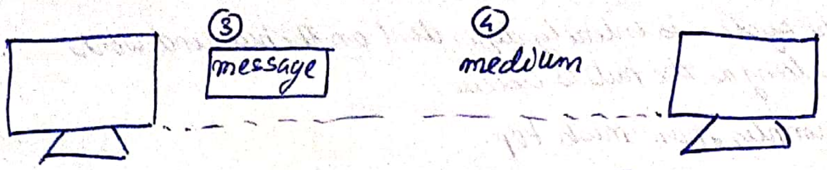
26/7/19

* Components of data communication



⑤ Protocol.

#

Simplex - communication can take place in one direction.

Half duplex - communication can take place in both dir. but one at a time.

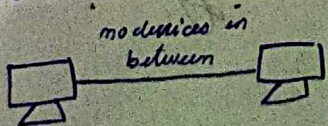
Full duplex - comm. can take place in both dir.

Criteria for communication

1. Performance
   - i> Throughput
   - ii> Delay
2. Reliability
3. Security

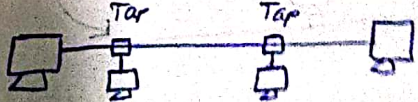
Attributes of physical structure of network

1. Type of connection



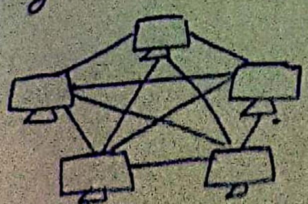
a) Point to point connection

(data will be visible to all nodes)



b> Multi point connection

2. Physical Topology

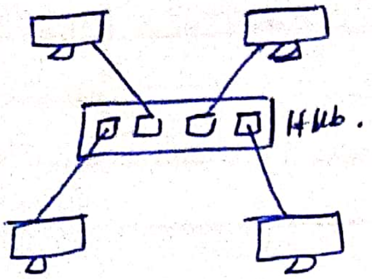


- data directly transferred to connected device.
- data transfer is fast
- Highly reliable because of the individual [illegible]
- No intermediate node [illegible]
  more security

i> Mesh topology

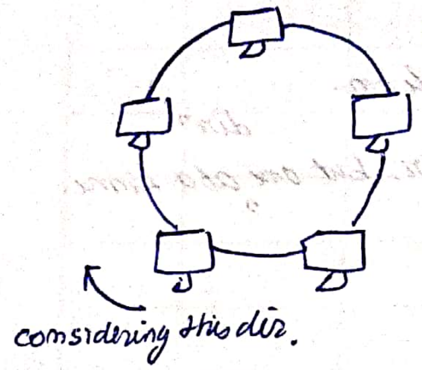
Cons:-
- Inability of physical space
- cost ineffective

ii> Star topology



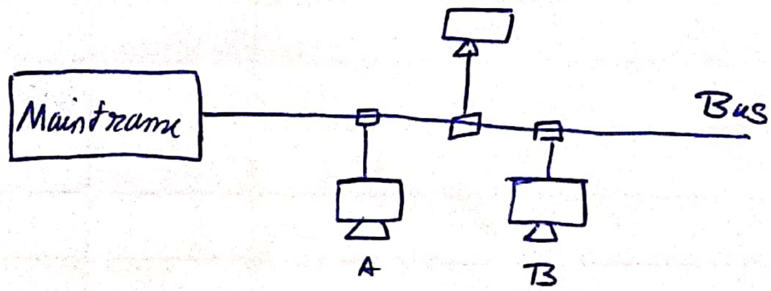
- We can have a central control over the network as the hub governs the systems in the network.
- The system is entirely dependent on the hub and works as long as the hub is active.
- Simpler than mesh top.

iii> Ring topology.

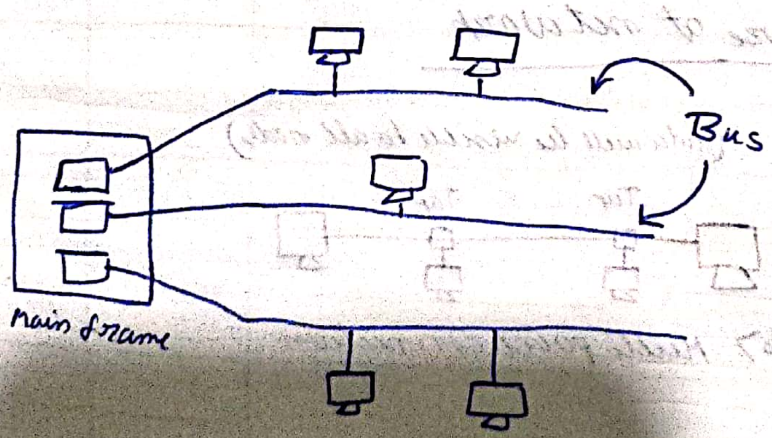


comm. can take place only in one direction

iv> Bus topology



* Hybrid topology



Carries same adv. & disadv. as star & bus topology.

#

1. Local Area Network (LAN) { 10m room, 1-2km campus, 1000m building }
2. Metropolitan area network (MAN) 10km city
3. Wide area network (WAN) { 100km country, 1000km continent }
4. Internet

Protocol

1. Syntax : structure of protocol
2. Semantics : interpret the info and instruction in the signal.
3. Timing : condition defined.

Standards

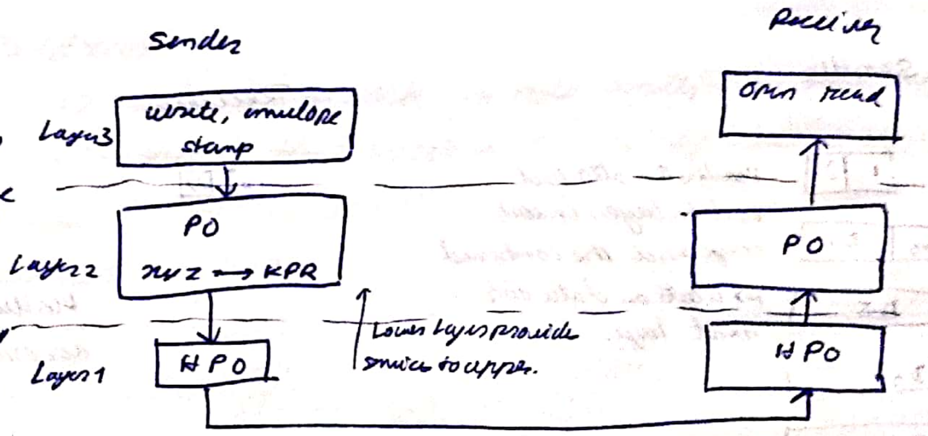
2/8/19

* Network Models

1. Open systems Interconnection (OSI) Model
2. TCP/IP Model

* i) Layers
  ii) Services
  iii) Interface
  iv) Protocol

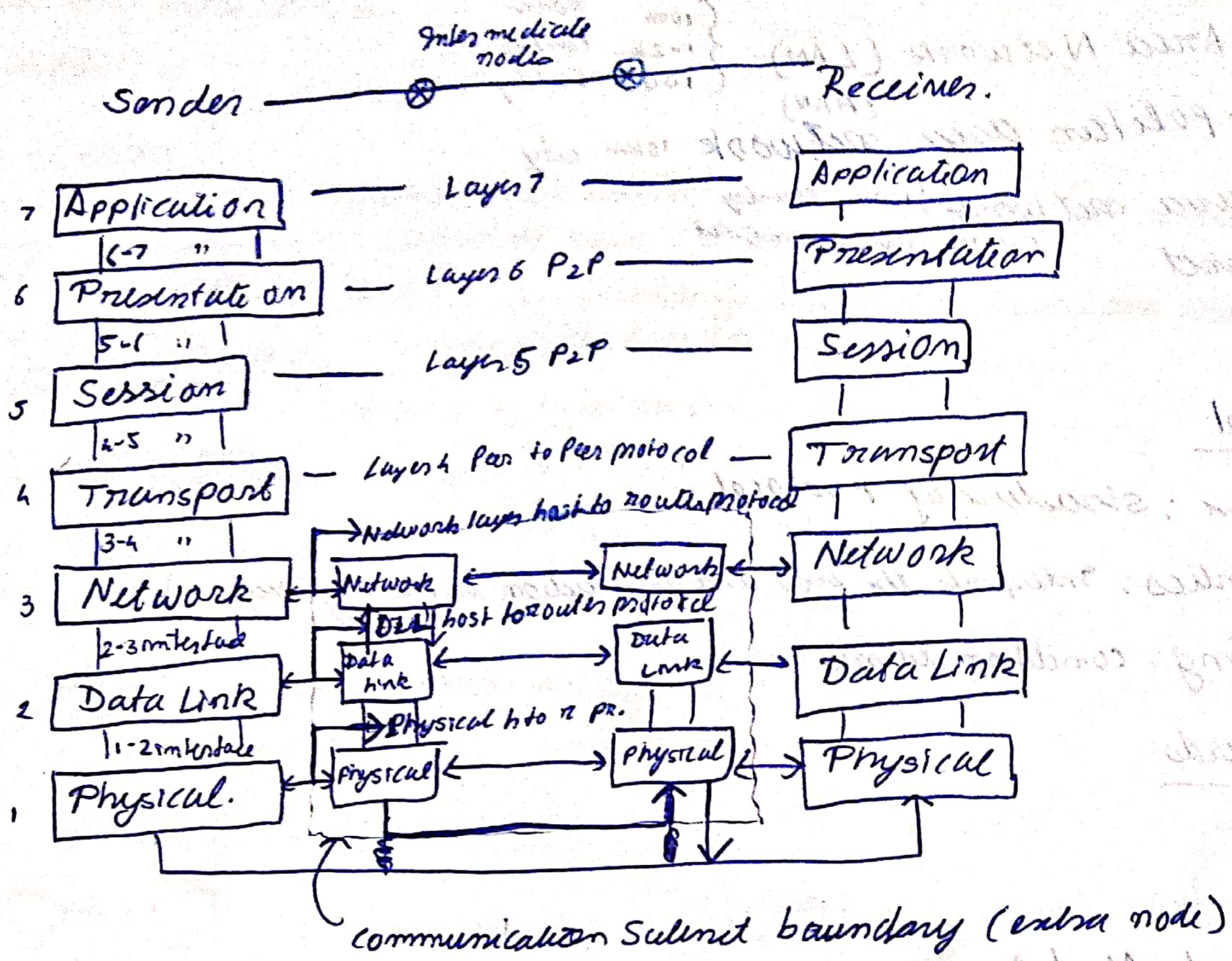
How we are going to access service from lower layer. By calling same f^n.
It is a connection b/w 2 layers.



Design issues of network model

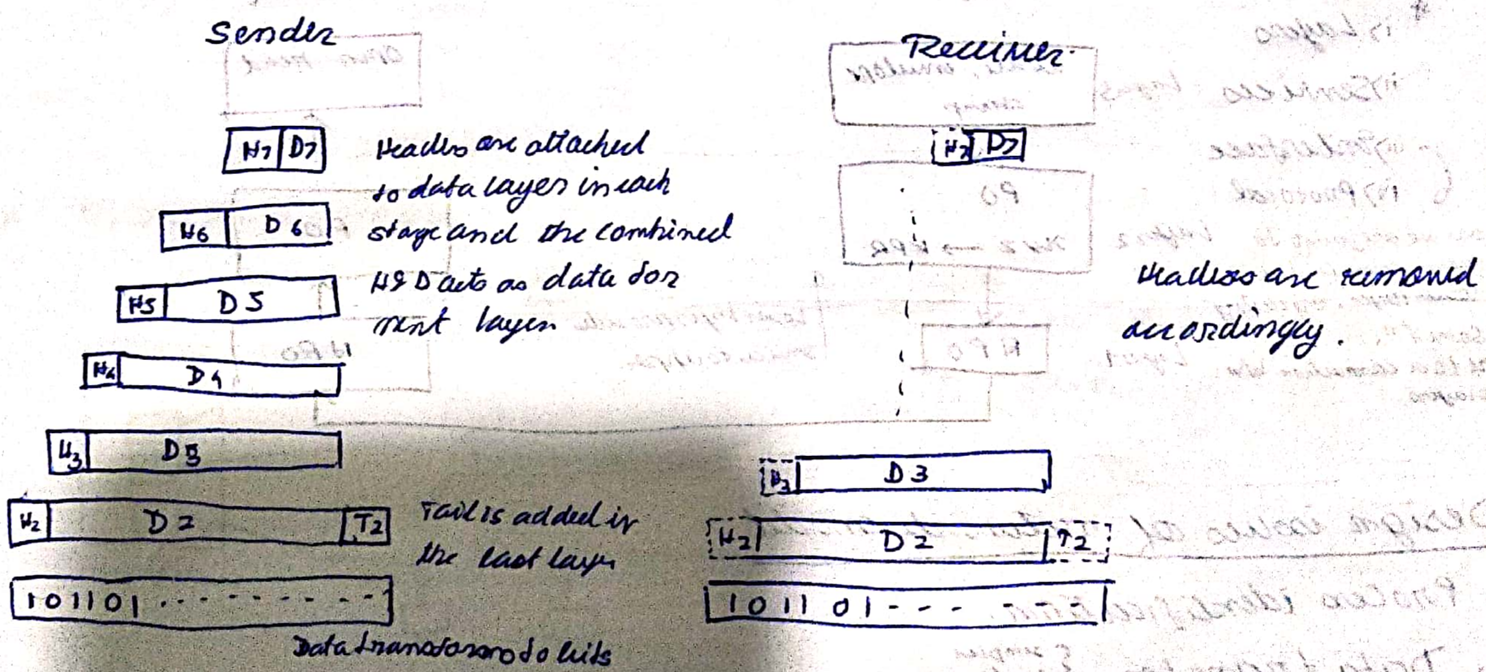
1. Process identification.
2. Data transfer { simplex, Duplex (Half or full) }
3. Error control { • detect, • try to do or retransmit }
4. Flow control {System may get overflowed with data.}
5. Message size

6. Routing (Find a suitable path from source to destⁿ)



OSI reference model

5/8/19



PHYSICAL LAYER

[Transmission of data through electrical signals]

Main:

1. Transmission of raw bits.
2. Physical characteristics of interface and medium
3. synchronization of bits.
4. Line configuration
5. Physical topology
6. Transmission Mode (simplex, half duplex, full duplex)
7. Representation of bits.
8. Data rate

NOTE: Revise representation of bits like NRZ-I, NRZ, Manchester, etc.

* Data Link layer

Main responsibility :-

① It transforms physical layer from being a raw transmiss of bits to a reliable link.

