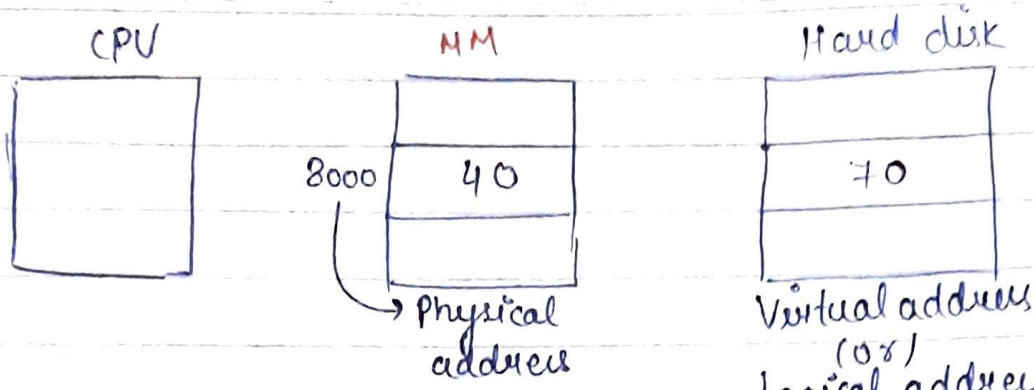


(Pointing to location at Main memory)

(Pointing to location at hard disk)

(Address of Computer)

- NIC Card
- (OR)
- MAC address
- (OR)
- Ethernet address
- (OR)
- Physical address

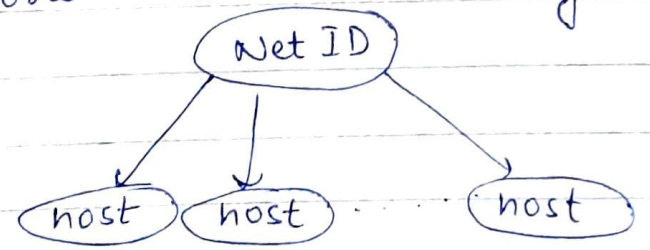
} 48 bit address

→ Source MAC

Destination MAC

- MAC address alone cannot be used in transmitting the data because every company has their own representations

- IANA :- Internet assigned number authority
  Come up with classful addressing (IP address) [32 bit address]
  → It supports two level hierarchy :-



In classful addressing are A, B, C, D, E (Research)

A, B, C → unicasting

D → multicasting

- Whenever an IP address is given to a computer, it is known as host

- Entire network will be represented by a number known as net-id

(i) Binary notation

IP address is represented in the form of 0's and 1's.

01011010 11110000 00001111 10101111

(ii) Dotted decimal notation

63.71.55.159

- In Binary notation, first few bits will decide the type of class
- In dotted decimal notation, the first octate will decide the type of class

⇒ **Class A**

0 (2^7-2) (2^{24}-2)

Net id (8 bits) | host (24 bits)

00000000 = 0

01111111 = 127

(0-127)

1-126

Reason for -2 in Net id

- Special address

0.0.0.0 ⇒ DHCP client (default address)

127.0.0.0 ⇒ loopback address

⇒ **Class B**

10 2^{14} (2^{16}-2)

Net bits (16 bits) | host (16 bits)

2^7 2^0

10000000 = 12

10 111111 = 1

(128-191)

Class B

eg:- 141.55.66.73 → class B coz 141 is in b/w 128 and 191

ie

⇒ In class B each network will have 2^{14} networks in which each network will have $(2^{16}-2)$ host

Class C

110 (2^{21}) — 2^8-2

Net bits (24 bits) — host bits (8 bits)

eg:- 110 00000 - 192

110 11111 - 223

(192 - 223)

Class D

1110 — 1110 0000 = 224

1110 1111 = 239

(224-239)

Class E

1111 — 1111 0000 = 240

1111 1111 = 255

(240 - 255

(i) 112 ⇒ 112 comes in

(i) 115 ⇒ 01110011

(ii) 15 = 00001111

(iii) 140 = 10001100

(iv) 60 = 00111100

(4)

Q:- IP ⇒ 201.55.66.123
Calculate the netid and direct broadcast address of network.

⇒ Network mask (or) and Default Mask :-

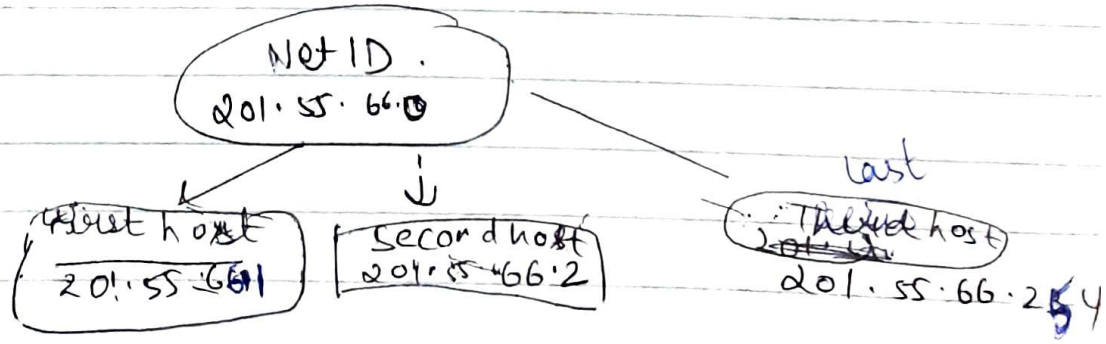
class A :- 11111111 00000000 00000000 00000000
255.0.0.0

class B :- 11111111 11111111 00000000 00000000
255.255.0.0

class C :→ 11111111 11111111 11111111.00000000
255.255.255.0

Q^nd solution :→

~~IP1 : 201.55.66.123~~
IP1 : 201.55.66.123
mask : 255.255.255.0
NetID : 201.55.66.0



⇒ 201.55.66.0 is not used for host.

⇒ Performing bitwise AND b/w IP numbers

⇒ Performing bitwise AND b/w IP address and network mask will give Net id

(a) $IP_1 = 144.81.63.79$

⇓ class B

NetId = 144.81.0.0

D.B.A = 144.81.255.255

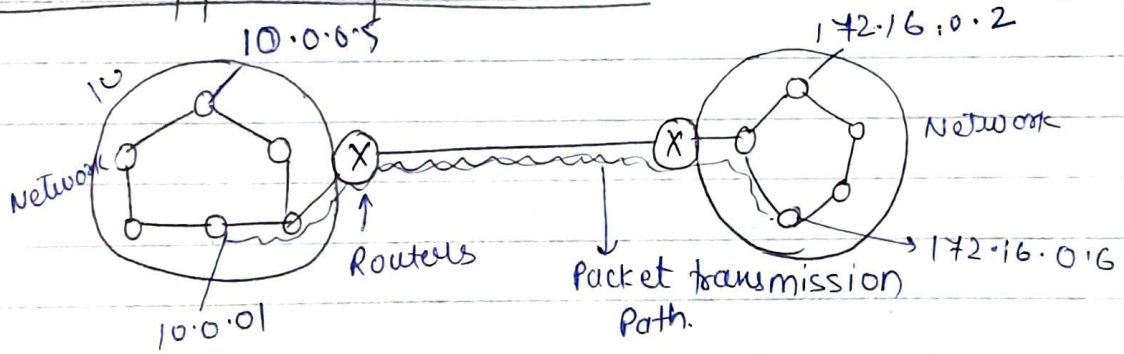
Direct Broadcast address

⇒ For a netid host bits are all zeros

⇒ DBA of a network put 255 in place of Hostid.

Direct Broadcast Address = 144.81.255.255

* Pseudo Approach of a Network :-



(i)

S.IP	D.IP
D | 10.0.0.1	172.16.0.6

⇓ Data ⇓ Source IP ⇓ Destination IP

} Packet

It is a unicast packet b/w the networks

(ii)

S.IP	D.IP
0 | 10.0.0.1	172.16.255.255

DBA

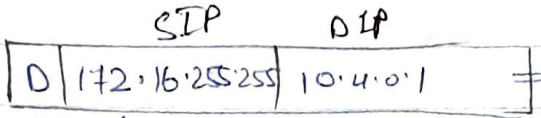
(Directed broadcast Address)

(6)

⇒ This packet is transmitted from one computer to a whole network (particular).

⇒ This is broadcasting broadcasting packet on other network

(iii)



⇒ only a single Comput

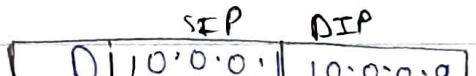
A particular n/w

This packet can't exist (coz many PC's wants this I

Direct broadcast address

⇒ Direct broadcast address will always be used as Destination.

(iv)

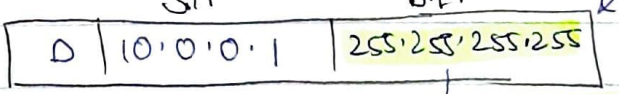


special care

packet

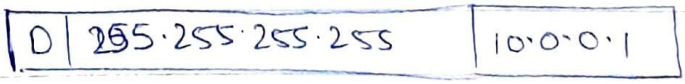
It is a unicast message within the network

(v) special case



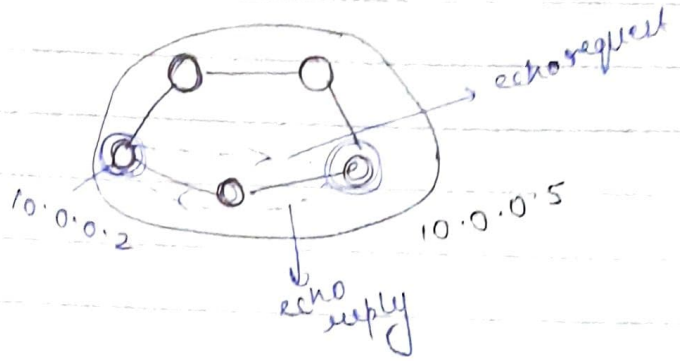
space is local

limited broadcast address (used for LAN)



not possit

⇒ Limited broadcast address will always be used a destination address.



Start → run → cmd → C:|> ping -t 10.0.0.5

Positive ack — TTL = 2 milisec, RTT = 4 milisec

C:|>Ping -t 10.0.0.5

negative ack — Unreachable or Time out message.

ping (Packet internet Gropher)

	SIP	D.IP
D	10.0.0.2	10.0.0.5

→ used for checking whether the connection is correctly established.

→ Ping is used for troubleshooting whether the Computers are connected to cables or not.

ARP request packet

S.MAC	D.MAC	S.IP	D.IP
10:12:13:1A:12:17	FF:FF:FF:FF:FF:FF	10.0.0.2	10.0.0.5

By adding this you are hiding this

MAC is encapsulating IP

FF:FF:FF:FF:FF:FF

Broadcast MAC address

Address Resolution protocol

ARP reply packet will return Destination MAC address.

- ARP Request packet is a broadcast packet which it doesn't contain destination MAC address.

- ARP Reply is a unicast containing the destination MAC address.

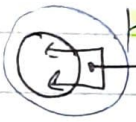
- ARP packet will encapsulate IP packet

- Troubleshooting itself (whether it itself properly connected or not)

C:\>ping -t 127.0.0.1 → loopback

TTL = 2msec , RTT = 4 msec.

	S. IP	D. IP
D	10.0.0.5	127.0.0.1



for checking connection correctness loopback is used

- Loopback address will always be used as destination address
- It is used for troubleshooting the self Computer whether it is properly connected to the cable or not
- loopback address packet will never enter into the network
- It is used for interprocess communication within the same system.

IP Address

Private IP address

Public IP address

(i) Works only in LAN

(ii) Scope is Local

(iii) Private IP address Range

10.0.0.0 – 10.255.255.255

172.16.0.0 – 172.31.255.255

192.168.0.0 – 192.168.255.255

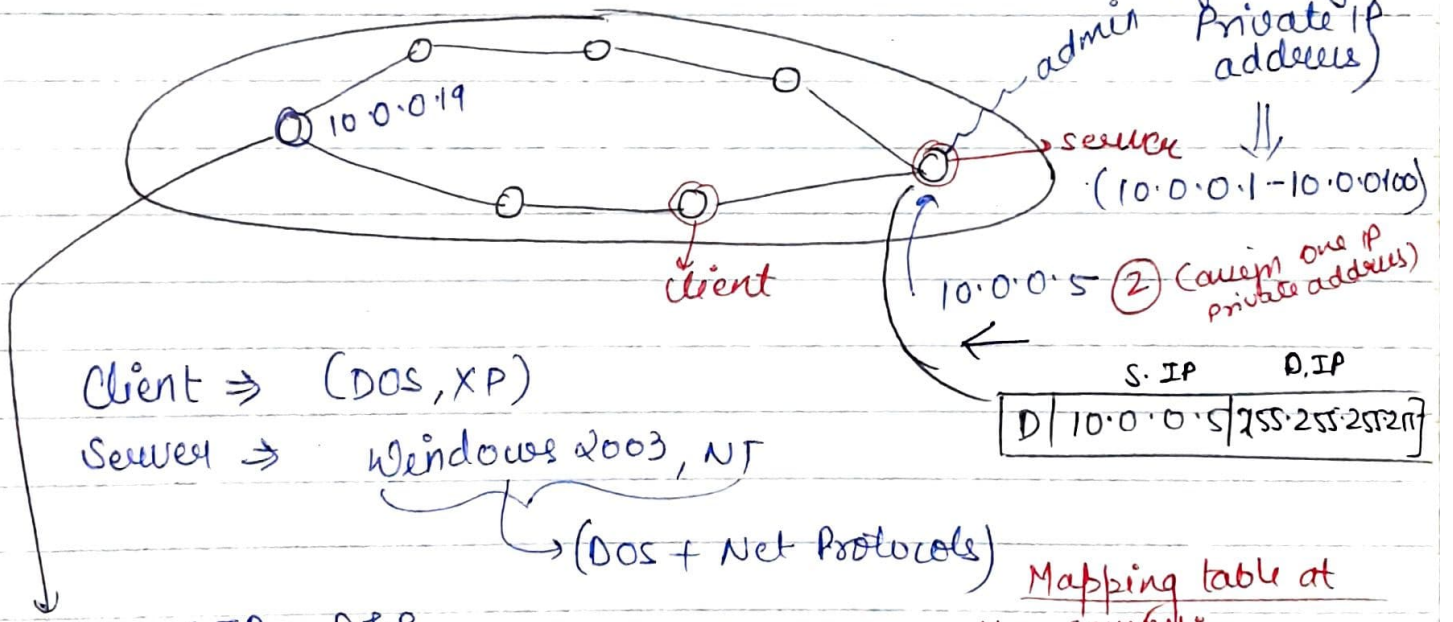
(iv) Loading operating System (NOS)

eg:- 172.16.0.5 → Private IP (network)

16.5.7.1 → Public IP

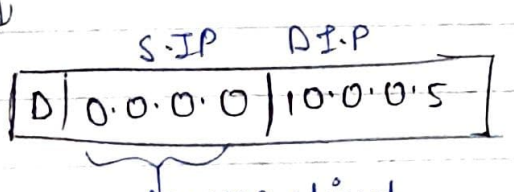
(v) Free of Cost

(vi) Will not get internet service.



Client ⇒ (DOS, XP)

Server ⇒ Windows 2003, NT → (DOS + Net Protocols)



+

MAC address - 17:13:1A:10:12:B

Mapping table at the server :-

MAC address	IP address
17:13:1A:10:12:13	10.0.0.19

» Private IP is used to communicate within the LAN only

(10)

Steps for assigning IP address to given MAC address :-

- Once the server is loaded into network Operating System then it will get group of private IP addresses
- Out of which one IP is assigned to the server
- The servers IP is informed to all clients with the help of limited broadcast address.

NOTE :- When a computer is not having an IP still it wants to transmit the data, it can use 0.0.0.0 as the source address.

DHCP client

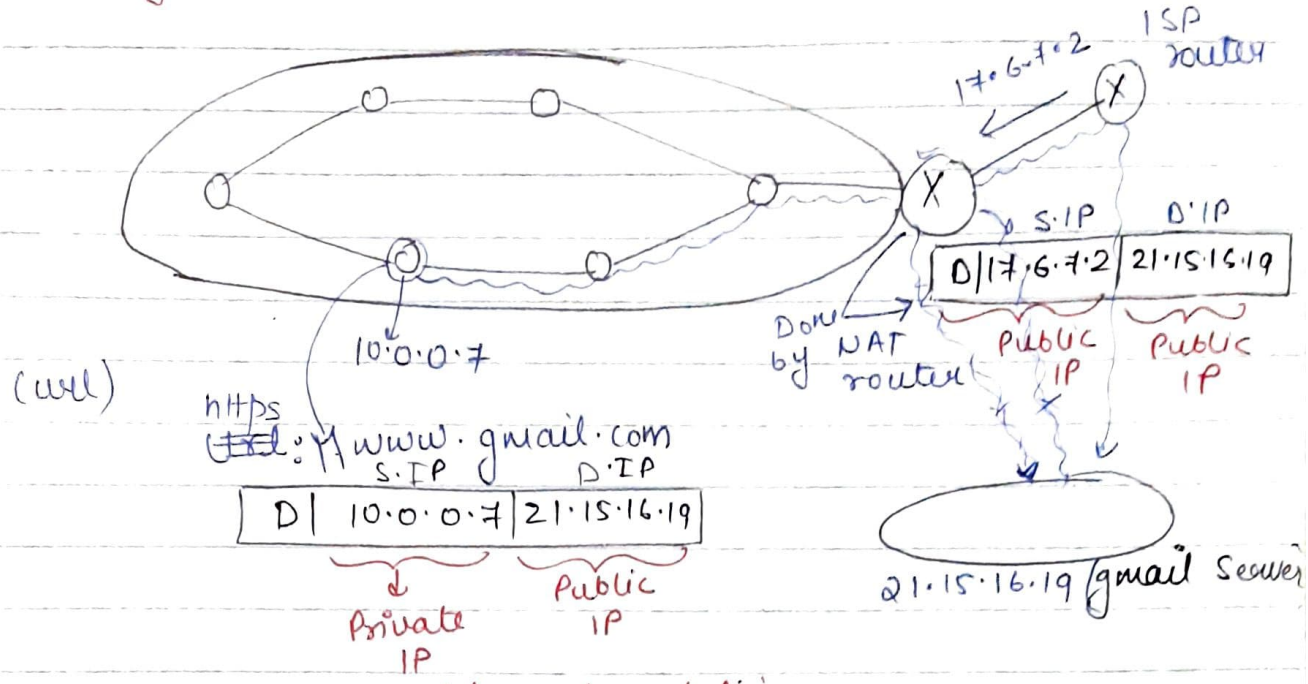
- When every computer is requesting, along with IP its MAC address is also transmitted so that admin can understand which IP is assigned to which computer

IPv4 is a stateful protocol using DHCP server because the information about the computer is available.

