is called conjunction

5)
i) To handle that is apply conjunction control algorithms
ii) provide the quality of service
provide the services to its upperlayer ie, transport layer

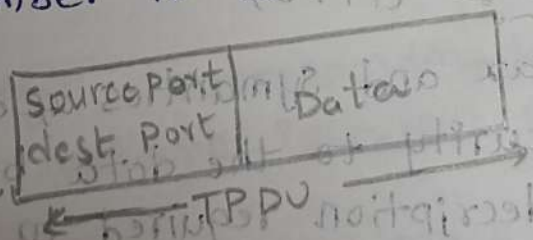
4) Transport layer:-

i) connection management:-
connection established
By use that connection to exchange the information
Release the connection.

ii) Transport protocol data unit (TPDU)

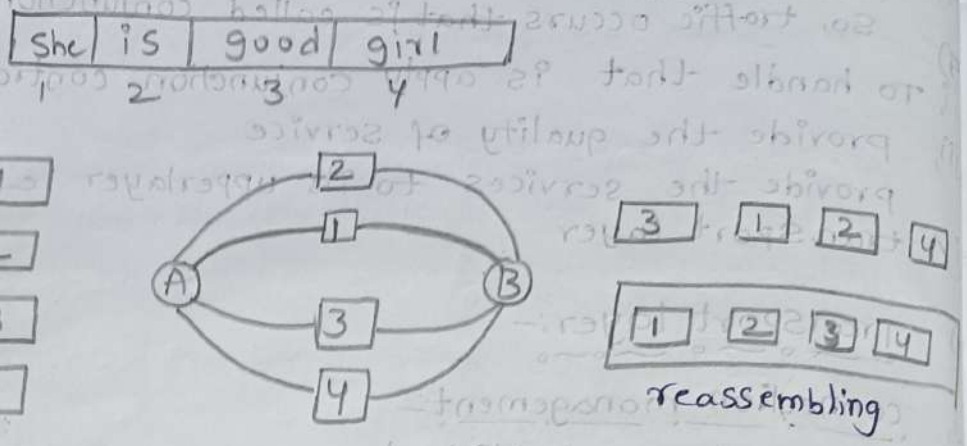


3) Assign the port number for each and every service that number is called port number size 16 bit



4) Provide Quality of service
5) Establishes end to end connection b/w different networks

6) Data fragmentation and Reassembling.



- The receiver reassemble the by re-arrangement of the fragmented parts in sequence by waiting for all parts to arrange in order.

7) Provide it services to its upper layer ie, session layer

5) Session layer :- (SPDU)

1) Session layer concentrate about login & logout
2) Provides the services to its upper layer ie, Presentation layer

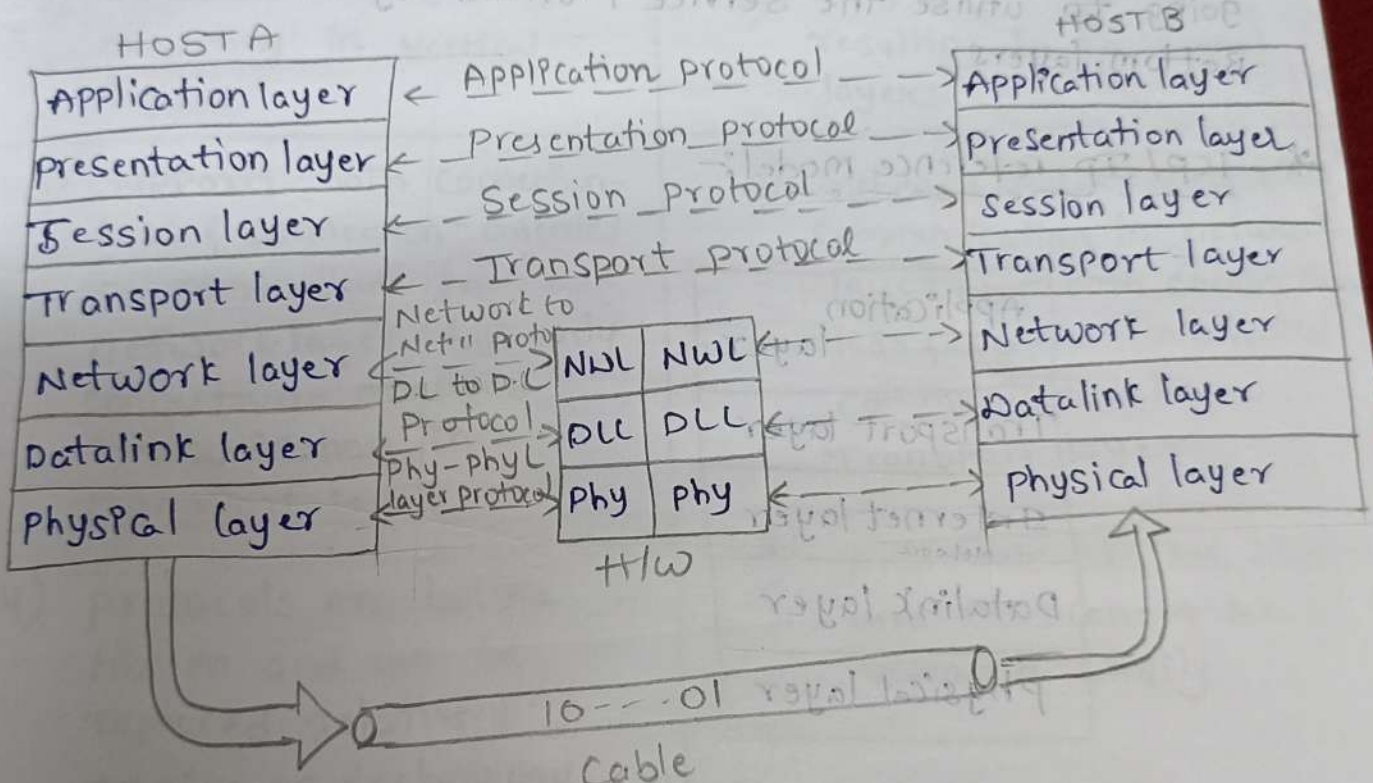
6) Presentation layer :- (PPDU)

1) Maintains syntax and symanties of data
2) Provides the security to the data by using encryption and decription required to provide security to the data
3) Provide services to its upper layer ie, application layer.

7) Application layer (APPL)

1) It provides services to the end user.

WWW – World wide web
DNS – Domain name system
FTP – File Transfer protocol
E-mail – Electronic mail
TELNET



* Peer entities:- Corresponding layers in the source & destination network is called Peer entities.

- Network layers are divided into 2:-

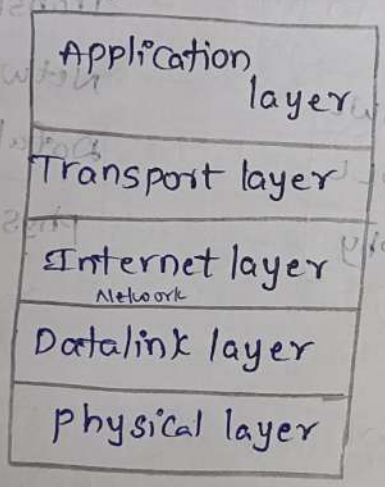
1) Service providers
2) Service users

Service providers:- The Bottom 3 layers of the network (physical, Datalink, network) are going to provide Services to upper layers

Note:- The network hardware is from physical, Datalink and network layer.