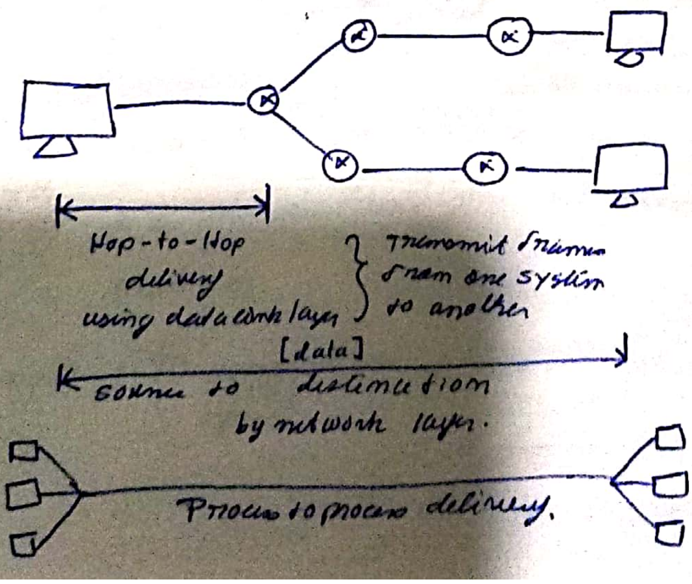
② Framing (converting the data to bits)

③ Physical Addressing
  i> within the network → add sender + receiver address
  ii> outside the network → address of next node.

④ Flow control (at frame level)

⑤ Error control

⑥ Access control.



* Network Layer

Main responsibility:-

① Transmit the ~~packet~~ packets from source to destination

② Routing

③ Logical Addressing

* Transport Layer

Main responsibility:-

① Process to process delivering of ~~data~~ segments.

② Service point addressing (port)

③ Segmentation and reassembly (frames combine to form packets at the destination and hence reassembly is necessary)

④ Connection control

⑤ Flow control

⑥ Error control (deals with errors during transmission of packets)

* Session Layer

Main responsibility:-

① Dialog control and synchronization

* Presentation Layer

Main responsibility:-

① Translation, Encryption, Compression

* Application layer

① Provides services to user.
(topmost layer)

7/8/19

* TCP / IP Protocol Suite

Layers in OSI	Layers in TCP/IP
7 Application	Application
6 Presentation	
5 Session	
4 Transport	Transport
3 Network	~~Network~~ Internet
2 Data Link	~~Data Link~~ Host to network
1 Physical	Host to network

TCP/IP vs OSI

1. Distinction of Services, Interfaces and Protocols.
2. Flexibility to New Technology.
3. Order of Protocol and Model Invention.
4. Number of Layers.
5. Way of communication.

Physical layer

Electrical signal

Analog | Digital.

Bit rate → No. of bits per second

Bit ~~frequency~~ length → is the distance one bit occupies on transmission medium.

[Bit length = Propagation speed × bit duration]

To transmit signals through communication medium

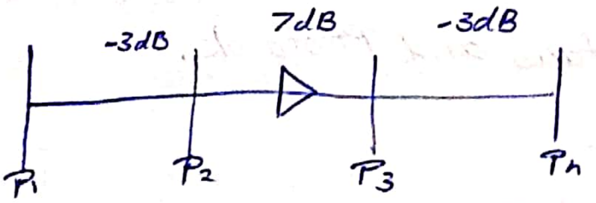
1. Baseband $\rightarrow$ Low pass
2. Broadband $\xrightarrow[\text{via}]{\text{transmitted}}$ band pass.

8/7/19

* Transmission Impairments

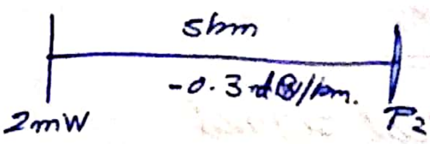
1. Attenuation (Loss in signal strength across the medium
2. Distortion (change in signal shape)
3. Noise (in wired or wireless)

$$10 \log_{10}\left(\frac{P_2}{P_1}\right) \quad \underline{\underline{dB}}$$



Power ~~gain/t~~ gain/loss $= -3+7-3$

Q. Suppose the loss in a cable at beginning is $-0.3\,dB/km$ and a signal having power $2\,mW$. What is the power of the signal at $5\,km$?



Soln.- $P_1 = 2\,mW$

Power loss $= -0.3\,mW/km$

$$10 \log_{10}\left(\frac{P_2}{2\times10^{-3}}\right) = -0.3\times5$$

$$\Rightarrow \log_{10}\left(\frac{P_2}{2\times10^{-3}}\right) = -0.15$$

$$\Rightarrow \log_{10}(500P_2) = -0.15$$

$$\Rightarrow P_2 = 0.001415$$

$$= 1.415\,mW$$

Scanned by CamScanner

* SNR (Signal to noise ratio)

$SNR_{dB} = 10 \log_{10}\left(\frac{S}{N}\right)$ dB

① Noiseless ⟶ Nyquist

Max bit rate $= 2B \log_2 L$

$B \rightarrow$ bandwidth
$L \rightarrow$ No. of levels of signal representation

② Noisy ⟶ Shanon

Max bit rate $= B \log_2 (1+SNR)$

If SNR = 0, then max bit rate = 0

Q. ~~The SNR~~ Assume that SNR = 36dB and the channel bandwidth is 2MHz. Compute the channel capacity.

Soln.- ~~Max bit rate = $B\log_2$~~

$SNR_{dB} = 36dB$

$10 \log_{10}\left(\frac{S}{N}\right) = 36$

$\log_{10}(S/N) = \cancel{\frac{36}{10}}\ 3.6$

$S/N = 10^{3.6}$

$S/N = 3981.07$

$MBR = \cancel{B} \ 2\times10^6 \log_2(1+3981.07)$

$= 23.918 \times 10^6$

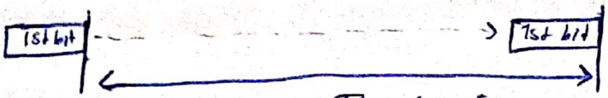
$= 23.918$ MB/sec

* Performance Measures

1. Bandwidth (Max. capacity of the channel)
2. Thoughput (Actual capacity)
   It is a measure of how fast we can actually send data through a network.
3. Latency (delay)

Latency :-

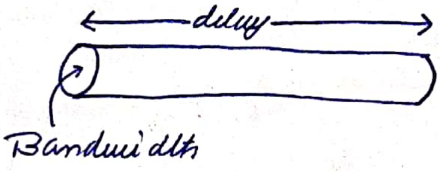
1. Propagation time (measures the time reqd. for a bit to travel from source to destination)
2. Transmission time (measures the time reqd. for entire message to leave from the source node)
3. Queuing time (the time needed for each intermediate or end device to hold the message before it can be processed)
4. Processing time.

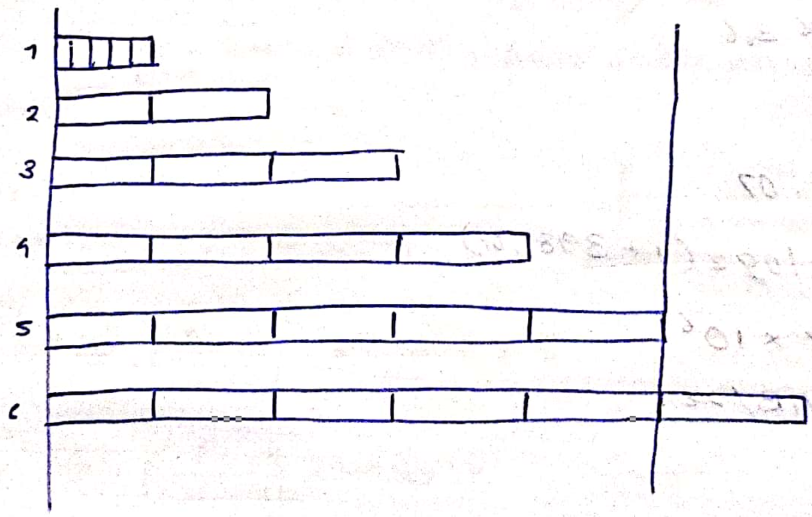


Propagation time = distance / propagation speed.

Latency = ① + ② + ③ + ④

4. Bandwidth delay product.





B = 5 bits/sec

delay = 5

Max = 25 bits.

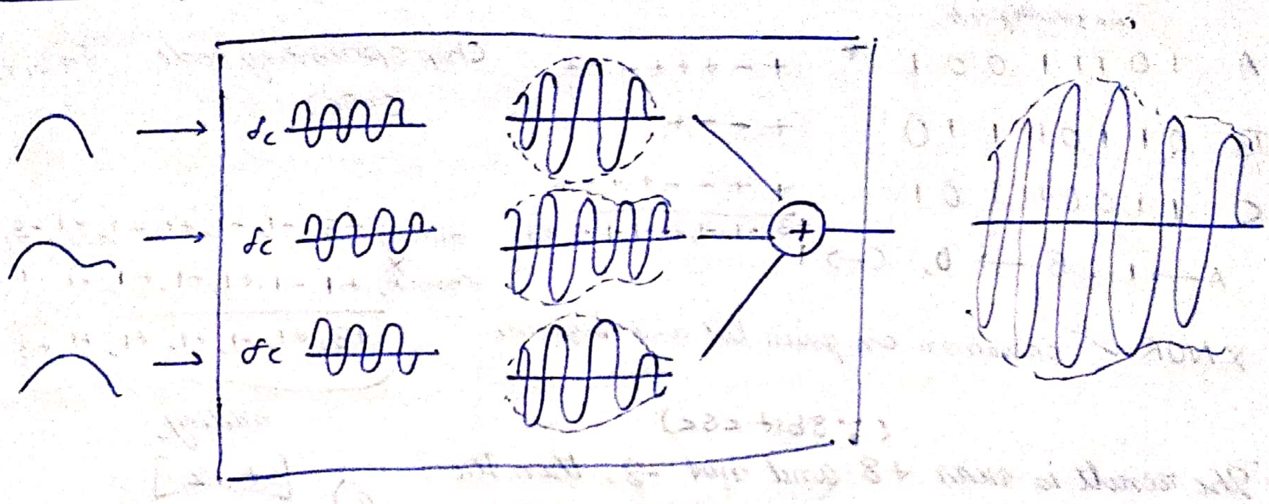
9/8/19

* Bandwidth utilization

- Analog
  - FDM
  - WDM
- Digital
  - TDM
    - Synchronous TDM
    - Asynchronous TDM

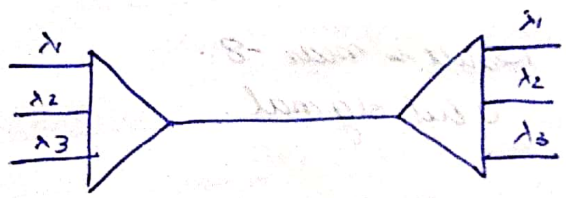
Scanned by CamScanner

Frequency Division Multiplexing (FDM)

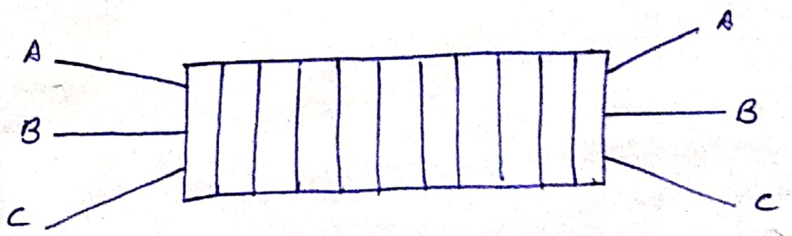


Wavelength division Multiplexing (WDM)

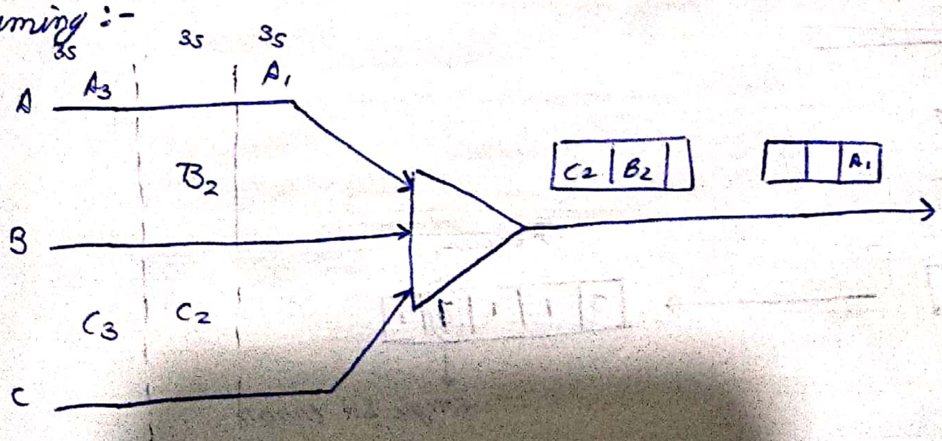
Used in optical fibre cable.



Time division Multiplexing (TDM)



Framing :-



Interleaving

* Code Division Multiplexing (CDM)

chip spreading code

A 1 0 1 1 1 0 0 1 → + − + + + − − +,

B 0 1 1 0 1 1 1 0 + − − + − − − +

C 1 1 0 0 1 1 0 1 + + − − + + − +

+3, −1, −1, +1, +1, −1, −3, +3

Chip spreading code (CSC) 64 bit.

A → 1, B → 0, C → 1

X NOR ✓ operation on given bit and sequence.

multiply +3, −1, −1, +1, +1, −1, −3, +3

× from A, +1, −1, +1, +1, +1, −1, −1, +1

+3, +1, −1, +1, +1, +1, +3, +3

adding, [+12]

(∵ 8 bit csc)

∵ The result is near +8 and not −8, then the result has arrived from A → 1. (it is a 1 Bit signal)

+3, −1, −1, +1, +1, −1, −3, +3

× −1, +1, +1, −1, +1, +1, +1, −1 (B)

−3, −1, −1, −1, +1, −1, −3, −3

−12

Result is near −8.. 0 bit signal.

* Types of Media

- Guided Media
- Unguided Media.

16/8/19

* DATA LINK LAYER

Error control

Sender: 0 1 1 0 1 → Receiver: 0 1 1 1 1

simple bit error.

0 1 1 0 1 → 0 1 1 0 0

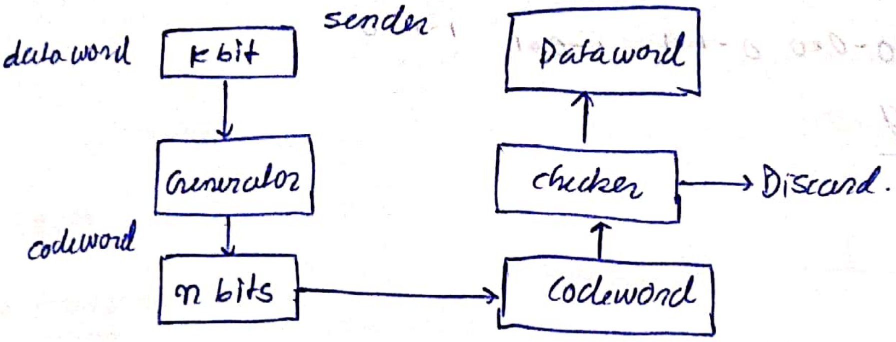
burst error length

burst error

i> Error detection

ii> Error correction
- → Forward error correction.
- → Retransmission

i> Error detection :-



2B/3B

dataword	codeword
00	000
01	011
10	101
11	110

010

This codeword isn't available
→ here, only 1 bit is changed, so we can detect the error.