⇒ Public IP address

1) Internet Service
2) With the help of ISP (Internet Service Provid
3) Globally unique.
4) Not free of cost

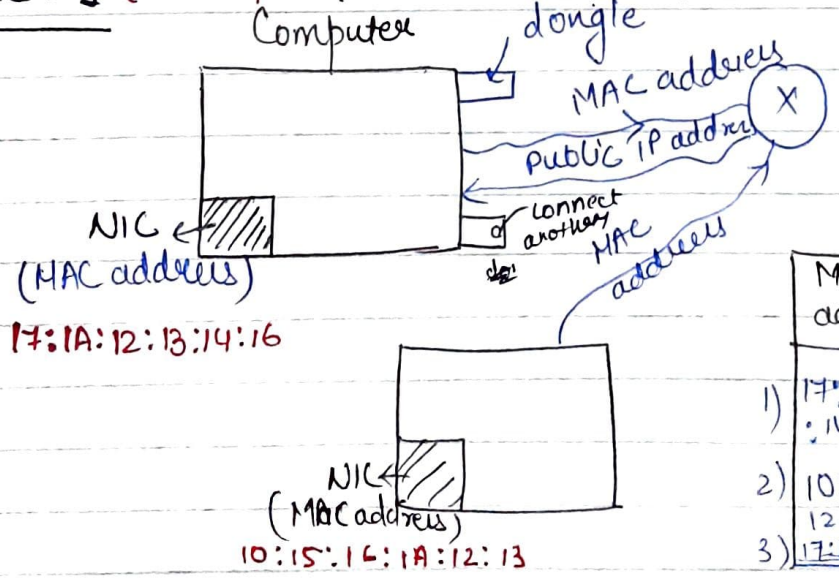
Getting Public IP address for a LAN



Network address translation

- NAT Router converts private IP into Public IP when the packet is going out of the network.
- It converts Public IP into private IP when the packet is coming inside the network.
- Using private IP addresses, Public IP addresses are efficiently and effectively utilized.

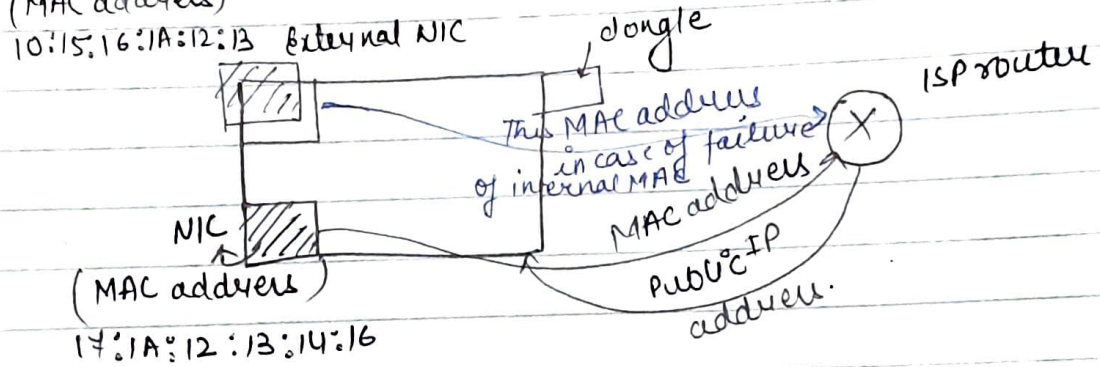
Practical-1 (A Computer can have more than 1 IP addrss at different instant of time)



	MAC address	Public IP	Enable
1)	17:1A:12:13:14:16	17:1:5:6 (fre)	✓ ✗
2)	10:15:16:1A:12:13	17:1:5:6	✓
3)	17:1A:12:13:14:16	12.5.5.6	✓

- A Computer can have multiple IP addresses at different instance of time (IPv_4)
- This Concept is known as "Same MAC multiple IP addresses at different instance of time"

Practical-2 :→ (A Computer can have multiple MAC)



	MAC address	Public IP	Enable
1)	17:1A:12:13:14:16	17.1.5.6	✓
2)	10:15:16:1A:12:13	17.1.5.6	✓

- A Computer can have multiple MAC addresses to support fault tolerance.
- This Concept is known as "multiple MAC same IP at different instance of time"

Drawbacks of classful addressing :→

Class A $(2^7 - 2)$ networks ⇒ each network $(2^{24} - 2)$ hosts

Class B (2^{14}) networks ⇒ each network $(2^{16} - 2)$ hosts

Class C (2^{21}) networks ⇒ each network $(2^8 - 2)$ hosts

How you define a Concept called "Subnetting"

Dividing a network into small parts so that IP addresses can be efficiently utilized is known as subnetting.

1# In class C, subnet mask is 255.255.255.224

If only subnet mask is given we can only calculate → no. of subnets
→ no. of hosts in each subnet

255 . 255 . 255 . 224

11111111 . 11111111 . 11111111 . 11100000

N | Subnet | H

Class C network mask is 255.255.255.0

11111111 . 11111111 . 11111111 . 00000000

N | H

During subnetting subnet bits are borrowed from host

no. of subnets = $2^3 - 2 = 6$

no. of hosts in each subnet = $2^5 - 2 = 30$

2# In class C, if subnet mask is 255.255.255.240
Find no. of subnets and no. of hosts in each subnet

Subnet mask
255.255.255.240
11111111.11111111.11111111.11110000
N | Subnet H

Class C network mask
255.255.255.0
11111111.11111111.11111111.00000000
N | H

no. of subnets = $2^4 - 2 = 14$
no. of hosts in each subnet = $2^4 - 2 = 14$

3# In class B if subnet mask is 255.255.254.0
Find no. of subnets
no. of hosts in each subnet

Subnet mask
255.255.254.0
11111111.11111111.1111111|0.0
N | Subnet | Host

N/w mask of class B
255.255.0.0
11111111.11111111.00000000.00000000
N | H

no. of subnets = $2^7 - 2 = 126$
no. of hosts in each subnet = $2^9 - 2 = 510$

4# $IP_1 = 201.55.66.89$
Subnet mask = 255.255.255.224

Subnet ID = 255.255.255.224 AND 201.55.66.89

89 = 01011001
224 = 11100000
64 = 01000000

201.55.66.89
255.255.255.224
201.55.66.64

∴ Subnet ID = 201.55.66.64

Subnet no.

Subnet mask ⇒ 11111111 . 11111111 . 11111111 . 11100000

Subnet ID ⇒ 201 . 55 . 66 . 01 000000
S H
↑ Subnet no.

• ⇒ for a subnet ID, host bits are all 0's

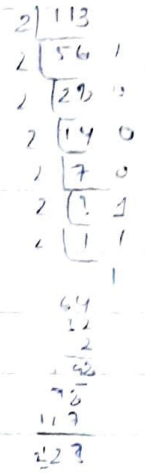
5# IP_1 = 200 . 89 . 79 . 113
Subnet mask = 255 . 255 . 255 . 240

Subnet ID

200 . 89 . 79 . 113
255 . 255 . 255 . 240
200 . 89 . 79 . 112 → Subnet ID

Perform Bitwise ~~AD~~ AND

113 = 01110001
240 = 11110000
112 = 01110000



Subnet no.

Subnet mask = 11111111 . 11111111 . 11111111 . 11110000
Subnet ID = 200 . 89 . 79 . 01110000
H
Subnet

6# IP_1 = 199 . 89 . 99 . 111
Subnet mask = 255 . 255 . 255 . 224 → 111 00000
S H

Trick

Binary representation of 3

(1) 3rd Subnet ID = 011 00000 = 199 . 89 . 99 . 96
S H

(2) 5th Subnet ID = 101 00000 = 199 . 89 . 99 . 160
S H

BR of 5

why starting 3 bits ?

Ans

7#) no. of hosts in each subnet = $2^n - 2$

IP_A = 200.80.70.125
Subnet mask = 255.255.255.224

Find →

(i) Subnet ID = 200.80.70.125
255.255.255.224
200.80.70.96 ←

125 = 01111101
224 = 11100000
96 = 01100000

255.255.255.224 → 11100000
N H S H

200.80.70.96 → 01100000
S H
It is 03rd subnet ID

(ii) First host of that subnet
= 01100001
↳ as '0' we have already used for subnet ID

(iii) Last host of that subnet
= 01111110
200.80.70.126

(iv) DBA of that subnet = 01111111
= 200.80.70.127
Direct Broadcast Address

* In the no. of host in each subnet we are subtracting '2' because one is used for subnet ID and other one is used DBA of the subnet.

8#

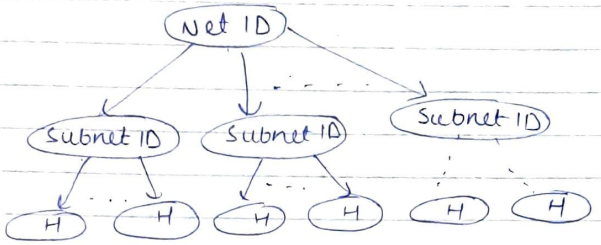
$IP_1 = \underbrace{203 \cdot 55 \cdot 66}_{N} \cdot 89$

$IP_2 = \underbrace{203 \cdot 55 \cdot 66}_{N} \cdot 99$

$IP_3 = \underbrace{203 \cdot 55 \cdot 66}_{N} \cdot 109$

Subnet mask = $\underbrace{255 \cdot 255 \cdot 255}_{N} \cdot \underbrace{224}_{S,H} \rightarrow \underbrace{111}_{S}\underbrace{00000}_{H}$

Identify IP's belong to same subnet?



$IP_1 = 203 \cdot 55 \cdot 66 \cdot (89)$

$\underbrace{010}_{S}11001 \rightarrow 2^{nd}$ subnet

$IP_2 = 203 \cdot 55 \cdot 66 \cdot (99)$

$\underbrace{011}_{S}00011 \rightarrow 3^{rd}$ subnet

$IP_3 = 203 \cdot 55 \cdot 66 \cdot (109)$

$\underbrace{011}_{S}01101 \rightarrow 3^{rd}$ subnet

So, IP_2 and IP_3 belongs to same subnet

(18)

9# $IP_1 = 199.59.79.112$

Subnet mask = 255.255.255.224 → 111 00000 (S H)

Calculate

(1) 2nd host of 4th subnet

(2) 4th host of 2nd subnet

(3) 1st host of 3rd subnet

(4) 3rd host of 1st subnet

Ans (1) 100 00010 = 130 (199.59.79.130)

S → 4th subnet; H → 2nd host

(2) 010 00100 = 68 (199.59.79.68)

S → 2nd subnet; H → 4th host

(3) 011 00001 = 97 (199.59.79.97)

S → 3rd subnet; H → 1st host

(4) 001 00011 = 35 (199.59.79.35)

S → 1st subnet; H → 3rd host

10# $IP_1 = 205.66.77.149$ (^ means class C)

Subnet mask = 255.255.255.224 → 111 00000 (S H)

(1) Net ID = 205.66.77.0 (N | H)

(2) First subnet ID = 001 00000 = 32

1st subnet ID → 205.66.77.32

(3) Calculate the DBA of the network.

205 · 66 · 77 · 255
N H → 11111111

used for n/w ID
0 Subnet ← 000 X
001 -1
010 -2
011 -3
100 -4
101 -5
110 -6
DBA Subnet → 111 X
used for DBA of n/w

(4) Calculate Last Subnet ID

= 110 11111

= 110 00000

Last Subnet ID → 205 · 66 · 77 · 192

* On the no. of ~~hosts~~ Subnets we are subtracting 2 because one is used for net ID and the other one is used for DBA of the network.

1 0 #

IP_1 = 200 · 99 · 89 · 149

Subnet mask = 255 · 255 · 255 · 240

240 → 1111 0000
S H

(1) Calculate the 1st host of 1st Subnet

00010001 = 17

200 · 99 · 89 · 17

(2) Calculate the last host of Last Subnet

11101110 = 238

200 · 99 · 89 · 238

2 | 2 · 10
1

1 1
127
64
32
223

64
-2
62

12#

$IP_1 = 144.99.89.117$

Subnet mask = 255.255.254.0

N → 255.255 ; 254.0 → 11111110.00000000 (S, H)

(1) First host of first subnet

S: 00000010.00000001 (H) = 2.1

144.99.2.1

(2) Last host of last subnet

11111110.11111110 = 253.254

S, H

144.99.253.254

13#

$IP_1 = 199.59.69.117$

Subnet mask = 255.255.255.224

224 → 11100000 (S, h)

(i) NetID = 199.59.69.0

Find → First subnet ID.

199.59.69.00100000

199.59.69.32

no. of subnets possible $= 2^n - 2$

$= 2^3 - 2$

$= 8 - 2$

$= 6$

→ Second subnet ID 199.59.69.01000000

199.59.69.64

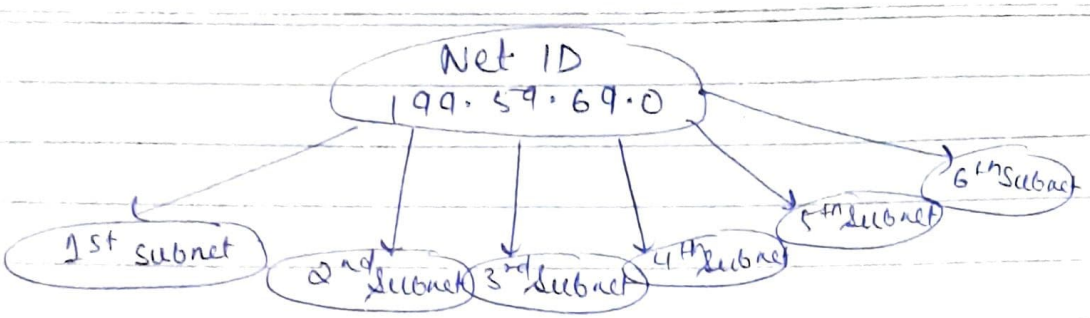
→ Third subnet ID 199.59.69.01100000

199.59.69.96

→ 4th Subnet ID 199.59.69.128

→ 5th Subnet ID 199.59.69.160

→ 6th Subnet ID 199.59.69.192



(ii) Calculate the 1st host of 1st subnet

00100001 = 33

199.59.69.33

(iii) Calculate the last host of 1st ~~host~~ subnet

00111110 = 62

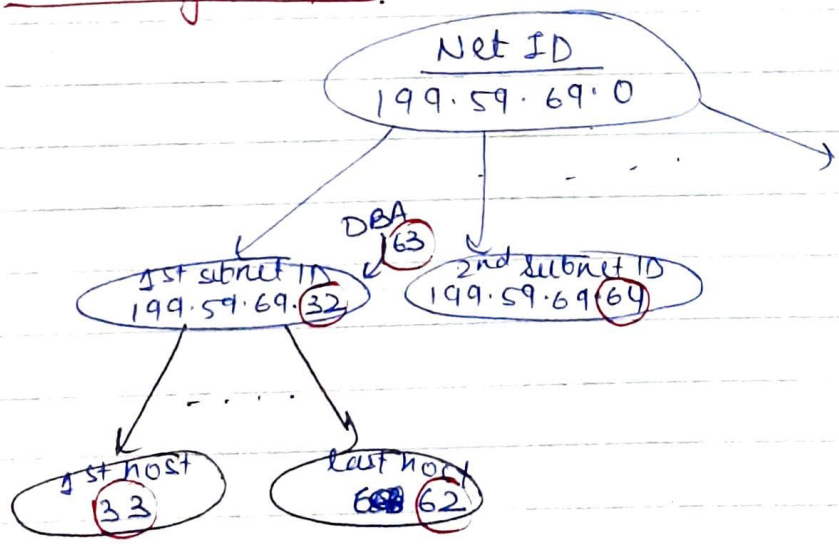
199.59.69.62

(iv) DBA of 1st subnet.

00111111 = 63

199.59.69.63

See the Logic or pattern.



255.255.255.224

11111111.11111111.11111111.11100000

N S H

Continuous mask

14#

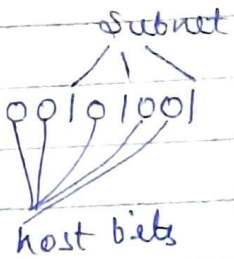
$IP_1 = 200 \cdot 93 \cdot 61 \cdot 123$ (200 → class C)

Subnetmask = 255 · 255 · 255 · 41

⇓

11111111 · 11111111 · 11111111 · 00101001

Discontinuous mask



(i) First subnet ID

1st Subnet → 001

0 0 0 0 0 0 0 1

200 · 93 · 61 · 1

(ii) 2nd subnet ID

0 0 0 0 1 0 0 0

200 · 93 · 61 · 8

» Continuous mask is practical whereas discontinuous mask is not practical

15#

DBA of subnet is 201 · 55 · 66 · 3 (201 → class C; 3 → 00011111)

which of the following can be subnet mask?

a) 255 · 255 · 255 · 192

b) 255 · 255 · 255 · 240

c) both a and b

d) none

{ For DBA, host bits all 1 }

a) 255 · 255 · 255 · 192

N → 11 (S) 000000 (H) ← 6 — 00 — 5 ← 000,11111

b) 255·255·255·240 → 1111 0000 (S, H) — 4 — yes — 5 to 4 also there — 000|11111 (H)

16# DBA of subnet is 200·66·19·15 (200 → class C) (15 → 00001111)
Which of the following can be subnet mask?

a) 255·255·255·224
b) 255·255·255·248
c) 255·255·255·192
d) none of above

a) ✗ 255·255·255·224 → 11100000 — no — 00001111 (h)

Continuously 5 1's we are expecting but here 4 are there

b) ✓ 255·255·255·248 → 11111000 (h) — 00001111 (h)

c) ✗ 255·255·255·192 → 11000000 (h) — 00001111 (h)

17# DBA of subnet is 198·131·55·63 (198 → class C) (63 → 00111111)
Which of the following can be subnet mask

a) 255·255·255·224
b) 255·255·255·240
c) 255·255·255·248
d) ✓ ~~None~~ All

a) 255·255·255·224 → 11100000 ✓ 00111111

b) 255·255·255·240 → 11110000 ✓ 00111111

c) 255·255·255·248 → 11111000 ✓ 00111111

24

"equal bhi nai chalega bada hi chaiye"

18# DBA of Subnet is 204.99.55.15 → 00001111

Which of the following can be Subnet mask?

a) 255.255.255.240 → 11110000 × 00001111

b) 255.255.255.248 → 11111000 ✓ 00001111

c) both a and b

d) none

Reason.