Service users:- The upper 4 layers of the network (Transport, Session, Presentation, Application) are going to utilise the service provided by the Bottom layers

* TCP/IP reference model:-



It Consists of 5 layers.

* TCP/IP reference model was designed & developed after protocols are invented

* Differentiate between OSI & TCP/IP reference model:-

OSI model	TCP/IP model
1) contains 7 layers	1) contains 5 layers
2) uses strict layering resulting in vertical layers	2) uses loose layering resulting in horizontal layers
3) Supports both connection-less & connection-oriented communication in network layer, but only connection-oriented communication in transport layer	3) Supports only connectionless communication in network layer, but both connection less & connection oriented communication in Transport layer
4) protocols are better hidden and can be replaced relatively easily as technology changes	4) protocols are not hidden and thus cannot be replaced easily
5) OSI Reference model was devised before the protocols were designed	5) The protocols came first and the model was a description of the existing protocols

Topology:- Way of nodes in the network are connected together

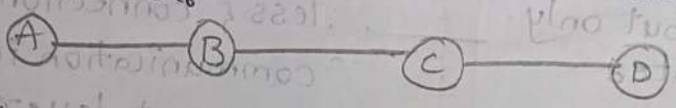
(or)

Architecture of nodes in the network.

* In general, the network will support the following topologies :-

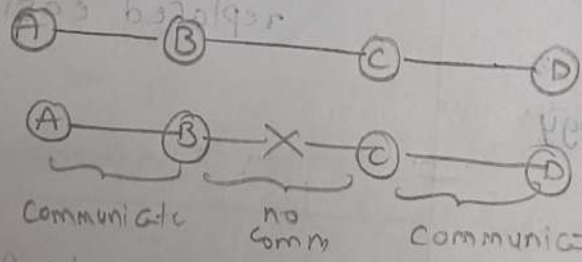
1) linear topology
2) BUS topology
3) RING topology
4) STAR topology
5) MESH topology
6) HYBRID topology

1) Linear topology :- nodes are connected in sequential manner

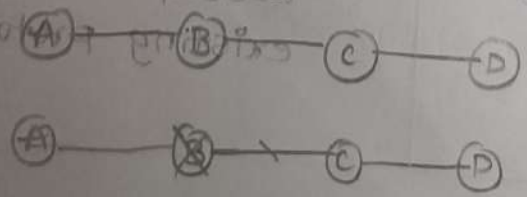


Advantage:- cost is low

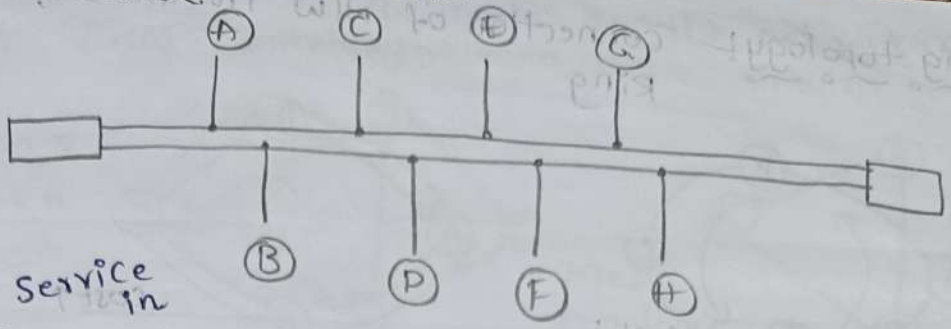
Disadvantage:- Failure of medium b/w 2 connection nodes. Its impact will not affect the other nodes



Node failure:- If the node failure it won't affect the entire functionality



2) Bus topology:- Ethernet



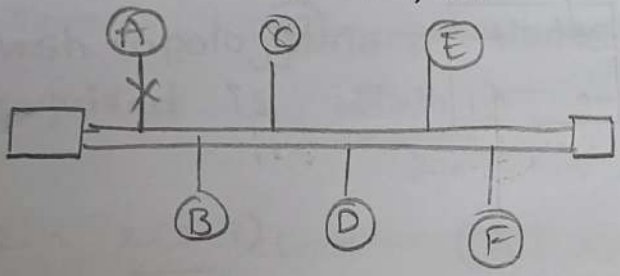
service in

1) Here, main cable is shared blw multiple nodes

Advantage:- i, very low cost

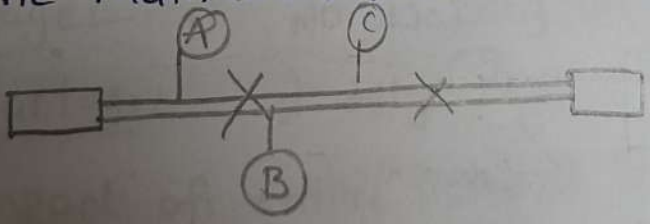
ii) Disadvantage:-

1) Line failure:- Here, the connection is failed, Remaining network has no impact



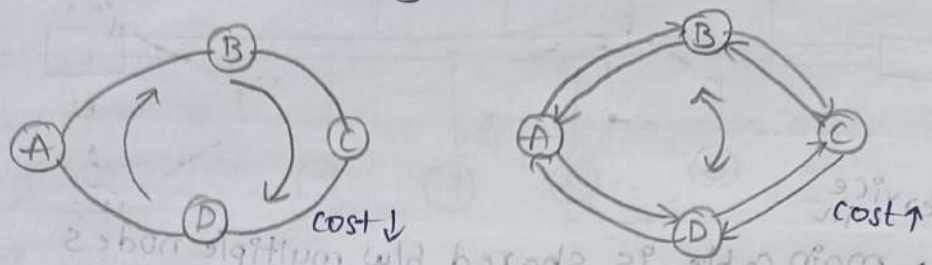
2) NODE failure:- No impact over entire network even the node failure

3) If the main cable fails entire network collapses



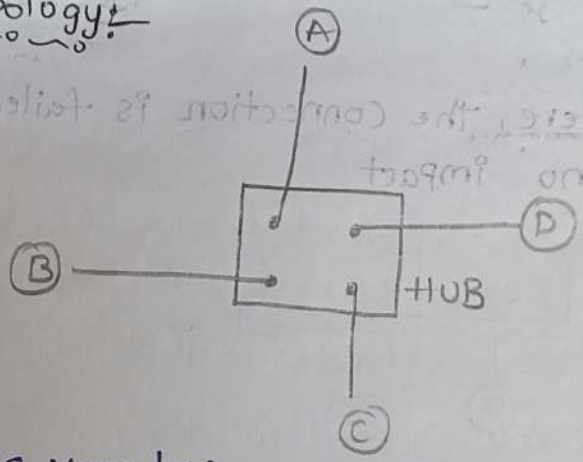
(no communication)