101

→ here, 2 bits have been changed. so we cannot detect the error.

2B/5B

DW	CW
00	00000
01	01011
10	10101
11	11110

Assuming that here is only 1 bit error, we will consider the case with all codewords.

~~010~~ 01111 → case

* Hamming distance

00000
10101

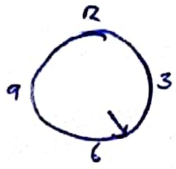
1 1 1

Hamming distⁿ = 3

* Minimum hamming distance

consider all possible pairs of codewords.
→ calculated on the basis of codewords & not dataword.

* Modulo N - Arithmetic



9:00 + 5 = 14 → 2

ADD : 0+0 = 0   0+1 = 1   1+0 = 1   1+1 = 0

SUB : 0-0 = 0   0-1 = 1   1-0 = 1   1-1 = 0

* Linear block encoding

2B/3B

00	000
01	011
10	101
11	111

$d_{min} = s+1$, s → no. of error it can detect.

$d_{min} = 2t+1$ t → no. of error it can correct.

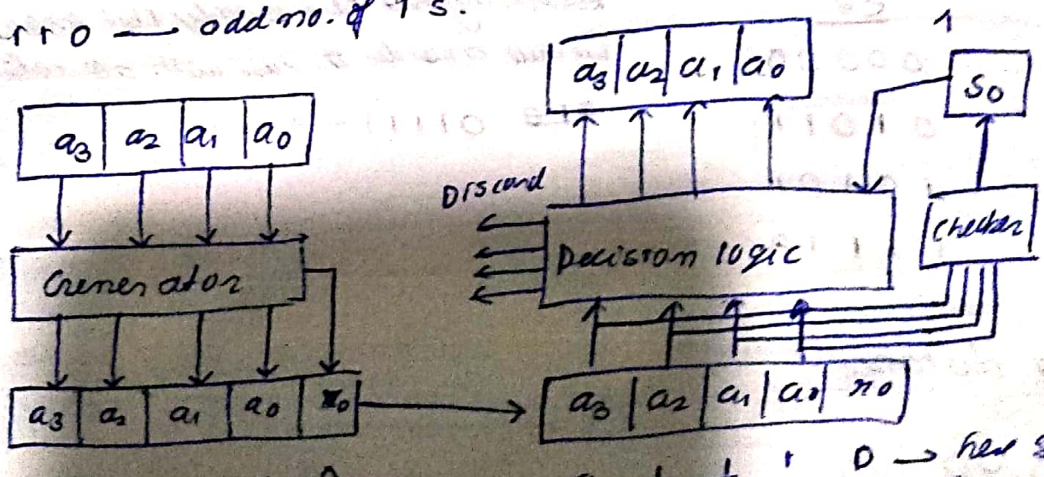
* Parity checking

↓
checking if the no. of bits are even or odd.

1010 → even no. of 1s

1110 → odd no. of 1's.

$a_3\ a_2\ a_1\ a_0$
0 1 0 1



0 1 0 1 0

0 1 1/0 1 0 → here S_0 → 1 because it has odd parity

0 0 1 1 1 → here S_0 → 1

we can detect error.

* Two dimension parity checking

1101 1100 1001 0101

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

arrange in rows & columns.
calculate parity row wise first and then column wise.

disadv: For 16 bit data we need 9 extra bits.

19/8/19

* Hamming code

$2^r \geq k + r + 1$ $r \rightarrow$ no. of redundant bits
$k \rightarrow$ no. of bits in data word.

i> The positions that are power of 2 are considered for parity bit.
$(2^0 \; 2^1 \; 2^2 \; 2^3 \; \ldots\ldots)$ 10011010

code word →

P_1	P_2	1	P_4	0	0	1	P_8	1	0	1	0			
~~2^0~~	~~2^1~~	~~2^2~~	~~2^3~~	~~2^4~~										
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Position 1 : 1, 3, 5, 7, 9, 11 (consider 1 bit & skip the next)
$P_1 = 0$ (even parity of 1)
Position 2 : 2, 3, 6, 7, 10, 11 (consider 2 & skip 2)
$P_2 = 1$
Position 4 : 4, 5, 6, 7, 12
$P_4 = 1$
Position 8 : 8, 9, 10, 11, 12
$P_8 : 0$

※

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

Now, for position 1
$P_1 = 1$
$P_2 = 0$
$P_4 = 1$ $P_8 = 0$

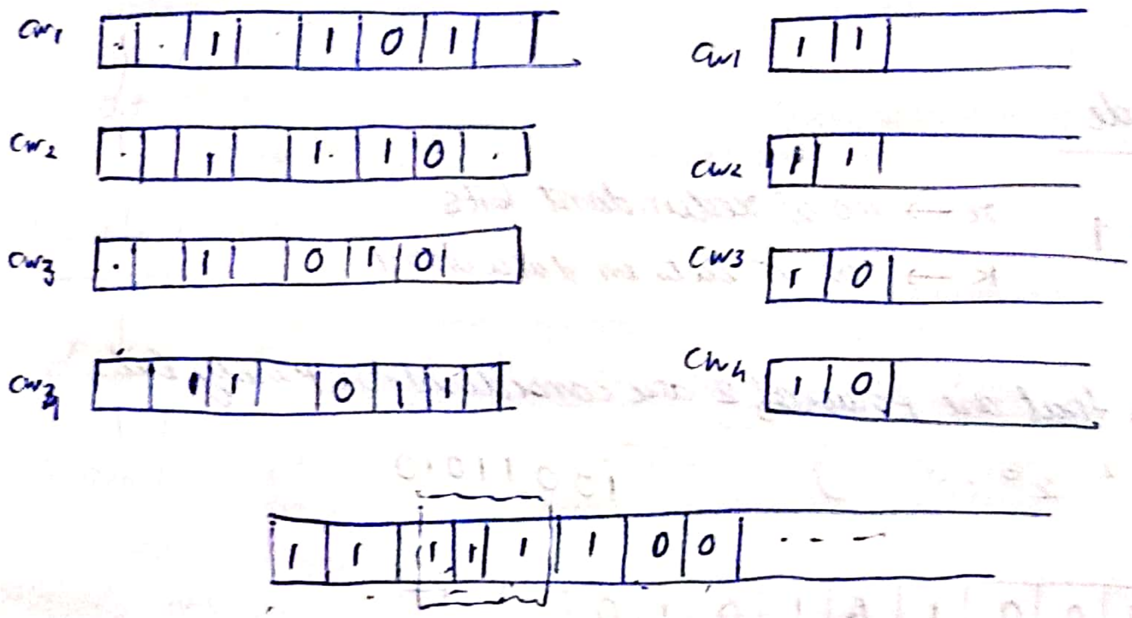
Here we are getting P_1 & P_4 as 1 which should have been 0.
Error = 1 + 4 = 5
Error in position 5

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

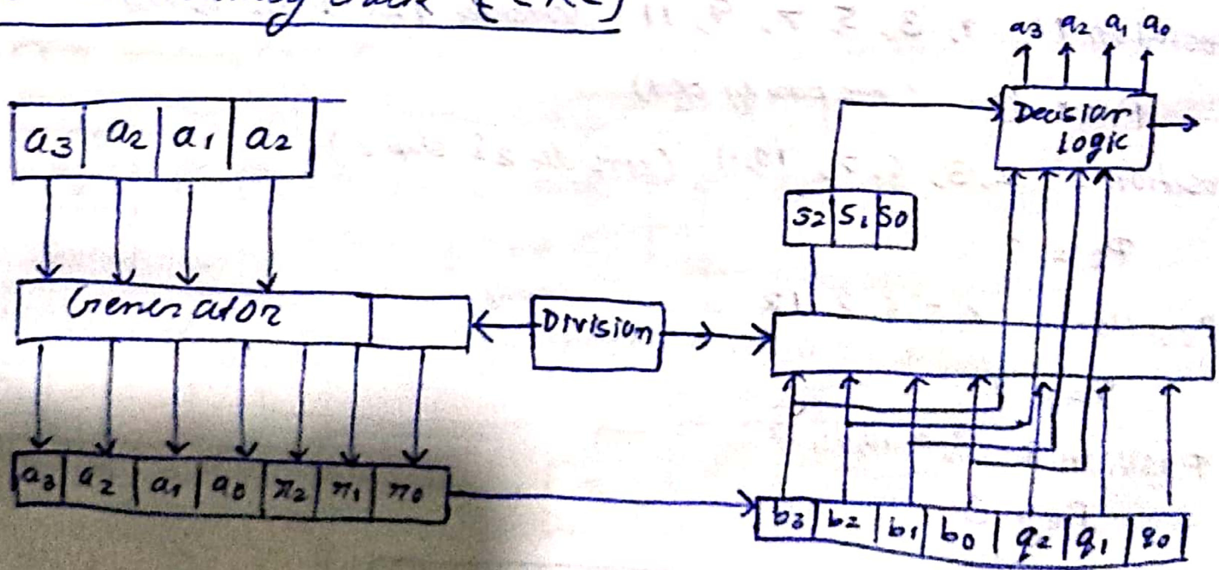
Now, $P_1 = 1$
$P_2 = 1$
$P_4 = 0$
$P_8 = 0$

Here there is no way of correcting it, all can only correct 1 bit error.

1101 (d_1) 1110 (d_2) 1010 (d_3) 1011 (d_4)



* Cyclic redundancy check (CRC)



DW 1001

Divisor ⟶ 1011

(There are 4 bits in dw & hence we add 3 bits after that)

~~1001~~

```
1011)1001000(1010
     1011
     ----
      0100
      0000
      ----
       1000
       1011
       ----
        110
       0000
       ----
        110
```

we will add the remainder bits behind the dw

```
 1001000
     110
 -------
 1001110  ⟶ CW
```

22/8/19

* Receiver side CRC checking

Divisor 1011

```
1011)1001110(10
     1011
     ----
      01110
      00000
      -----
       1110
```

```
1011)1001110(1010
     1011
     ----
      0101
      0000
      ----
       1011
       1011
       ----
          0
          0
```

Rem ⟶ 0

hence, no error.

* $x^3 + x^3 = 0$ $\quad x^3 - x^3 = 0$ $\quad x^3/x^2 = x$ $\quad x^3 \cdot x^2 = x^5$

eg: $(x^3 + x^2 + x)(x^2 + x + 1) = x^5 + \cancel{x^4} + \cancel{x^3} + \cancel{x^4} + x^3 + \cancel{x^2} + x^3 + x^2 + x$

$= x^5 + x^3 + x$

1011 $\quad\quad$ 1001000

$\downarrow$ $\quad\quad$ $\downarrow$

x^3+x+1 $\quad\quad$ $x^3(x^3+1)$

$x^3+x+1\ )\ x^6+x^3\ (\ x^3+x$

$x^6+x^4+x^3$

x^4

x^4+x^2+x

$x^2+x \longrightarrow 0110$

dataword. $d(x)$

codeword $c(x)$

generator $g(x)$

syndrome $s(x) \longrightarrow$ remainder

error $e(x)$

In receiver's side we divide $c(x)/g(x)$

If there is an error $\frac{c(x)+e(x)}{g(x)} \Rightarrow \frac{c(x)}{g(x)} + \frac{e(x)}{g(x)}$

★ 1000110

$c(x) = x^6+x^3+x^2+x+\cancel{x^4}$

$e(x) = x^3$

Find $g(x)$ such that it divides $c(x)$ but not $e(x)$.

10100101

$\downarrow$ $\quad$ $\downarrow$

x^j $\quad$ x^i

$x^j+x^i \longrightarrow$ error
where $j>i$

If 10100101 poly, x^3+x+1
will detect all double bit errors.

x^3+x+1

i> It ~~should~~ should have at least 2 terms.

ii> The coefficient of x^0 should be 1

iii> It should not divide $x^t + 1$, where $t \in (2, n-1)$

iv> It should have factors of $x+1$

~~(7, 11, 12, 0, 6, 36)~~

* Checksum (4 bit)

Dataword (7, 11, 12, 6, 36

Codeword (7, 11, 12, 0, 6, 36)

* 1's complement arithmetic

Wrapping

10101 → represent it as 4 bit no.

$$
\begin{array}{r|l}
1 & 0101 \rightarrow 21 \\
 & \quad\;\; 1 \\
\hline
 & 0110 \rightarrow 6
\end{array}
$$

1's complement of 6 → 9

0110   6

1001   9

$(2^n - 1) - no = complement$

Sender

7

11

12

0

6

0

0100   36 sum

 10

0110   6 – complement

1001   9 → complement

$\overline{CW}$ (7, 11, 12, 0, 39)

Receiver

```
 7
11
12
 0
 6
 9
---
45
```

```
10|1101
    10
-------
  1111  → wrapping

  0000  → complement.
```

If 46,

```
 10|1110
      10
---------
 1|0000  (complement it)
      1
---------
   0001  → wrapping
   1110  → complement
```

23/8/19

iii) Framing

Structure and Frame

Flag	Address	Control	Information	FCS	Flag
8 bit	8 bits extendable	8 or 16 bits	variable size	16 or 32 bits	8 bits

i) Identify a frame from where it starts ← indicated by flag byte

It is a bit pattern but same bit pattern may appear elsewhere.

a) Byte stuffing

b) Bit stuffing

a) Byte stuffing

If flag byte is appearing somewhere in between, we add ESC Flag.

Before → After (stuffing)

A Flag B → A Esc Flag B (Esc = escape byte)

(bytes)

A Esc B → A Esc Esc B

A ESC Flag B → A Esc Esc Esc Flag B

If multiple flag & esc bytes are available, we add additional esc byte for each of them.

b) Bit Stuffing

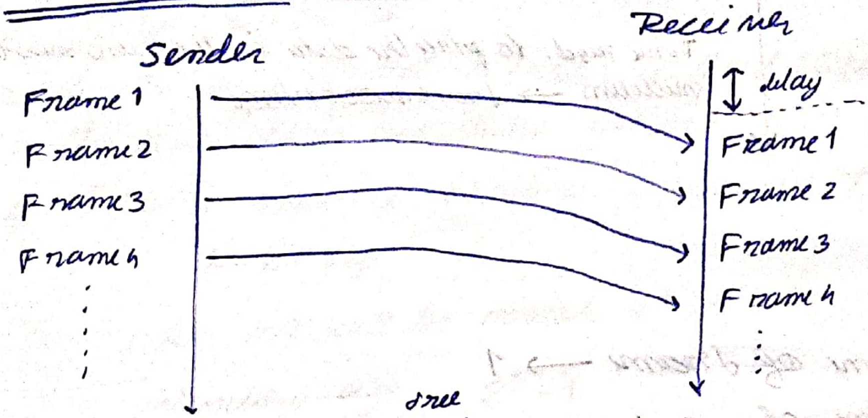
Flag 01111110

5 consecutive 1s and 0s before & after it.

