Declaration and statement of authorship

I, bearing Roll No. 106119100, agree and acknowledge that:

1) The assesment was answered by me as per instruction applicable to each assessment, and that I have not resorted to any unfair mean. to deliberately improve my performance

2) I have neither impersonated anyone, nor have been impersonated by any person for the purpose of assessment.

Signature : Rpandey

Full Name : Rajneesh Pandey

Roll No : 106119100

Sub code : CSPC53

Mobile No : 8290968008

04/12/21

CSPC53 – CN

ENDSEM

106119100

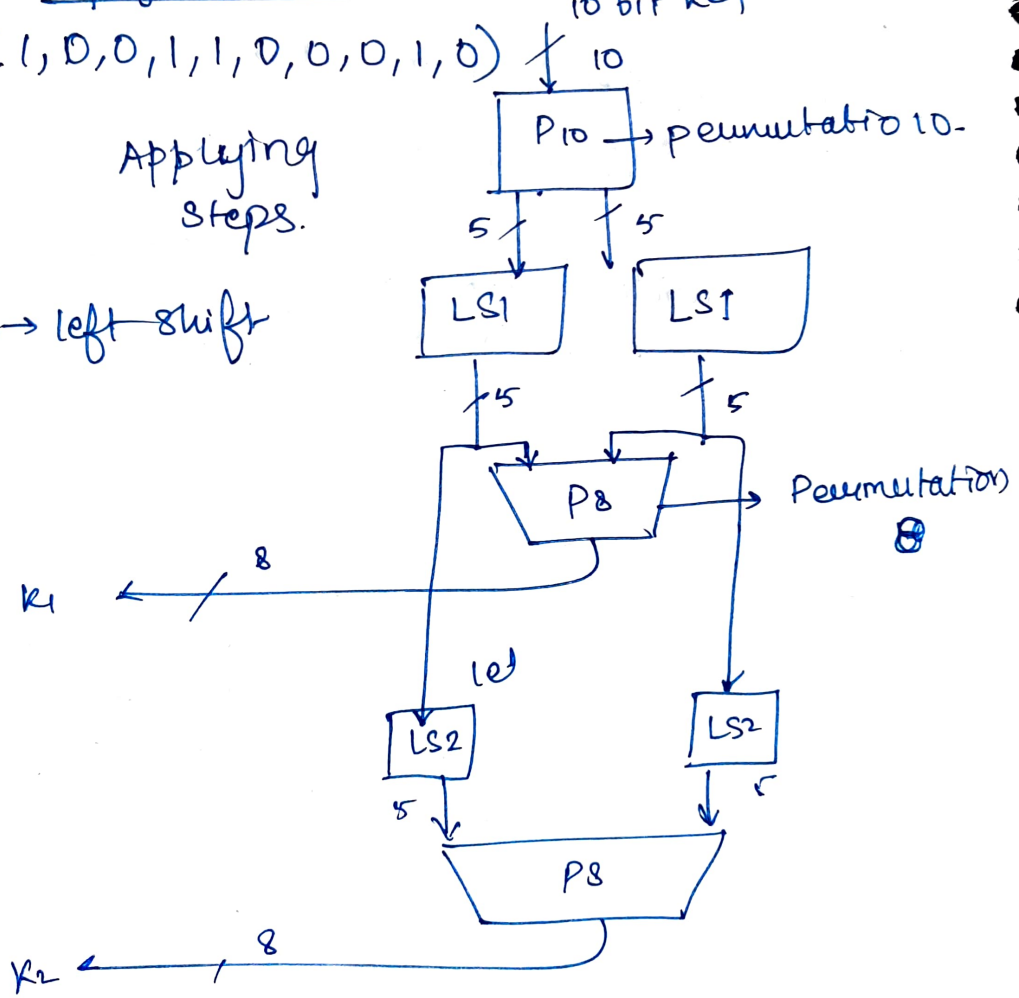
Rajneesh Pandey

Question (1)

String 01110101

key got: 1001100010

K=(1,0,0,1,1,0,0,0,1,0)



Applying steps.

