(5) It is a multicast address because the The bit after MSB is an odd number and the LSB is a 1. And it 12 bits & Hexadecimal digits.

A3:34:45:11:92:f1

---

(1) Given:

distance (length) = 5000m

Propagation Speed = 2×10^8 m/s

$\frac{5000}{2 \times 10^8}$ = Propagation Time

$\frac{2500}{5000 \times 10^{-6}} = 25 \times 10^{-6} = 25\,\mu s$

Transmission Time = $\frac{\text{Message size}}{\text{Bandwidth}}$

Message size = 512 bits

Bandwidth = 10 Mbps

$\frac{512}{10 \times 10^{6}} = 512 \times 10^{-6}\,s = 512\,\mu s$ 0.512 ms

---

(3) Given:

Pure Aloha

message size = 200 bits frames

Transmission speed = 200 kbps

$T_{fr} = 1s = 1000ms$

$\therefore G = 1$ S = throughput = $1 \cdot e^{-2G} = 0.135$

$= 54$ bit-frames

Vulnerable time = $2 \times T_{pr} = 2 \times 1000 = 2000$ ms

if $k = 2 \longrightarrow 0 \rightarrow 2^k - 1 \rightarrow \{0, 1, 2, 3\}$

$R = \{0, 1, 2, 3\}$

T_b # can be 0, 2s, 4s, 6s.

---

(4) Data:

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

Bit stuffing:

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

Zeros added after 5 consecutive 1's.

Unstuffing:

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

Zero after 5 ones

Zero after 5 ones

Remove and find the Actual message

---

(2) Encapsulation is the process of ~~adding~~ converting data from upper layers into lower form of data so that data communication is possible. Extra addresses and codes are added and made into a single package.

Message → Segment → Datagram → Frame → Bits/Signals.

(9) Password Authentication Protocol (PAP):

→ This protocol was invented to ~~se~~ make have Authentication during the transaction/communication to ensure privacy and security.

→ In this method the password is sent to the sender & the ~~message~~ is Authentication request is sends the password along with other credentials like username to the reciever.

→ If the password is correct it sends an acknowledgement to the sender.

→ Here password is exposed so it is less secure.

Frame format:

Flag	Header	Code	ID	Username	Password	Password Value	Flag

Flag	Header	Code	Acknowledgement	Flag

Challenge Handshake Authentication Protocol (CHAP):

→ It works similar to the PAP protocol.

→ It is more secure then the PAP protocol as the password is not exposed to adversaries.

→ It uses a hash function type function to create a changed/altered value of the original password of the and sends the function to the sender.

→ ~~If the altered~~.

→ Sender uses the same hash function to change this password and sends it to the reciever.

→ If the hash values match an acknowledgement is sent.

Frame format:

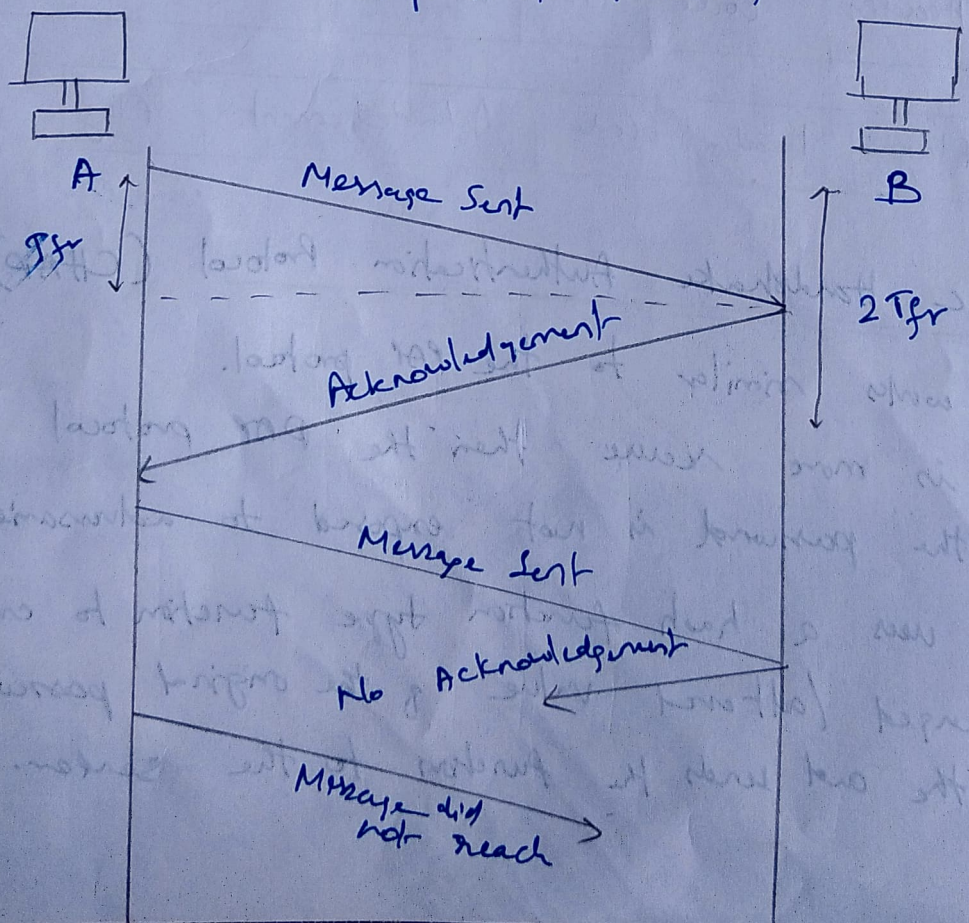
Flag	Header	code	ID	Username	Function	Flag