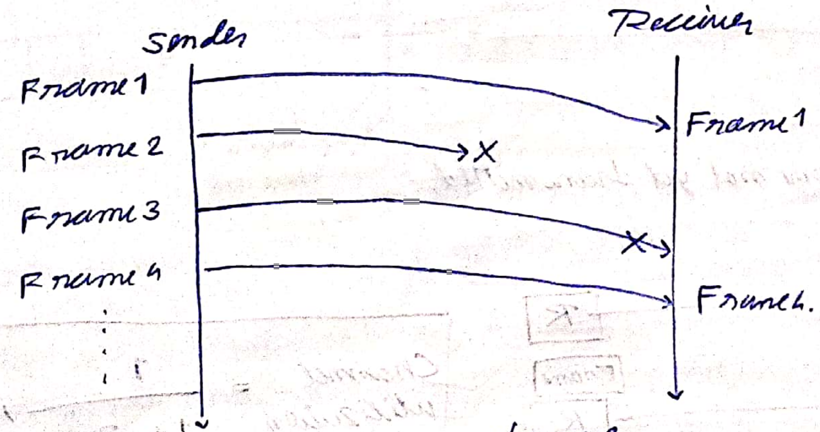
1 0 1 0 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1

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

iv) Flow Control



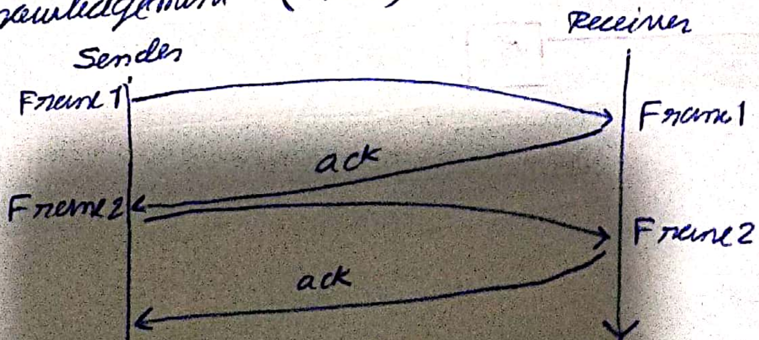
error free channel.



noisy channel

There should be same instruction by which sender give info to the receiver.

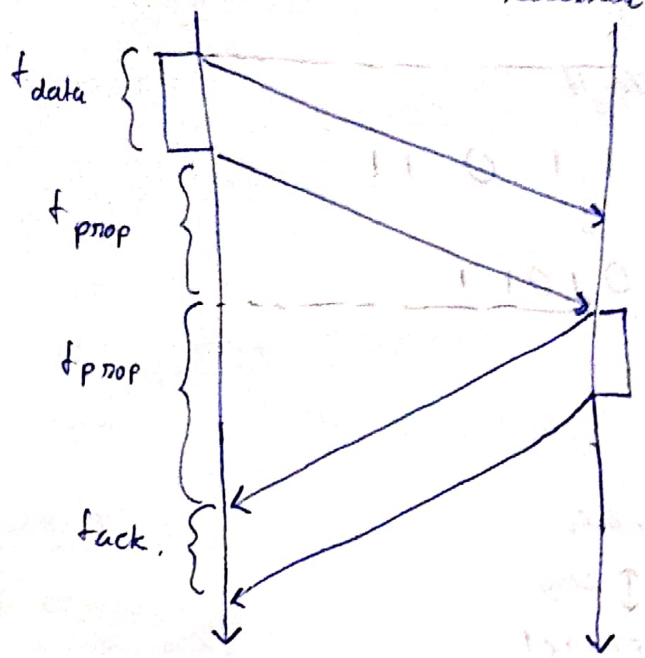
→ Acknowledgement (ACK)



error free channel

* receiver will send an acknowledgement
* sender will wait for ack

Stop and wait flow control



$1 \text{ cycle} = t_{data} + 2t_{prop} + t_{ack}$

Sender was busy during 1 cycle (for transmitting frames) $= t_{data}$.

$$\boxed{\text{channel utilization} = \frac{t_{data}}{t_{data} + 2t_{prop} + t_{ack}}}$$

Time reqd. to place the data in the transmission medium $\longrightarrow$ transmission time

Assumptions

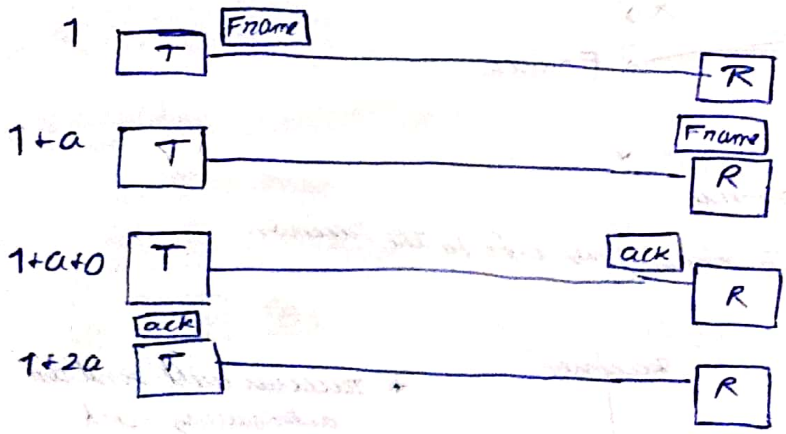
i> Transmission time of frame $\longrightarrow 1$

ii> Transmission time of ack $\longrightarrow 0$

iii> Propagation time $\longrightarrow a$

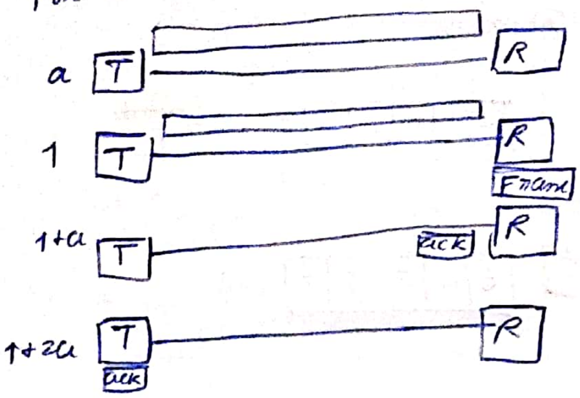
iv> noise free channel

For $a > 1$ $t = 0$, frame not yet transmitted.



$$\boxed{\text{Channel utilization} = \frac{1}{1+2a}, \; a > 1}$$

For $a < 1$, $t = 0$, frame not yet transmitted.



$$\boxed{\text{Channel utilization} = \frac{1}{1+2a}, \quad a<1}$$

It is always < 1.

Sliding Window Flow Control

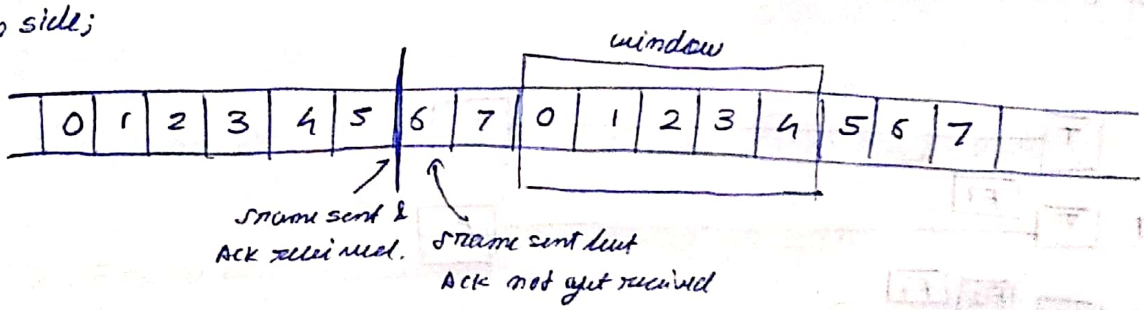
1. Window of size W
2. Sender can transmit W frames without receiving "ack".
3. Receiver sends cumulative ~~ack~~ Ack.
4. Frame sequence numbers to identify frames

    k- bit seq

    Seq. no. will be modulo 2^k.

    Window size $= 2^k - 1$

Sender side;

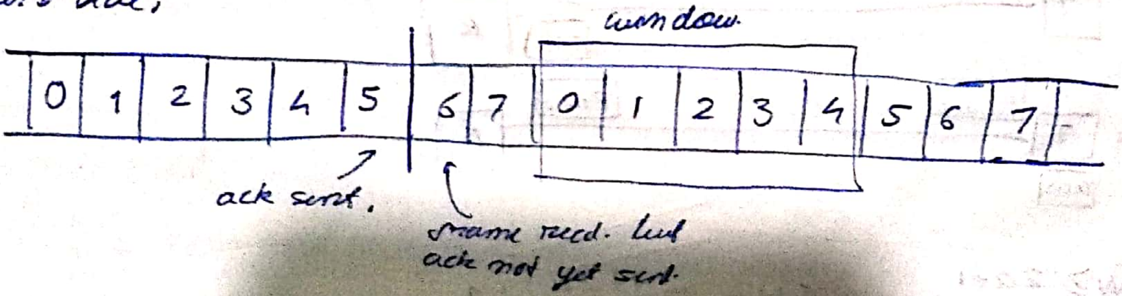


when we receive ack, the size of the window increases by the number of frames for which ack received.

Here, when ack for 6 received, window $(5) \longrightarrow (6)$

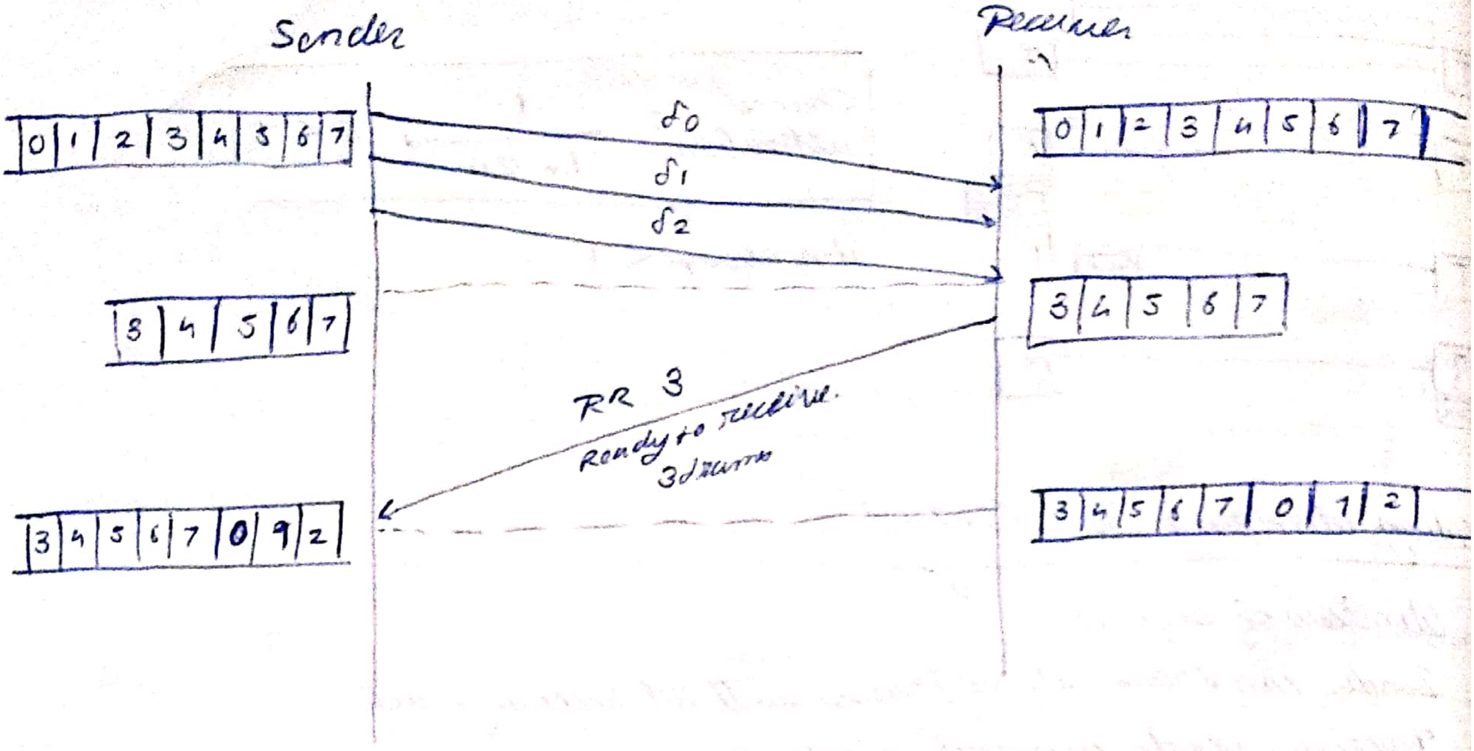
when frame sent, decrement window size by 1.

Receiver's side;

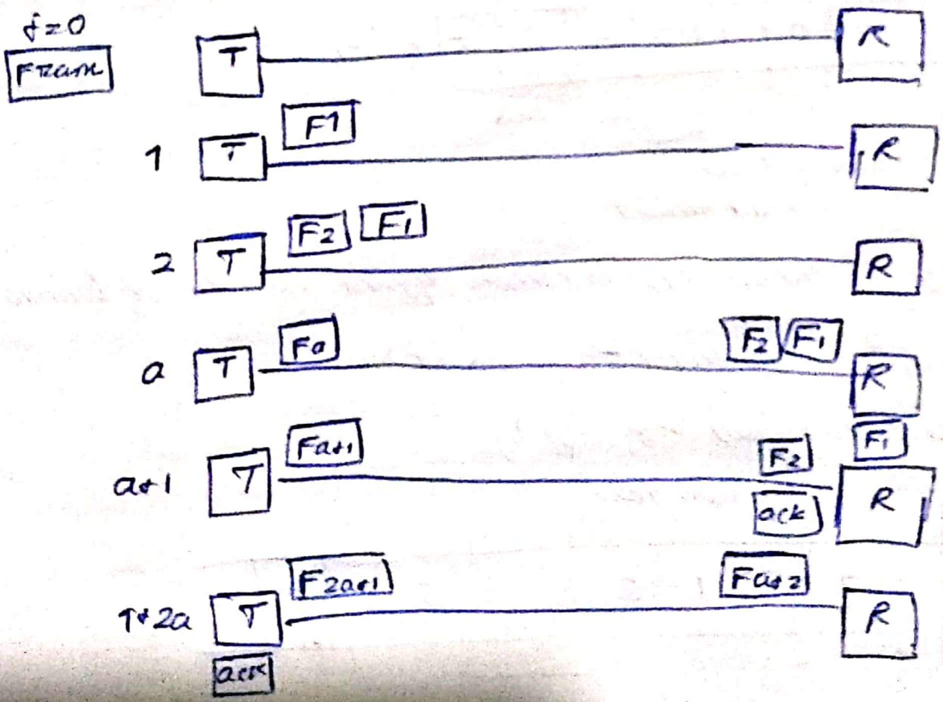


when Ack is send, window size is incremented by 1.