Subnet will start with 00001 atleast

≡ that means 1st Subnet DBA

19# Which of the following IP can be advertised to Internet?

a) 192.168.0.1

b) 172.16.8.1

c) 17.5.601

d) none

20# If Subnet mask is 255.255.255.224 → 11100000 (255 → class A)

which of the following can be DBA of ~~Subnet~~.

a) 201.55.66.15

b) 201.55.66.31

c) 201.55.66.63

d) All

a) 201.55.66.15 → 00001111 × 11100000

b) 201.55.66.31 → 00011111 × 11100000

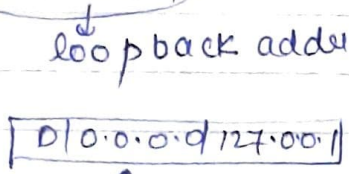
c) 201.55.66.63 → 00111111 ✓ 11100000

16
32
3

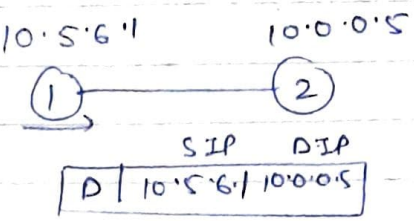
21# Which of the following IP can be used as both Source IP and destination IP

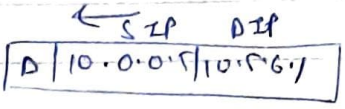
a) 10.255.255.255
b) 255.255.255.255
c) 10.5.6.1
d) 127.0.0.1

loopback address



If a computer is not assigned any IP then 0.0.0.0 is an IP





=> Even without assigning an IP address to a computer we can go for loopback test.

22# If a Company requires 60 hosts what is the best possible subnet mask.

Start with class C. | N+S+H

Subnet mask = no. of host in subnet = $2^6 - 2 = 62$

N + S + H
24 + 2 + 6

11111111 11111111 11111111 11000000
N S H

255.255.255.192

23:- If a company requires 30 hosts find subnet mask?

Class C ⇒ no. of host in subnet = $2^5 - 2 = 30$

N+S+H

24+3+5

11111111 11111111 11111111 111 00000

N S H

255.255.255.224

24# If a Company requires 500 hosts find subnet mask?

class B ⇒ no. of host in subnet = $2^9 - 2$

$= 510$

N+S+H

16 7 9

11111111.11111111.1111111 0 00000000

N S H

255.255.254.0

Here 10 is a wastage.

"Supernetting" :-

Joining two or more network to form a larger network according to the requirement of user. These known as Supernetting.

127.127.255.255 ⇒ used for loopback testing

1.> On class C, if Supernet mask = 255.255.252.0
Find no. of networks that can be joined = $2^{②} = 4$
↓ log 2 bits are modified

255.255.252.0

11111111.11111111.11111100.00000000

N | Supernet bits | H

» During Supernetting, Supernet bits are borrowed from Network portion.
» During Supernetting, we can join power of 2 n/ws and
2.> Continuous networks

2.> If Class C, if Supernet mask is 255.255.240.0
Find no. of networks that can be joined.

255.255.240.0

11111111.11111111.1111 0000.00000000

N | Supernet bits | H

3.> If one of address of Supernet is 201.99.87.93 (→ class C)
Supernet mask is 255.255.252.0
Find Range of Supernet? (Supernet ID → DBA of Supernet)

IP = 201.99.87.93
Supernet mask = 255.255.252.0
Supernet ID = 201.99.~~87~~84.0

87 = 01010111
252 = 11111100
84 = 01010100

23

255 · 255 · 252 · 0

11111111 · 11111111 · 11111100 · 00000000

N — Supernet bits — H

Supernet ID ⇒ 201 · 99 · 84 · 0

84.0 – 84.255 (1st n/w)
01010100 · 00000000 (H)
⋮ this 9 nos from supernet mask
01010100 · 11111111 (h)

85.0 – 85.255 (2nd n/w)
01010101 · 00000000 (h)
⋮
01010101 · 11111111 (h)

86.0 – 86.255 (3rd n/w)
01010110 · 00000000 (h)
⋮
01010110 · 11111111 (h)

87.0 – 87.255 (4th n/w)
01010111 · 00000000 (h)
⋮
01010111 · 11111111 (h)

2 bits of supernet so $2^2 = 4$ n/ws are joined

Range ⇒ 201 · 99 · 84 · 0 ⟶ 201 · 99 · 87 · 255

IP addresses can be effectively utilized using Subnetting and Supernetting.

4.>> Can the network mask of class C be the subnet mask of class B?

class C = 255.255.255.0 (n/w mask)
class B = 255.255.0.0

During subnetting the bits are borrowed from host

If in class B we borrow bits from host then class C n/w mask can be obtained

So True

5.>> Can the network mask of class B be the supernet mask of class C.

Class B = 255.255.0.0
Class C = 255.255.255.0

During supernetting the bits are borrowed from n/w

If in class C we borrow bits from n/w side then class B n/w mask can be obtained

So True

Subnetting

* Special Case

(1) $IP_1 = 201.55.73.149$

Subnet mask = 255.255.255.128

(Explicitly Configured zero subnet and DBA subnet)

(OR)

(Network wishes to form subnets) [NO network Only subnet]

(30)

255 . 255 . 255 . 128

⇓

11111111 . 11111111 . 11111111 . 10000000

N — Subnet — H

1) ⇒ zero Subnet ID = 0 0000000 = 201.55.73.0

S H

(i) ⇒ First host of zero Subnet = 0 0000001 = 201.55.73.1

S H

(ii) ⇒ Last host of zero Subnet = 0 1111110 = 201.55.73.126

S H

(iii) ⇒ DBA of zero Subnet = 0 1111111 = 201.55.73.127

S H

2) DBA Subnet ID = 1 0000000 = 201.55.73.128

S H

(i) First host of ~~zero~~ DBA Subnet = 1 0000001

S H

= 201.55.73.129

(ii) Last host of DBA Subnet = 1 1111110

S H

= 201.55.73.254

(iii) DBA of DBA Subnet = 1 1111111

S H

= 201.55.73.255

Subnet mask = 255.255.255.128
Network is divided into subnets.

no. of subnets = $2^n - 2$
= $2^1 - 2 = 0$ subnets

For class C, subnet mask is 255.255.255.224
network wishes to form subnets

| no. of subnets = 2^n |

For class C, if subnet mask is 255.255.255.224
network is divided into subnets.

| no. of subnets = $2^n - 2$ |

000 → zero subnet
001 → 1st subnet
010
011
100
101
110 → last subnet
111 → DBA subnet

Classless addressing

Classless → no class

Block = group of IP address

161.55.71.79/26 ⇒ CIDR notation (Classless Interdomain Routing notation) and Slash notation

161.55.71.79 → IP address

26 → mask

/26 ⇒ 11111111 11111111 11111111 11000000 (255.255.255.192)

/30 ⇒ 11111111 11111111 11111111 11111100 (255.255.255.252)

/27 ⇒ 11111111 11111111 11111111 11100000 (255.255.255.224)

/22 ⇒ 11111111 11111111 11111100 00000000 (255.255.252.0)

1# One of the address of Block is 130.55.79.93/26

no of addresses in Block = 2^{32-n}

$= 2^{32-26}$

$= 2^6$

= 64 IP address are possible.

11000000

93 ⇒ 01011101

01 000000 ⇒ 64 → 1st address of this Block

01 111111 ⇒ 127 → last address of this Bl

⇒ Range of Block = 130.55.79.64/26 → 130.55.79.127/26

→ Net Id = 130.55.79.64/26

→ First host of net = 130.55.79.65/26

→ Last host of net = 130.55.79.126/26

→ DBA of net = 130.55.79.127/26

Properties of classless addressing

1) Addresses in a block are continues
2) The first addres of a block should be exactly ~~delived~~ divisible by ~~first~~ no. of addresses of a block.

eg:- 64 is 1st addres of a Block

64 | 64 | 1

64 / x

no. of addresses

1st address of block

= One of the addres of Block is 210.55.79.119/27

no. of addreses in block = 2^{32-n}

$= 2^{32-27}$

$= 2^5$

= 32 IP addreses are possible.

119 ⇒ 01110111

011 00000 → 96 ⇒ 1st address of this block

⋮

011 11111 → 127 ⇒ last address of this block

Range of Block = 210.55.79.96/27 – 210.55.79.127/27

32 | 96 | 2
96
x

3# One of the address of Block is 17.99.89.113/20

no. of address in Block = 2^{32-n}
= 2^{32-20}
= 2^{12} ⇒ $2^4 \times 2^8$

(least two octates we will take.)

89.113 ⇒ 01011001.01110001

80.0 ⇒ 0101 0000.00000000 → 1st address of the block

⋮

95.255 ⇒ 0101 1111.11111111 → last address of the block

Range of Block = 17.99.80.0/20 – 17.99.95.255/20

80.0 – 80.255 ⇒ 2^8
81.0 – 81.255 ⇒ 2^8
82.0 – 82.255 ⇒ 2^8
⋮
95.0 – 95.255 ⇒ 2^8

$16 \times 2^8 \Rightarrow 2^4 \times 2^8$

4# One of the addrss of Block is = 80.73.117.127/22

no. of addresses of Block = 2^{32-22}

$= 2^{10} = 2^2 * 2^8$

This gives an idea to take last two octates

117.127 ⇒ 01110101.01111111

⇒ 01110100.00000000 ⇒ 116.0 → 1st address of the block

⇒ 01110111.11111111 → 119.255 → Last address of the block

Range ⇒ 80.73.116.0/22 - 80.73.119.255/22

5# Which of the following can be 1st address of Block if Block contains 32 IP address ($2^5 < 2^8$)

a) 201.99.66.16 32|16 ✓

b) 201.99.66.160 32|160 ✗

c) 201.99.66.16

d) None

→ 1st address exactly divisible by no. of IP addresses

6# Which of the following can be first address of Block contains 1024 IP addrss

a) 15.6.7.0 ✗ 4|7

b) 15.6.2.0 4|2 ✓

c) 15.6.16.0 4|16 ✓

d) None

↓ Here $2^{10} > 2^8$ so

$2^{10} \Rightarrow 2^2 \times 2^8$

4 × 256

check for this (divisibility)

64 =
117 = 1110101

Q:→ One of the address of a block is 130.66.79.117/26 of this block is divided into 4 equal sub blocks then calculate the Range of Block and range of subblock.

$2^{32-26} = 2^6 = 64$

Range of Block = 130.66.79.64/26 - 130.66.79.127/26

no. of addresses in each subblock = $\frac{64}{4} = 16 = 2^4$

2^{32-28} ← Subnet mask

64 ⇒ 0100 0000

64 → 0100 0000 } Range of 1st subblock
79 ⇒ 0100 1111 }

Range of 1st subblock = 130.66.79.64/28 - 130.66.79.79/28

Range of 2nd sub block = 130.66.79.80/28 - 130.66.79.95/28

Range of 3rd subblock = 130.66.79.96/28 - 130.66.79.111/28
Range of 4th subblock = 130.66.79.112/28 - 130.66.79.127/28

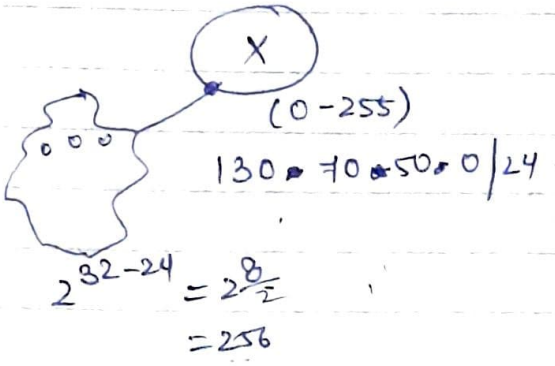
64 ⇒ 0100 0000 } 1st subblock
79 ⇒ 0100 1111 }

80 ⇒ 0101 0000 } 2nd subblock.
95 ⇒ 0101 1111 }

96 ⇒ 0110 0000 } 3rd subblock
111 ⇒ 0110 1111 }

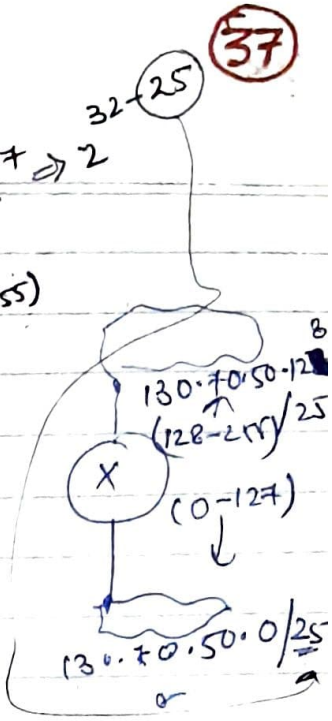
112 ⇒ 0111 0000 } 4th subblock
127 ⇒ 0111 1111 }

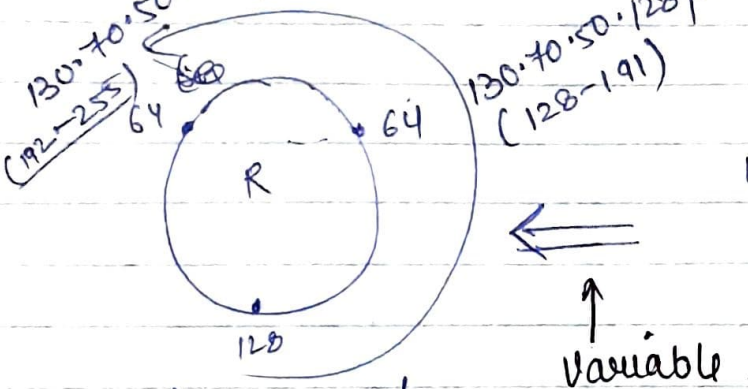
Equal length Subnetting :→



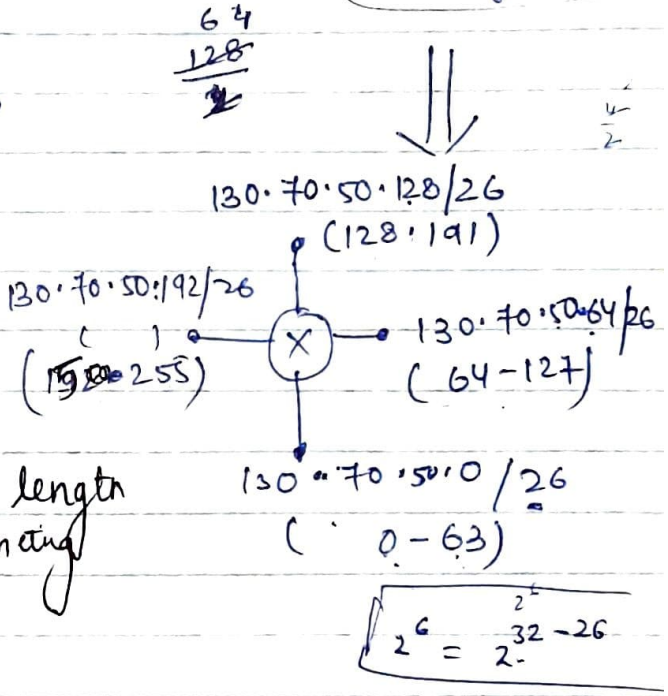
$2^{32-24} = 2^8 = 256$

Equal length Subnetting





Variable length Subnetting



$2^6 = 2^{32-26}$

$\left[2^{32-25} = 2^7\right]$

How ISP provide IP addresses?

Q:- An ISP has a block 191.60.0.0/16

1st group has 128 customers, each customer requires 256 IP addresses.

2nd group has 64 customers, each customer requires 128 IP addresses

3rd group has 16 customers, each customer requires 64 IP addresses in that order.

Soln ⇒ 1st group

$256 \Rightarrow 2^8 = 2^{32-24}$

1st customer :- 191.60.0.0/24 — 191.60.0.255/24

2nd customer :- 191.60.1.0/24 — 191.60.1.255/24

⋮ ⋮

128th Customer :- 191.60.127.0/24 - 191.60.127.255/24

{ customers completed - 127
but system completed only upto 127 as remaining 1 is left }

⇒ 2nd group

$128 \Rightarrow 2^7 \Rightarrow 2^{32-25}$

Done by me

1st customer :- 191.60.0.0/25 - 191.60.0.127/25

2nd customer :- 191.60.1.0/25 - 191.60.1.127/25

⋮ ⋮

64th Customer :- 191.60.63.0/25 - 191.60.63.127/25

Done by Sir

⇒ 2nd group

$128 \Rightarrow 2^7 \Rightarrow 2^{32-25}$

1st Customer :- 191.60.128.0/25 - 191.60.128.127/25

2nd Customer :- 191.60.128.128/25 - 191.60.128.255/25

⋮

1 series ⇒ 2 customers

×31 ⋮ 32 series ⇒ 64 customers

Last before Customer : 191.60.159.0/25 - 191.60.159.127/

Last Customer : 191.60.159.128/25 - 191.60.159.255/

→ 3rd group

$$64 \Rightarrow 2^6 = 2^{32-26}$$

1st Customer : 191.60.160.0/26 – 191.60.160.63/26
2nd Customer : 191.60.160.64/26 – 191.60.160.127/26
3rd Customer : 191.60.160.128/26 – 191.60.160.191/26
4th Customer : 191.60.160.192/26 – 191.60.160.255/26

1 series ⇒ 4 customers
4 series ⇒ 16 customers

Last Customer :- 191.60.163.192/26 – 191.60.163.255/26

Q:- Calculate the left over IP addresses with the ISP after assigning to these groups and the answer should be in scaling factor of power of 2.

ISP block 191.60.0.0/16

$$2^{32-16} = 2^{16}$$

$$2^{16} - \left[\underbrace{128*256}_{\text{1st group}} + \underbrace{64*128}_{\text{II}^{nd}\text{ group}} + \underbrace{16*64}_{\text{III}^{rd}\text{ group}} \right]$$

$$2^{16} - \left[2^{15} + 2^{13} + 2^{10} \right]$$

$$64*2^{10} - \left[32*2^{10} + 8*2^{10} + 1*2^{10} \right]$$

$$\left[64 - 32 - 8 - 1\right] * 2^{10}$$

$23 * 2^{10}$ Ans → left over IP addresses with ISP

* Special Cases

1) Calculate the no. of 1's in binary representation of following expression.
(128 + 512 + 1024 * 2 + 2)

If any no can be represented in power of 2, it contain only 1 one.
i.e.

$8_{10} \Rightarrow 2^3 \Rightarrow 1000 \Rightarrow 1$
$16_{10} \Rightarrow 2^4 \Rightarrow 10000 \Rightarrow 1$
:
$\Phi \Rightarrow 2^{128} \Rightarrow 100\ldots0 \Rightarrow 1$

$\therefore$ $128 + 512 + 1024 * 2 + 2$
$2^7 + 2^9 + 2^{11} + 2^1$ {can't combine so}
$\Rightarrow$ so 4 1's are there.

