43, 37, 36, 29

(70) Codewords :-

1 → (00000000)
2 → (00001111)
3 → (01010101)
4 → (10101010)
5 → (11110000)

∴ d(1,2) = 4   d(1,3) = 4   d(1,4) = 4   d(1,5) = 4

d(2,3) = 4   d(2,4) = ~~8~~ 4   d(2,5) = 8

d(3,4) = 8   d(3,5) = 4

d(4,5) = 4

∴ dmin = 4

∴ Maximum no. of bits (errors) that can be detected = 8.

(69)

UDP	TCP
→ Connectionless, i.e, no path setup before.	→ Connection required, i.e, a path is created before transmission.
→ Not reliable	→ Reliable
→ No acknowledgement	→ Acknowledgement
→ Relatively fast	→ Relatively slow
→ Retransmission is not automatic. The application must sense and ask for retransmission.	→ Automatic Retransmission.

(67) Longest common Prefix Matching is required in CIDR because the prefix in CIDR defines the network. So, for the same network the prefix remains the same (because the network part should remain constant) in a given network.

67

66

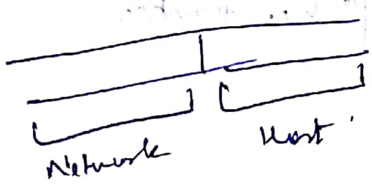
Hub	Switch
→ Operates in Physical layer	→ Operates in Data Link layer
→ Broadcasts the data	→ transmits to only intended recipients
→ Least Network Security	→ Relatively Better Network Security
~~→ Passive devices~~	~~→ Active device~~
→ No looping problem	→ Looping problem (Maintains spanning trees)

65

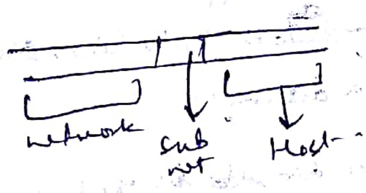
Virtual Circuit Switching	Circuit Switching
→ No dedicated path is allocated only a route is defined	→ A dedicated path is allocated and established
→ The route can be shared by other connections also	→ The route once established and allocated cannot be used by other connections.
→ Data transfer takes place in the form of packets	→ Data is not packetized.

Yes, Virtual Circuit is a type of packet-switched network techniques.

(b4) Internet is a two level hierarchy - host and subnet as ~~do~~ the address is ~~[illegible]~~ divided into 2 levels of ~~address~~ address, the ~~[illegible]~~ prefix and the suffix. The prefix defines the address of the network while the suffix part defines the host in that network.



Now ~~[illegible]~~ internet is also said to ~~be~~ have a three level hierarchy due to the introduction of 'subnets'. Now an organization (having large no of ips) divides them in to different sub-networks within the organisation ~~such that Anyone~~ as if there are different networks in the organisation.



~~(b3) Size of various Networks:- 144.16.0.0 - 144.16.63.225~~
~~144.16.64.0 - 144.16.67.225~~
~~144.16.67.0 - 144.16.68.63~~
~~144.16.68.64 -~~
~~[illegible]~~
~~144.16.0.0~~

(b[illegible])

(c3) ~~Teth0~~

(c2) Only two bits are taken as address length (source or destination) for the correct operation of CSMA/CD which is ~~[illegible]~~ implemented in Ethernet ~~[illegible]~~ (wired) communication.

(C1)

Shared Ethernet	Switched Ethernet
(a) No switches are used. There is a possibility of collision.	(a) Use of switches. Collisions are eliminated.
(b) Point to Multipoint	(b) Point to Point
(c) Relatively More congestion.	(c) less congestion

Ethernet is known as CSMA/CD protocol because ~~as~~ the wired Ethernet protocol is developed on the concepts of CSMA/CD and strictly follows that.

(C6) CRC can detect ~~of~~ all single bit errors and almost all double bit errors if the divisor is chosen wisely. Our choice of divisor defines ~~the~~ how efficient our system will be. Generally ~~these two~~ a guidelines should be followed while choosing a divisor,

→ ~~adios~~ Let the divisor ~~should~~ be represented as an polynomial

For eg,

$P = 1001 \longrightarrow \boxed{x^3+1}$

The rules are:-

→ Divisor shouldn't be divisible by X (should always end with one) [~~One~~ guarantees all one bit errors are detected]

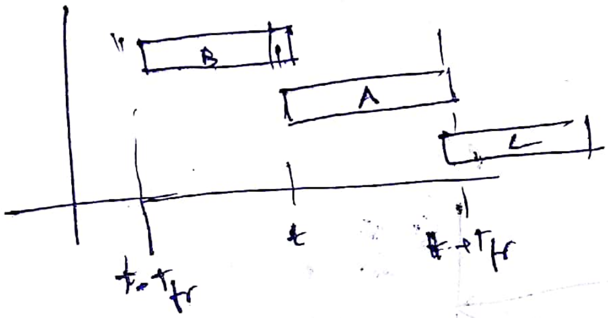
→ and almost all ~~odd~~ two bit errors are eliminated.