Scanned by CamScanner

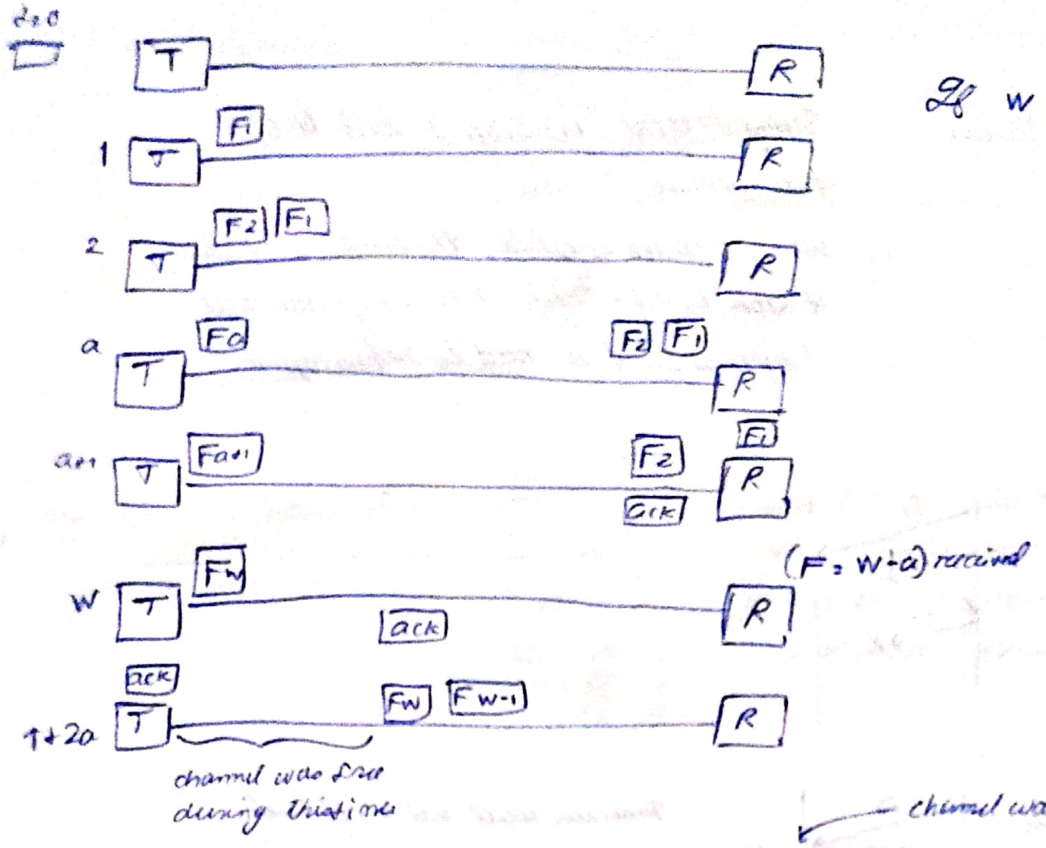


1. window size $\longrightarrow$ W
2. Transmission time $\longrightarrow$ 1
3. Propagation time $\longrightarrow$ a
4. Transmission of ack $\longrightarrow$ 0
5. Noise free channel.



If $W \geq 2a+1$ $\qquad CU = \dfrac{1+2a}{1+2a} = 1$

If $W < 2a+1$.



$$E_U = \frac{W}{1+2a}, \quad W < 2a+1$$

29/8/19

* Error control in Noisy channel

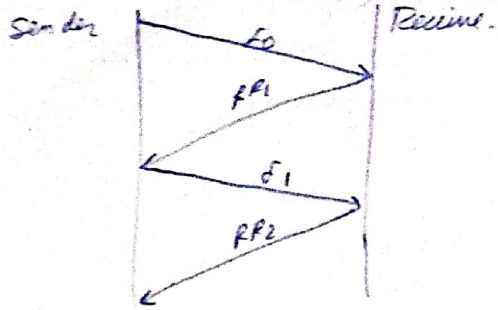
1. Frame Damaged ⟶ Frame error correction
measure ⟶ Retransmission
2. Frame Lost ⟶ measure ⟶ Retransmission

i) Positive ack (Ready to receive frame i) RR - i

ii) Negative ack (NAK)
- REJ - i (Particular frame i has been lost)
- SREJ - i

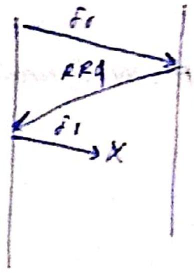
Automatic Repeat Request (ARQ)
- ⟶ Stop and wait (ARQ)
- ⟶ Go Back - N ARQ
- ⟶ Selective Reject ARQ

Stop and Wait.

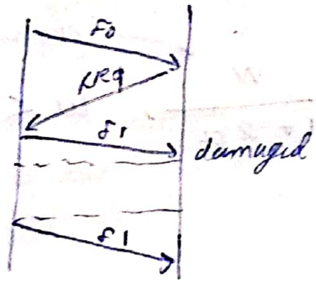


Every frame in Stop & wait ARQ has a timer.
when frame is sent, the timer is started, if ack is not received in time, time out happens and we need to retransmit.

i> Frame lost

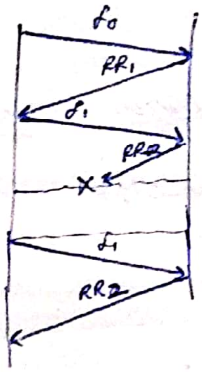


ii> Frame Damaged



Receiver will not send ack.
There will be time out.
↓
retransmission.

iii> Ack lost



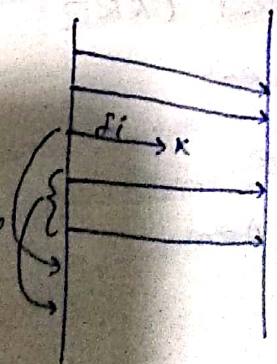
retransmission.

iv> Ack damaged. ⟶ retransmission.

Go Back N ARQ

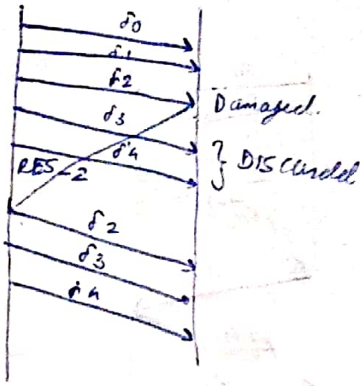
REJ - i

frame i will be retransmitted along with the frames transmitted afterwards.

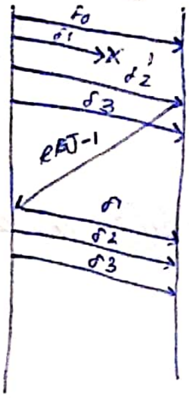


Scanned by CamScanner

a) Frame damaged.

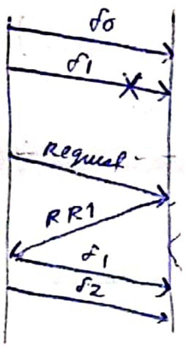


b) Frame lost



when further frames are transmitted after a particular frame is sent, we can identify the lost frame on the basis of the subsequent frames.

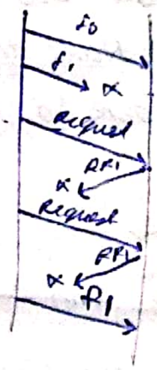
when no additional frames have not been transmitted



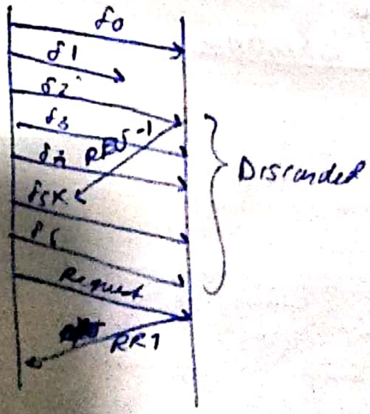
sender sends request on the basis of timer.

c) Positive ACK (RR) lost

~~d) Negative ACK REJ lost.~~

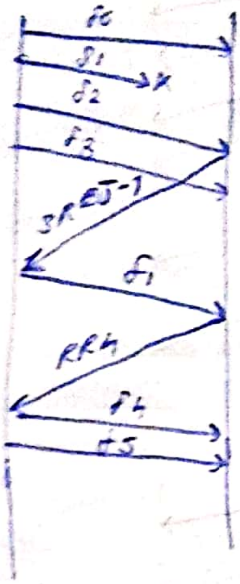


d) Negative ACK REJ lost



Selective Reject ARQ

SREJ - i



* Piggybacking

It we send the acknowledgement along with the data.

* Protocols in Data Link Layer

1. HDLC (High Level Data Link Control)
2. PPP (Point to Point Protocol)

1. HDLC

It is a bit oriented protocol.

→ Selective ARQ or Go-back-N ARQ.

→ Full duplex or Half duplex

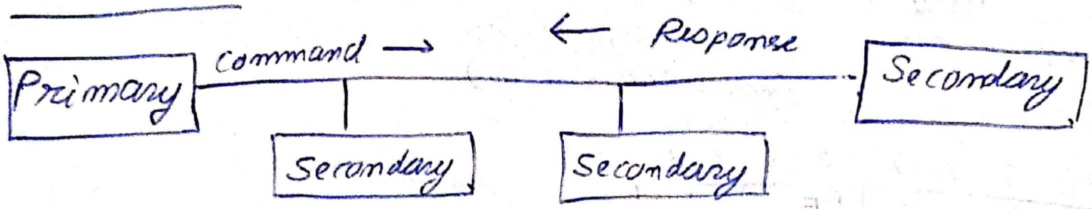
→ Physical layer clock to Synchronize.

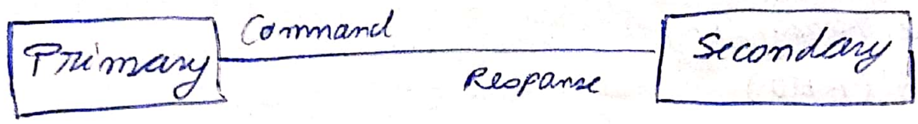
HDLC station types

1. Primary stations → initiates the communication mou
2. Secondary stations — act in response to primary station
3. Combined station

HDLC Link configuration.

Unbalanced.

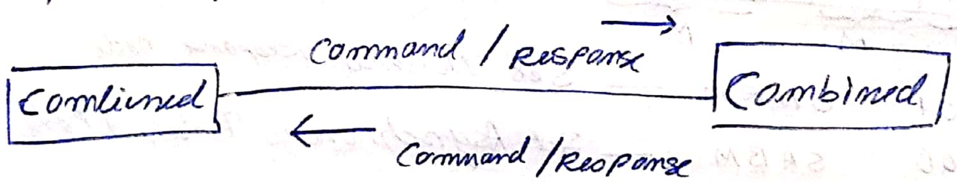




point to point.

Balanced

point to point



HDLC Data Transfer Modes

1. Normal Response Mode (NRM)
2. Asynchronous Response Mode (ARM)
3. Asynchronous Balanced Mode (ABM)

HDLC Frame Types.

1. Unnumbered (U Frame)
2. Information (I Frame)
3. Supervisory (S Frame)

HDLC Frame structure:-

Flag	Address	Control	Information	FCS	Flag
8 bit	8 bit intendable	8 bit.		CRC	8 bit

I Frame:

1	2	3	4	5	6	7	8
0				P/F			

$\underbrace{2\ 3\ 4}_{N(S)}$ $\underbrace{6\ 7\ 8}_{N(R)}$

P → Poll 1

F → Final 0

N(S) Send sequence no:

N(R) Receive sequence no: (acknowledgement no.)

S Frame.

1	2	3	4	5	6	7	8
1	0			P/F			

$\underbrace{6\ 7\ 8}_{N(R)}$

00 → Receive Ready (RR)

01 → Reject (REJ)

10 → Receive Not Ready (RNR)

11 → Selective Reject (SREJ)

U Frame

1	2	3	4	5	6	7	8
1	1			P/F			

$\underbrace{3\ 4}_{M}$ $\underbrace{6\ 7\ 8}_{M}$

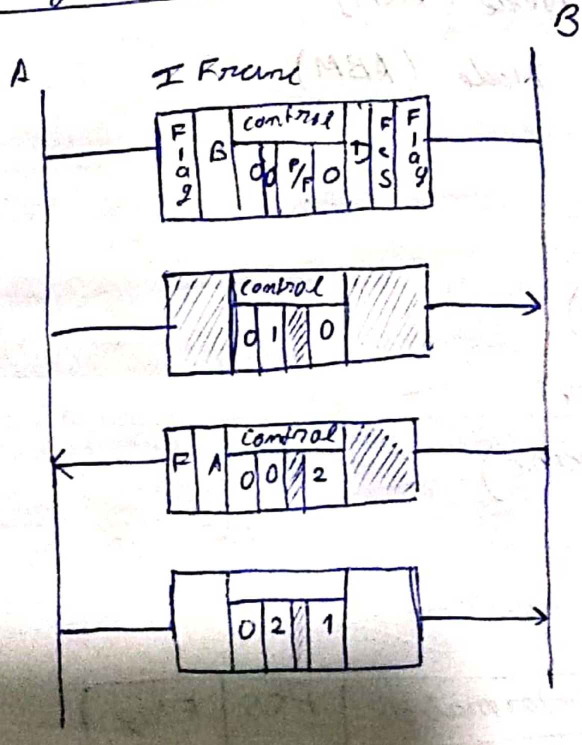
00 001 SNRM — Set Normal Response Mode

11 100 SABM — Set Asynchronous Balanced Mode.