2) Calculate the no. of 1's

$(128 + 2*64 + 256 + 512)$

$2^7 + 2^7 + 2^8 + 2^9$ {can combine so}
~~so 4 1's are there~~
$2^7 + 2^7 + 2^8 + 2^9$
$2^8 + 2^8 + 2^9$
$2^9 + 2^9$
$2^{10} \Rightarrow$ only 1 one is there

3) $(11)_2 + (22)_3 + (33)_4 + (44)_5 = (XYZ)_6$

HINT:- Any base if you want to convert into 10 multiply with that no. only to every bit.

eg:- $(1011)_2 = (11)_2$

$1\times2^3 + 0\times2^2 + 1\times2^1 + 1\times2^0 = 11$

Done by me

$(1\times2^1+1\times2^0)_{10} + (2\times3^1+2\times3^0)_{10} + (3\times4^1+3\times4^0)_{10} + (4\times5^1+4\times5^0)_{10}$

$= (XYZ)_6$

$(2+1)_{10} + (6+2)_{10} + (12+3)_{10} + (20+4)_{10} = (XYZ)_6$

$(3)_{10} + (8)_{10} + (15)_{10} + (24)_{10} = (XYZ)_6$

$(50)_{10} = (XYZ)_6$

6 | 50		
6 | 8	2	
6 | 1	2	
0	1	

$= (122)_6$

$\therefore$ X = 1, Y = 2, Z = 2

4) $(123)_X = (12X)_3$

$X^2 + 2X + 3 = 9 + 6 + X$

$X^2 + 2X - X = 9 + 6 - 3$

$X^2 + X - 12 = 0$

$X = 3$ ✓

$X = -4$ ✗

$(XY)_3$ then $X < 3$, $Y < 3$

$(123)_3 = (123)_3$ ✓ correct — why

But ans $\neq 3$ ans is no value

(4c) (42)

5) $(0.1111111111)_2 = (\quad)_{10}$ Should be power of 2

Let's try this first $(0.111)_2$

$= 1*2^{-1} + 1*2^{-2} + 1*2^{-3}$

$= \frac{1}{2} + \frac{1}{4} + \frac{1}{8}$

$= \frac{4+2+1}{8} = \frac{7}{8} = \left(1 - \frac{1}{8}\right) = (1 - 2^{-3})_{10}$

So,

$\boxed{(0.1111111111)_2 = (1 - 2^{-10})_{10}}$ Ans

In general

Trick * $\boxed{(0.111111\ldots n)_2 = (1 - 2^{-n})_{10}}$

Q:- $IP_1 = 201.55.66.65$ → class C

Calculate host on this network?

↓

This host wants to transfer data only within the n/w

So, make n/w bits = 0

host on this network = 0.0.0.65

Class C mask ⇒ 255.255.255.0

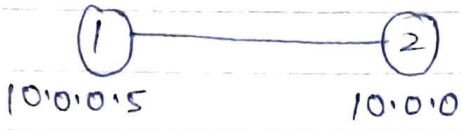
$IP_1 = 201.55.66.65$

Wild card mask = 0.0.0.255 (Complement of Subnet mask)

host on this n/w = 0.0.0.65

If IP address is performed bitwise AND with Wild card mask will get host on this network.

eg:-1



	S.IP	D.IP
D	10.0.0.5	10.0.0.7

✓

or

	S.IP	D.IP
D	0.0.0.5	0.00.7

✓ Valid because both ① and ② computers are in the same n/w.

eg:-2

D	144.5.9.3	193.15.16.9

✓

(OR)

D	0.0.9.3	0.0.0.9

✗ not valid because both ① and ② computers are in different n/w

Q:- X indicates net Id
Y indicates host on this network
X (bitwise AND Y) = DHCP client
= 0.0.0.0

eg:-
$IP_1 = 201.55.66.99$
net ID on this n/w => 201.55.66.0
host on this n/w => 0.0.0.99
0.0.0.0 Ans (DHCP client)

Ques X indicates no. of 1's in DHCP client address
Y indicates no. of 0's in Limited broadcast address

$$X + Y = 0$$

Because

DHCP client ⇒ 0.0.0.0
0 1's are there

Limited broadcast address ⇒ 255.255.255.255
⇒ 0 0's are there

$$X + Y \Rightarrow 0 + 0 = 0$$

Ques Calculate 2's Complement representation of limited broadcast address.

Limited Broadcast address ⇒ 255.255.255.255

Trick

2's Complement
all Positive weights → weighted code
all negative weights except MSB → Positive ⇒ MSB = 0
Negative ⇒ MSB = 1

eg Calculate 3 bit representation of 2's complement

111 = −1	000 = +0
110 = −2	001 = +1
101 = −3	010 = +2
100 = −4	011 = +3

$1\,0\,1_2 = 2^2 2^1 2^0 = -4+1 = -3$

$1\,1\,0_2 = 2^2 2^1 2^0 = -4+2 = -2$

∵ MSB = 0 that's why ⊕ +

(−4, −3, −2, −1, 0, 1, 2, 3)

Range (−4 to +3)

eg:- Calculate 4-bit representation of 2's complement

1111 = -1	0000 = +0
1110 = -2	0001 = +1
1101 = -3	0010 = +2
1100 = -4	0011 = +3
1011 = -5	0100 = +4
1010 = -6	0101 = +5
1001 = -7	0110 = +6
1000 = -8	0111 = +7

-8+1
-7

(-8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7)
(-8 to 7)

eg:- Calculate 2 bit representation

11 = -1	00 = +0
10 = -2	01 = +1

(-2 to 0 +1)

$-2^2 2^1 2^0$
111101

so cancel extra

as here -ve comes so Cancelled before this

Trick

-2 = 10 → 2 bits
-2 = 110 → 3 bits
-2 = 1110 → 4 bits

Q:- Identify the no.'s in 2's complement.

a) 01111 = +15

b) 11111 = -1 (start from here)

c) 111111011111 = -17

$-32+15 = -17$

9×9 → 81 → 2 bit
1 1
1 bit 1 bit

Q:- Multiply two nos in two's Complement

a) (1111) * (1111) = +1 ⇒ 00000001
-1 (4 bits) -1 (4 bits) (8 bits)

b) (01111) * (11111) = -15 ⇒ -16+1
+15 -1
⇒ $-2^4 2^3 2^2 2^1 2^0$
11111 000 1
Ans

c) (11011) * (00111) = -35 ⇒ -64+29
$2^4 2^3 2^2 2^1 2^0$
-5 +7

29 ⇒ 16, 8, 4, +1

⇒ -64+16+8+4+1
$\frac{1}{2^6}, \frac{1}{2^4}, \frac{1}{2^3}, \frac{1}{2^2}, \frac{1}{2^0}$
⇒ 1110111 01

**Q:- Calculate overflow of addition of 2's Complement

1) 1101 ← -3
+ 1001 ← -7
10110 -10

1) See the range of 4 bit
it is [-8 to +7]

Not falling in b/w the limits
so overflow. So overflow = 1

2) 1010 ← -6
1111 ← -1
-7

-7 → falling in the range
so not overflow
so overflow = 0

3) 0111 ⇒ +7
0111 ⇒ +7
+14 → overflow = 1

4) 1011 ⇒ −5
0111 ⇒ +7
+2 → overflow = 0

⇒ Calculate limited broadcast address 2's complement representation

255 . 255 . 255 . 255
−1 − − −

11111111
2^0
↓
−1

IPv4 → 32 bit address
→ ARP (for MAC address)
→ DHCP (stateful protocol)
(i) dotted decimal notation

IPv6 → 128 bit address
→ hexadecimal notation

IPv6

→ hexadecimal notation
→ MAC address
48 bit address
⇒ 40:12:13:15:16:1A
0100 0000
→ Unicast MAC address
⇒ FF:12:13:15:16:1A
1111 1111
→ Multicast MAC address

FF:FF:FF:FF:FF:FF
Broadcast MAC address

48 bit MAC address
FFFE → default
64 bit MAC address (Extended MAC) or (Interface Id)

eg:- 24bit 24bit
40:12:13:15:16:1A
FFFE
40:12:13:FF:FE:15:16:1A
4012:13FF:FE15:161A

128 bit Address ⇒ Network Prefix + Extended MAC
64 bits 64 bit

IPV4 => 201.55.166.74 => 32 bits

8 bits

IPV6 ~~128~~ → 128 bits = $\frac{128}{16}$ = 8 fields

(1) IPV6 = FE80 : 1234 : 1496 : 12FF : FF23 : 1234 : 0215 : FF20

(2) IPV6 = FE80 : 0000 : 0000 : 1230 : 2360 : 1230 : 0002 : FF12

(OR)

FE80 : : 1230 : 2360 : 1230 : 2 : FF12

(3) IPV6 = 201C : 0000 : 0000 : FF20 : 1420 : 0000 : 0000 : 1230

(OR)

201C : : FF20 : 1420 : : 1230 ✗ representation

20's	20's	ambiguity
10's	30's	
30's	10's	

∴ (OR)

201C : : FF20 : 1420 : 0 : 0 : 1230 ✓

(OR)

201C : 0 : 0 : FF20 : 1420 : : 1230 ✓

- In IPV6 address, whenever zero's are there in the field then it can be replaced by "::"
- In IPV6 address, whenever we have continous zero at different position then only at 1 position 0's are replaced by "::"

eg :- 1) FE80 :: → After that all 7's are zero

2) :: ⇒ Unspecified address (IPV4 0.0.0.0 → DHCP client)

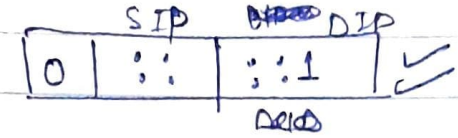
3) ::1 ⇒ loopback address (IPV4) (127 series)

::1

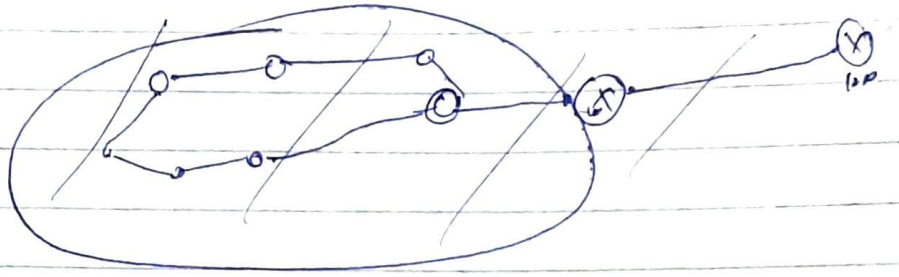
⇓

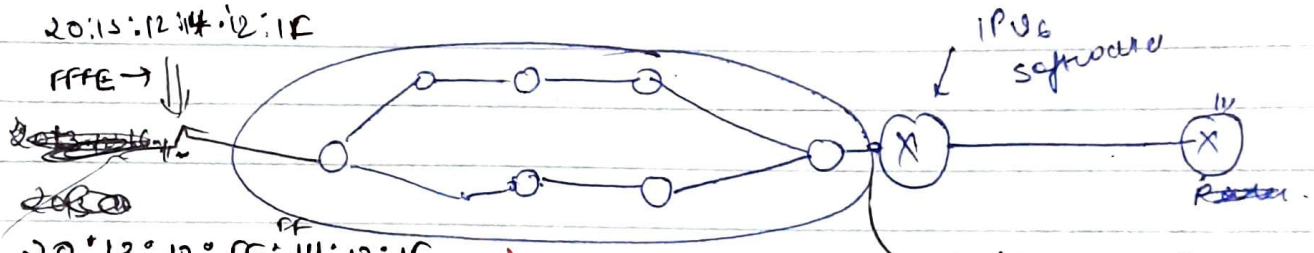
0:0:0:0:0:0:0:1

4)



IPv6 ⇒ Stateless autoconfiguration protocol





FE80:1240:F200:1260; 2013:12:FF; FE14:121F

⇓ link local address

IPv6 ⇒ IP address

2EC0:: 2013:12FF:FE14:12:14 (64 bit Extended M

⇓ global Unicast address

128 bit

Computer will use.

(i) neighbour Solicitation message

↳ to ensure that no two systems have the same MAC address then 48 bit MAC is converted into 64 bit unique MAC address

Computer will use router Solicitation message to get the net id's of the router.

NOTE :-

- A single interface can have multipe address in IPv6
- IPv6 is a (stateless Protocal)
- It doesnot require ARP and doesn't require the DHCP by default.
- For wireless Communication IPv6 is best suitable

(1) neighbour Solicitation message

↳ neighbouring Query

↳ neighbour answer

(2) Router Solicitation

↳ Router query

↳ Router reply.

Anycast address :-

- In anycast address all nodes in a area will be given the based on same address but the nearest node will provide the service
- It is supported by IPv6

IPv6 generally doesn't require network operation router conversion

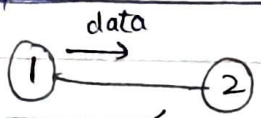
BASIC CONCEPTS :-

Data Communication and networking
— Forouzan.

1) Simplex transmission

→ Only one side data is transmitted

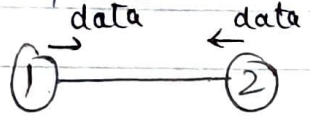
2) Half-duplex transmission



eg:- [Walkie talkie]

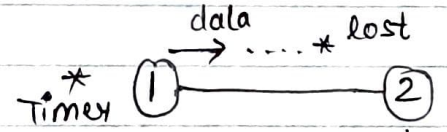
{ Data transmitted both sides but one after another }

3) Full-duplex transmission



eg:- [Mobile].

4)



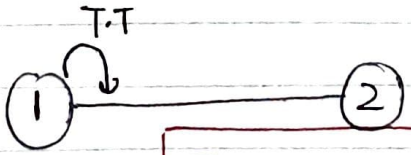
Buffer

11110

So, no acknowledgement

⇒ We require timers because waiting time is finite
⇒ In order to resend the data buffer is required

1)



* Transmission Time (T.T) = $\frac{\text{Data size}}{\text{Bandwidth}}$

eg:-

Data size = 2 Kbits
BW = 10Mbps

$$T.T. = \frac{2*10^3 \text{ bits}}{10^7 \text{ bits/sec}}$$

$$T.T. = 2*10^{-4} \text{ sec}$$

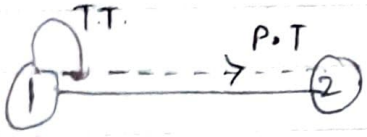
$$\boxed{T.T = 200 \mu sec}$$

Kilo = 10^3
Mega = 10^6
Giga = 10^9
milli = 10^{-3}
(μ)micro = 10^{-6}
nano = 10^{-9}

of storing the data then kilo = 2^{10}

→ Transmission time is the time in which the data is placed one the n/w for transmission.

2.)



* Propogation time = $\frac{\text{length}}{\text{velocity of medium}}$

eg:-

length = 2Km
$v = 2*10^8$ m/sec

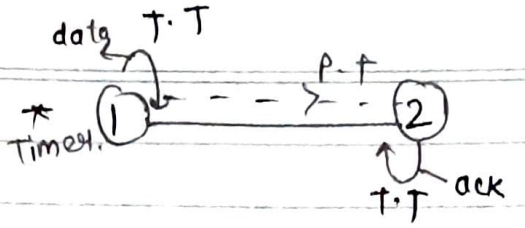
$$P.T = \frac{l}{v} = \frac{2*10^3 m}{2*10^8 m/sec}$$

$$P.T. = 10^{-5} sec$$

$$P.T = 10 \mu sec.$$

54

3.>>

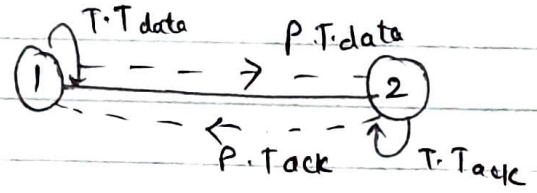


* ack size <<< data size

* $T.T_{ack} = \frac{\text{ack size}}{\text{Bandwidth}}$

T.T.ack is negligible coz ack size is small

4.>>



* $P.T_{data} = P.T_{ack}$

Total time = $T.T_{data} + P.T_{data} + T.T_{ack} + P.T_{ack}$

* Total time = $T.T + 2P.T$

comp 1 is utilizing the channel only one time and that too while placing the data on the channel.

$\therefore$ **Link utilization of Sender** $= \dfrac{T.T.}{T.T + 2*P.T}$

* 1) $LU\% = \dfrac{T.T}{T.T + 2*P.T} * 100\%$

eg:-1 $\%.LU = 50\%$

$$50 = \frac{TT}{TT + 2*P.T} \times 100^{2}$$

$$T.T + 2*PT = 2*TT$$

⇒ Relationship b/w T.T and P.T $\quad T.T. = 2*P.T$

↑ when link utilization is 50%.

eg:-2 $LU = 50\%$

$l = 200\ m$

$v = 2*10^8\ m/sec$

$BW = 10\ Mbps$

Data size = ?

Since $LU = 50\%$

So, $T.T = 2*P.T$

$T.T = \dfrac{\text{Data size}}{BW}$

$P.T = \dfrac{l}{v} = \dfrac{200\ m}{2*10^8\ m/se}$ (200 → 100)

$2*10^6 * 10\ Mbps = DS$

$DS = 20 \times 10$

$P.T = 10^2 * 10^{-8}\ sec$

$P.T = 10^{-6}\ sec$

$TT = 2*10^{-6}\ sec$

$TT = 2\mu sec$

Done by me

Done by Siri :- $T.T = 2 * P.T$

$$\frac{\text{Data size}}{BW} = 2 * \frac{l}{v}$$

$$\frac{x}{10^7 \text{ bits/sec}} = 2 * \frac{200m}{2 * 10^8 m/sec}$$

Data size = 20 bits

* Throughput / data rate of sender (Transmission rate) $= \frac{\text{Data size}}{T.T + 2 * P.T}$

Throughput ⇒ The rate at which the user transmits the data is known as throughput

Time to time what is changing is throughput

eg :- Data size = 100 bits
Bandwidth = 10 Mbps
$l = 200m$
$v = 2 * 10^8 m/sec$

$$T.T = \frac{\text{data size}}{BW} = \frac{100 \text{ bits}}{10^7 \text{ bits/sec}} = 10^{-5} sec = 10 \mu sec$$

$$P.T = \frac{l}{v} = \frac{200m}{2 * 10^8 m/sec} = 10^{-6} sec = 1 \mu sec$$

$$\text{throughput} = \frac{100 \text{ bits}}{10\,\mu\text{sec} + 2 * 1\,\mu\text{sec}}$$

$$= \frac{100 \text{ bits}}{10 + 2\,\mu\text{sec}} = \frac{100 \text{ bits}}{12\,\mu\text{sec}}$$

throughput = 8.3 Mbps
(its less value which changes)
megabits/sec.