LS → left shift

Question (1)

(B)

(i)

Network layer in OSI

— data get its addressing and routing instruction in prep.

— Its uses network layer for routing stand. protocols.

Network layer in TCP/IP

— In Network access, data gets a header and a trailer. and these ↓ go to. tell data to.

Now, in At, Net. interface layer packet of data formatte + pre..

— It uses internet layer as, a main Network laye

— ~~real~~

(ii) **Error control :**

Data link

→ Error control used in frames.

→ Methods like. CRC is used

transport

→ It use segments. ~~for~~ in which the error control is used

→ methods like checksum is used

congestion control :

Network layer

- CC for transport layer
- for packets

transport

- Congestion control service to application layer
-

(iv) sequence NO :

Data link

- sequence numbers for frames.
- for frame ip header.

transport

- Sequence Number for segments
- for IP header

(v) Data link layer delivery.

- Hop-to-hop / Node-to-Node delivery
- sends in frames

transport layer delivery

- port-to-port Delivery
- sends in segments

(vi) checksum will all 0

→ Helpful for detecting error. any case

all 1's in UDP

→ when sum = all 0's then checksum fails

(vii) substitution

→ character's identity changed, position remains unchanged

→ example caesar cipher

transposition

→ the position changed, but identity not changed

→ Rail fence cipher.

Question (2)

(A)

rajneeshpandey

01001100010

word length data ⇒ rajnees

Hamming code structure

pos.	7	6	5	4	3	2	1
Bits	d_4	d_3	d_2	p_2	d_1	p_1	p_0

So,

11	10	9	8	7	6	5	4	3	2	1
d_6	d_5	d_4	p_3	d_3	d_2	d_1	p_2	d_0	p_1	p_0
1	0	0	1	1	0	0				

data = 1001100

$p_0 = d_0 \oplus d_1 \oplus d_3 \oplus d_5 = 1$

$p_1 = d_0 \oplus d_2 \oplus d_3 \oplus d_6 = 1$

$p_2 = d_1 \oplus d_4 \oplus d_5 \oplus d_6 = 1$

$p_3 = d_4 = 0$

data we got :

1	0	0	0	1	1	0	1	0	1	1
			6	5	4	3		2	1	0

Hamming codee.

Nawe, Errorcheck

1	0	0	0	0	1	0	1	0	1	1

↑ Error bit

Naw, at recievers end it will check the coodd by redund.

Question (2)

(B)

Name : rajneeshpan

Vowels → 1
consonats → 0

↓

key : 0100|1100010 (10 bit)

key = 1001100010

Message

polynomial = $x^5 + x^4 + x^2 + 1$

for burst error,

Let $e(x) = x^i(x^{j-i} + \cdots + 1)$

$\frac{c(x) + e(x)}{g(x)}$

$g(x) = x^r + \cdots + 1$

Highest degree = 5

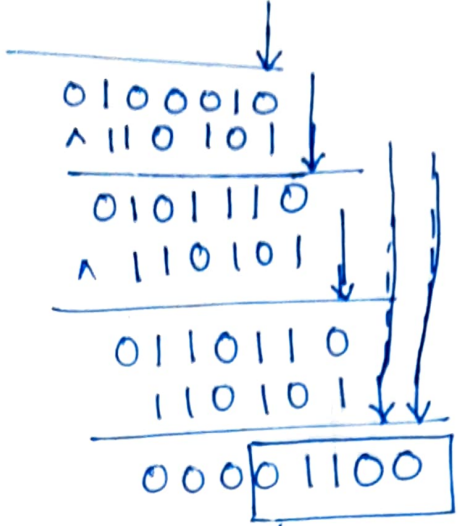
So, 1001100010 00000 (added bit.)

bit from polynomial.

= 110101

Now,

```
110101 | 1001100010 00000
       ^ 110101 ↓ ↓
         0100110
       ^ 110101
         0100110
       ^ 110101
         0100111
       ^ 110101
         0100100
         110101
```



So, the bits needs to use/append ⇒ 01100.