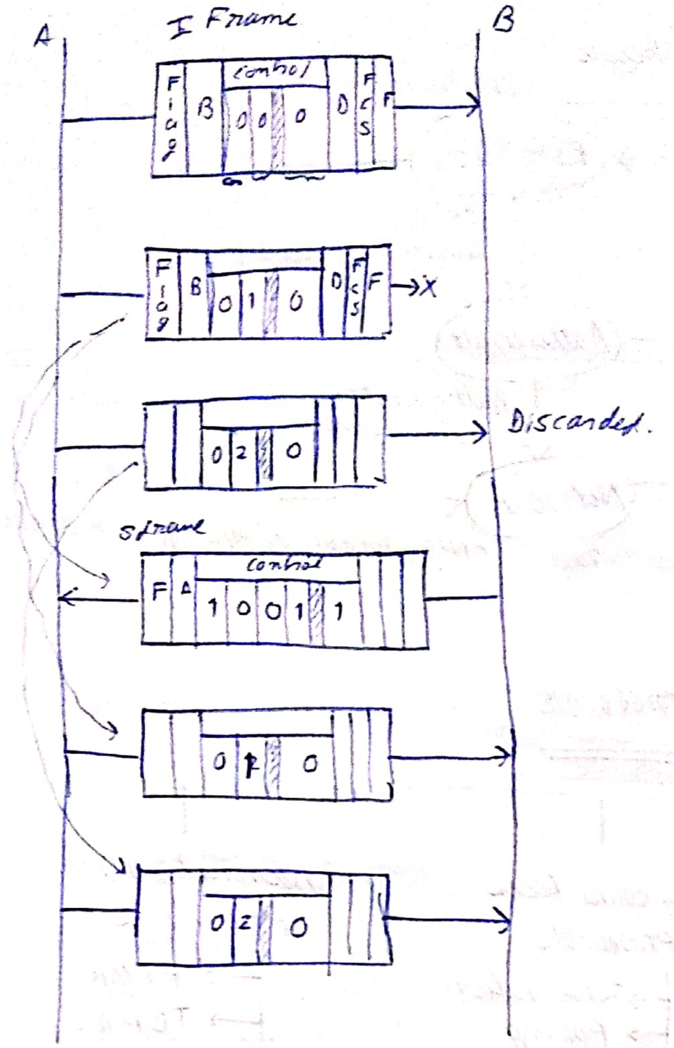
00 110 UA → Unnumbered ACK

00 010 DISC → Disconnect.

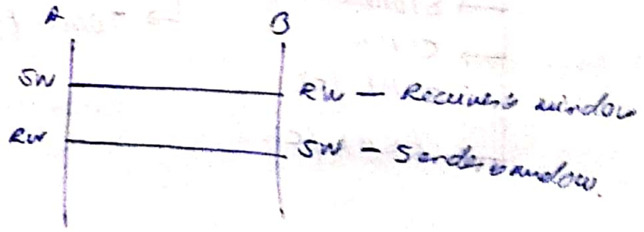
Piggybacking of HDLC Frame without error



Piggy backing of HDLC Frame with error



* when data comm. occurs both sides, then there are 2 windows on each side



* PPP

- → Byte oriented
- → Point to point

Flag	Address	Control	Protocol	Payload	FCS	Flag
	11111111	11000000	↑			

i> Link Control Protocol (LCP)

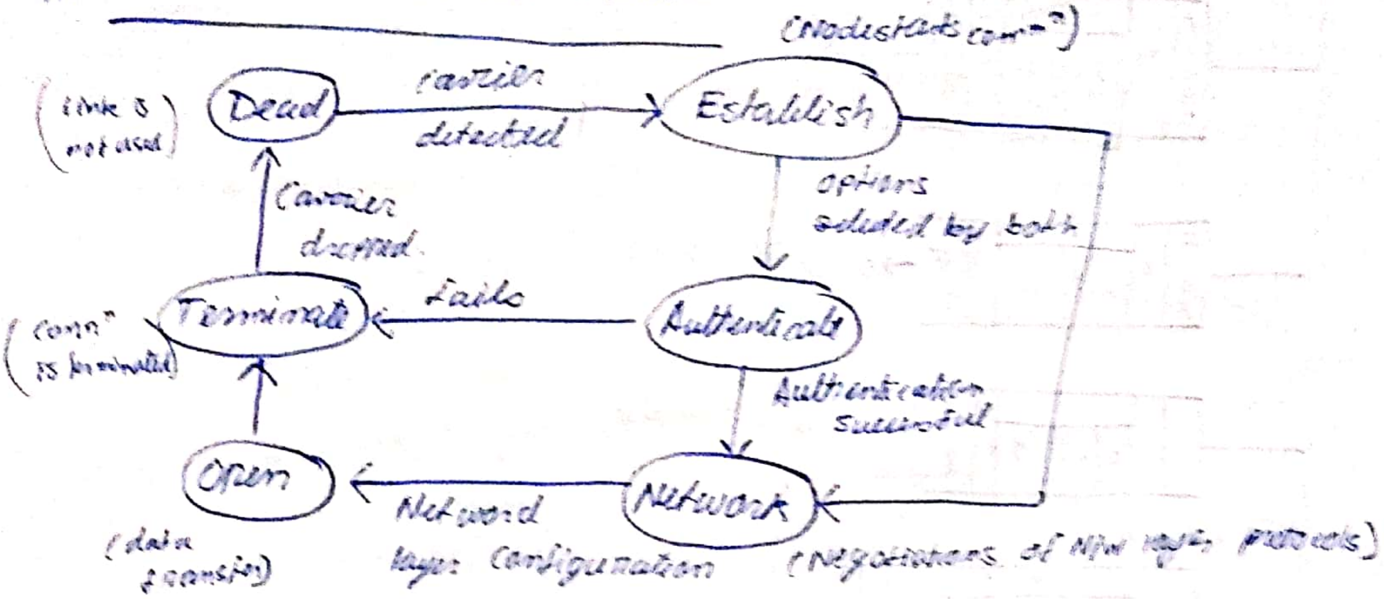
ii> Authentication Protocol

a> Password authentication Protocol (PAP)

b> Challenge Handshake Authentication Protocol (CHAP)

iii) Network Control Protocol.

PPP Transition Phase



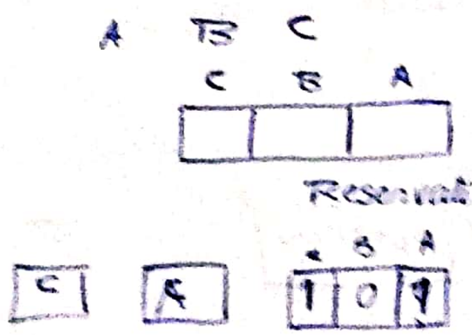
4/9/19

* Multiple Access Control Protocols

- Random access protocols
  - ALOHA
  - Slotted ALOHA
  - CSMA
  - CSMA/CD
  - CSMA/CA
- Controlled Access Protocols
  - Reservation
  - Polling
  - Token passing.
- Channelization Protocols.
  - FDMA
  - TDMA
  - CDMA.

#

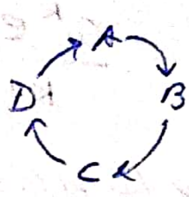
1. Reservation



Suppose A & C has data to be sent frame would be:

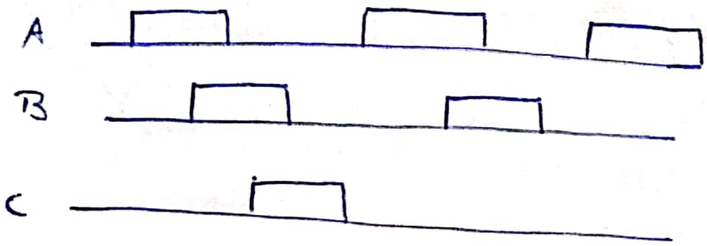
3. Token passing

Token is passed from one station to another. If a station has data, then it is transmitted otherwise the token is passed on there by preventing collisions.



Random Access Protocols

1. ALOHA



Every frame is having a collision. Hence, parts of the signal is damaged.

*) Frame time :- Time taken by frame to reach from source to destn.

ii) N frames on an average (transmitted during frame time)

iii) $0 < N < 1$

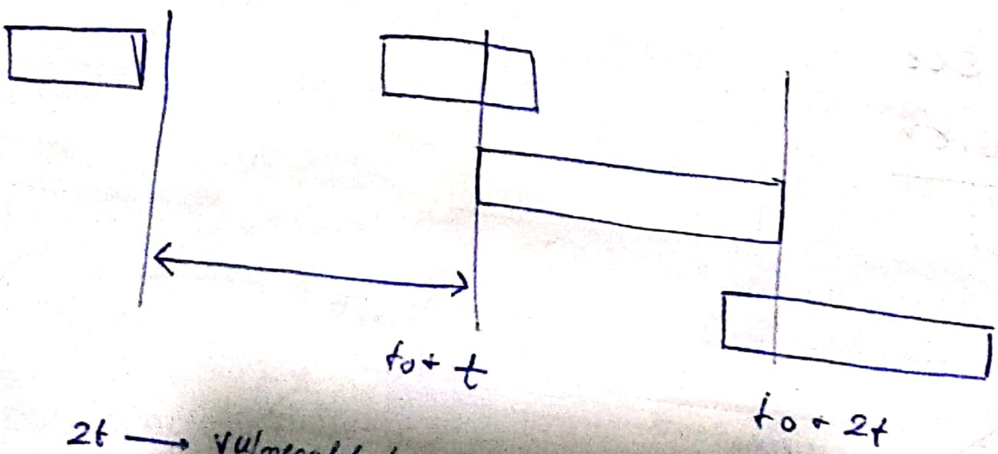
iv) G frames (new + old) $\longrightarrow$ avg no.

v) $N \approx 0$, $G \approx N$

$N > 1$, $G > N$

vi) Throughput $S = G P_0$

$P_0 \longrightarrow$ Prob. that a frame does not suffer a collision.



$2t \longrightarrow$ Vulnerable to collision during this period.

Scanned by CamScanner

Exactly K frames are being transmitted (Prob.)

$$P(K,G) = \frac{G^k e^{-G}}{K!}$$

when 0 frames are being transmitted, (during frame time → t)

$$P_0 = e^{-G}$$

for 2t period of time (vulnerability period)

$$P_0 = e^{-2G}$$

Throughput for ALOHA protocol,

$$S = G P_0$$

$$\boxed{S = G e^{-2G}}$$

$G = 0.5$ $\quad S = \frac{1}{2e} = 0.184$

18.4% frames will be transmitted successfully without collision.

2. Slotted ALOHA

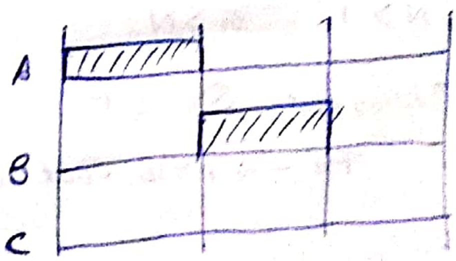
$$S = G P_0$$

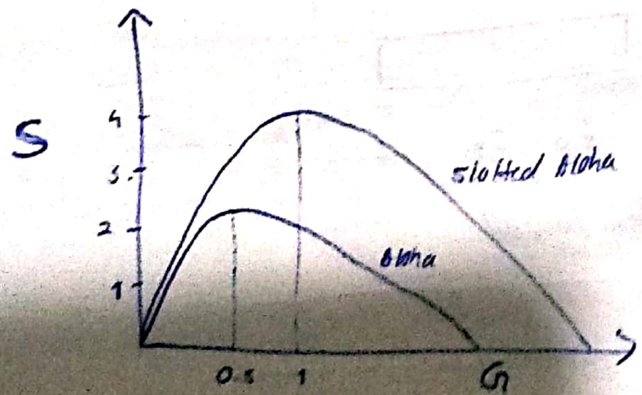
for t, $P_0 = e^{-G}$

$$S = G e^{-G}, \quad G = 1$$

$$\Rightarrow S = 1/e = 0.368$$

36.8%

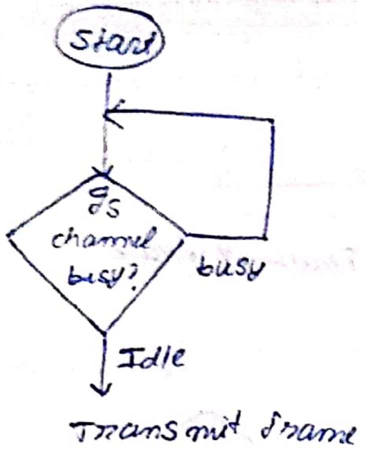




3. Carrier sense multiple access (CSMA)

- 1-persistent
- Non persistent
- P-persistent

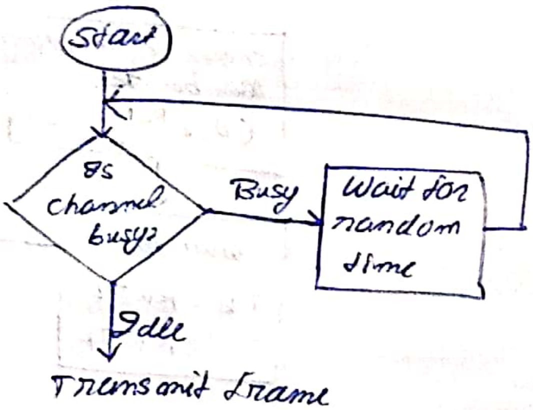
i) 1-persistent



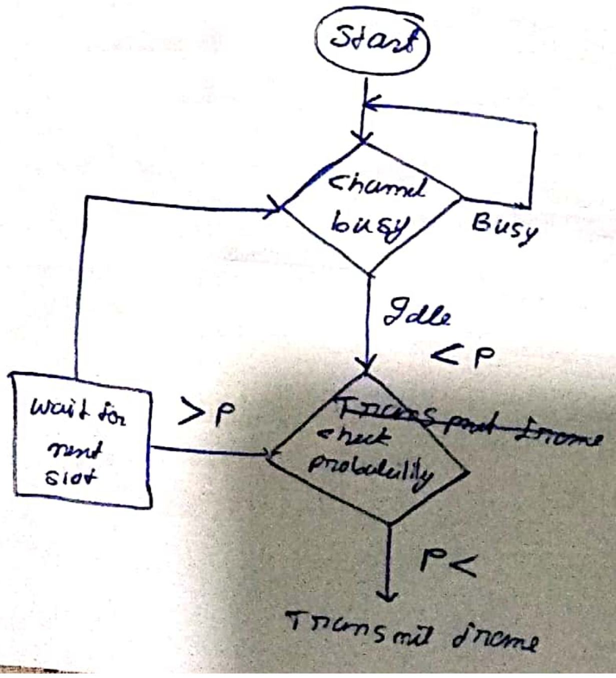
Checks if the ~~frame~~ channel is ideal. If it is, then frame is transmitted. Otherwise it checks repeatedly until channel is ideal.