Bandwidth = 10 Mbps (given)
Maximum

⇒ Bandwidth is the maximum capacity of the link

$$\%\,LU = \frac{T \cdot T}{T \cdot T + 2 * P \cdot T} * 100\,\%$$

$$= \frac{\text{Data size}/BW}{T \cdot T + 2 * P \cdot T} * 100\,\%$$

$$= \text{Throughput}/BW$$

*2) $$\%\,LU = \frac{\text{Throughput}}{\text{Bandwidth}} * 100\,\%$$

$$\%\,LU = \frac{8.3 \text{ Mbps}}{10 \text{ Mbps}} * 100\,\%$$

$$\%\,LU = 83\,\%$$

IP addressing Chapter-2

Workbook

1)

C_1 assumes C_2 is on same n/w

$C_1 = 203.197.2.53$

mask C_1 = 255.255.128.0

203.197.0.0

2 = 00000010

128 = 10000000

Bitwise AND 00000000

$C_2 = 203.197.75.201$

→ mask = 255.255.128.0

203.197.0.0

75 ⇒ 01001011

128 ⇒ 10000000

00000000

C_2 assumes C_1 is on different n/w

$C_2 = 203.197.75.201$

mask C_2 = 255.255.192.0

203.197.64.0

75 = 01001011

192 = 11000000

64 ⇒ 01000000

$C_1 = 203.197.2.53$

→ mask = 255.255.192.0

203.197.0.0

2 = 00000010

192 11000000

00000000

So, option C

* On performing Bitwise AND b/w IP address and Subnet mask / Supernet mask / n/w mask we get Subnet ID / Supernet ID / n/w ID

2)

Class B ⇒ 130.50.0.0

N + S + H

16 bits + 6 + 10

$2^6 - 2$ $2^{10} - 2$

= 62 = 1022

So, option a

Q3:- i) First host of 1st Subnet

000001 00 . 00000001

4 1

∴ 130 . 50 . 4 . 1

(ii) First host of 4th Subnet

000100 00 . 00000001

16 . 1

∴ 130 . 50 . 16 . 1

option (a)

Q4:- 2048 address

$\Rightarrow 2^{11} \Rightarrow 2^{32-21}$

$\Rightarrow 2^{32-n}$

/21

option (b)

Q5:-

130 . 127 . 48 . 130 — 130 ⇒ 10000010

255 . 255 . 255 . 192 — 192 ⇒ 11000000

* 130 . 127 . 48 . 128 — 128 ⇒ 10000000

a) 130 . 127 . 48 . 120 — 120 ⇒ 01111000

255 . 255 . 255 . 192 — apply mask — 192 ⇒ 11000000

130 . 127 . 48 . 64 — 64 ⇒ 01000000

* and (a) are different

b) 130.127.48.187
255.255.255.192
130.127.48.128

187 = 10111011
192 = 11000000
128 ⇒ 10000000

* and b) are same
∴ option (b)

Q6 :-

IP address = 172.60.50.2 (class B)
Subnet mask = 255.255.224.0
172.60.32.0

50 = 00110010
224 = 11100000
32 = 00100000
↑
1st Subnet

255.255.224.0
N
11100000.00000000
S H

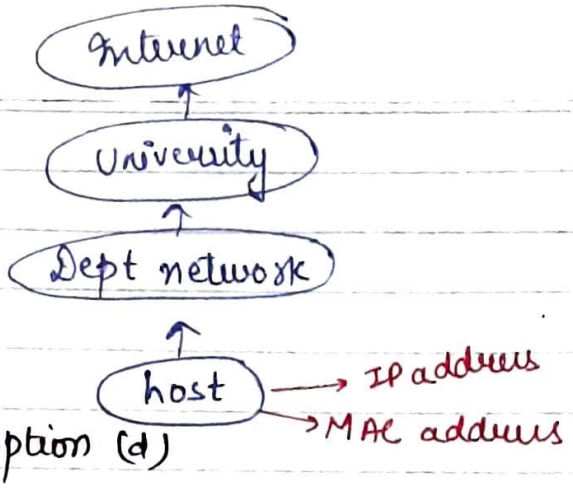
First host of that subnet
⇒ 00100000.00000001
~ 32.1

Last host of that subnet
⇒ 00111111.11111110
63.254

∴ option (b)

Q7 ⇒ option (c)

Q8 :→



∴ option (d)

Ethernet address ⇒ MAC address.
If nothing is specified then max. this MAC address is visible or identified is within the scope i.e. within the LAN

Q9 :→ Key is "wishes to form subnet"

hosts

A ⇒ 72 = (2^7-2) = 126 ⇒ N+S+H = 24+1+7

B ⇒ 35 = (2^6-2) = 62 ⇒ N+S+H = 24+2+6 ⇓ 255.255.255.192

C ⇒ 20 = (2^5-2) = 30 ⇒ N+S+H = 24+3+5 ⇓ 255.255.255.224

D ⇒ 18

∴ option (a)

11111111.11111111.11111111.10000000

N S H

255.255.255.128

Q10 :- Subnetted class B

Class B Broadcast address ⇒ 144.16.95.255

01011111.11111111

64 32 16 8 4 2 1

72 ⇒ 1 0 0 1 0 0 0

2^7 −

72 / 32 / 40 / 16 / 24 / 8 / 16

(a) 255.255.224.0

11111111.11111111.11100000.00000000

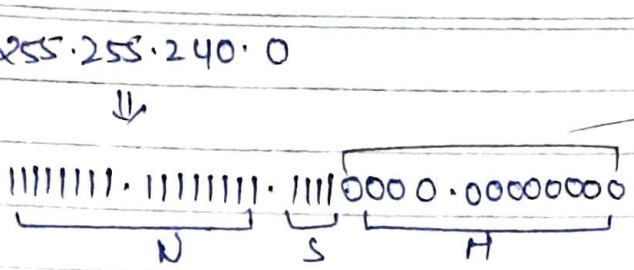
N S H

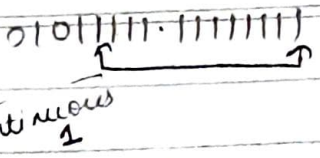
possible

(62)

division = $2^n - 2$
wishes = 2^n

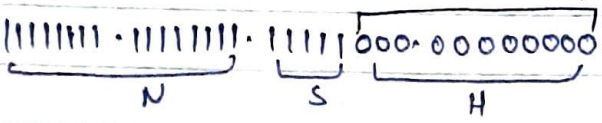
b) 255.255.240.0

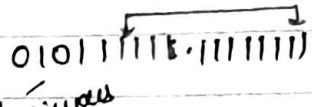




possible

c) 255.255.248.0





possible

∴ option (d)

Q11 :-

"wishes" to form Subnet

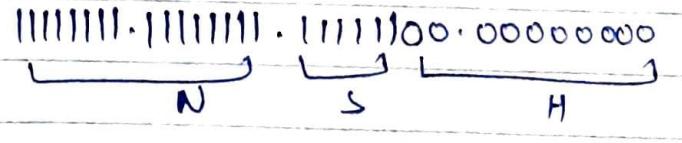
↓

64 for departments Subnets

no. of Subnets = 2^6

N + S + H

16 + 6 + 10



255.255.252.0

∴ option (d)

Q12 :-

"Split" class B ⇒ N + S + H

16 + 6 + 10

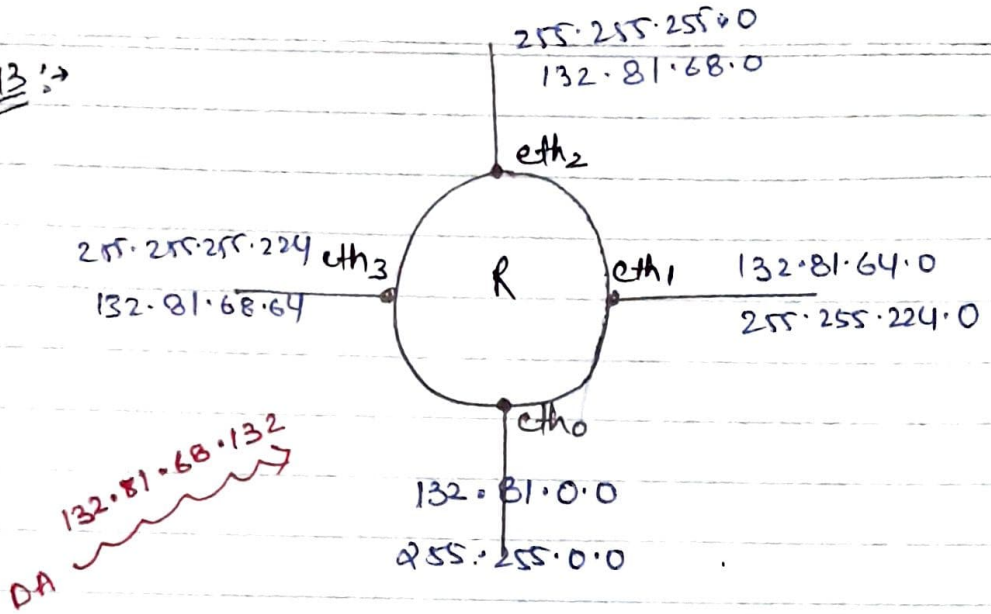
↓ ↓

$2^6 - 2$ $2^{10} - 2$

= 62, 1022

∴ option (c)

Q13 :→



when a packet comes to a Router since (it) has many interfaces it has to follow one of the path and that's (it) will perform Bitwise AND with mask and if equal to the (Destination) (IP address of eth) given to that Subnet then it will follow that path otherwise it will for other.

I
DA

So,

1) $IP_1 = 132.81.68.132$
$255.255.0.0$
$132.81.0.0$ eth0 ✓

2) $IP_2 = 132.81.68.132$
$255.255.224.0$
$132.81.64.0$ eth1 ✓

3) $IP_2 = 132.81.68.132$
$255.255.255.0$
$132.81.68.0$ eth2 ✓ ∴ option (d)

4) $IP_3 = 132.81.68.132$
$255.255.255.224$
$132.81.68.128$ eth3 ✗

If Question modified ⇒ can be forwarded is there then

longest mask matching
(more no. of 1's in mask)

If a packet comes to a ~~com~~ router and it can be forwarded to multiple path then the path with longest mask matching is choosen. ie. the path with more no. 1's in mask is choosen.

Longest mask matching :-

Whenever a packet comes to a router and router identifies multiple paths for the packet then packet will be forwarded via the path which contains more no. of 1's in the mask

Q14 :→ P: 128.128.255.255 → classB
(128.128 = N, 255.255 = H)

Broadcast on class B n/w

so P is true.

Q: 127.127.255.255
(127 → loopback address (as 1st octate is 127; 127.127.255.255 → this can be any no.)

so Q is true.

∴ option (c)

Q15 :→ option d

Q16:

128.8.129.43	128.8.161.55
255.255.31.0	255.255.31.0
128.8.1.0	128.8.1.0

129 = 10000001	161 = 10100001
31 = 00011111	31 = 00011111
1 = 00000001	1 = 00000001

Both are same. ∴ option (d)

Q17 :- $(C2|2F|15|82)_{16}$

$16^1\ 16^0$
$C2 = C \times 16^1 + 2 \times 16^0$
$= 16C + 2$
$= 192 + 2$
$= 194$

$16^1\ 16^0$
$2F = 2 \times 16^1 + F \times 16^0$
$= 32 + 15$
$= 47$

$16^1\ 16^0$
$15 = 1 \times 16^1 + 5 \times 16^0$
$= 16 + 5$
$= 21$

$16^1\ 16^0$
$82 = 8 \times 16^1 + 2 \times 16^0$
$= 130$

∴ option (a)

Q18 :- Same as 16 ∴ option (d)

Q19 :- option (c)

Q20 :- host in a n/w :-
130.83.126.0
↳ class B
no. of hosts $= 2^{16} - 2 = 65534$

Q21:-

Subnet mask = 255.255.248.0

no. of host of subnet = $2^{11}-2$

= 2046

Q22:-

no. of hosts $\Rightarrow$ 1½ year double

1996 $\Rightarrow$ 7 million

1997½ $\Rightarrow$ 14 million

1999 $\Rightarrow$ 28 million

2000½ $\Rightarrow$ 56 million

2002 $\Rightarrow$ 112 million

2003½ $\Rightarrow$ 224 million

2005 $\Rightarrow$ 448 million

2006½ $\Rightarrow$ 896 million

2008 $\Rightarrow$ 1792 million

$\Downarrow$

1.792 (Billion)

There many IP addresses

Q23:-

One Class A = $(2^{24}-2)$ hosts

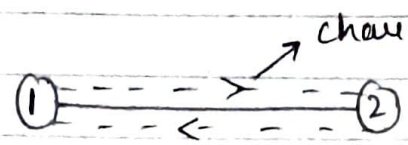
But as per problem $\Leftarrow$ $1.792 * 10^9$ hosts

$\Downarrow$

$$= \frac{1.792 * 10^9}{2^{24}-2}$$

= 107 networks

Basic Concepts (Continue....)



RTT = 2 * P.T

↑ Round trip time
TT → characteristic of Computer

P.T → characteristics of link

Ques BW = 10 Mbps
Calculate 1-bit delay?

Ans → 1 sec = 10^7 bits
1-bit delay = 10^{-7} sec

T.T = $\frac{1}{10^7}$
= 10^{-7}

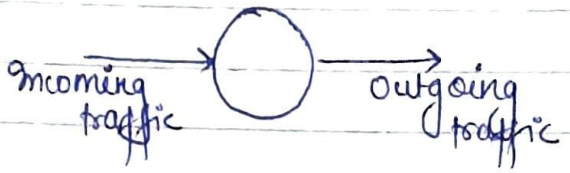
Ques ***

BW = 10 Mbps
$v = 2 * 10^8$ m/sec
Calculate 1-bit delay in metres of cable?

Ans → 1 sec = 10^7 bits
1 bit delay = 10^{-7} sec
1 sec = 2×10^8 m
1 bit delay ⇒ 10^{-7} sec ⇒ 20 m of Cable.

⇒ Constant traffic (Steady state traffic)

$\Rightarrow \left[\frac{\text{Incoming}}{\text{Outgoing}} = 1\right]$



$\Rightarrow$ [Effective queue size is constant]

If Incoming traffic = Outgoing traffic then that is called Constant traffic.

eg:- 5 people getting a ticket and leaving and at the same time 5 people came in the queue. then this is called Constant traffic

⇒ Bursty traffic

If Incoming traffic >>>> Outgoing traffic then this is called Bursty traffic

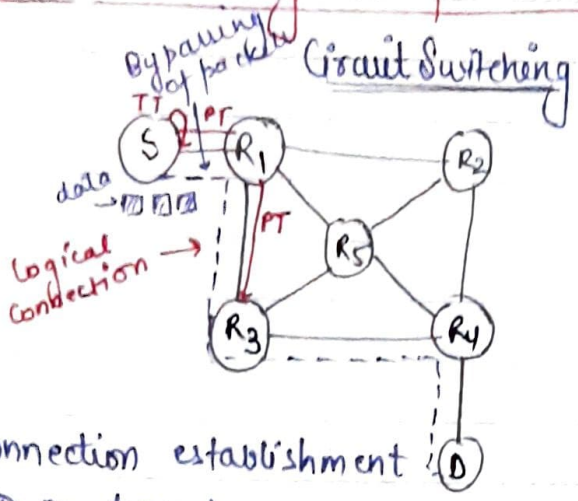
$\Rightarrow$ [Effective queue size is increased]

$\Rightarrow \left[\frac{\text{Incoming traffic}}{\text{Outgoing traffic}} >> 1\right]$

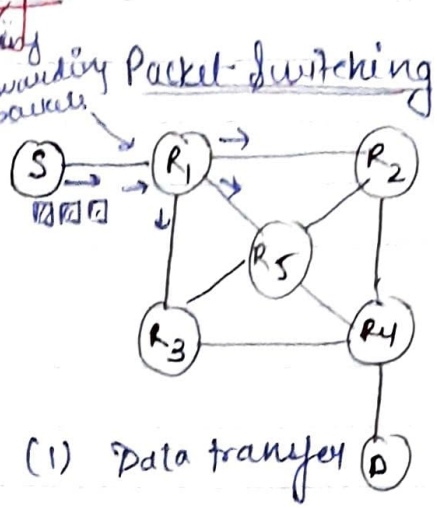
When more number of ~~traffic~~ packets are coming in less time then the queue will be full and the packets will be ~~dro~~ drop., because the router is congested.

Congestion :- More packets are coming in less time.

Circuit Switching and packet Switching



(1) Connection establishment
(2) Data transfer
(3) Connection release



(1) Data transfer

1) In Circuit Switching there are three phases (1) Connection establishment (2) data transfer and (3) Connection release.
whereas in Packet Switching data will be transmitted directly.

2) In circuit Switching each data unit will have the entire path address
Path
whereas in Packet-Switching each data will have destination address and the intermediate path is decided by routers

3) Circuit Switching is not a store and forward technique whereas packet Switching is a store and forwarding because packets are stored, Routing algorithm is applied and forwarded on the best path.
store and forward

4) In circuit Switching processing of the packets are done by source whereas in packet Switching processing of the packets are done by not only by the source but also by the intermediate routers

Processing

5) Circuit Switching will use Synchronous TDM (Time division multiplexing) whereas packet Switching will use Asynchronous TDM or statistical multiplexing

TDM

6) There is an ~~addm~~ admission control in circuit Switching because the no. of slots are fixed whereas in packet switching there is no admission control, packets can be allowed from different sources.

Admission control

7) In circuit Switching congestion can occur ~~during~~ during Connection establishment whereas in Packet switching congestion can occur during data transfer.

Congestion

8) In circuit Switching the delay b/w the data units is uniform whereas in packet switching the delay b/w data units is non-uniform or variable.

delay

9) Resource Reservation is a ~~feature~~ feature of Circuit Switching whereas resources are shared among users in packet Switching

Resource Reservation

10>> Wastage of resources is more in Circuit Switching whereas ~~it is~~ it is less in packet switching

11>> Reliability
Circuit Switching is reliable whereas packet Switching is unreliable.

12>>

Circuit Switching	Packet Switching
1) Establishment sec	1) Data transfer - μsec.
2) transfer μsec	⇒sec
3) Connection release sec	

speed
· Circuit Switching is slow and packet Switching is fast

13>> message size
Circuit Switching is preferable for long messages whereas ~~for~~ packet Switching is preferable for short messages.

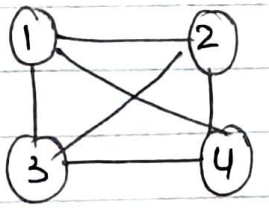
14>> drop packets
In circuit Switching there is a call drop whereas in packet switching there might be a packet loss when the queue is full.