So,

the message to transmitt,

1001100010 01100

As, r-bit CRC detect all the burst pattern of length r+1 except the pattern of itself.

hence,

the burst error can be detectect as, $x^n \rightarrow x^5$

5-power (highest)

it can detect all burst error of upto length 5.

$$e(x) = (x^4 + x^3)$$

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

Question (3)

(A)

In Random access protocol,

the main issue is ↓ the collision related to

so,

In Aloha (pure or slotted)

we need vulnerable time as (2x trans time) pure and (tran. time) slotted

because else there could be the chance of collision

hence, by taking this issue under consideration we need to avoid collision.

In CSMA/CD

→ we use the concept of the time of transmission should be greater than the 2 x propogation delay in order to detect the collision.

In CSMA/CA (for wireless LAN)

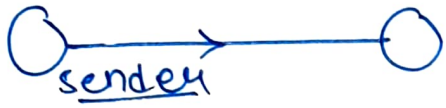
the energy of transmission can't be detect back,

→ hence we, use collision avoidance to reduce the chance of collision. by sender. ↓ before* sending check

(B)

Lineauly connected staitons.

if we connect nodes lineauly.



in unicast,

one-to-one communication is there,

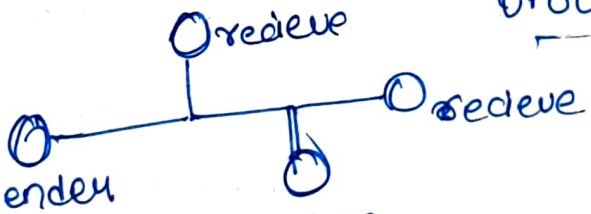
and broadcast

- Limited
  - inside the network
- Direct
  - ~~inside~~ to other Network

if,

if one reciever is there then it will be broadcast.

else, if



if this is the case then broadcast will be different from unicast

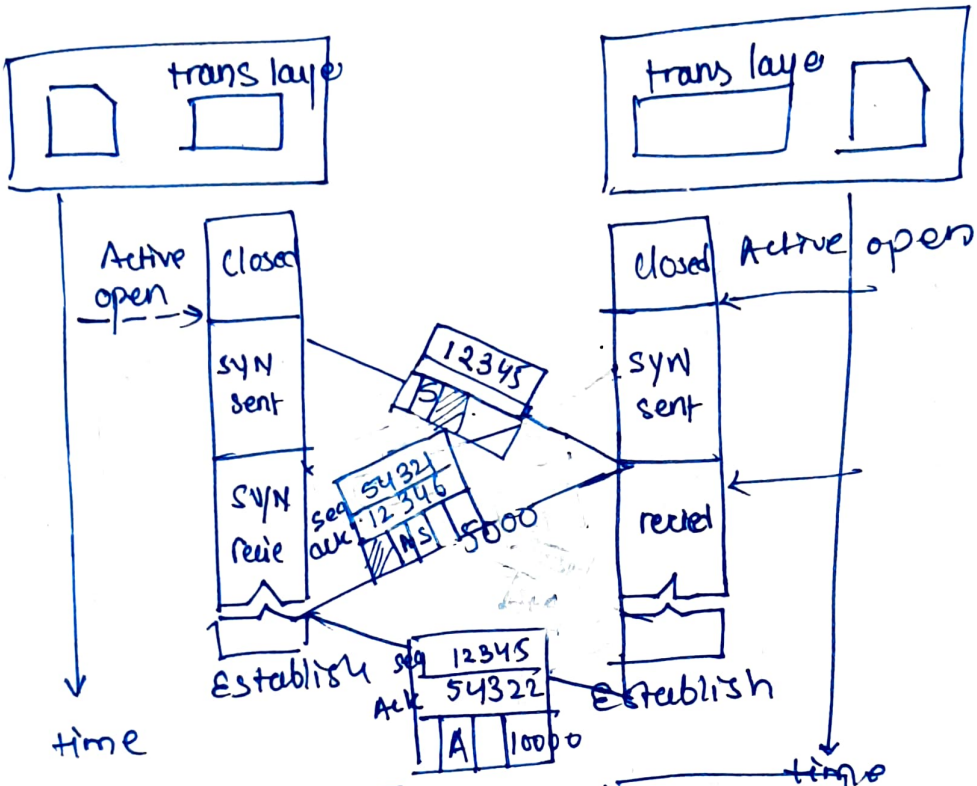
Question (4)