(C9) The padding field is required in an ethernet frame as acc. to the minimum length restrictions the min. length of the packet should be 64 bytes (For correct operation of CSMA/CD). So if the length is less than this amt then padding is done to make up the difference.

Scanned by CamScanner

(58) In aloha the vulnerable time is $2 \times T_{fr}$

T_{fr} is the time taken by frame to travel.



As we can see if A want to send a frame collisions can occur with B and C if B has sent a frame in between $t - T_{fr}$ and t and C has sent between t and $t + T_{fr}$. So the vulnerable time is $2T_{fr}$.

while in slotted aloha the time are divided into slots so the vulnerable time is equal to the width of the slot $= T_{fr}$.

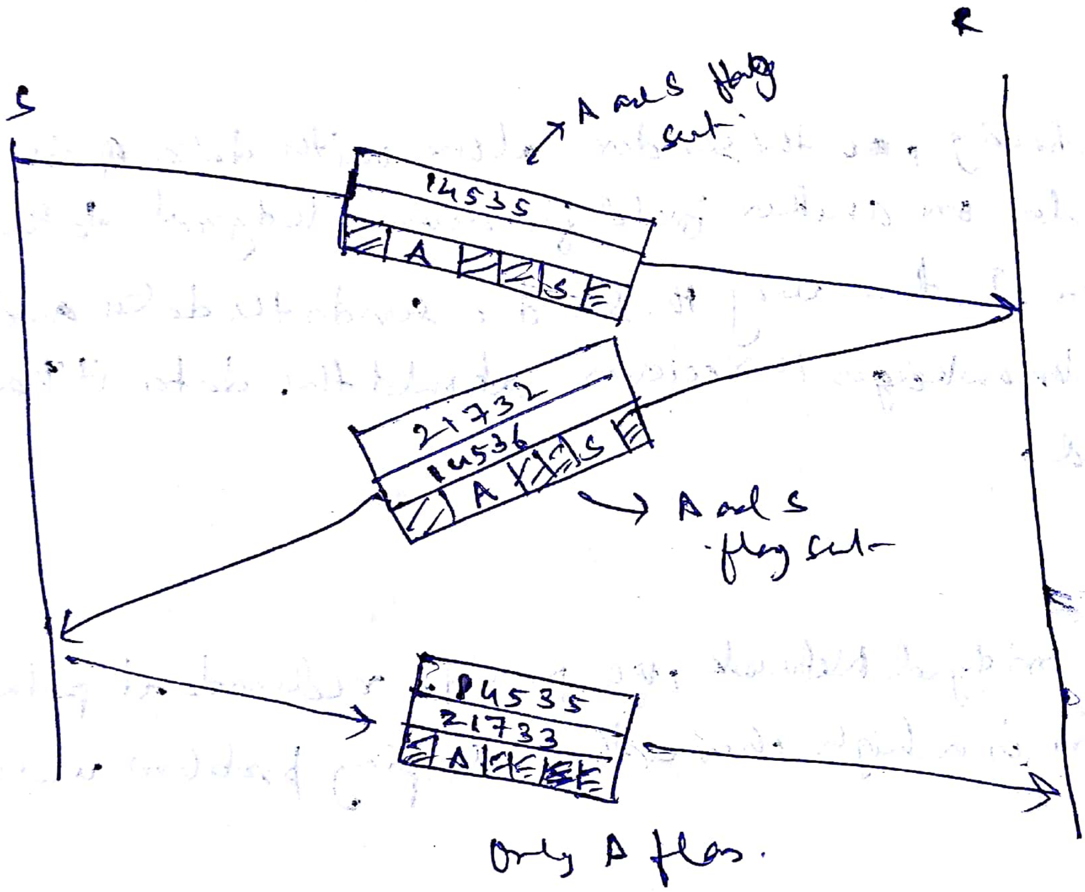
$\because \eta(\text{efficiency}) \propto T_{fr}$