3) Ring topology:- connection of Nlw in the shape of Ring



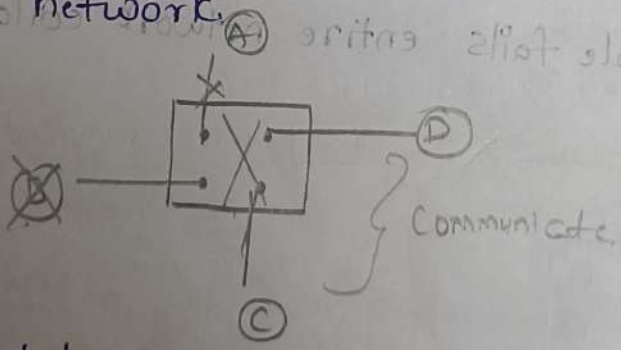
Drowback:- Line failure, node failure

4) Star topology:-



Adv:- cost is very low

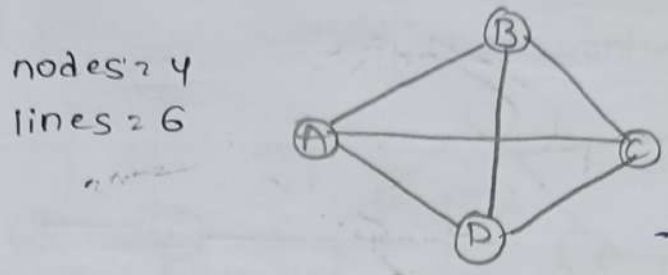
Disad:- i, No impact if line & node fails for entire network.



central

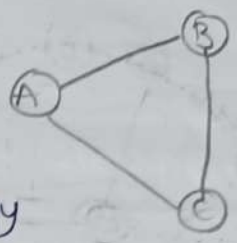
3) If entire/ HUB fails entire network gets collapsed

5) Mesh topology:- The nodes in the network are connected or fully connected.

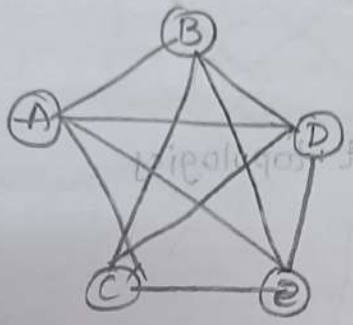


nodes = 4
lines = 6

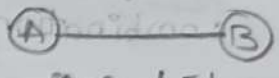
Mesh topology



nodes = 3
Lines = 3



Nodes = 5
Lines = 10



N=2, L=1

→ In mesh topology no. of Nodes are 'N' then max. no. of lines required is $\frac{N(N-1)}{2}$

$N=2 = \frac{2(2-1)}{2} = 1$

$N=3 = \frac{3(3-1)}{2} = \frac{6}{2} = 3$

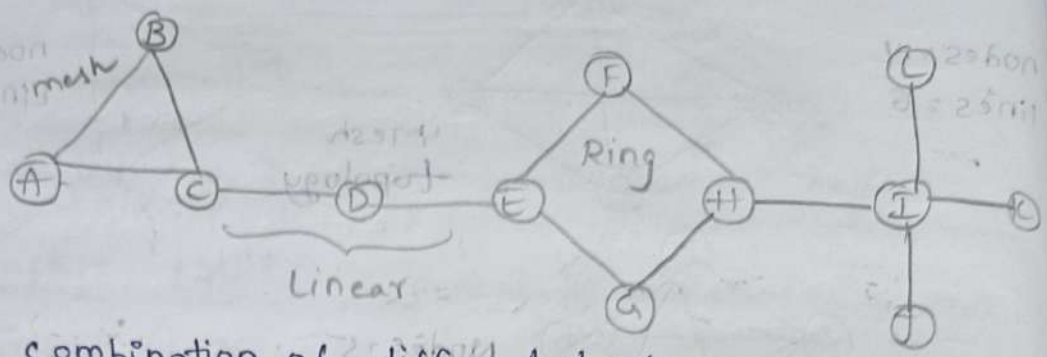
Advantage:- 1) No waiting time

Disadvantage:- 1) High cost

2) No impact of entire network if line fails

3) No impact of entire network if node fails

6) Hybrid topology:- Based on the requirement, we may combine 2 (or) more standard topologies



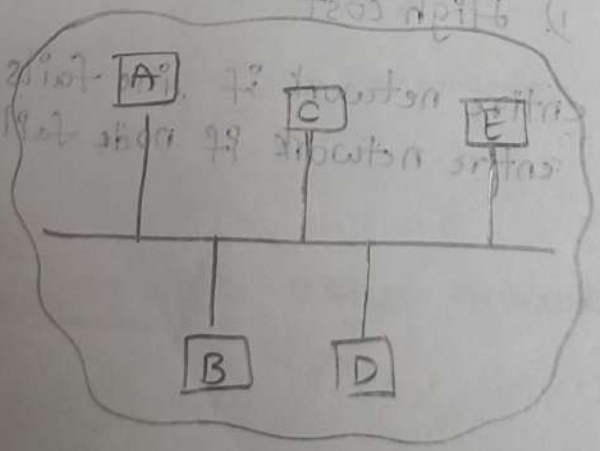
combination of different topologies

* Network types:-

Based on size and Range of the network. The networks are divided into 3 types:-

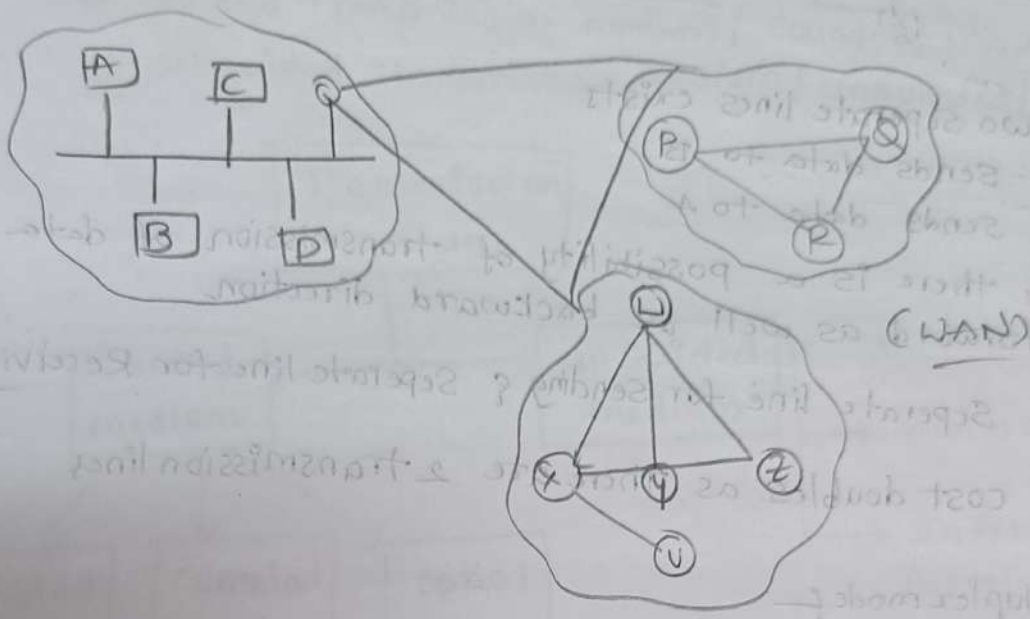
1) LAN - Local Area networks
2) MAN - Metropolitan area networks
3) WAN - Wide Area networks