Transmission with probability 1.

ii) Non persistent

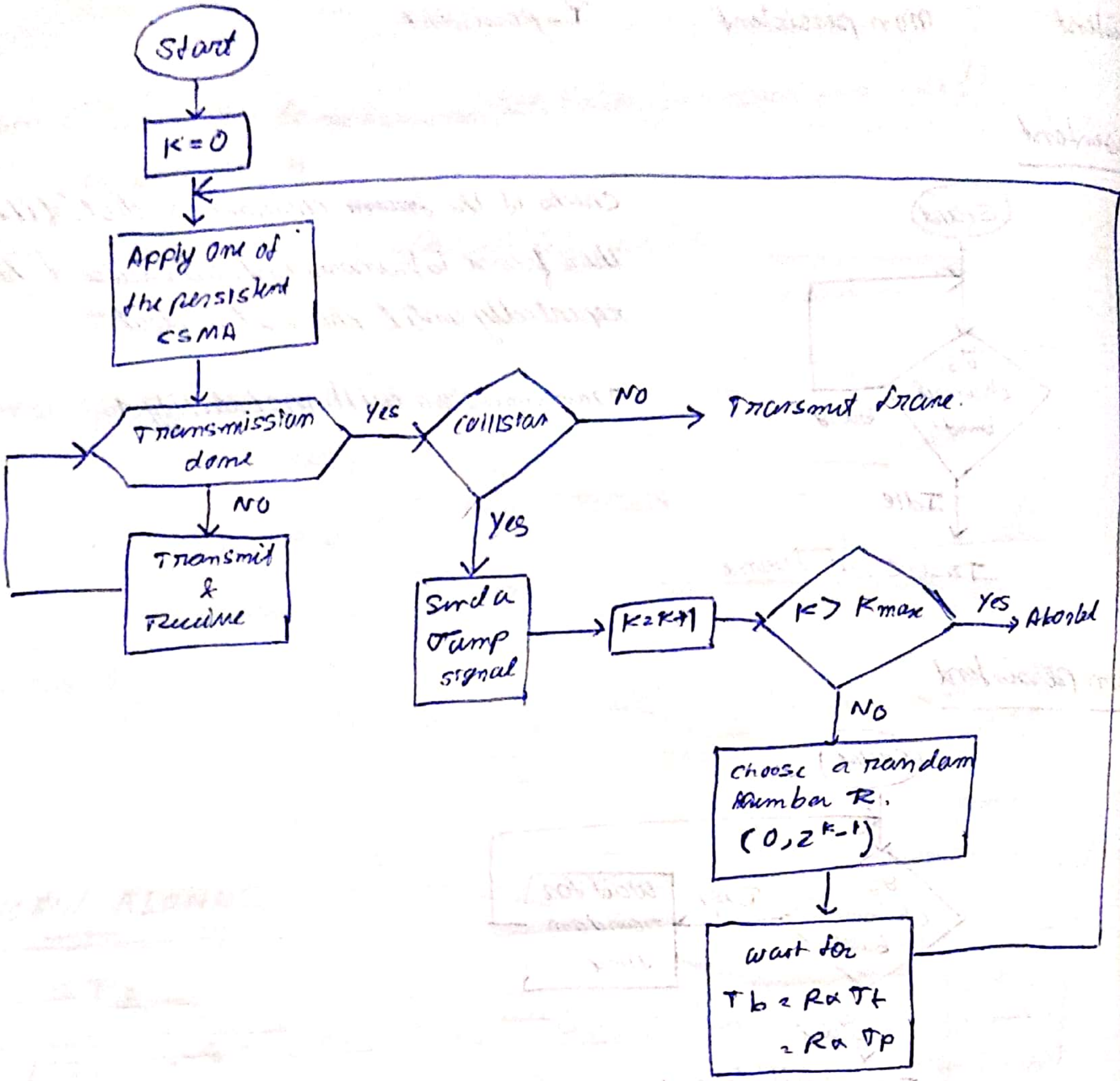


iii) P-persistent



12/9/19

4. CSMA /CD (Collision Detection)



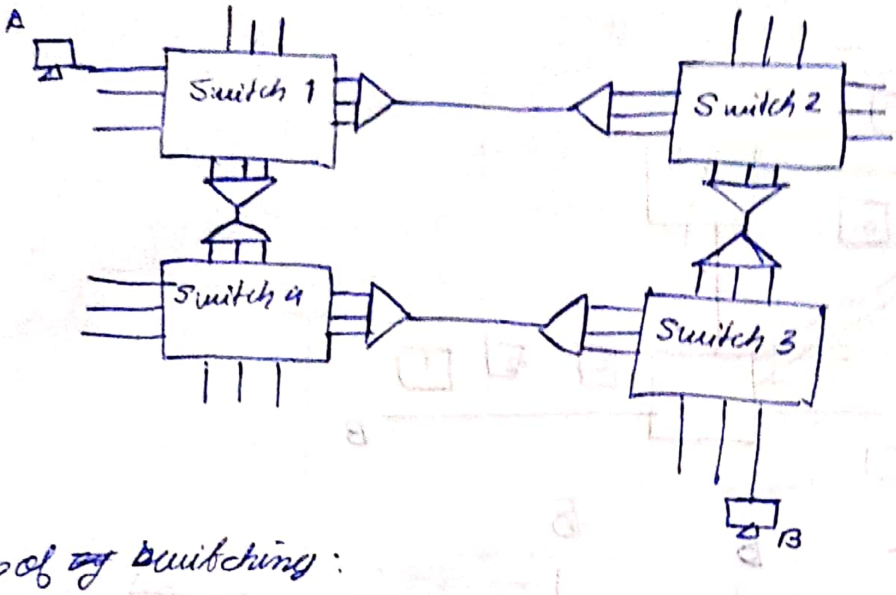
5. CSMA / CA

i> Inter frame Space (IFS)

ii> Contention Window

iii> Acknowledgement

* Switching



Types of ~~of~~ switching :

- → Circuit Switching
- → Packet Switching
  - Datagram network
  - Virtual Circuit Network.
- → Message Switching

1> Circuit Switching:-

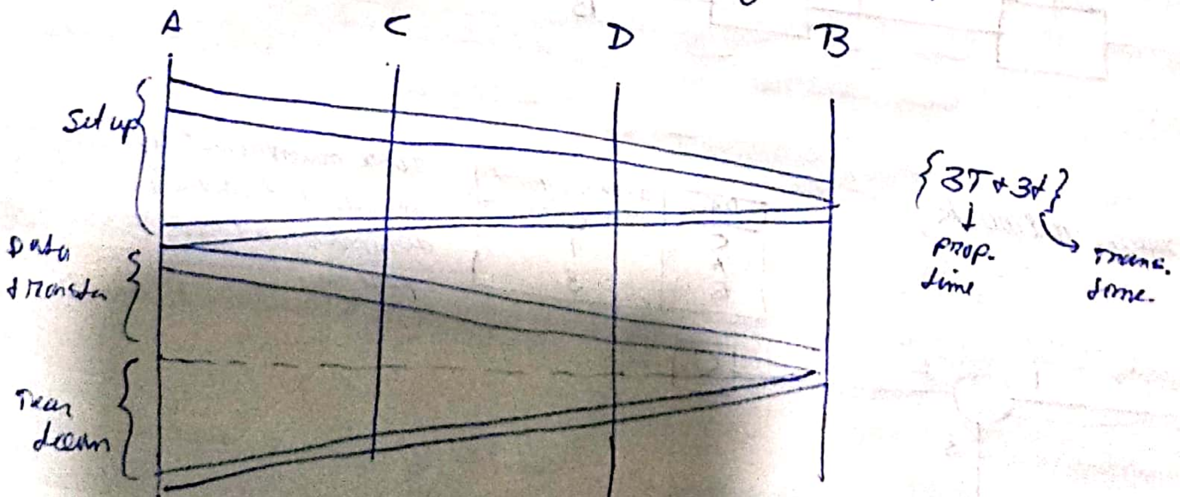
i> Set up phase

ii> Data transfer phase

iii> Teardown phase.

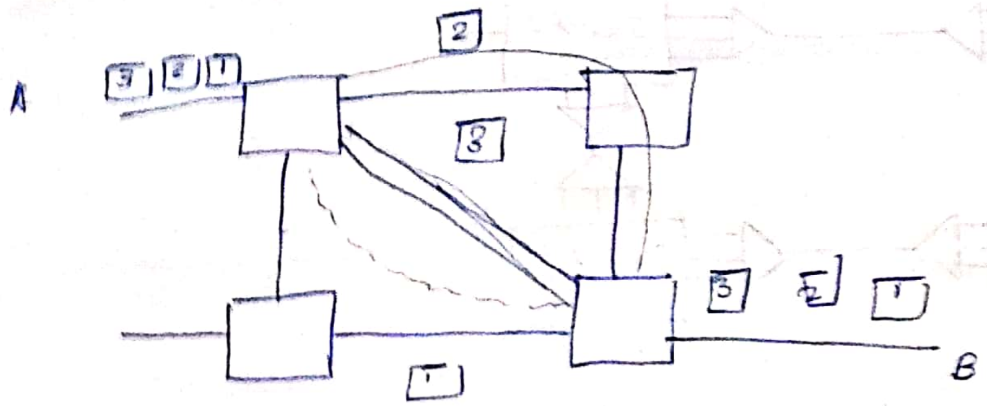
A particular path is set for transmission of data and that path cannot be used by others.

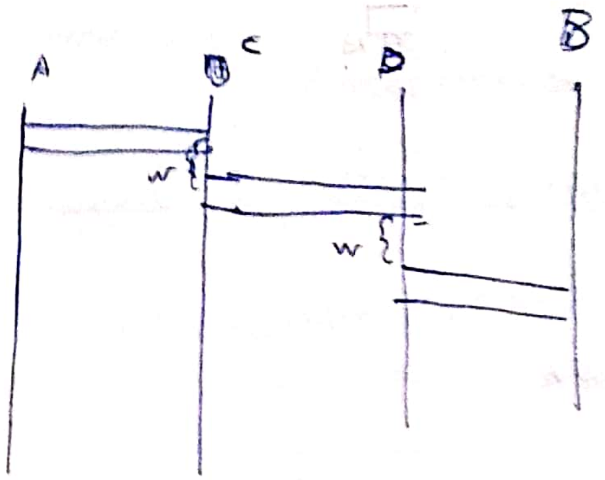
Its performance depend on: efficiency & delay.



2. Packet switching

i) Datagram network



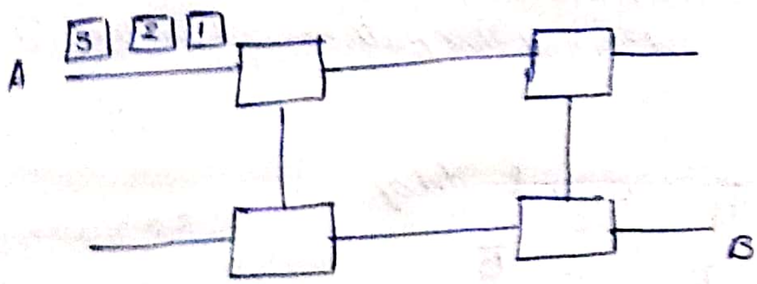


~~3T + 3 (t + 2t)~~

Delay = 8T + 3t + 2w

w → waiting time

ii) Virtual Circuit ~~Network~~ Network



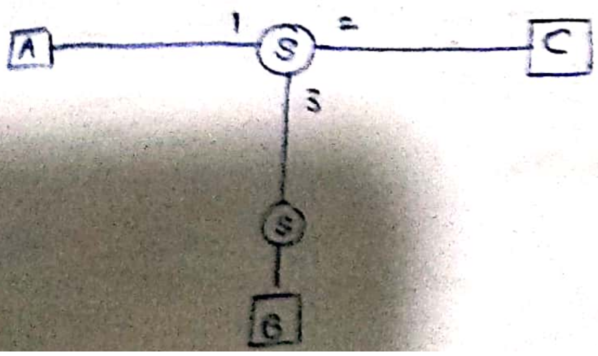
They have the same 3 phases as circuit switching.

13/9/19

From Datagram network,

DA	Interface Port
C	2
A	1
B	3

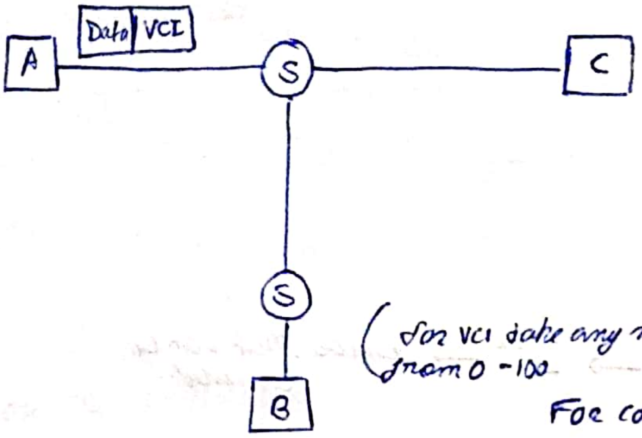
Table maintained by switch that contains destination address & port no.



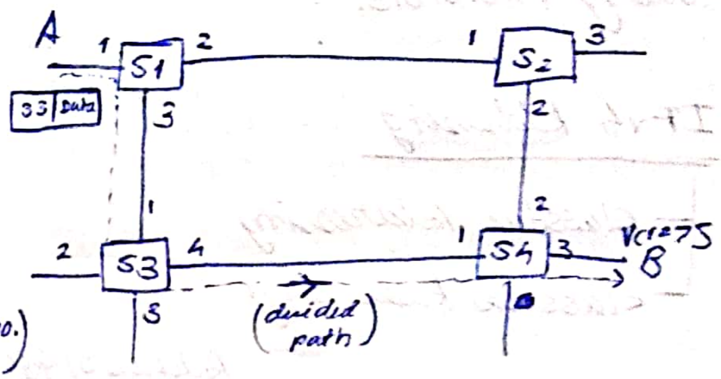
For virtual circuit network;

VCI → Virtual Circuit Interface.
(It will be used locally / b/w two devices)

Incoming		Outgoing	
Port	VCI	Port	VCI



(for VCI take any no. from 0 - 100)



For comm from A to B

S1

In		Out	
Port	VCI	Port	VCI
1	33	3	21

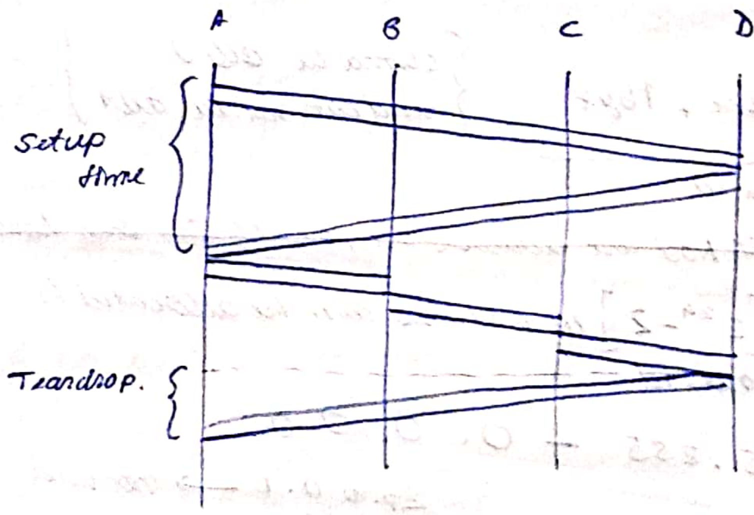
S3

In		Out	
Port	VCI	Port	VCI
1	21	4	55

S4

In		Out	
Port	VCI	Port	VCI
1	55	3	75

After the data is sent, A sends a request for ack. After the ack is received by all the switches and A, the VCI are deleted as well as the data. The tables are updated.