Flag	Header	Code	ID	hashValue	Flag

Flag	Header	code	ID	Acknowledgement	Flag

(8) FSM → Finite State Machine.

Stop-Wait Protocol



The Stop-Wait Protocol is a protocol in which the sender sends a signal / message and wait for an acknowledgement before sending the next signal.

There are 3 cases in this protocol:

(i) Message reached and Acknowledgement is received:

It is the case where the message a transaction is a success.

(ii) Message Reached but the Acknowledgement is stalled / does not reach:

In this case we might infinitely wait for the acknowledgement message.

(iii) Message did not Reach:

The sender cannot send the acknowledgement until he receives a message so, due to this the machine waits an infinite amount of time.

Case (ii) and (iii) Can be fixed by Making / Sending message again after a fixed Amount of time ($2T_{fr}$).

Which is used in Stop-wait ARQ protocol.

(13) Given/
500 bit-frames
500 kbps

Frame Transmission Time = $\frac{500 \text{ bits-frames}}{500 \text{ kbps}}$ = 1 ms

Total amount of Frames = 1000

So, For one Frame ⇒ $\frac{1}{1000}$ = 0.001 ⇒ 1 ms.

G = 1

(i) Pure Aloha:

S = Throughput

⇒ $G.2e^{-2G} = 1 \times e^{-2} = 0.135$

1000 × 0.135 = 135 frames

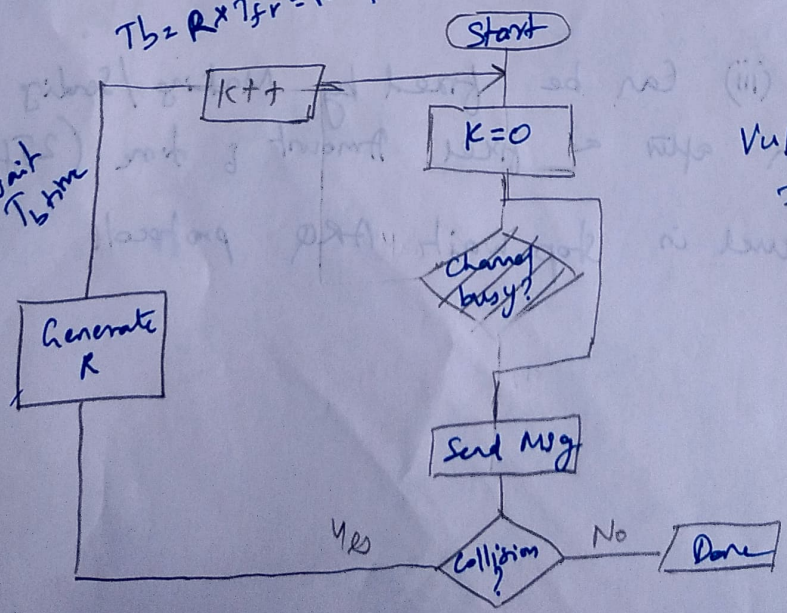
(ii) Slotted Aloha:

$S = G \times e^{-G} = 1 \times e^{-1} = 0.368$

1000 × 0.368 = 368 Frames

Pure Aloha:

$T_b = R \times T_{fr} = R \times T_p$



Vulnerable time = 2 T_{fr}

i) It sends a message and if it detects a collision

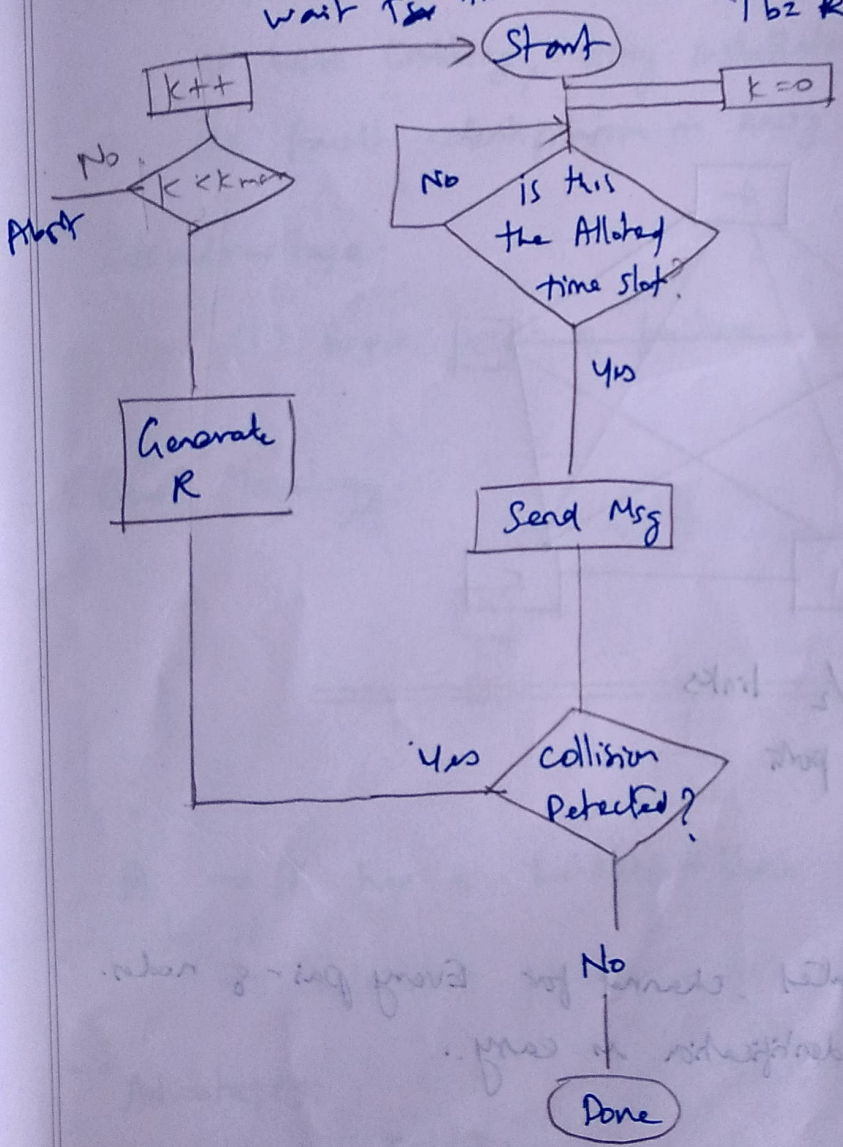
ii) It generates a random number in the range 0 to $2^k - 1 \rightarrow R$

iii) It waits a random time $T_b = R \times T_{fr}$

iv) This process is repeated until $k < k_{max}$.

Slotted Aloha: T_b time wait

$T_b = R \times T_{fr}$



SL.NO:CAA 170005

SRI SIVASUBRAMANIYA NADAR COLLEGE OF ENGINEERING

(An Autonomous Institution, Affiliated to Anna University, Chennai)
Rajiv Gandhi Salai (OMR), Kalavakkam – 603 110

THEORY EXAMINATIONS

Register Number	20500 1083		
Name of the Student	Rex Abraham Jacob		
Degree and Branch	BE CSE	Semester	V
Subject code and Name	UCS1501 and Computer Networks		
Assessment Test No.	1	Date	15-9-2022

Details of Marks Obtained

Part A		Part B				Part C			
Question No.	Marks	Question No.	(a) Marks	(b) Marks	Total Marks	Question No.	(a) Marks	(b) Marks	Total Marks
1	2	7	6			10			
2	2					11	9		
3	2	8	4			12	7		
4	2								
5	2	9	4			13			
6	2								
Total (A)	12	Total (B)			14	Total (C)			16

Grand Total (A+B+C)			42	Marks (in words)			
Signature of Faculty							

PART-A

1)

$$\text{Transmission time} = \frac{\text{size of bits}}{\text{transmission rate}}$$

$$= \frac{512}{10 \times 10^6}$$

$$= 512 \times 10^{-6}$$

$$= 5.12 \times 10^{-3}$$

$$= 5.12 \text{ ms}$$

$$\text{Propogation time} = \frac{\text{Distance}}{\text{propogation speed}}$$

$$= \frac{5000}{2 \times 10^8}$$

$$= 2500 \times 10^{-8}$$

$$= 0.025 \text{ ms}$$

2) Encapsulation is the proces of transferring data from ~~higher level to~~ one level to higher levels. Encapsulation puts the data in the form of a frame which can be fixed or variable size.

3. 400 bit frames, channel = 400kbps

TP =

No frames = $\frac{400}{400 \times 10^3}$

$= 1 \times 10^{-3}$

$\Rightarrow G = 1$

For pure aloha:

Throughput = $G \times e^{-2G}$

$= 1 \times 0.135$

$= 0.135$

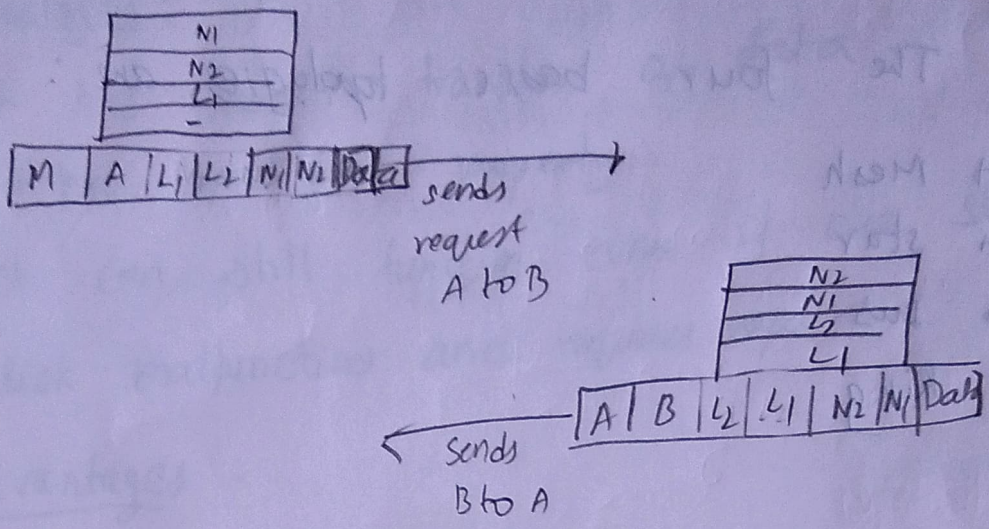
No of frames that can pass in the channel

$\Rightarrow 0.135 \times 400$

$\Rightarrow$ 54 out of 400 frames

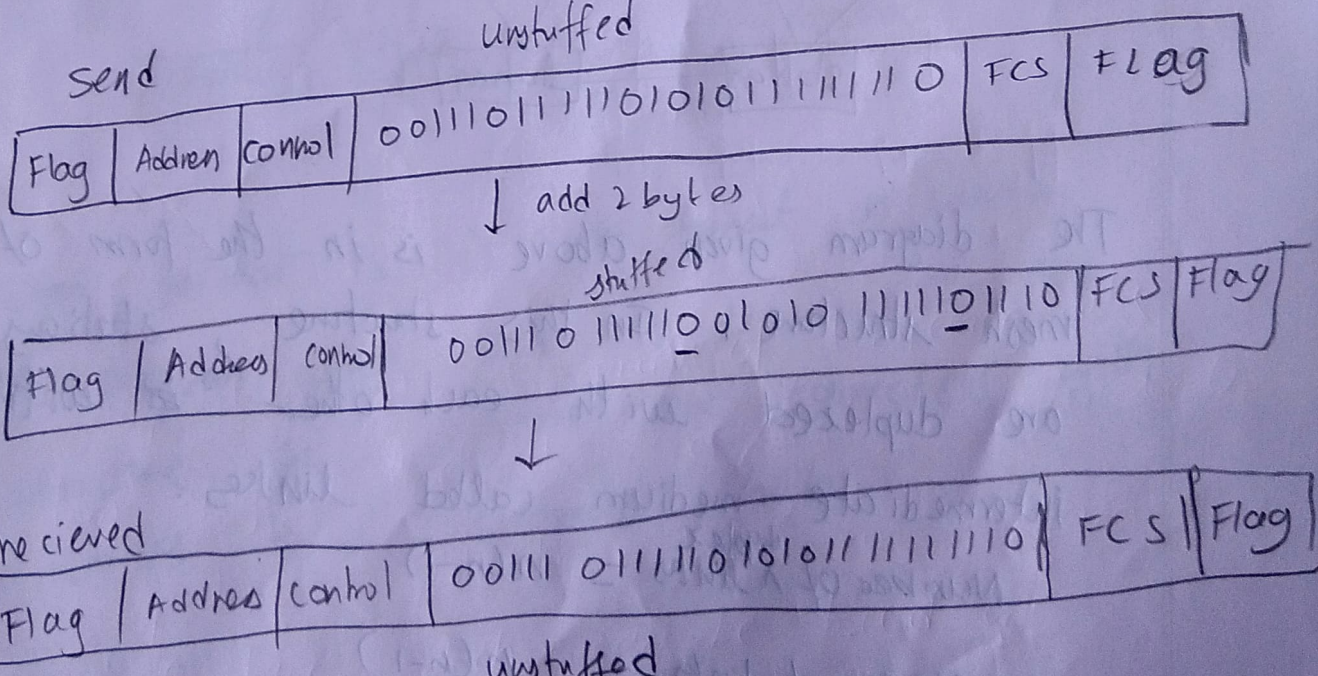
The transmission time of this aloha network is 1ms

4.



5. This address is <u>multicast</u> in nature. It is because the least significant bit of its hexadecimal notation is <u>1</u>.