1) Local Area networks:- It is limited in size
The nodes are connected in the same room/building



2) Metropolitian Area network
It is limited with in the city (max 1000 systems)

3) WAN Within entire countries



(WAN)

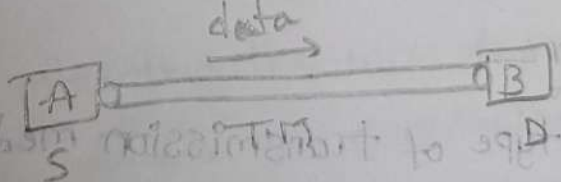
Note: PAN :- Personal Area network

* Modes of Data transmission/mode

→ There are 3 types :-

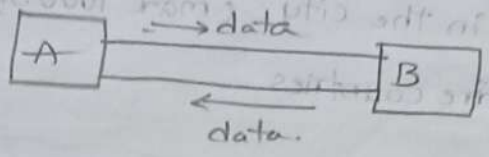
1) Simple x mode
2) HALF DUPLEX mode
3) FULL DUPLEX mode

1) Simplex mode :-



1) Source Sends the data
2) Destination receives the data only in forward direction
3) NO Backtracking in this model
   • A → B exists • B → A doesn't exists

2) Half duplex mode

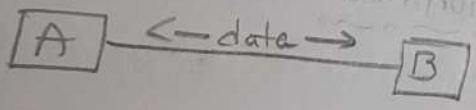


1) Two seperate lines exists
2) • A Sends data to B
   • B Sends data to A
3) So, there is a possibility of transmission of data in forward as well as backward direction
4) Use Seperate line for sending & Seperate line for Receiving

dis~~Adv~~ ~ cost doubles as there are 2 transmission lines

3) Full duplex mode

1) Single transmission line which can send as well as Receive the data



dis ~ If A & B Sends data simultaneously. It leads to collision of data

* ~~Phy~~Sical layer

1) Select the type of transmission medium

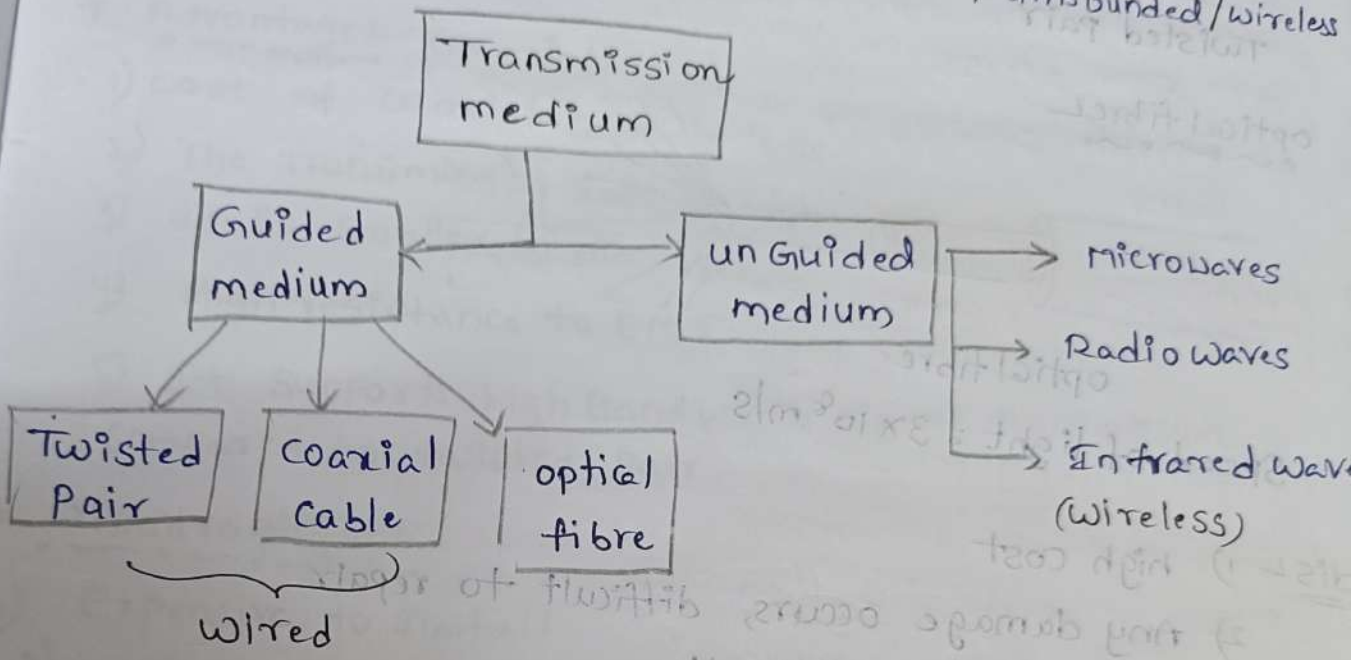
ex ~ copper wire, twisted pair etc

2) Convert data in 0's & 1's
3) Uses the amplifiers repeater to restrengthen the weak signal

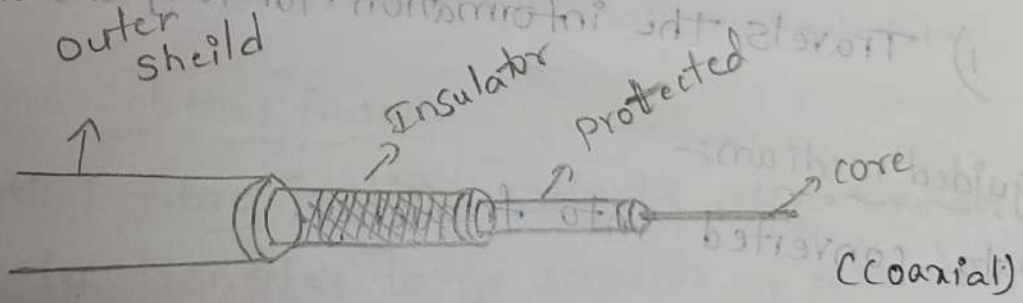
* Transmission media:-

Physical layer supports the following 2 types of transmission medium :-

1) Guided Transmission medium / Bounded / Wired
2) unguided Transmission medium / unBounded / wireless