$\therefore \eta_{Aloha} = k \times 2T_{fr}$

$\eta_{S-Aloha} = k \times T_{fr}$

$\therefore \eta_{Aloha} = 2 \times \eta_{S-Aloha}$

(57)

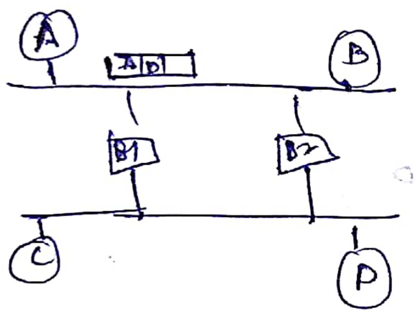


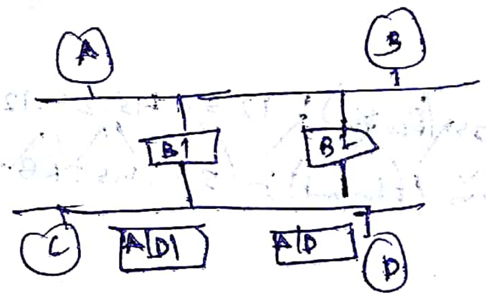
(56) IP address (Router) :- 125.45.23.12

Physical Address (Ethernet) :- (23:45:AB:4F:67:CD

(53) In piggybacking, the sender along with data of itself incorporates one another field for acknowledgement to the receiver. In this way the sender sends the data and also acknowledges the receiver about the data it has recieved.

(54) If in a bridged Network, we provide redundant paths, then there is a high chance that looping problem will occure





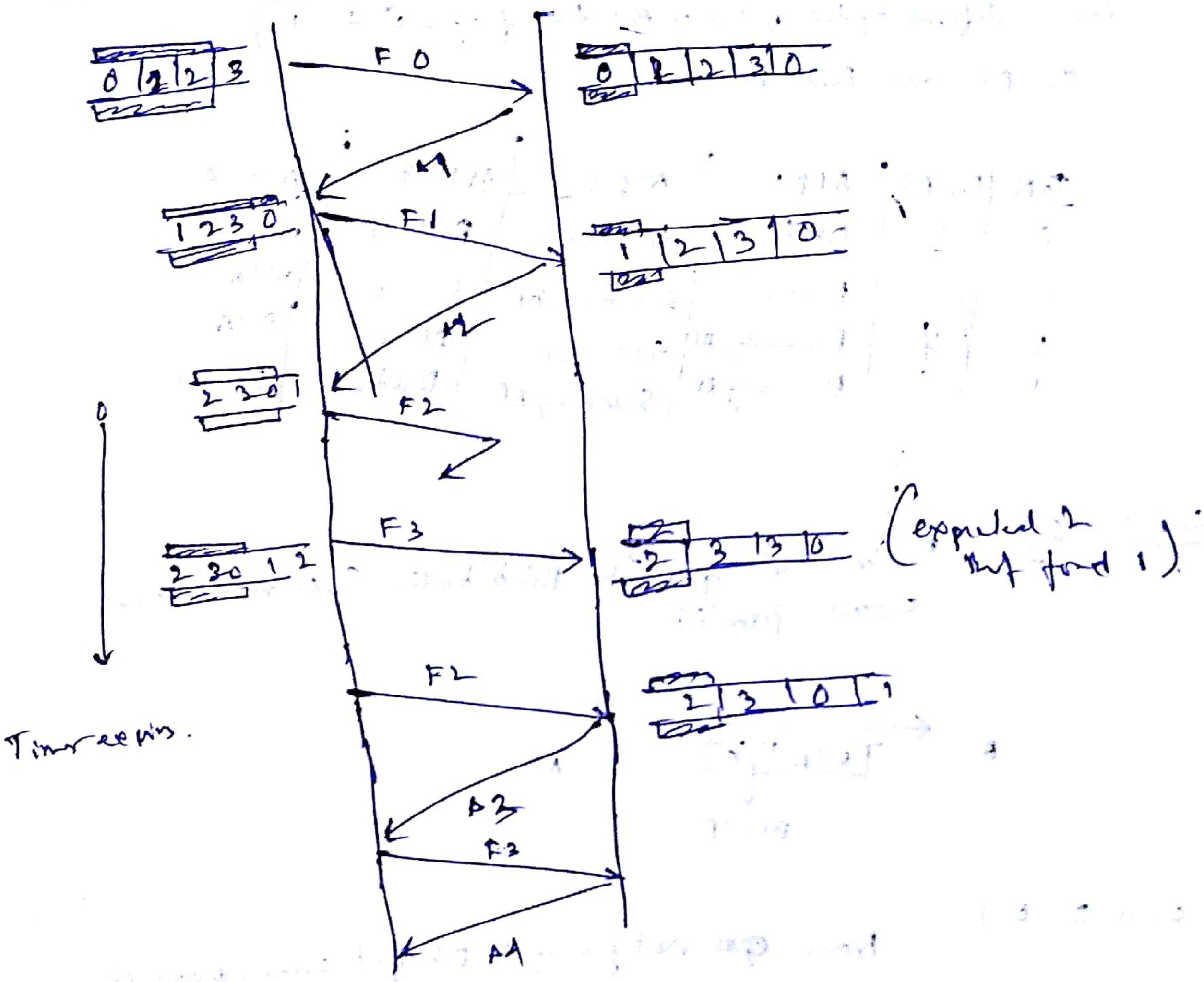
A wants to send Data to D.