6 -



12) (i) Frame 1 :

L2	L1	N1	N8	Data

(ii) Frame 2 :

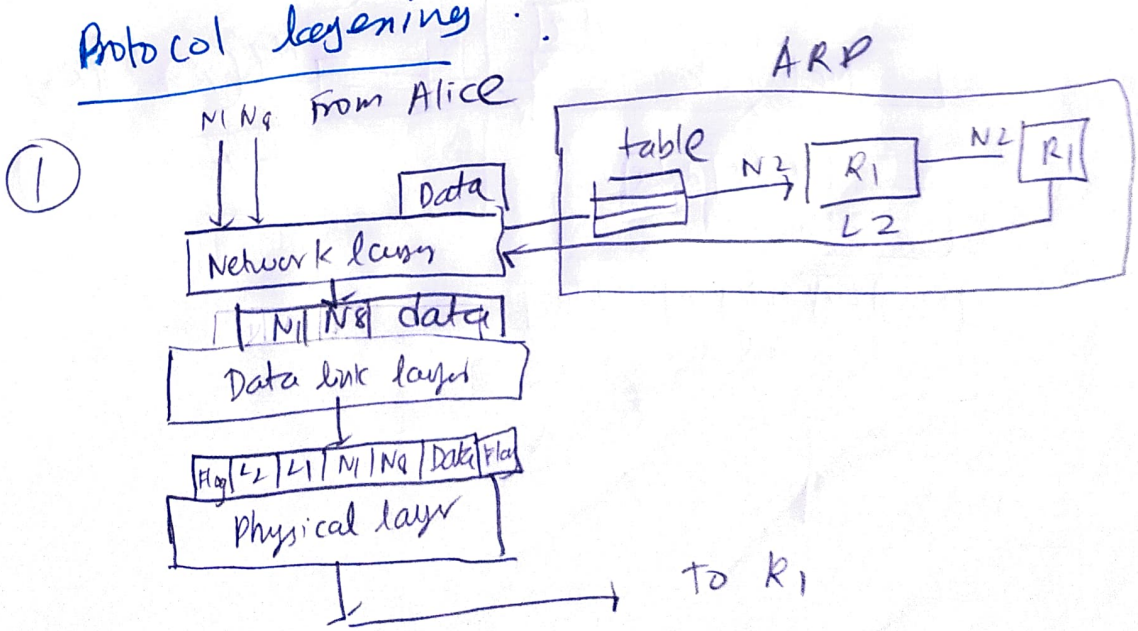
L5	L4	N1	N8	Data

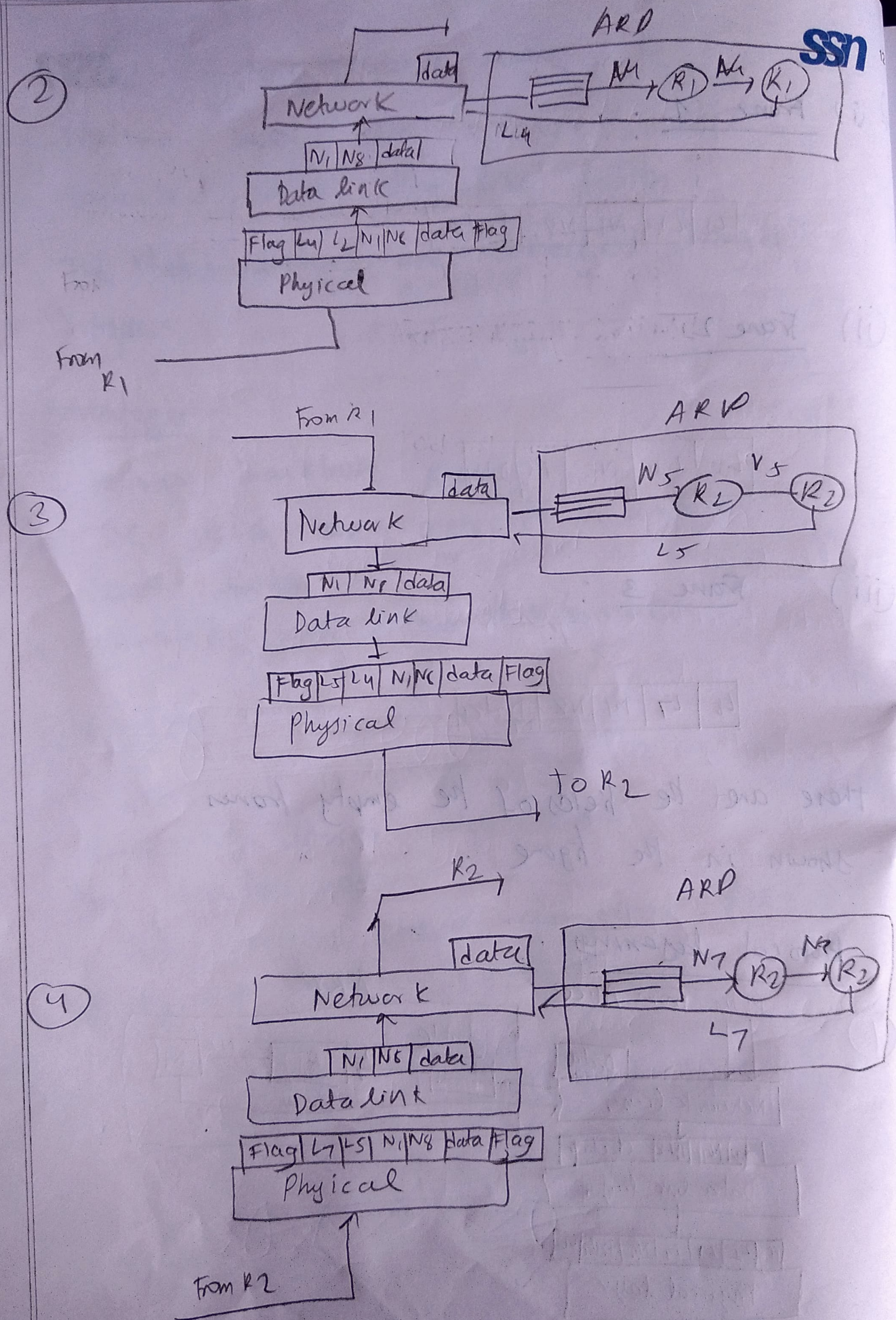
(iii) Frame 3 :