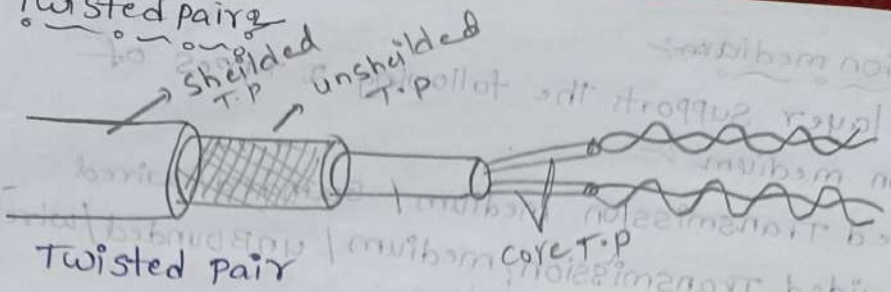


1) Guided:-



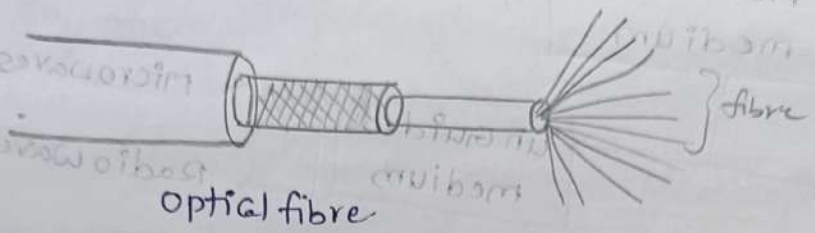
1) Outershell is protecting the wire from environment
2) protected layer protects the data in the core
3) Insulator is the combination of meshes Inorder to Prevent the Generation of electro magnetic-force

Twisted pair:



Twisted pair

optical fibre:



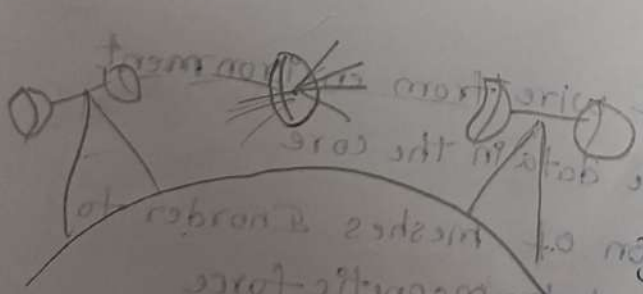
optical fibre

Speed of light = 3×10^8 m/s

dis:- 1) high cost
2) Any damage occurs, difficult to repair
3) maintenance is difficult

Adv:- 1) Travels the information for long distance

* unguided medium:-
→ Data converted into frequency.



i) It is in parabola shape for easy reflexion

ii) All the rays received from diff directions reaches the center of the disc and then transmit the rays to the respective users

* No wires in this transmission all the signals are converted to different frequencies these frequencies reaches the nearby towers & then transmitted

1) FDM :- Frequency division multiplexer
2) TDM :- Time Division multiplexer

* Advantages (coaxial)

1) cost of coaxial cable is less
2) The transmisson rate is high
3) It is smaller in dia
4) High resistance to EMI
5) It supports high Bandwidth signal transmission compared to twisted pair

* Disadvantages

1) Expensive to Install
2) cost of maintanence is high
3) It has more security problem

1858

* Advantages (optical fibre)

1) The optical fibre is light weight & more compact
2) Ability to transfer large amounts of data to longer distance
3) External disturbance is well-protected by optical fibre

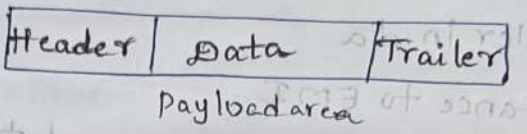
* Disadvantages

1) Repair is difficult
2) An expensive investement (or) installation (or) maintanence

* Datalink layer:-

1) Framing
2) Error detection and correction
3) Flow control
4) End to end connection
5) Medium access
6) Provide services to its upper layer ie, network layer.

* Framing:-



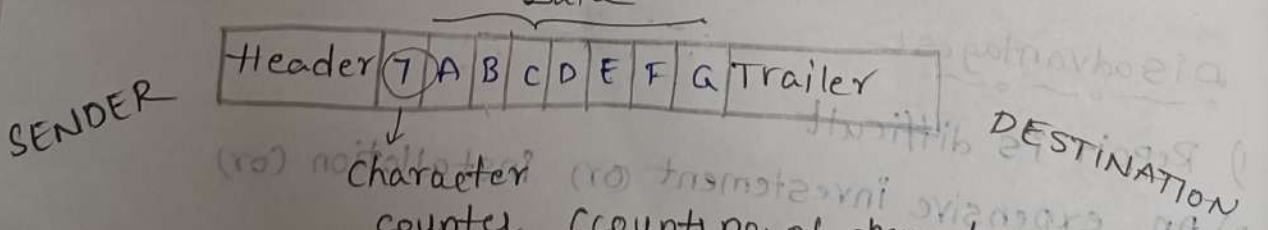
1) Header mainly consists of :-
   i) Source details (Address)
   ii) Destination details (Address)

2) Trailer contains all the error checking & corrections ie, It concentrates abt error checking in frame

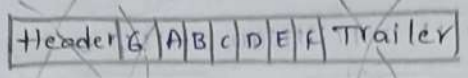
Technologies used in framing:-

1) COUNT no. of characters / character counter
2) BIT stuffing
3) BYTE stuffing

1) character counter:-



2) Destination removes header & Trailer and accepts only the Data in the frame



Destination

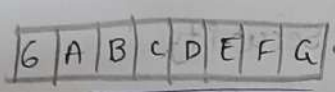
excludes: Header, trailer, character count

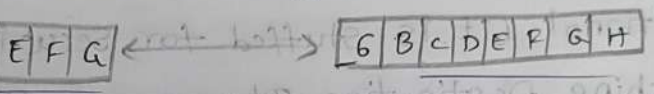
3) character count is just for verification b/w source & Destination

Drawbacks:

1) The Data may changes while travelling from source to Destination.

2) Destination Doesn't identify the change in data.

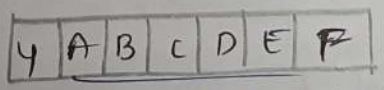
S 



D

* Data changes but Destination accepts it just by observing the character count as it is same in both frames

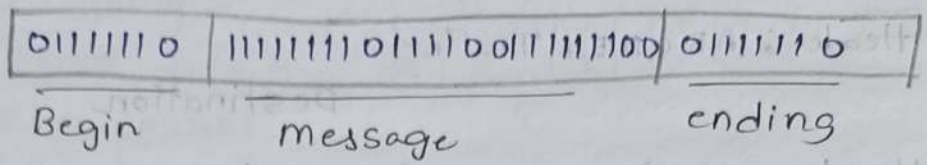
3) If count changes its accepts only the no. of characters changed not the entire data



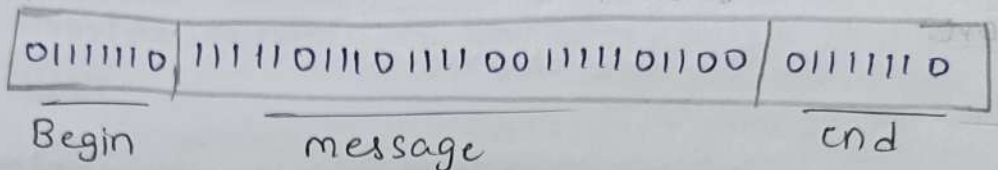
→ accepts only 4 characters

2) BIT Stuffing:- adds a bit for effective transformation of information from source to Destination