B1 doesn't know where D is floods the entire network with the frame.

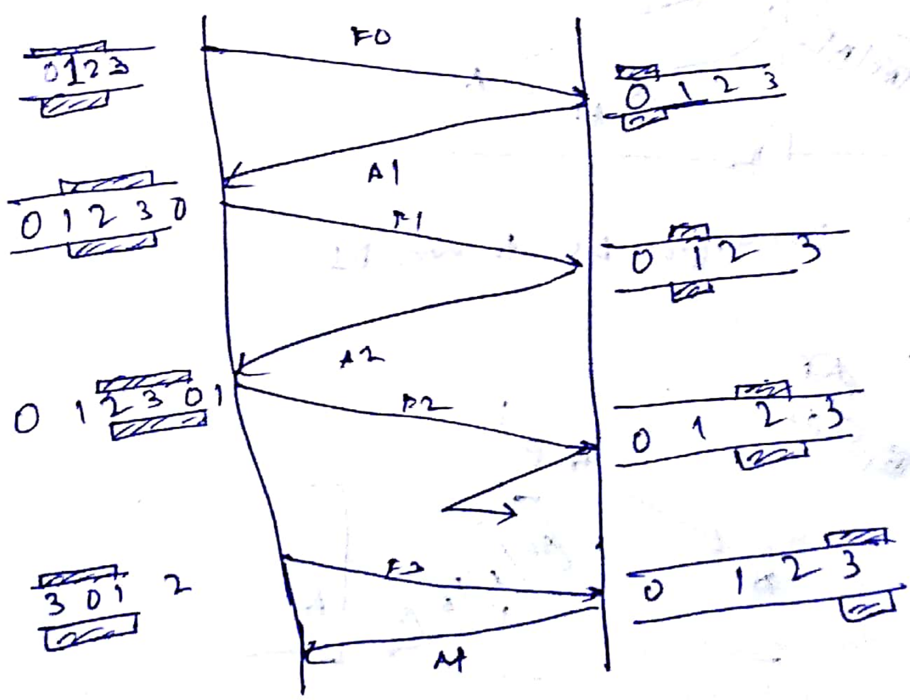
Now, there are two copies in the network once the frame reaches 'B2', it also floods the network again and this loop goes on.

Transparent Bridge maintains a spanning tree to remove the loops and hence the redundant paths.

(53) ~~Case 3~~. Size 3
let m=2.



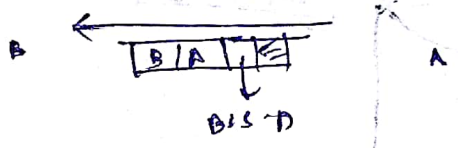
(52)



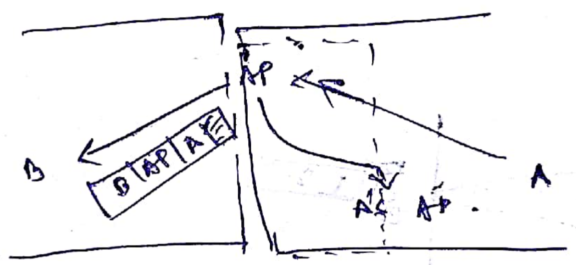
(4) The IEEE 802.11 addressing mechanism specifies 4 cases, defined by the value of the two flags in the FC field, To DS and From DS.