(A)

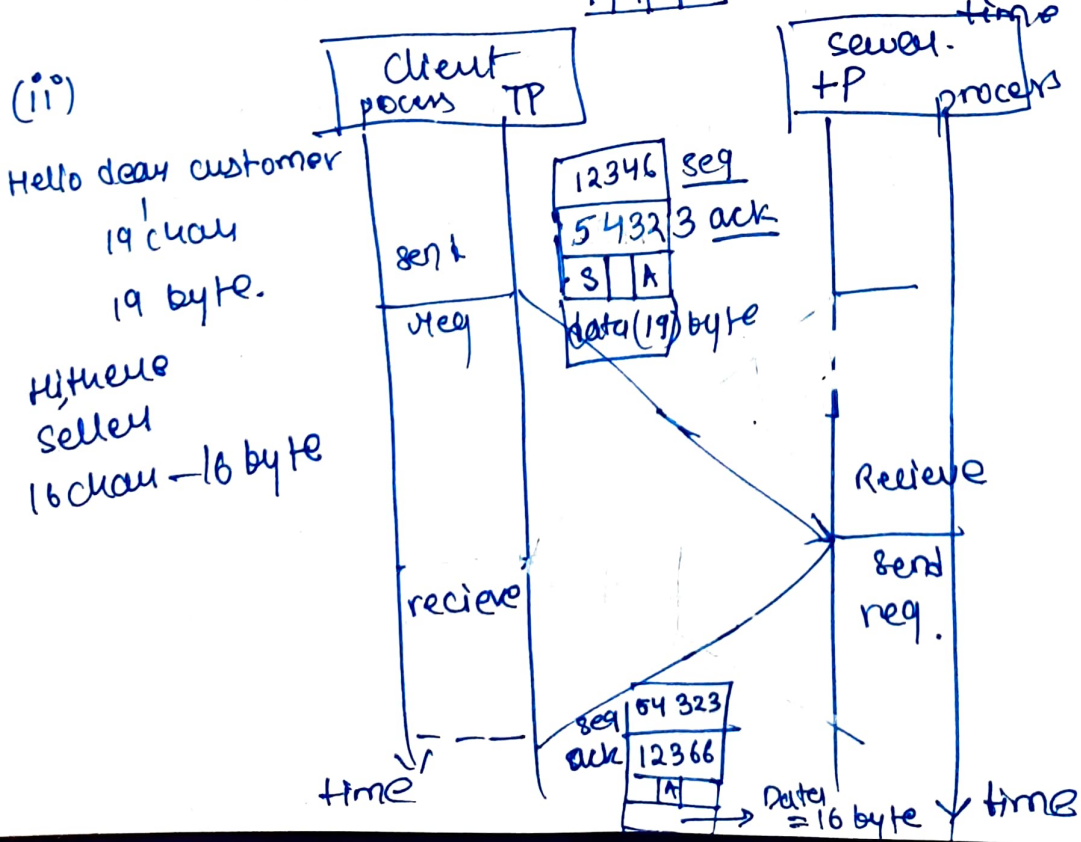
ISN = 12345
client

Server