It takes a specific format as 01111110 indicates Begining and ending of message



* It is transfered to destination as :-



* Stuffs an additional "0 bit" to the message after "5 consecutive 1's"
* only "1" additional bit is stuffed for security.
* After reaching Destination. It removes the additional stuffed bit ie "0"
* After '5' consecutive '1's' the destination deletes the "6 bit" even though there is '0 or 1'
* It automatically deletes the "6th bit"

* Types of connections:-

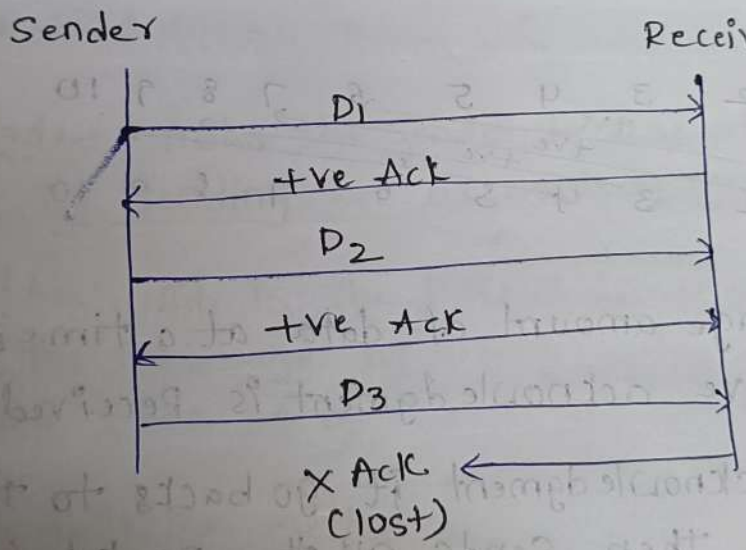
1) connectionless service with no acknowledment
2) connection oriented service with no acknowledgment
3) connection " " " acknowledgment

* sliding window protocols:-

* sliding window → Moving Buffer

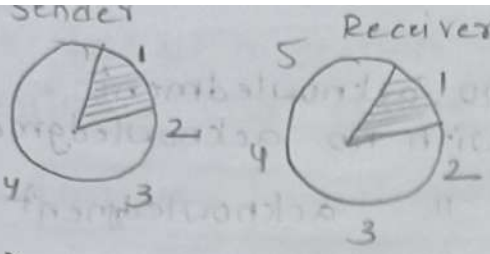
1) Simple stop & wait protocol
2) Go Back by n protocol
3) Selective Repeat protocol

1) Sender waits until acknowledment is received from the Receiver (Simple stop & wait protocol)



*In case of acknowldgment lost in between before receiving the Sender then, Sender will wait for some period of time and it resends the same data again to the Receiver (Sender side)

* If Receiver gets the same data again it will consider as the duplicate data and doesn't Process it

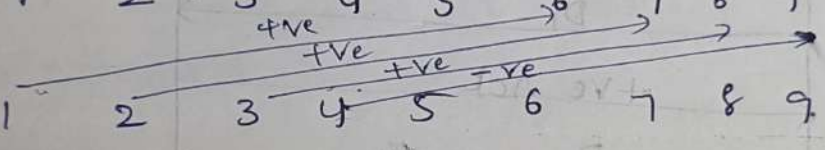


1) 1 bit Sent · sender waits at 1st bit until acknowledgement is Received

2) 2 buffers exist 1) Sender side buffer
2) Receiver side "

i) Sender side buffer stores the data sent in the buffer
ii) Receiver " " transmits the sent data to next layer and ready to receive data from sender [stores received data & checks for errors]

3) Go back by n
4) Sender 1 2 3 4 5 6 7 8 9 10



Receiver 1 2 3 4 5 6 7 8 9 10

i) Sender sends large amount of data at a time & waits until the +ve acknowledgment is Received.
ii) In case of -ve acknowledgment it go backs to the Particular packet & then sends all the packets from nth positive. [from -ve acknowledgment ~~to~~]

5) Disadvantage 1) More number of retransmissions
2) channel inefficiency

[sends all the data from the -ve acknowledgment packet]

3) Selective Repeat Protocol :-

1) Sends only the -ve acknowledgment data not all the Remaining data
   ie, retransmissions are Reduced

* Errors :-

1) Single Bit errors :- only 1 bit changes during transmission
2) Multiple Bit errors :- more than 1 bit " but not continuously bits
3) Burst error :- more than 1 bit but continuous bits changes

* Error correction mechanisms :-

1) Forward error correction method
2) Backward " " "

Backward :- Asks the Sender to resend the data once again by sending -ve acknowledgement

Forward :- It is the process in which receiver tries to guess the message by using reduandant bits. It is possible when no. of errors are small
(reduandant bits = additional bits)

* Error detection methods :-

1) Single bit Parity check :- Additional 1 bit is added to the original messages
   1) no. of 1's are even in message = 0 (Parity bits)
   2) no. of 1's are odd = 1 (Parity bit)

2) 2 dimensional parity bit :-

1) Row wise parity bits are identified, column wise also.
2) Multiple frames data is collected

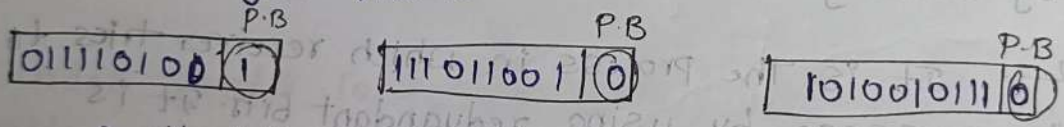
* Error detection methods :-

1) Single bit parity check (or) Simple parity check
2) 2 dimensional parity check
3) checksum
4) CRC

1) Single bit :- i, In a given frame if it contains even no. of 1's then add 0 as parity bit

ii, If the frame contains odd no of 1's then add 1 as parity bit

ex:- In a given frame



Parity bit is identified based on no. of 1's

* limitations :-

1) This method detects only single bit errors. ie if multiple bits were change (or) parity bit itself change then also it cannot identify the errors.

2) 2 dimensional parity check:-

*It computes row wise parities and column wise parities.

f_1	01111010	1
f_2	11100101	1
f_3	10100101	0
f_4	00111010	0

(S) $f_1\ f_2\ f_3\ f_4$ (R) →

* All 4 frames are transmitted to the Receiver. Receiver again computes the parity for all frames

01111010	0
11100101	0
10100101	0
00111010	0
00000000	0

(All bits should be 0)

*If the parity bit is other than 0 at Receiver then it identifies that the error is in the frame

3) Checksum:-

(1) Take 'n' frames 2) add the frames one by one 3) compute 1's complement of the sum]

4) Take n frames
2) Add the frames one by one
3) Compute 1's complement of the sum
4) Send all the frames + one's complement

Note:-

- 1's complement of sum of n frames is called as "checksum"

Receiver:- It receives n+1 frames

2) It performs sum of all the frames by adding 2 frames.