L8	L7	N1	N8	Data

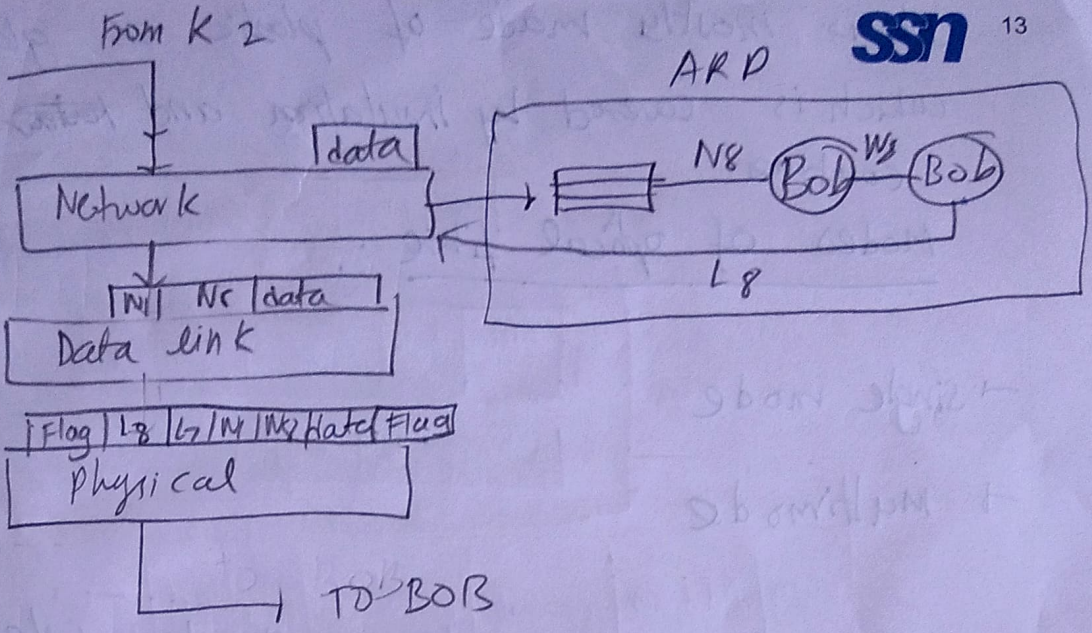
these are the fields of the empty frames shown in the figure.

Protocol layering :




2
ARP
data
Network
N1
R1
R1
L4
N1 N8 data
Data link
Flag L4 L2 N1 N6 data Flag
Physical
From R1
3
From R1
ARP
data
Network
N5
R2
R2
L5
N1 N2 data
Data link
Flag L5 L4 N1 N6 data Flag
Physical
To R2
4
R2
ARP
data
Network
N7
R2
R2
L7
N1 N6 data
Data link
Flag L7 L5 N1 N8 Data Flag
Physical
From R2

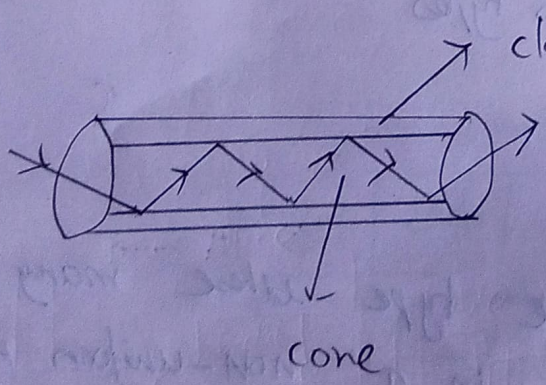
(5)



This is how protocol layering is used to trasmit the data from alice to bob

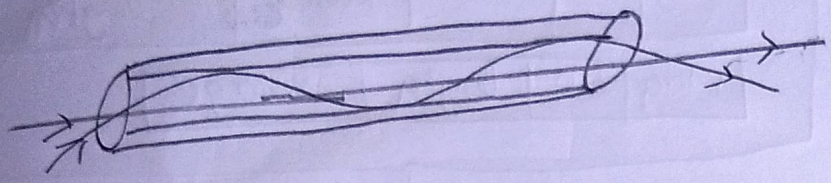
PART - B

7) Optical fibre construction.



Optical fibre contains core and cladding * in its diagram. The cladding is the area where it light bounces off due to refraction.