ISN = 54321

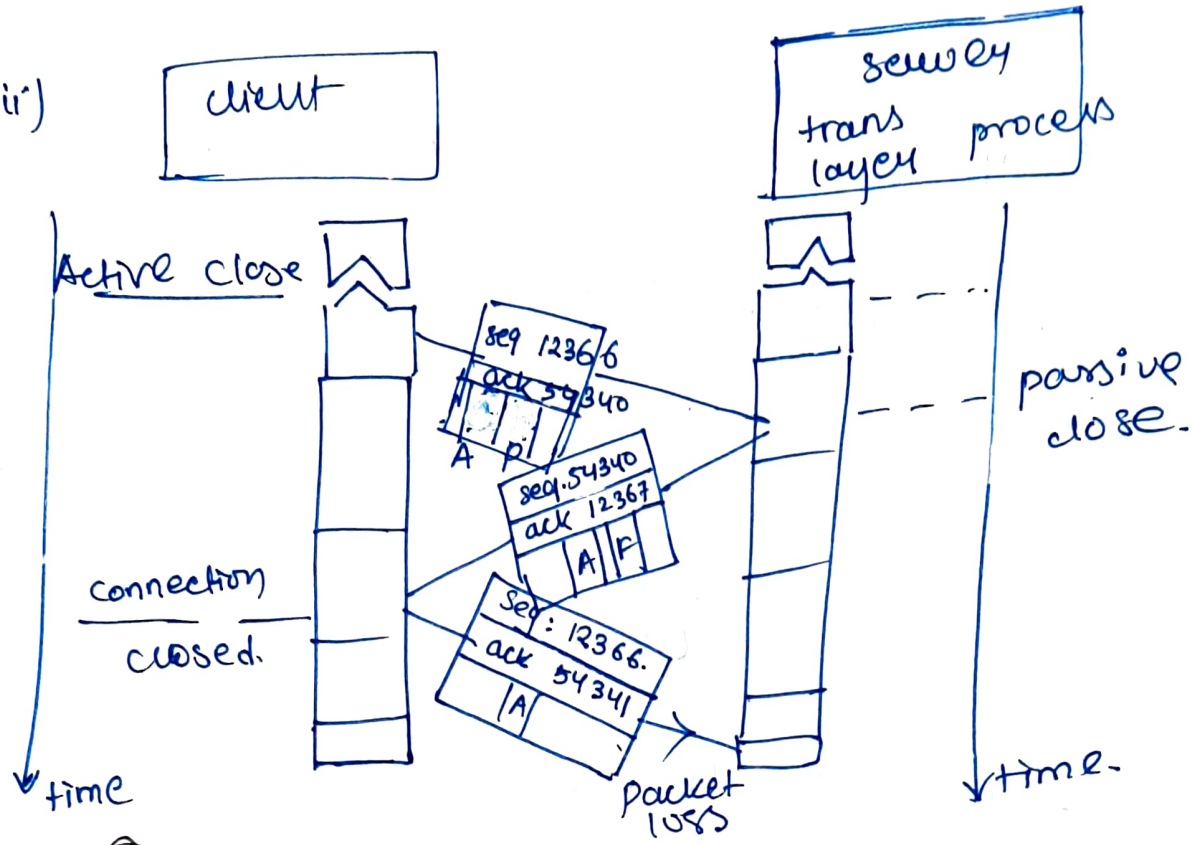
(i)



(ii)