3) Compute 1's compliment of the Sum

4) If 1's compliment is 0 means there is no error in the transmission otherwise, there is an error in the data

ex:- consider 4 frames

10011001 (f_1) 11100010 (f_2) 00100100 (f_3) 10000100 (f_4)

(f_1) (Result) $+ f_3$

Result $+$ (f_4)

```
  10011001 → f1
+ 11100010 → f2
------------
  01111011 → f1+f2
 <-------- 1 1 1 → carry
  01111100 → f1+f2
+ 00100100 → f3
------------
  10100000 → f1+f2+f3
+ 10000100 → f4
------------
  00100100
           1 → carry
------------
  00100101 → 1's complement
```

$f_1+f_2+f_3+f_4$

00100101

1's compliment

11011010

(checksum)

Sender sends all four frames + checksum

Receiver side

```
  10011001  f1
  11100010  f2
  ---------
  01111011
      111   f1+f2
  ---------
  0.1111100
  00100100  +f3
  ---------
  10100000  f1+f2+f3
  10000100  f4
  ---------
 1)00100100
     1 - carry
  ---------
  00100101  → f1+f2+f3+f4
  11011010  → checksum
  ---------
  11111111  → 1's complement for this
  ---------
  00000000  (no error in frame)
```

Receiver again computes the same process along with the checksum and at last find the 1's compliment we should get all 0's

*Receiver side: (if Bits are modified in the frame)

f1 → 10011101 , f2 → 11101010, f3 → 00100100

f4 → 10000000

```
  10011101  → f1
  11101010  → f2
  ---------
 1)100001 11  → f1+f2
      1111
  ---------
  10001000  → f1+f2
  00100100  → f3
  ---------
  10101100  → f1+f2+f3
  10000000  → f4
  ---------
 1)00101100
       1
  ---------
  00101101  → f1+f2+f3+f4
  11010010  → 1's compliment
  ---------
 1)00000111
```

```
  00000111
      1111
  ---------
  00001000  → is
  ---------   comp

  11110111
```

other than 0 so error is detected in frame

(Receiver identifies)

CRC :- Cyclic Redundancy check

Procedure :-

1) Take m bits of message and r redundant bits
2) r is the degree of g(x)
   (or)
   r = n-1 bits where g(x) contains n bits no. of bits of message > g(x)
   M(x) > g(x)
3) Add r no. of zeros to message m(x) = Data
4) Divide Data with G(x) by XOR operation
5) Take the Remainder of r bits
6) Replace the additional r bits with Remainder and send to Receiver

Receiver Side :-

1) It Receives m+r bits
2) Divides the message with G(x)
3) It will check the Remainder.
   i, if (remainder == 0) then no error and data can be accepted
   ii, otherwise data can be discarded

ex:- Message = 1010000

$G(x) = x^3 + 1$

$= 1 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x + 1$

$= 1001$

$m(x) = 1010000\underbrace{000}_{r}$, $G(x) = 1001$

Sender:-

```
1001) 10100000000 (1011011
      1001
      -----
       0110
       0000
       ----
       1100
       1001
       ----
       1010
       1001
       ----
       0110
       0000
       ----
       1100
       1001
       ----
       1010
       1001
       ----
        011
```

Sender → 10100000011

Receiver:-

```
1001) 10100000011 (1011011
      1001
      -----
       0110
       0000
       ----
       1100
       1001
       ----
       1010
       1001
       ----
       0110
       0000
       ----
       1101
       1001
       ----
       1001
       1001
       ----
       0000
```

no error:-
Data is accepted by the receiver

Data: 1010100011 (single bit)

```
1001) 1010100011 (1011111
      1001
      ----
       0111
       0000
       ----
        1110
        1001
        ----
         1110
         1001
         ----
          1110
          1001
          ----
           1111
           1001
           ----
            1101
            1001
            ----
             100
```

remainder is not "0"
error!
Data is discarded by the Receiver

Data:

1010101011 (multiple bit)

```
1001) 1010101011 (1011110
      1001
      ----
       0111
       0000
       ----
        1110
        1001
        ----
         1110
         1001
         ----
          1100
          1001
          ----
           1011
           1001
           ----
            0101
            0000
            ----
             101
```

other than 0
error!
Data is discarded!

* Error correction methods:-

1) Hamming codes:-

Procedure:-

1) If there is m bits of data then sender adds r bits of data such data $2^r \geq m+r+1$

2) In m+r length of the message the redundant bits can be placed in the locations of powers of 2.

3) For identifying the values of redundant bits

0- 0000	0111 - 7	1101 - 13
1- 0001	1000 - 8	1110 - 14
2 0010	1001 - 9	1111 - 15
3 0011	1010 - 10	
4 0100	1011 - 11	
5 0101	1100 - 12	
6. 0110		

r_1 = (1, 3, 5, 7, 9, 11, 13, 15)

r_2 = (2, 3, 6, 7, 10, 11, 14, 15)

r_3 = (4, 5, 6, 7, 12, 13, 14, 15)

r_4 = (8, 9, 10, 11, 12, 13, 14, 15)

4) The bit values can be computed based on the no. of 1's in the given message in the specified locations

5) If there are even no. of 1's the bit value is 0

6) If there are odd no. of 1's the bit value is 1.

ex:-

I Message(m): 1001101

i, (r=1): $2^r > m+r+1$
: $2^1 > 7+1+1$
: $2 > 9$

ii, (r=2): $2^2 > 7+2+1$
$4 > 10$

iii, (r=3) $2^3 > 7+3+1$
: $8 > 11$

iv, (r=4) $2^4 > 7+4+1$
$16 > 12$ (True)

∴ Redundant bits = 4

II

1	0	0	1	1	1	0	0	1	0	1
11	10	9	8	7	6	5	4	3	2	1
			(2^3) r_4				(2^2) r_3	(2^1) r_2	(2^0)	r_1

Redundant bit locations = 2^0 powers

i, $r_1 = (1, 3, 5, 7, 9, 11) = (\boxed{1}, 1, 0, 1, 0, 1)$

no. of 1's = 3 (odd)

⇒ Place 1 in the redundant bit r_1

ii, $r_2 = (2, 3, 6, 7, 10, 11) = (\boxed{0}, 1, 1, 1, 0, 1)$

no. of 1's even = 04

⇒ Place 0 in the redundant bit r_2

ii, $r_3 = (4, 5, 6, 7) = (\boxed{0}, 0, 1, 1)$

no. of 1's = 02 (even)

place 0 in the redundant bit r_3

iv) r_4: (8,9,10,11) : (1,0,0,1)

no. of 1's = 1 (odd)

Place 1 in redundant bit r_4

∴ → message = 10011100101 (Sender sends)

2) Message = 11011101001

($r=1$) $2 \geq 11+1+1$

$2 \geq 13$

($r=2$) $4 \geq 11+2+1$

$4 \geq 14$

($r=3$) $8 \geq 11+3+1$

$8 \geq 15$

($r=4$) $16 \geq 11+4+1$

$16 \geq 16$ (True)

∴ Redundant bits = 4

(1)