$[3T + 3t]$

3. Message switching

(Store & forward network) msg is first stored and then forwarded.

Scanned by CamScanner

NETWORK LAYER

- Internet Protocol (IP) ⟶ IP addressing
  └⟶ IPv4, IPv6

- Routing Protocols.

* IPv4 Addressing

- classful Addressing
- classless Addressing

Address space ⟶ 2^{32} ⟶ devices that can be connected.

32 bit

___ . ___ . ___ . ___
1byte 1byte 1byte 1byte

Network id   Host id

Classful Addressing

separated into classes.

class A

$\underbrace{0 \text{ 7bit}}_{\text{Network id}}$. $\underbrace{\text{1byte . 1byte . 1byte}}_{\text{Host id}}$

{ cannot be all 0 and cannot be all 1 }

Thus, we can have 2^7 network id

~~2^{24} Host are address are possible for each host~~

Thus $[2^{24} - 2]$ ip address can be allocated to each net. id.

classA : addressing range

0. 0. 0.0 – 127. 255. 255. 255

27.0.0.1 ⟶ not used.

class B

$\underbrace{10 \text{ 6bit . 1byte}}_{\text{Network id}}$. $\underbrace{\text{1byte. 1byte}}_{\text{Host id}}$

2^{14} network ids.

$2^{16} - 2$ Hosts can be connected to each net id

range: [128. 0. 0. 0
191. 255. 255. 255]

class C

110 $\underline{5\text{bits}}$. 1 byte . 1 byte . 1 byte

$\underbrace{110\ 5\text{bits} . 1\text{byte} . 1\text{byte}}_{\text{Network id}} . \underbrace{1\text{byte}}_{\text{Host id}}$

2^{21} network ids.

$2^8 - 2$ hosts can be connected to each net id.

range of class C [192.0.0.0
223.255.255.255

class D

1110 $\underline{4\text{bits}}$. 1 byte . 1 byte . 1 byte

Here the network id & host id is not defined as it is reserved for future

range of class D [224.0.0.0
229.255.255.255

class E

1111 $\underline{4\text{bits}}$. 1 byte . 1 byte . 1 byte

Here the network & host id aren't defined and it is reserved for research purpose

range of class E [240.0.0.0
255.255.255.255

16/9/19

* Classful IP address allocation

Eg: Given that we need 240 ipaddresses
(meaning → 240 host id for a network id)
Hence, we can use class C as there can be $2^8 - 2$ host ids = 254 host ids

Subnet mask

class A	255.0.0.0	
class B	255.255.0.0	By default
class C	255.255.255.0	

n bits are 1
& 32-n bits are 0

In class A → n = 8
class B → n = 16
class C → n = 24

Eg: IP address is 192.1.2.5

Hence it belongs to class C (observing the ranges)

To find its network id.

convert to binary, [192.1.2.5 & 255.255.255.0]

11000000 . 00000001 . 00000010 . 00000101

11111111 . 11111111 . 11111111 . 00000000

(AND)

11000000 . 00000001 . 00000010 . 00000000

(192.1.2.0)
↳ Network id

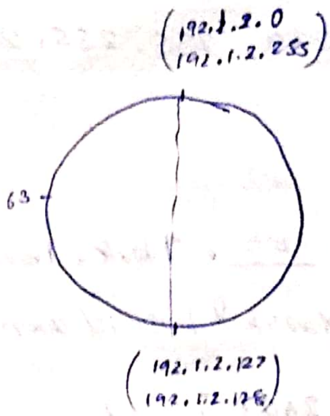
Subnetting

Grouping the network into subgroups / subnets.

Eg: network id → 192.1.2.0

to be divided into 4 groups.

Initially dividing it into 2 groups.



1st { 192.1.2. 0|000 0000
0|111 1111 (127)

2nd { 192.1.2. 1|000 0000 (128)
1|111 1111

Further dividing. because we divided into 2 groups

Network id (1st) = 192.1.2.0 (AND with 255.255.255.128)

Network id (2nd) = 192.1.2.128

Considering 1st net id 192.1.2.0 and dividing further. Subnet mask 255.255

1st { 192.1.2.00|00 0000 (0)
00|11 1111 (63)

2nd { 192.1.2.01|00 0000 (64)
01|11 1111

3rd { 192.1.2.10|00 0000
10|11 1111

4th { 192.1.2.11|00 0000
11|11 1111

Scanned by CamScanner

Subnet mask for all the four group.

255. 255. 255 . 192

* For 2^n groups ⟶ we need n bits

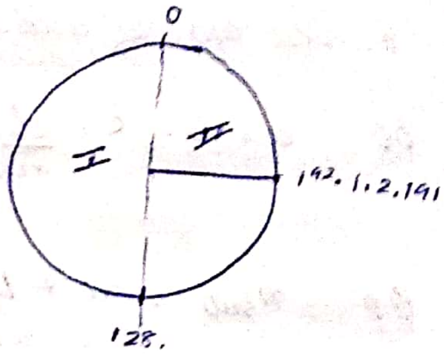
Eg: If 3 groups and classfull address is given then we need, $2^2 = 4$ groups.

Variable length subnet mask (VLSM)

Eg. 3 groups. [192.1. 2.0]

① group 128 addresses

② group 64 addresses.



For 1st group ⟶ 128 address

⟶ 2^7

we need 7 bits.

192. 1. 2. 0|0000000

Its subnet mask will be

~~255.255.255~~. 1.0000000

⇓

~~192~~ 255. 255. 255. 128

192. 1. 2. 0|000 0000

192. 1. 2. 0|1111111 (127)

Now network id for part II = 192.1. 2.128

For 64 address ⟶ 2^6

6 bits reqd.

192.1. 2.10|00 0000   192.1.2.11|00 0000

192.1.2.10|11 1111   192.1.2.11|11 1111

Subnet mask for 2 groups in part II

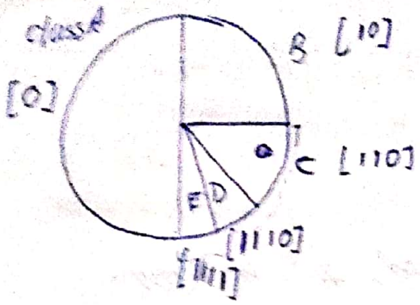
255. 255. 255. 192

19/9/19

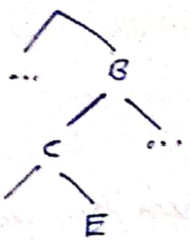
* Classless IP Addressing

CIDR - Classless Interdomain routing

* Classless IP addressing can be mapped to classful IP address.



class A represents the entire group.



Rules for CIDR block

1. All IP address should be continuous.
2. The no. of address in each sub network should be power of 2.

ϕϕ a . b . c . d
$\underline{n}$ ← network prefix or prefix

ϕϕ $n_{sub} = n + \log_2 (N/N_{sub})$

3. The starting address in each sub network should be divisible by the number of address in that sub network.

ϕϕ In each case dividing 12 by powers of 2.

	Q	R	Q	R
[By 2^1]	6	0	110	0
[By 2^2]	3	0	11	00
	1	4	1	100
	0	12	0	1100

$N_{sub} = 2^k$

Now,
we have 32 address

192. 1. 2. 0 /24

24 bits are used to represent the net. id
then, 8 bits left for host id
can be represented a

$n_{sub} = 2^8$

ϕϕ 130. 34. 12. 64 /26
4 equal groups

$n = 26$
$N = 2^{32-26} = 2^6 = 64$ ip address

$N_{sub1} = N_{sub2} = N_{sub3} = N_{sub4} = 64/4 = 16$

$n_{sub1} = n_{sub2} = n_{sub3} = n_{sub4} = n + \log_2 (N/N_{sub})$

$= 26 + \log_2 4$

$= 28$

130 . 34 . 12 . 0100 0000	130 . 34 . 12 . 0100 0000
255 . 255 . 255 . 1111 0000	0 . 0 . 0 . 0000 1111
First (AND) 130 . 34 . 12 . 64/28	Last (OR) 130 . 34 . 12 . 79/28
130 . 34 . 12 . 80/28	130 . 34 . 12 . 80
255 . 255 . 255 . 1111 0000	0 . 0 . 0 . 0000 1111
130 . 34 . 12 . 80/28	130 . 34 . 12 . 95/28
130 . 34 . 12 . 96/28	130 . 34 . 12 . 96/28
255 . 255 . 255 . 1111 0000	0 . 0 . 0 . 0000 1111
130 . 34 . 12 . 96/28	130 . 34 . 12 . 111/26
130 . 34 . 12 . 112/28	130 . 34 . 12 . 112/28
255 . 255 . 255 . 1111 0000	0 . 0 . 0 . 0000 1111
130 . 24 . 12 . 112/28	130 . 34 . 12 . 127/28

Q) 14.24.74.0/24 3 blocks 120, 60, 10 addresses.

$n = 24 \quad N = 2^{32-24} = 2^8 = 256$

$120 \xrightarrow{\text{nearest}} 128 = 2^7 = N_{sub}$.

$n_{sub} = 24 + \log_2 \left(\frac{2^8}{2^7}\right) = 25$

14 . 24 . 74 . 0	14 . 24 . 74 . 0
255 . 255 . 255 . 1000 0000	0 . 0 . 0 . 0111 1111
first (AND) 14 . 24 . 74 . 0/25	last (AND) 14 . 24 . 74 . 127/25

$60 \longrightarrow 64 = 2^6 = N_{sub}$

$n_{sub} = 24 + \log_2 (2^8/2^6) = 26$

14 . 24 . 74 . 128	14 . 24 . 74 . 128
255 . 255 . 255 . 1100 0000	0 . 0 . 0 . 0011 1111
first (AND) 14 . 24 . 74 . 128/26	last (OR) 14 . 24 . 74 . 191/26

Scanned by CamScanner

$10 \longrightarrow 16 = 2^4 = N_{sub}$

$n_{sub} = 24 + \log_2 (2^8/2^4) = 28$

$$\begin{array}{r} 14.24.74.192/ \\ 255.255.255.11110000 \\ \hline \end{array}$$

(AND) first. $14.24.74.192/28$

$$\begin{array}{r} 14.24.74.192 \\ 0.0.0.00001111 \\ \hline \end{array}$$

OR (last) $14.24.74.207/28$

$$\begin{array}{r} 128 \\ +64 \\ +16 \\ \hline 208 \end{array}$$

$$\begin{array}{r} 256 \\ 208 \\ \hline \end{array}$$

20/9/19.

Q. 190.100.0.0/16

Divide into 3 groups with:

Group 1 has 64 customers. Each needs 256 address.

Group 2 has 128 customers. Each needs 128 address

Group 3 has 128 customers. each needs 64 address

Soln. $N = 2^{32-16} = 2^{16}$ Here $n = 16$

3 groups ⟹

① $64 \times 256 = N_{sub1} = 2^6 \times 2^8 = 2^{14}$

② $128 \times 128 = N_{sub2} = 2^7 \times 2^7 = 2^{14}$

③ $128 \times 64 = N_{sub3} = 2^7 \times 2^6 = 2^{13}$

$n_{sub1} = n + \log_2 (N/N_{sub1}) = 16 + \log_2 \left(\frac{2^{16}}{2^{14}}\right)$

$= 18$

$n_{sub2} = 16 + \log_2 (2^{16}/2^{14}) = 18$

$n_{sub3} = 16 + \log_2 (2^{16}/2^{13}) = 19$

For group 1.

(First)

190.100.0.0/18

(last)

$$\begin{array}{r} 190.100.0\ \ .0 \\ \cancel{255}0.0.00111111\ \ 11111111 \\ \hline 192.100.63\ .255/18 \end{array}$$

Group 2.

190.100.64.0/18 (or) ~~190.100.191.127/18~~

190.100.0100 0000.0000 0000
00.00.0011 1111.1111 1111

190.100.127.255/18

Group 3.

190.100.128.0/19

190.100.1000 0000.0000 0000
0.0.0001 1111.1111 1111

190.100.159.255/19

Now, range of IP for customer 1. of grp.1

grp1. [190.100.0.0/18 — 190.100.63.255/18]

$N = 2^{14}$

$N_{sub} = 256 = 2^8$

$n_{sub} = n + \log_2 (N/N_{sub}) = 18 + \log_2 (2^{14}/2^8) = 24$

($\because$ each customer have equal no. of address, n_{sub} is fixed)

(first) 190.100.0.0/24

(last) 190.100.0.0
0.0.0.1111 1111

190.100.0.255/24

for cust 2 ⟹ 190.100.1.0/24 — 190.100.1.255/24

cust 3 ⟹ 190.100.2.0/24 — 190.100.2.255/24

⋮

For group 2;

$N = 2^{14}$ $N_{sub} = 2^7$

$n_{sub} = 18 + \log_2 (2^{14}/2^7) = 25$

(first) 190.100.64.0/25

(last) 190.100.64.0
0.0.0.0111 1111

190.100.64.127/25

Customer 1

customer 2 ⟹ 190.100.64.128/25 — 190.100.64.255/25

customer 3 ⟹ 190.100.65.0/25 — 190.100.65.127/25

⋮

* Supernetting and Aggregation

107.1.2.32
107.1.2.33
⋮
107.1.2.47

} 16 addresses

First IP address to divisible by total no. of address.
(1st at least 4 bits 0 from right)

32 ⇒ 0010 0000

∴ $2^4 = 16$

		Total no. of address	To check contiguous		
N_1	190.1.0.0/24	2^8	0.0	- 0.255	✓
N_2	190.1.1.0/24	2^8	1.0	- 1.255	✓
N_3	190.1.2.0/24	2^8	2.0	- 2.255	✓
N_4	190.1.3.0/24	2^8	3.0	- 3.255	✓

} contiguous

all are powers of 2.

190. 1. 0000 00|00 . 0
190. 1. 0000 00|01 . 0
190. 1. 0000 00|10 . 0
190. 1. 0000 00|11 . 0

subnet mask 255.255.252.0

190.1.0.0/22