To DS	From DS	ADD 1	ADD 2	ADD 3	ADD 4
0	0	Dest.	Source	BSS ID	N/A
0	1	Dest.	Sending AP	Source	N/A
1	0	Receiving AP	Source	Dest.	N/A
1	1	Receiving AP	Sending AP	Dest.	Source

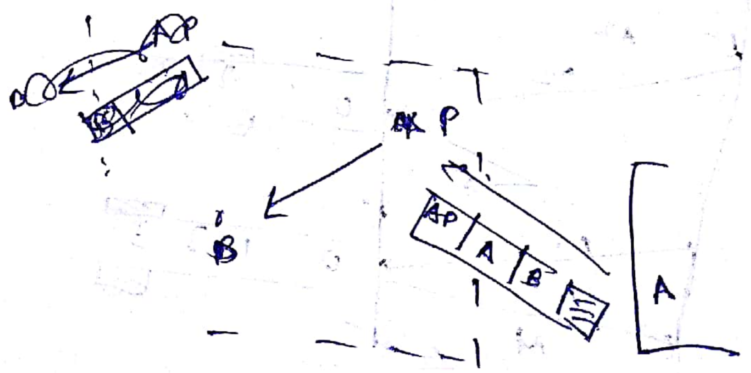
Case 1 00 : Frame not going to Distributed System neither coming from it.



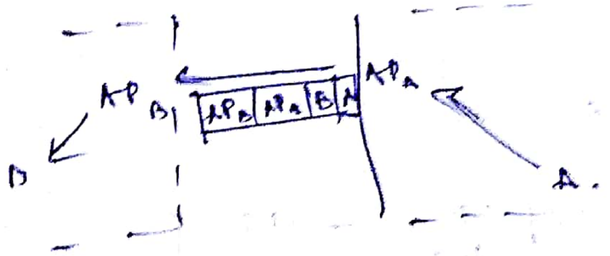
Case 2 01 Frame not going to DS but coming from it.



Case 10 : Frame from DS to non DS.



Case II from DS to DS.



(52) Let G be the average no. of frames generated by system during one frame transmission time.

∴ It can be proved that avg. no. of successful transmission is $S = G \times e^{-2G}$.

∴ S_{max} occurs when e^{-2G} is max or $2G = 1$

or $G = 1/2$.

∴ $S_{max} = 0.184$ $(G = 1/2)$.

Similarly, for slotted aloha, $S = G \times e^{-G}$

∴ S_{max} occurs when $G = 1$

∴ $S = 0.368$ $(G = 1)$

∴ (S_{max}) slotted aloha $= 2 \times S_{max}$ (aloha).

(43) TCP sets a timeout when it sends data and if data is not acknowledged before timeout expires it retransmits data. This time used by TCP is known as retransmission timer.

keepalive timers are used to check the ~~clients~~ connections in TCP. whenever we set up a TCP connection the host ~~sends~~ starts a keepalive time. after the timer expires, the host sends a keepalive probe packet (without data). If that packet is acknowledged then we can assure the connection is still there and timer is set again otherwise it is considered that connection is lost.

(38) Beginning address

14.24.74.0/24

One subblock of 10 → 16
" " " 60 → 64
" " " 120 → 128

[Next power of two]

Now, we allocate the large block first.

∴ first allocate 128
then 64
then 16.

	Starting Address	Ending address.
(1)	14.24.74.0/24	14.24.74.127/24
(2)	14.24.74.128/25	14.24.74.191/25
(3)	14.24.74.192/26	14.24.74.207/26.

127
64
191
16
207

(27) 50 kbps satellite channel.

500 msec round trip (propagation delay)

Frame size = 1000 bit

(a) 50 kbps
= ~~50 kilo~~ (50,000 bits/s.

(a) Bandwidth delay product

$= 50\times10^3 \times 500\times10^{-3}$

$= 25\times10^4$ bits.

∴ We can send 25×10^3 bits

but will send 1000 bits.

∴ % usage = $\frac{1000}{25\times10^3} = \frac{1}{25} = \boxed{4\%}$

∴ Sender will idle 96%

(b) Ideally we should have 100% utilization ~~of the chat~~

$\Rightarrow$ 25×10^3 bits should be sent.

$\Rightarrow$ the size of the window should be,

$$\frac{25 \times 10^3}{\cancel{56 \times 10} \; x \times 1000} = 1.$$

$\Rightarrow$ $\boxed{x = 25}$ frames.

$\therefore$ the size of the window should be 25 f.

Scanned by CamScanner