1	1	0	1	1	1	0	1	1	0	0	0	1	0	0
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
							(2^3)				(2^2)		(2^1)	(2^0)
							r_4				r_3		r_2	r_1

(11) i) r_1: (1,3,5,7,9,11,13,15) : (0,1,0,1,0,1,0,1)

no. of 1's = 4 (even)

⇒ place 0 in redundant bit r_1

ii) r_2: (2,3,6,7,10,11,14,15) : (0,1,0,1,1,1,1,1)

no. of 1's = 6 (even)

⇒ place 0 in redundant bit "r_2"

iii) r_3: (4,5,6,7,12,13,14,15) : (0,0,0,1,1,0,1,1)

no. of 1's = 4 (even)

place 0 in redundant bit "r_3"

iv) r_4 = (8, 9, 10, 11, 12, 13, 14, 15)
= (1, 0, 1, 1, 1, 0, 1, 1)
no of 1's = 5 (odd)

⇒ Place 1 in redundant bit r_4

∴ Message = 110111011000100 (Sender sends)

* Receiver again follows the same procedure. So it check the parities. It should get all 0's then, there is no error in the message

Receiver side:

Change 5th bit = 110110110010 0
14 13 12 11 10 9 8 7 6 5 4 3 2

= 1 1 0 1 1 1 0 1 1 1 0 1 0 0 1
16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1

change 5th bit = 1 1 0 1 1 0 0 1 1 0 1 0 1 0 0
15 14 13 12 11 10 9 8 7 6 5 4 3 2 1

i) We will get redundant bit as 0101 instead of all 0's

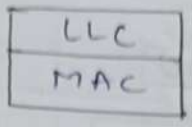
ii) Receiver identifies that there is an error at 5th position and changes 1 to 0 (or) 0 to 1

iii) In this method receiver just identifies single bit error

iv) Multiple bit errors identification is difficult

* MAC Sublayer (Medium Access control)

Datalink layer



* 3 types of protocols:-

1) Random Access protocols
   (or)
   Contention protocols
2) Controlled Access protocols
3) Channelisation protocols

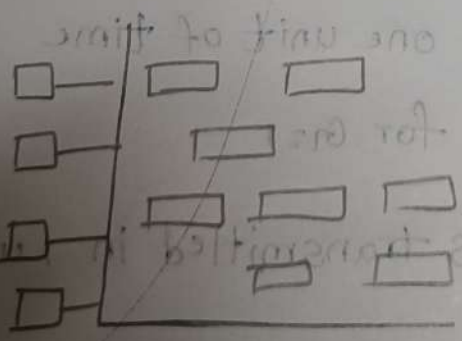
1) Random Access protocols:- More than one station can communicate with other station at the same time.
   1) ALOHA Protocols
   2) CSMA "
   3) CSMA/CD protocols
   4) CSMA/CA Protocols

[All stations are having equal priority]

1) ALOHA protocols:- //All stations

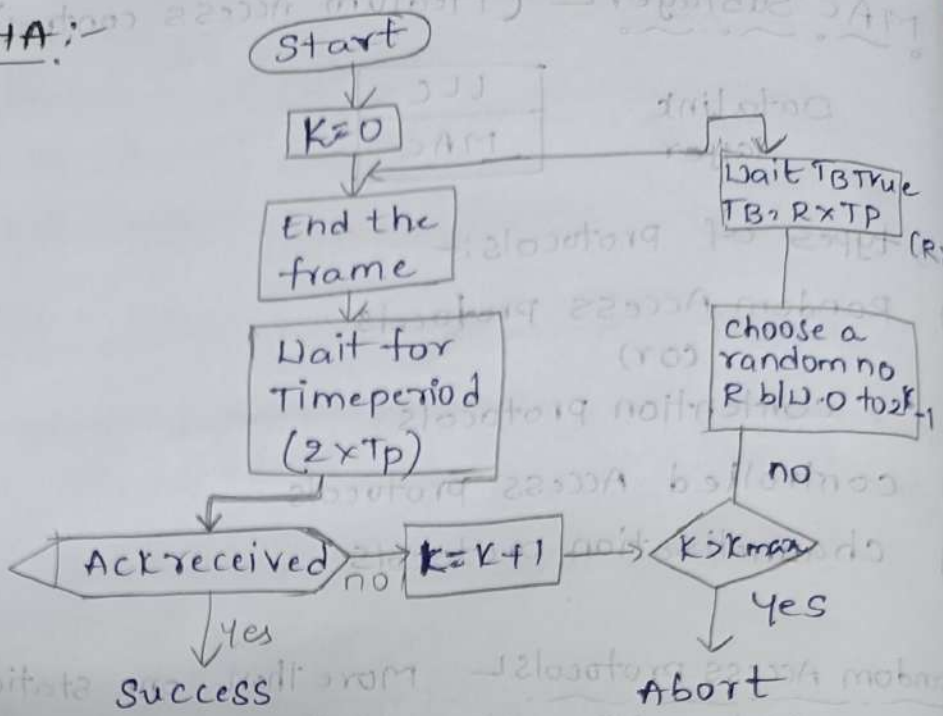
ALOHA → Pure ALOHA
ALOHA → slotted ALOHA

Pure ALOHA:-



All channels sends the data at the same time in the network. So, that the data gets overlapped.

Pure ALOHA:-



K = no. of attempts

Tp = Max propogation time

Tfr = Average transmission time

TB = Back of the time, kmax is normally 15.

Vulnerable time :- $2 \times Tfr$

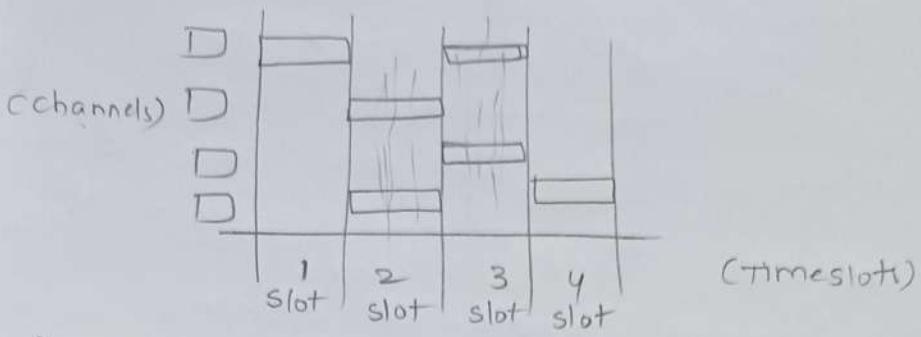
ii, Throughput (S) = $G \times e^{-2G}$

* G = average no. of frames generated by the system in one unit of time

iii, Smax = 0.184 for G = 1

Throughput :- no. of frames transmitted in 1 unit of time

2) Slotted ALOHA protocol:-



1) Data is sent at the starting of slot
2) Only data in the particular slot is corrupted in case of overlapping.

i) Vulnerable time is T_{fr}
ii) Throughput $S = G \times e^{-G}$

* G is avg no of frames generated by the system in one unit of time

iii) $S_{max} = 0.368$ for $G = 1$