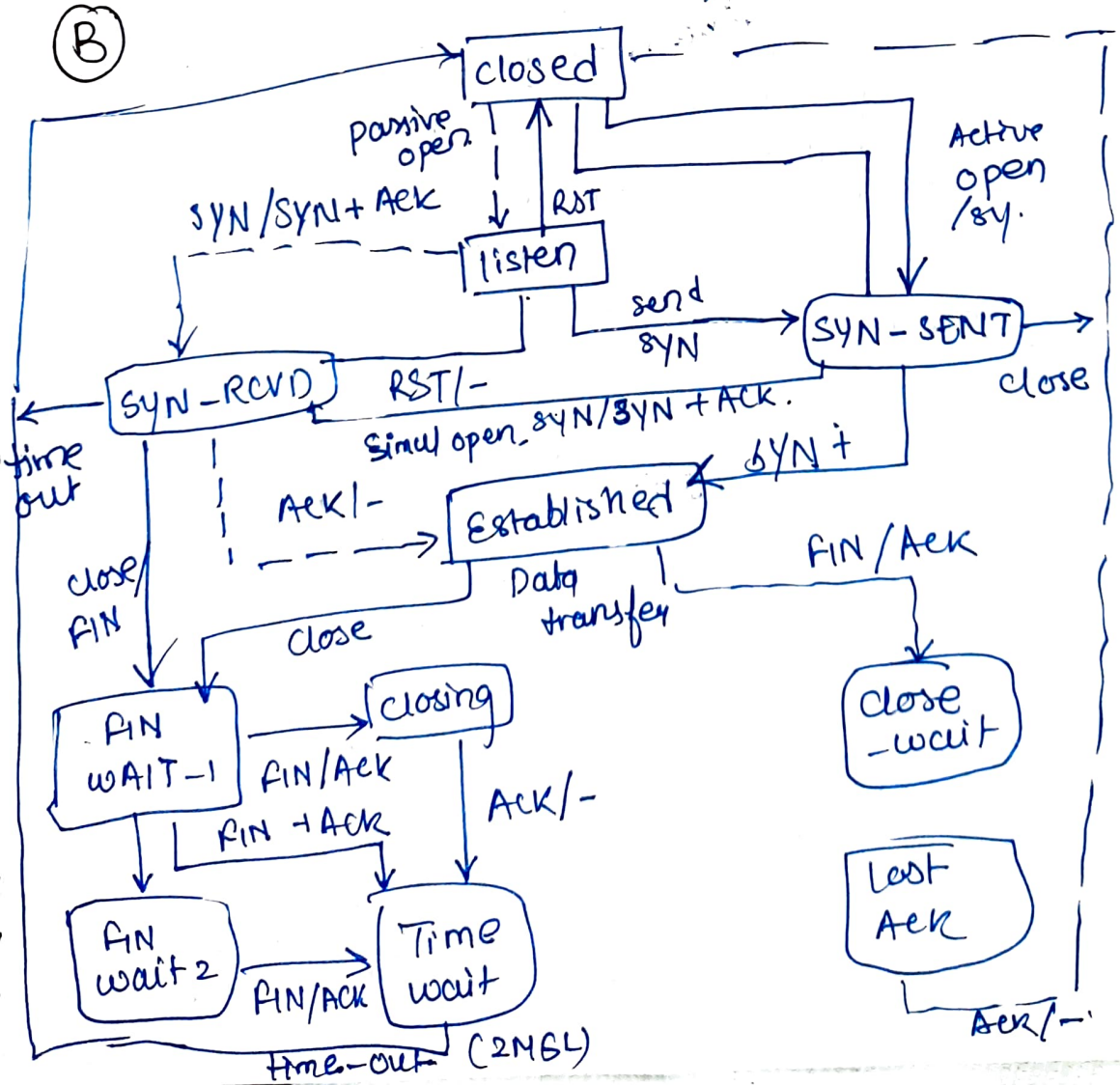


(iii)


client
server
trans layer
process
Active close
seq 12366
ack 54340
A
F
seq. 54340
ack 12367
A
F
Seq : 12366.
ack 54341
A
passive close.
connection closed.
time
Packet loss
time.

Quest (4)

(B)


closed
passive open
Active open /Sy.
SYN/SYN+Ack
RST
listen
send SYN
SYN-SENT
close
SYN-RCVD
RST/-
time out
Simul open SYN/SYN+ACK.
SYN+
ACK/-
Established
close/ FIN
close
Data transfer
FIN/Ack
FIN WAIT-1
closing
close_wait
FIN/Ack
FIN+ACK
ACK/-
FIN wait 2
Time wait
Last Ack
FIN/ACK
time-out (2MSL)
Ack/-

Question (5)

Four, headquarter, A, B, C, D.