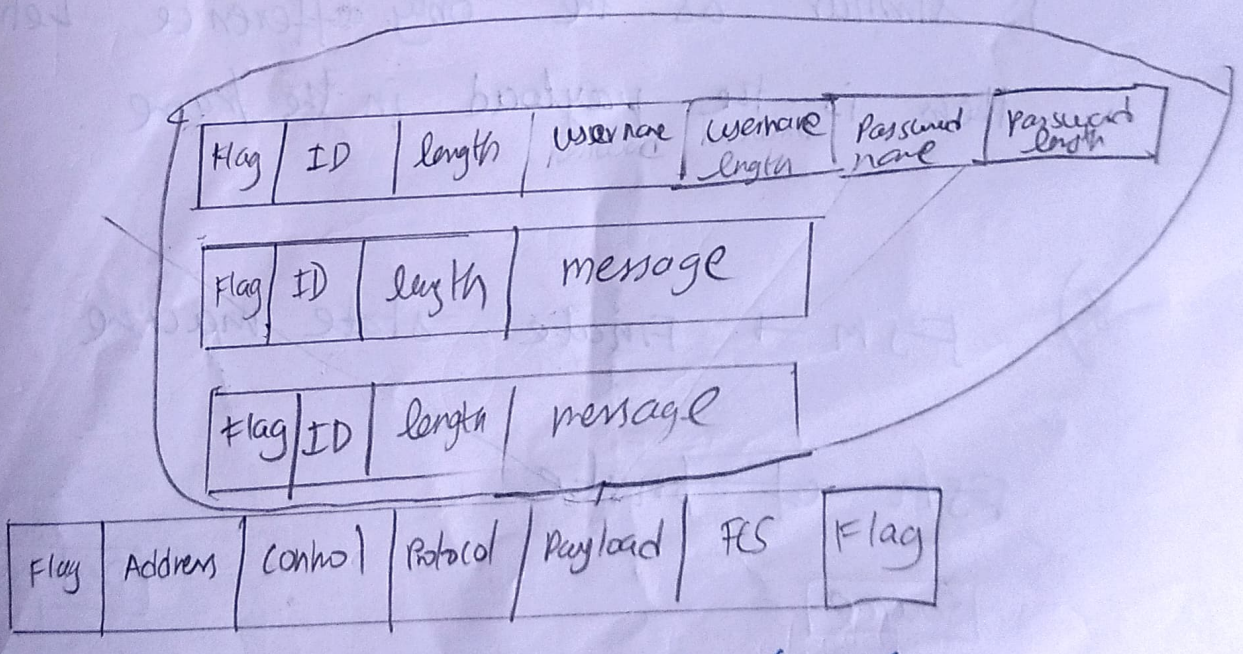
+ Graded index is the type where. light rays are refracted uniformly without interference



There are the modes of an optical fibre.

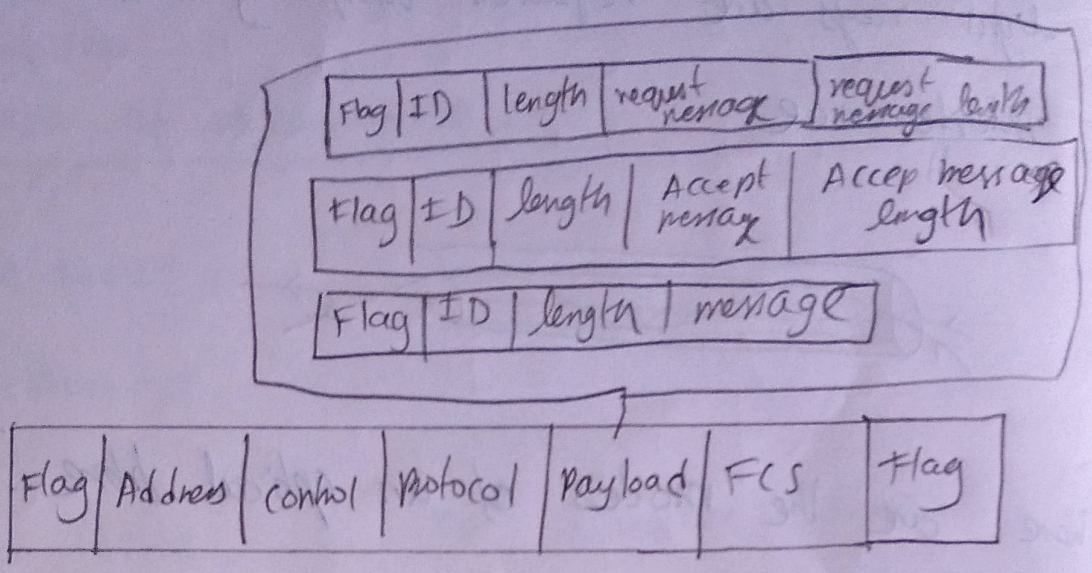
a)

PAP protocol.