15>> fault tolerance
Out of circuit, ~~switching~~ Switching and packet Switching, Packet Switching is a fault tolerant technique.

Topologies (LAN topologies)

- (1) Physical topologies (Mesh, star, Bus, Ring)
- (2) Logical topologies (IEEE 802.3, IEEE 802.11)
  - IEEE 802.3 → (Bus)
  - IEEE 802.11 → (wireless LAN)

1) Mesh topology :-



4 devices, 6 links

n devices, $\frac{n(n-1)}{2} \Rightarrow {}^{n}C_2$ links

In Mesh topology every system is connected to every other system by a dedicated cable.

Advantages :-

1. Data is reliable and secure

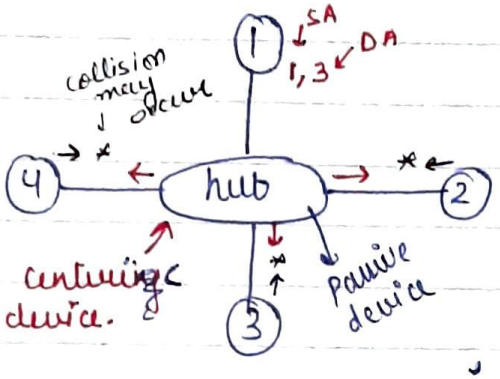
Disadvantages :-

1. for 100 devices ${}^{100}C_2 = \frac{100 \times 99}{2} = 4950$ links

   ∴ cost is high

2. Maintanence difficulty

2) Star topology :->



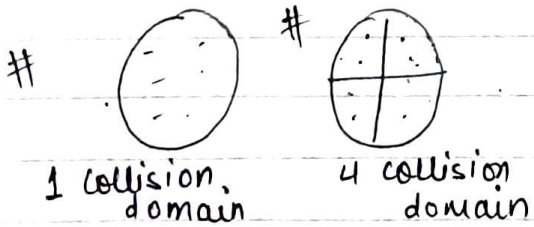
→ 4 devices, 4 links are required

LAN :->

100 devices, 100 links are required.

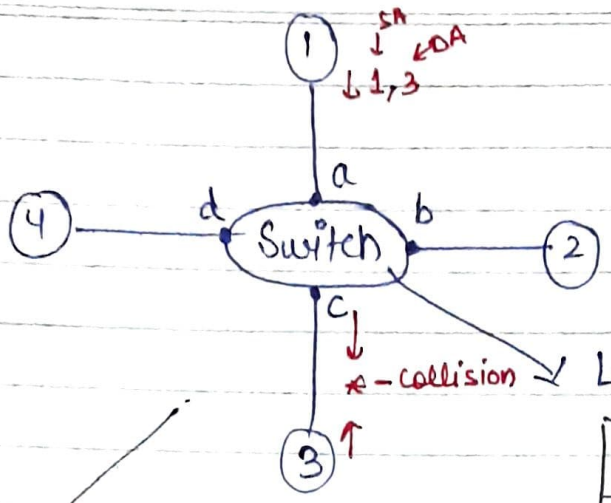
∴ the cost is less compared to Mesh.

- In star topology every system is connected to a centric device known as hub
- Hub is a passive device (Non-intelligent device)
- Hub is a broadcasting device because whenever a packet comes to a hub it is diverted in all the directions.
- When two or more system transmits their data at the same time then there is a possibility of collision. The place or area where collisions are confined to is known as collision domain

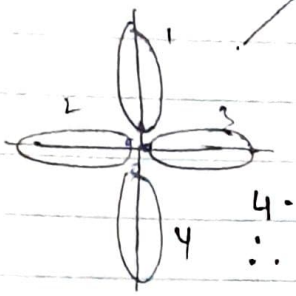


- Hub is not a collision domain seperator because the entire network has a same collision domain.

74



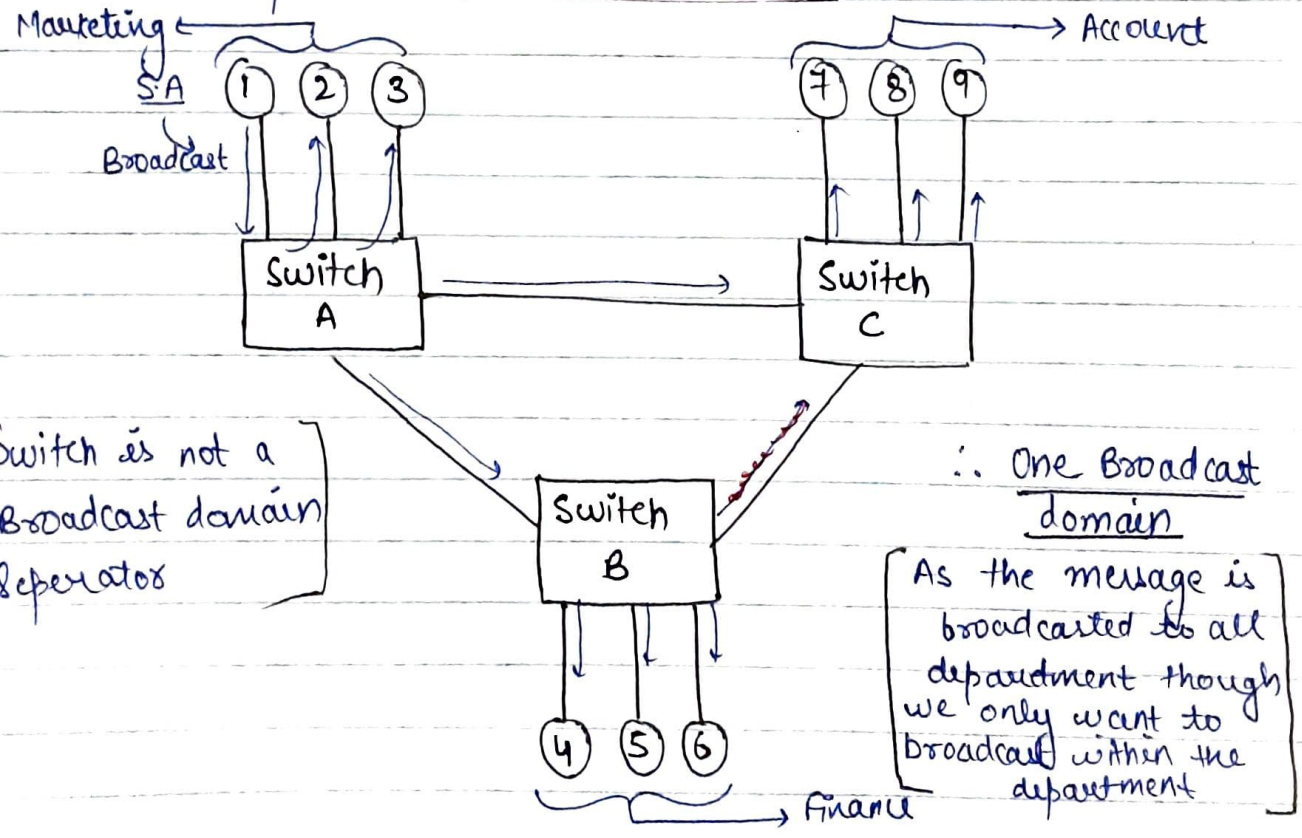
a	1
b	2
c	3
d	4



4 - collision domain
∴ collision domain seperator

If n-ports are there then n - collision domain

» If switch used as a centric device then each port has a seperate collision domain.



Switch is not a Broadcast domain seperator

∴ One Broadcast domain

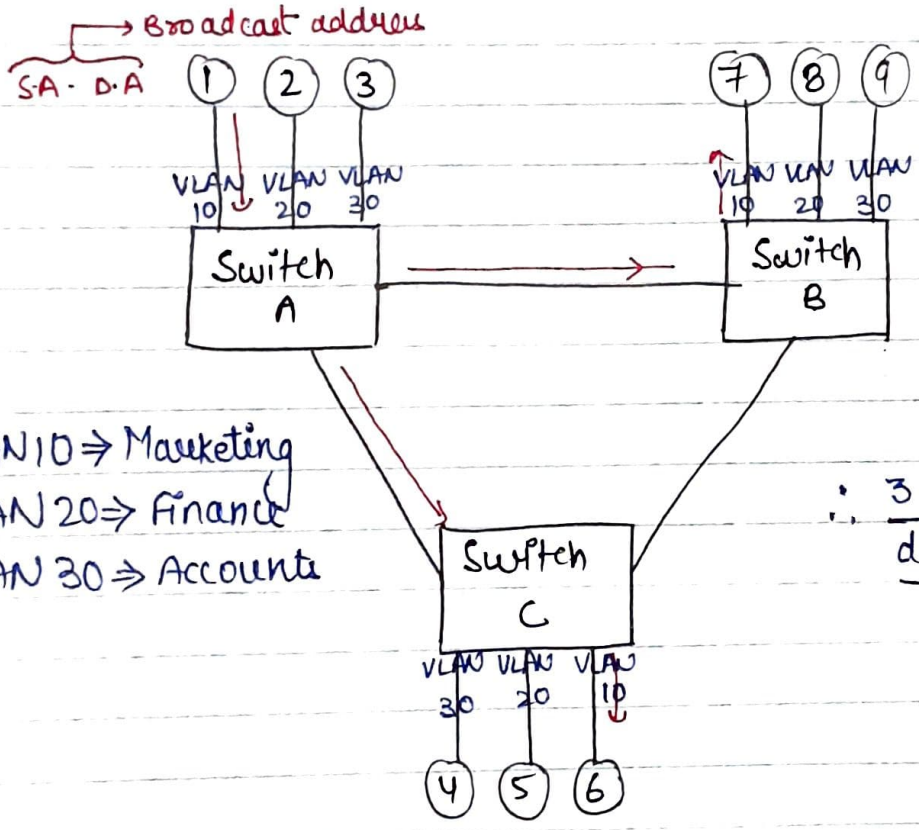
As the message is broadcasted to all department though we only want to broadcast within the department

» By default Switch is not a broadcast domain Seperator

VLAN (Virtual LAN) :→

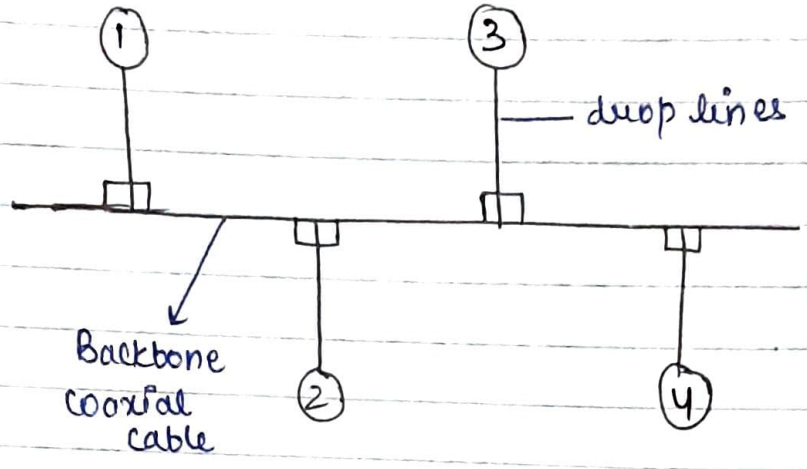
Physically Systems can be placed anywhere but they are logically connected belonging to a group

By configuring the ports of Switch it can be converted into VLAN



» If a LAN is converted into VLAN then Switch will act as broadcast domain Seperator

3) **Bus topology** :→



Standard Ethernet

10 base 2

10 base 5

"n" devices, "n" droplines + 1 Coaxial Cable

⇒ 10 base 2 → $l = 200m$

↓ ↳ Baseband signalling

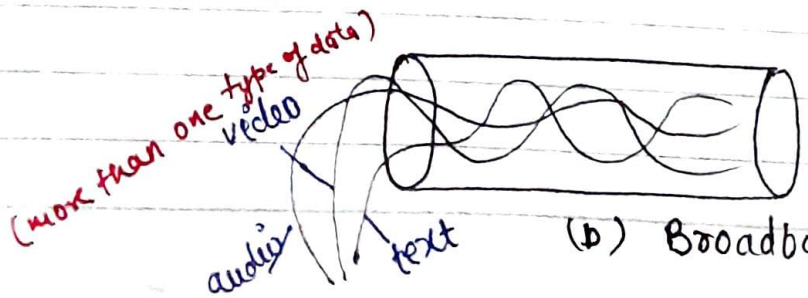
BW = 10 Mbps

⇒ 10 base 5 → $l = 500m$

↓ ↳ Baseband signalling

BW = 10 Mbps

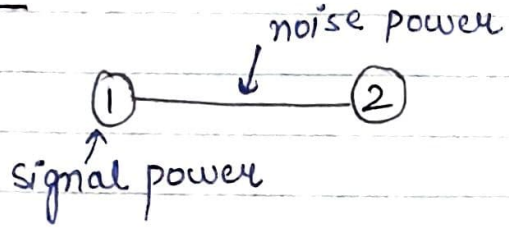
(a) Baseband Cable



(b) Broadband Cable

- If only 1 type of data is allowed in the cable, it is known as Baseband Cable
- If more than 1 type of data is allowed in the cable, it is known as Broadband Cable

Bell labs



* frequency
  - ⇒ HZ
  - ⇒ cycles/sec
  - ⇒ bits/sec *

Signal to noise ratio = $\log_{10} \frac{\text{Signal power}}{\text{noise power}}$ (bels) ← unit

$$\Downarrow$$

Signal to noise ratio = 10 (decimal) * $\log_{10}\left(\frac{Sp}{np}\right)$ (decibels) ← unit

Question 1

Signal power = 100 milliwatt
noise power = 10 milliwatt

$$\left(\frac{S}{N}\right)_{ratio} = 10 \log_{10}\left(\frac{Sp}{np}\right)$$

$$= 10 \log_{10}\left(\frac{100 \text{ milliwatt}}{10 \text{ milliwatt}}\right)$$

$$= 10 \log_{10} 10$$

$$\left(\frac{S}{N}\right)_{ratio} = +10 \text{ dB} \quad (+ve)$$

So, Signal power is dominating noise power.

Question 2

Signal power = 10 milliwatt
Noise power = 1000 milliwatts

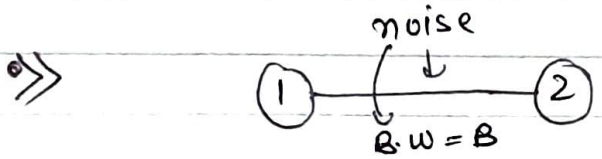
$$\left(\frac{S}{N}\right)_{ratio} = 10 \log_{10}\left(\frac{10}{1000}\right)$$

coz we are comparing two power

$$= 10 \log_{10} 10^{-2}$$

$$= -20 dB \quad (-ve)$$

→ Noise power is dominating signal power

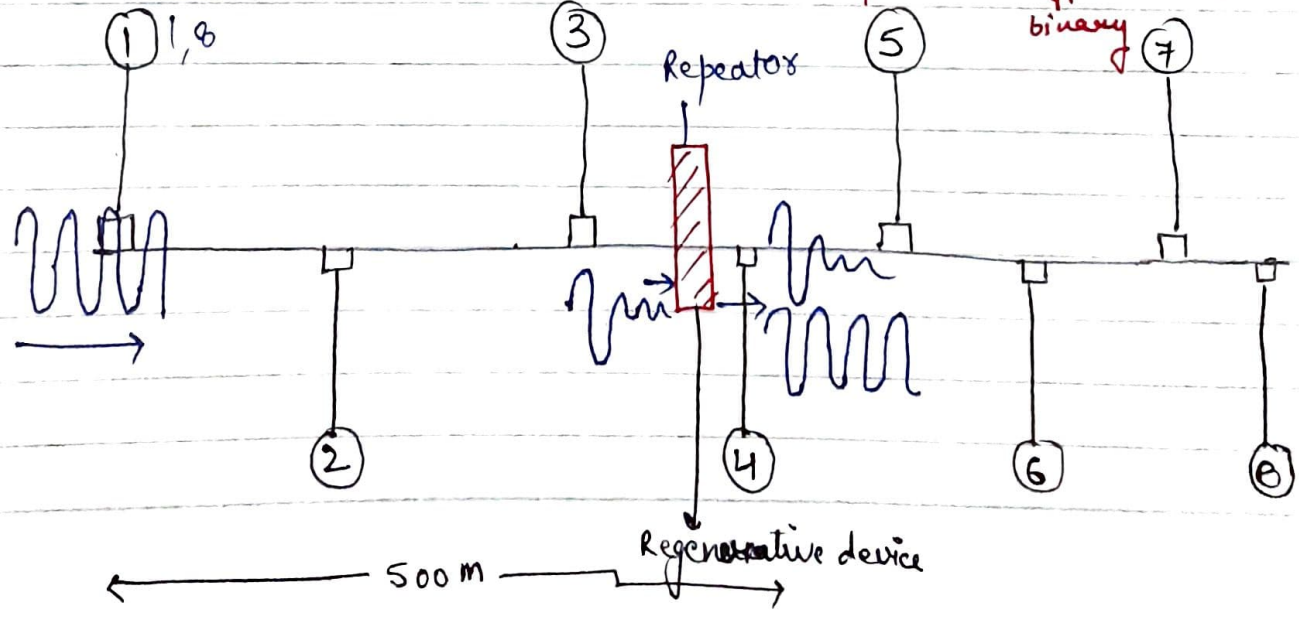


$$\text{max data rate} = B \log_2\left(1 + \frac{S}{N}\right) \text{ bps}$$

B → Bandwidth (so unit bps)

coz data will be transmitted in binary form. (bits per sec) ← binary

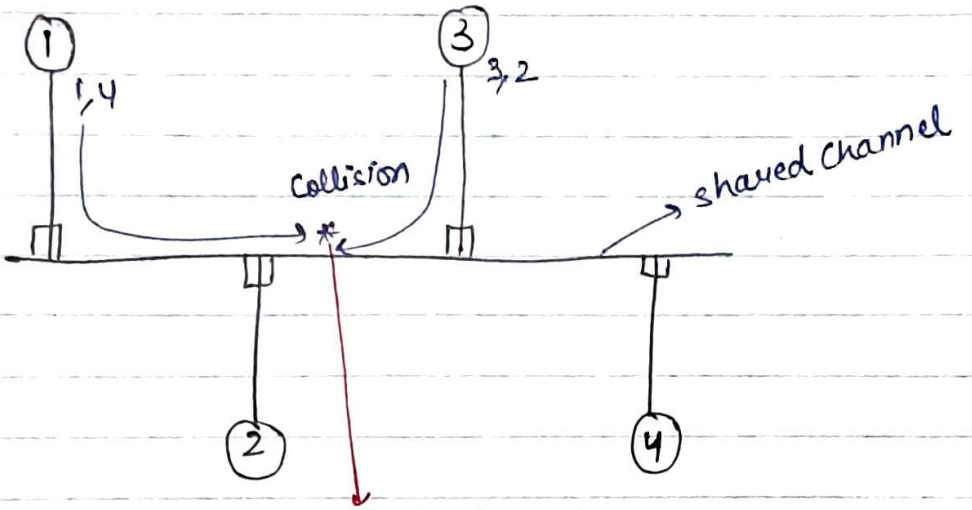
10 Base 5



- Repeator is a Regenerative Device because it regenerates the signal to its original strength