Now, each has 4096 addresses also, B/c no allocati

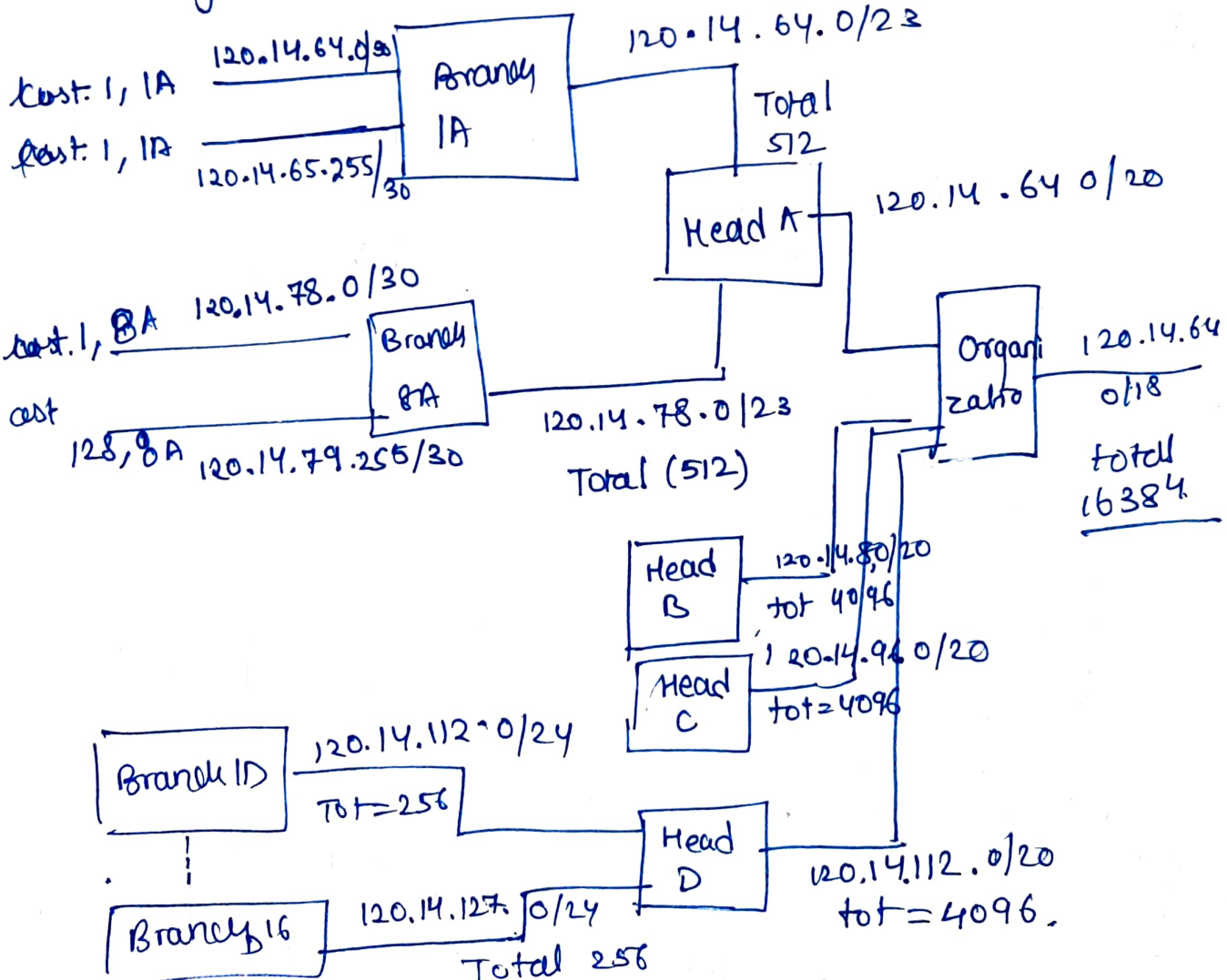
(a) A → 8 branch (512 address)

↓

128 customer (4 add).

(b) D have 16 branced (256 address)

Diagram.



hence, we got

→ organisation starting :- 120.14.64.0/18.

ending 120.14.127.255/18

→ Headquarter A

(i) starting — 120.14.64.0/20

(ii) ending — 120.14.79.255/20

(iii) Branch 1A starting : 120.14.64.0/23

ending : 120.14.65.255/23.

similiar for all branch.

(iv) Customer 1/A starting : 120.14.64.0/30

ending : 120.14.64.3/30

Similiarty for all other customer

→ Head B st : 120.14.80.0/20
end : 120.14.95.255/20

→ Head C st : 120.14.96.0/20
end : 120.14.111.255/20

→ Head D st : 120.14.112.0/20
end : 120.14.127.255/20.

(iii) Branch 1,D st = 120.14.112.0/24
end = 120.14.112.255/24

similiarty for all the branch.