This is the PAP format. this format is used for authentication of data

CHAP

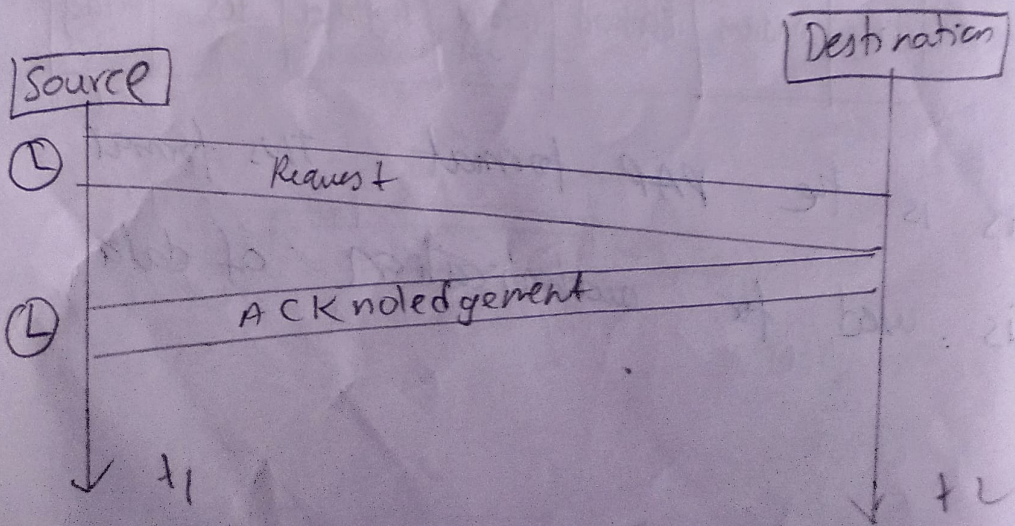


This is the CHAP protocol frame format

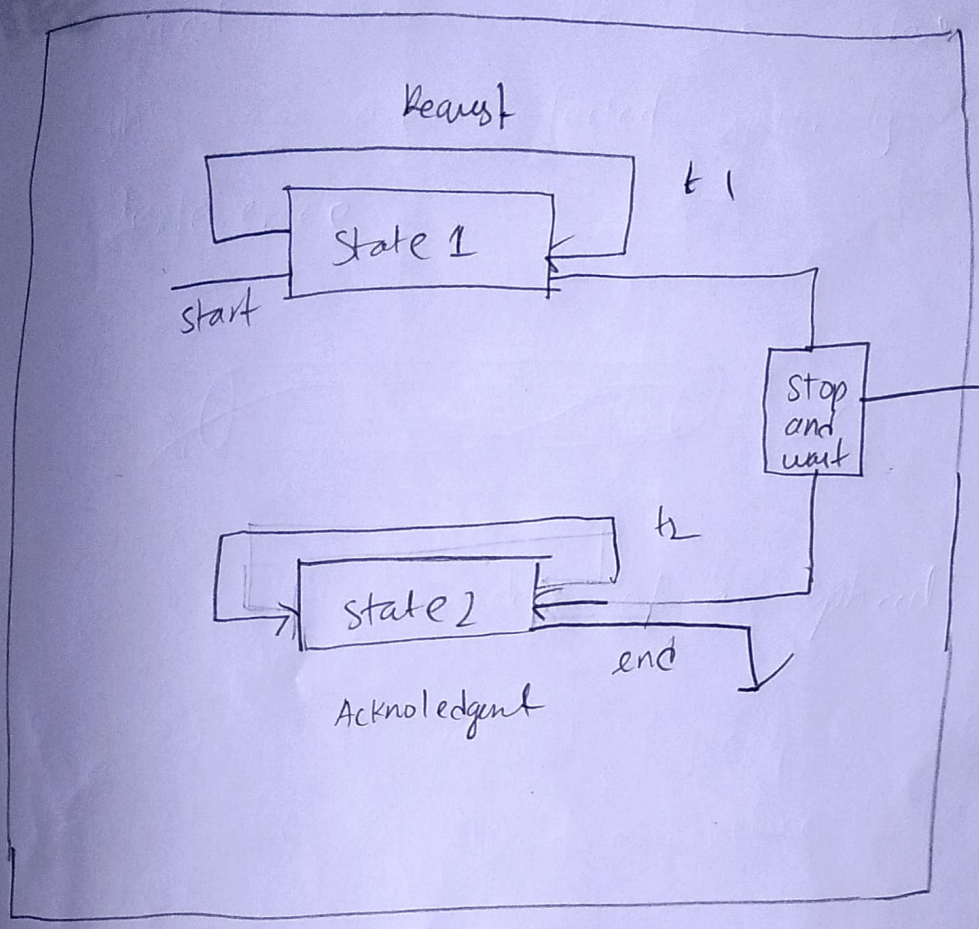
- Both PAP and CHAP frame format is similar as the only difference between them is the payload in the frame.

8) FSM → Finate state macine

~~FSM of finite~~



FSM



In this finite state machine, we have two states where one is for request and another is for destination.

A stop and wait is introduced to avoid congestion in the network channel.