- Both Hub and Repeator are Passive devices. Whatever data is there they will just transfer it

- Hub is a multiport device and Repeator is a 2-port device



(MAC layer)

[Pure aloha, slotted aloha, CSMA, CDMA/CD] → wired

CSMA/CD → wireless

OSI Model :→ (7 layers)

Port address & socket address
IP address

messages
- Application layer
- Presentation layer
- Session Layer

TCP ↓ UDP ↓ (Port address)
Segment, datagram ← Transport layer → Gateway (All-layer switch) → Active device

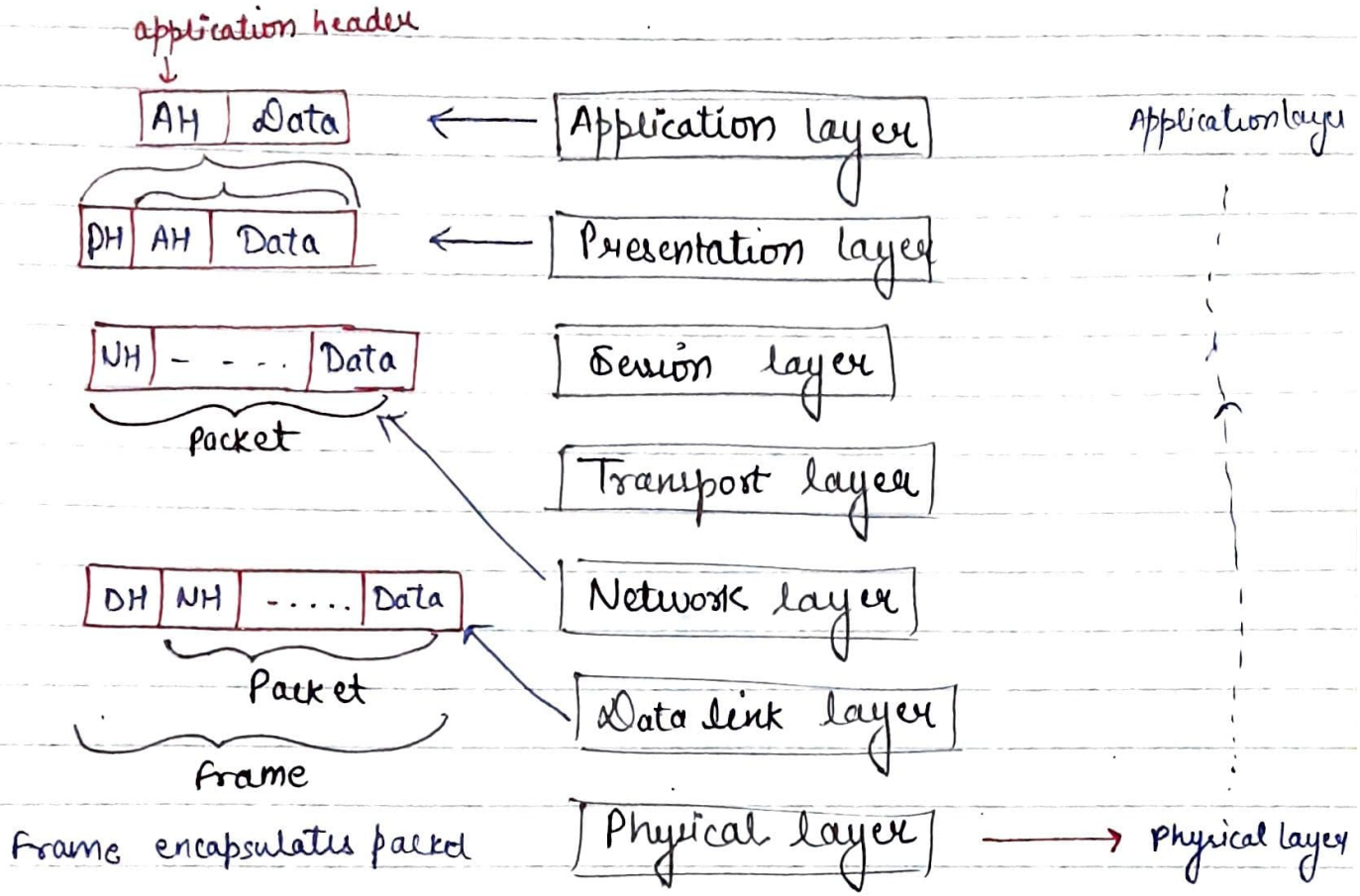
(IP address)
Packets ← Network layer (WAN) → Router & 3-layer switch

(MAC address)
Frames ← Data link layer (LAN) → Bridge & 2-layer switch

bits ← Physical layer → hub, repeator & Passive device

- Data link layer is responsible for node-to-node delivery within the LAN
- Network layer is responsible for source to destination delivery ~~within~~ across the network
- Transport layer is responsible for process to process delivery or end to end delivery

⇒ The scope of MAC address is within the LAN and that why we have introduced IP addressing



>>> Network architecture known as "Protocol stack architecture" because the last header that is added at the sender side is the first header that is removed at the receiver side.

Q1 :- "M" is a message transmitted, "N" layers are present in hierarchy, "H" is a header that is added at every layer. Then calculate the fraction of headers in the whole content that is transmitted.

(H+M) ← Application layer

(PH+M) ⇐ H+H+M ← Presentation layer

⋮

(NH+M)

Services provided by each layer :-

* **Application layer** ⇒ Application services like http, ftp, SMTP, DNS, Telnet etc

* **Presentation layer** ⇒ Syntax and semantics of data

ASCII ⇝ BCD

1's complement ⇝ 0's complement

* **Session layer** ⇒ dialog control and session management
  { full duplex / Half duplex }

- 7 layers of OSI Model has been reduced to 5-layers of TCP/IP model in which presentation layer and session layer functionality are ~~int~~ included in Application layer.

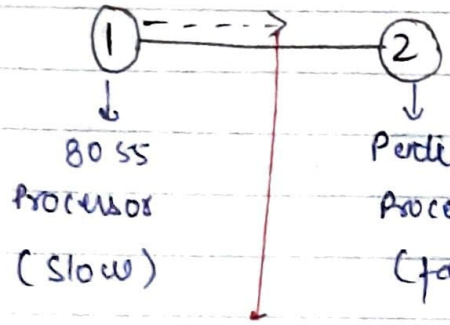
* **Transport layer** ⇒ flow control, error control, Segmentation, Congestion policies

* **Network layer** ⇒ Traffic shaping, Routing algorith. fragmentation

* **Data link layer** ⇒ Flow control, error control, framing, Access control

* **Physical layer** ⇒ Physical electrical characteris of cable.

⇒ Flow control

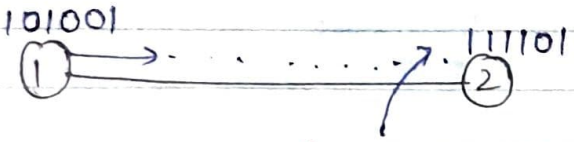


Flow control policies

(1) Stop & wait ARQ
(2) Go back N ARQ
(3) Selective repeat ARQ

} for noisy channel

⇒ error control



Error control policies

error correction policy
eg:- hamming code

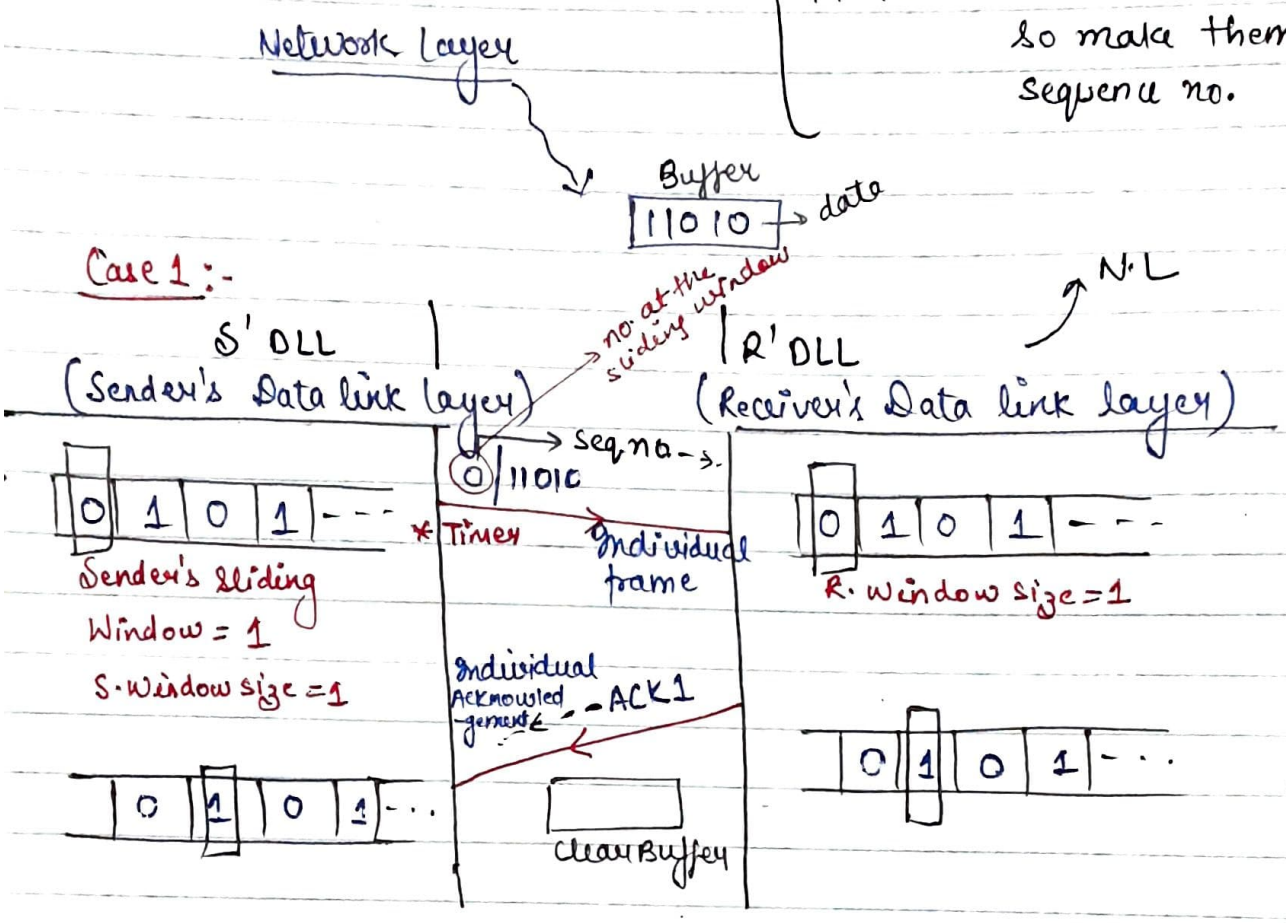
error detection policy
eg:- Parity
Checksum
CRC

* frame encapsulates packet

Flow control policies of Data link layer

1) Stop and Wait ARQ

The seq. no. are based on modulo-2 arithmetic
Mod 2 ⇒ either 0 or 1 comes
so make them sequence no.



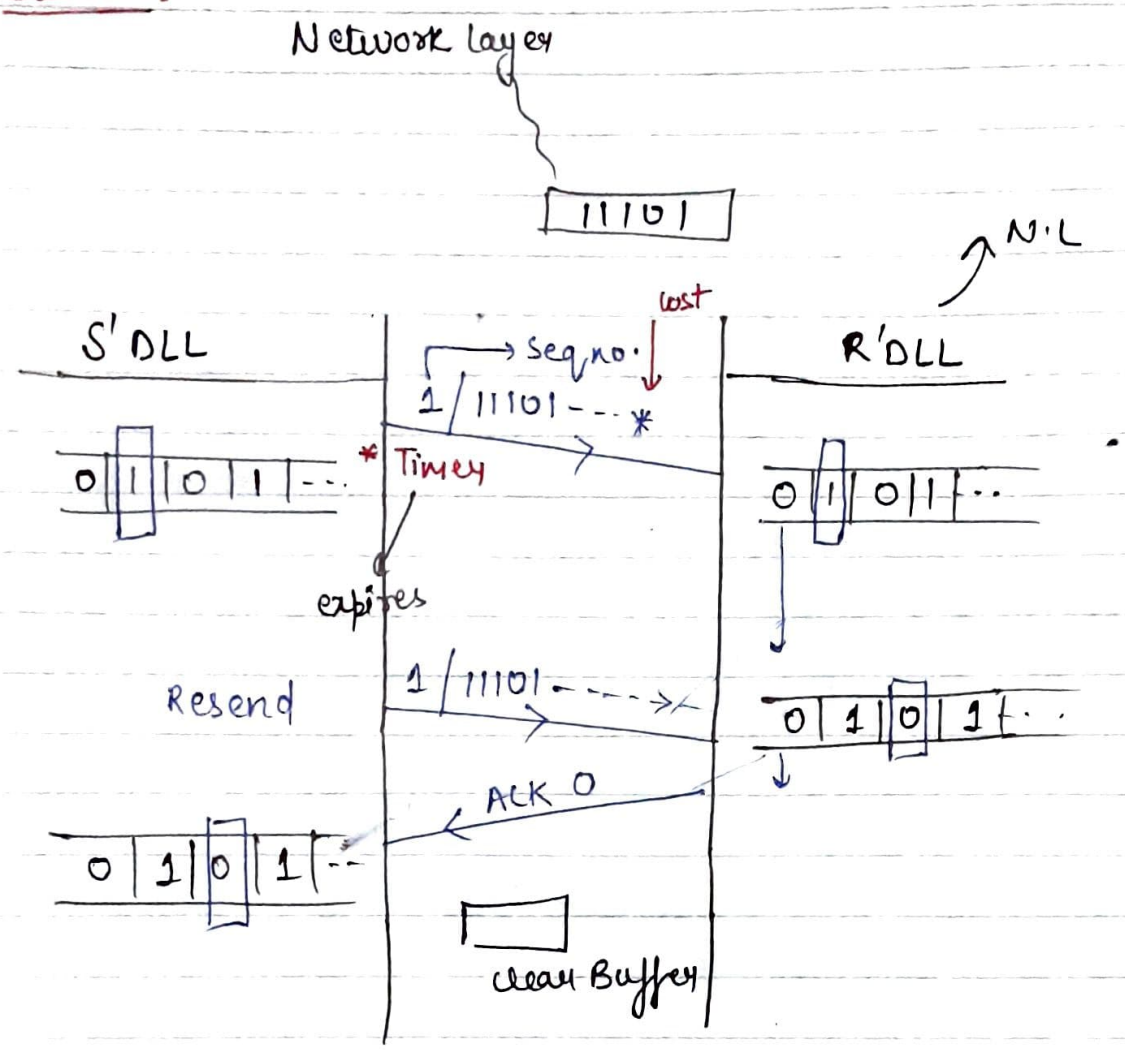
1) Once the data reaches to destination the sequence no. of the data is compared with receiver sliding window number, if there is a match data is accepted and receiver window will slide by 1 bit

2) The Acknowledgement number will always be the sequence number of next expected data then only acknowledgement is accepted.

* The sending device keeps a copy of the last frame transmitted until it receives an acknowledgement for that frame.

"Error Correction in Stop-and-Wait ARQ is done by keeping a copy of the sent frame and retransmitting of the frame when the timer expires."

Case 2 :-

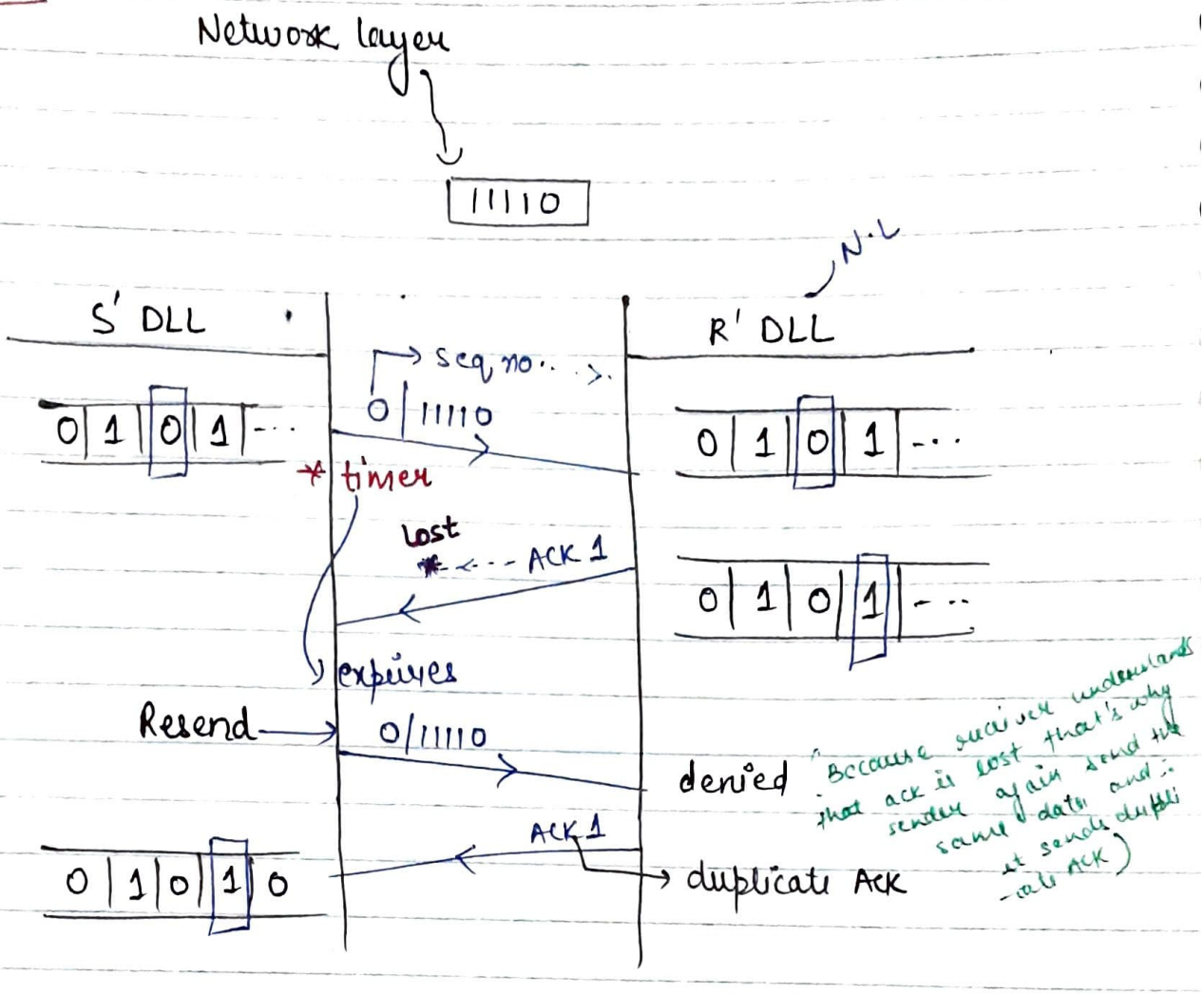


1) Once the data is lost automatically timer will expire then the protocol will resend the data and the data is accepted.

ARQ = (Automatic repeat request)

- Stop and wait is theoritical concept or protocol and it is without sliding window
  stop and wait ARQ is a practical protocol and it is with sliding window.

Case 3 :→



- Stop and Wait ARQ supports individual frames and individual acknowledgement
- In all Sliding Window protocols, maximum Sender window size indicates number of frames that are transmitted in Round trip time
- The maximum Sender window size + maximum receiver's window size will always be equal to distinct sequence number count.
- There is no pipelining in stop and wait ARQ so,

Bandwidth utilization is less

- We are transmitting only one frame in Round trip time so bandwidth utilization is less.

Q1 :-

BW = 100Mbps
RTT = 50 μsec
frame size = 50 bits

1 sec = 10^8 bits

RTT → 50 μsec ⇒ $50 * 10^{-6} * 10^8$ bits

∴ no. of bits in R.T.T ⇒ 5000 bits

no. of frames in RTT ⇒ Total bits / Frame size

$= \frac{5000}{50}$

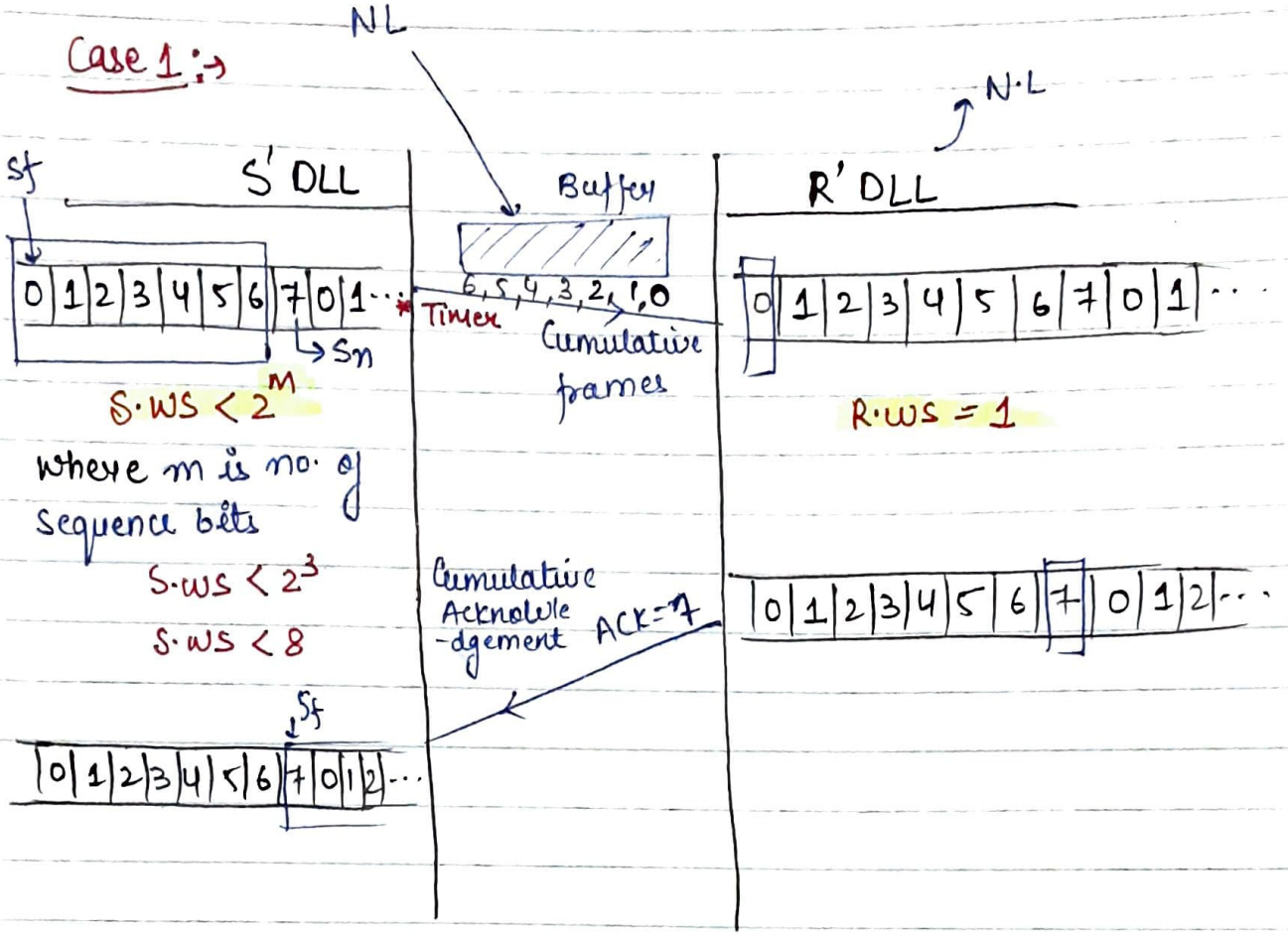
= 100 frames

% BW utilization (Stop and wait ARQ) $= \frac{1}{100} * 100 = 1\%$

-

no. of sequence bits	Sequence no.
1 bit	0, 1
2 bits → 00, 01, 10, 11	0, 1, 2, 3
3 bits →	0, 1, 2, 3, 4, 6, 7, 5

2) Go Back N ARQ — the Sequence no. are modulo 2^m



-> In Go Back N ARQ it suppose cumulative frames and Cumulative ACK

Q1:- 6 bit Sequence number is used

$S.WS < 2^m$

$< 2^6$

Go Back N ARQ

$63 < 64$

S.WS	R.WS
63	1

Q2:→ max size of sender window = 7

no. of sequence bits in Go Back N ARQ

$S.WS < 2^m$

$S.WS_{max} = 2^m - 1$

* Don't get confused with sequence no and sequence bits.

(3) → sequence bit

2 : 8, 0 (1)

max sequence no

$$m = \log_2 (1 + S.WS_{max})$$

$$m = \log_2 (1+7)$$

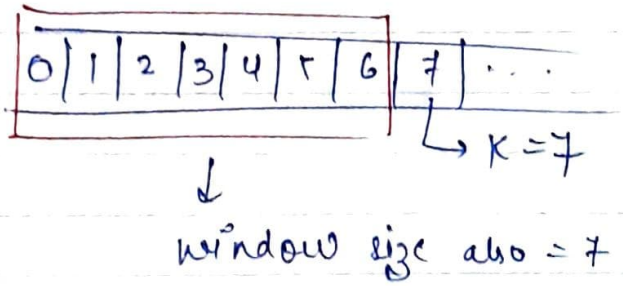
$$m = \log_2 8$$

$$\boxed{m = 3 \text{ bits}}$$

Q3:- max size of sender window = Q
then no. of sequence bits = $\log_2(1+Q)$

Q4:- Max sequence no. in GO Back N ARQ is "K"
then maximum size of sender window
a) K-1 b) K+1 c) K d) none.

eg:-



∴ K

Q5:- In GOBACK N ARQ in sender window condition
$S.WS < 2^M$
then when M=1 it behaves as.

$S.WS < 2^M$

$S.WS < 2^1$

$1 < 2^1$

$S.WS = 1$, $R.WS = 1$ → Stop and wait ARQ

(90) The receiver discard all subsequent frames until it receives the one it is expecting.

→ Go Back N ARQ supports individual ACK's and Cumulative ACK's

Q6:→

B.W = 100 Mbps
RTT = 50 μsec
frame size = 25 bits

1) Window size = ?
2) No. of sequence bits in Goback N ARQ = ?

We know

maximum Sender window size = no. of frames transmitted

∴

1 sec = 10^8 bits

RTT → 50 μsec → $50 \times 10^{-6} \times 10^8$ bits

(1) no. of bits in RTT = 5000 bits

$$\text{no. of frames in RTT} = \frac{\text{Total bits}}{\text{frame size}}$$

$$= \frac{5000}{25}$$

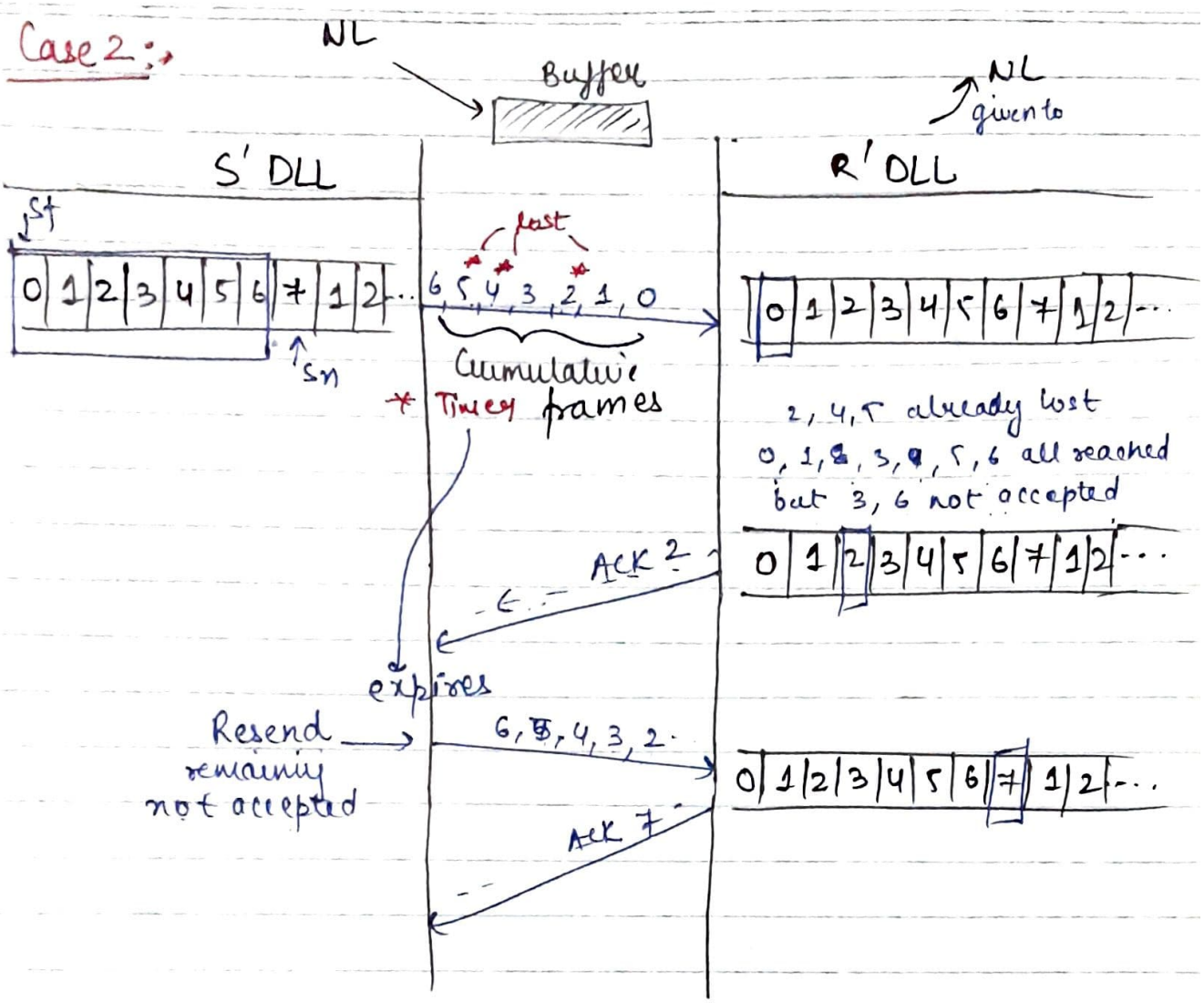
$$= 200 \text{ frames.}$$

∴ window size = 200 frames

(2)

	S.WS	R.WS
7 bits = 2^7 = 128	127 ✓	1
8 bits = 2^8 = 256	255 ✓	1

Case 2 :-



- Definition of GO BACK N ARQ

When a frame is lost in the network then that frame which is lost as well as all following frames should be retransmitted

- Both "stop N wait ARQ" and "GOBACK N ARQ" will accept inorder frames only because receiver window size = 1

For noisy channels

- Go Back N ARQ

more no. of retransmission

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

6, 5, 4, 3, 2

6, 5, 4

6

- For noisy channels there are more no. of retransmission if Go Back N ARQ is applied so, overall utilization will decrease.

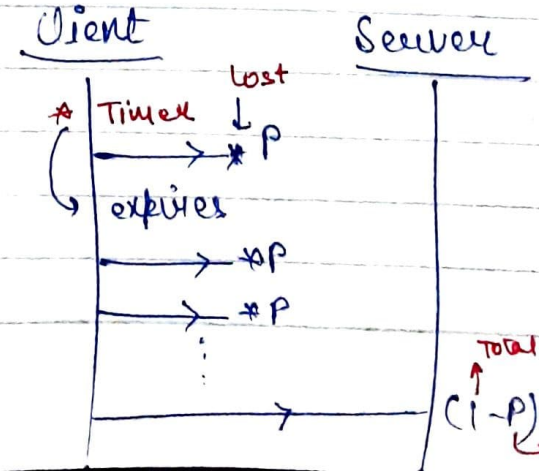
- For noiseless channel, for maximum utilization Go Back N ARQ is used

- For noisy channel, for maximum utilization selective Repeat ARQ is used

Q:-1

Ans

Probability of frame being lost is "p" then mean no. of transmissions of a frame is



K transmissions

$$\underbrace{P,\ P,\ P,\ P, \ldots}_{(k-1)\text{ times}} \ldots (1-P)$$

(k-1) times ↓ failure

k^{th} time (1 time)

$$E(k) = \sum_{k=1}^{\infty} k\, P(k)$$

$$= \sum_{k=1}^{\infty} k * p^{k-1} * (1-p)^1$$

$$= (1-p) * \sum_{k=1}^{\infty} k * p^{k-1}$$

$$= (1-p) * [1 + 2p + 3p^2 + 4p^3 + \ldots]$$

$$= (1-p) * (1-p)^{-2}$$

$$= \frac{1}{(1-p)}$$

$$\left[\begin{array}{l} 1+2x+3x^2+4x^3\ldots = (1-x)^{-2} \\ 1+x+x^2+x^3+\ldots = (1-x)^{-1} \end{array}\right]$$

Q2:→ Probability of frame reaching safely is "p" then mean no. of transmission of a frame is.

Client   Server

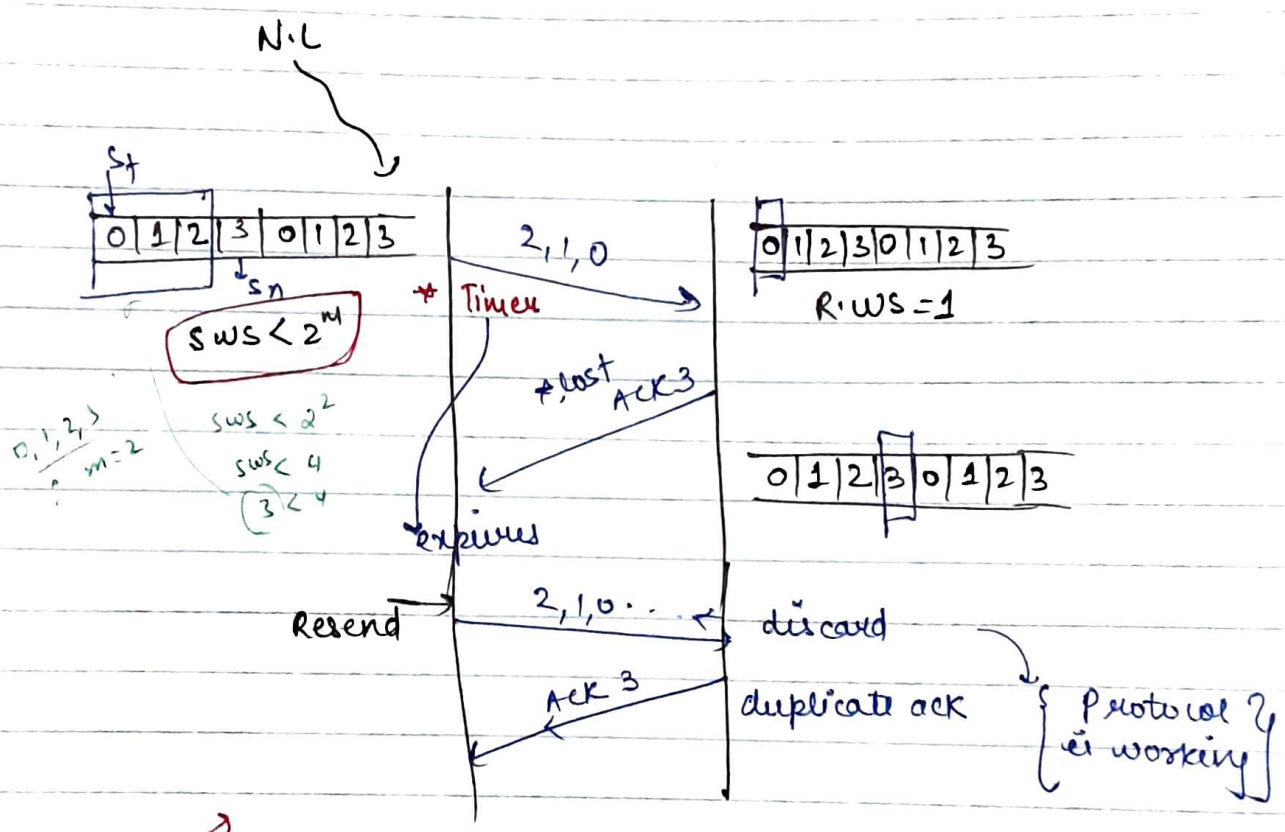
In the previous ques in place of p put "p" "1-p"

then

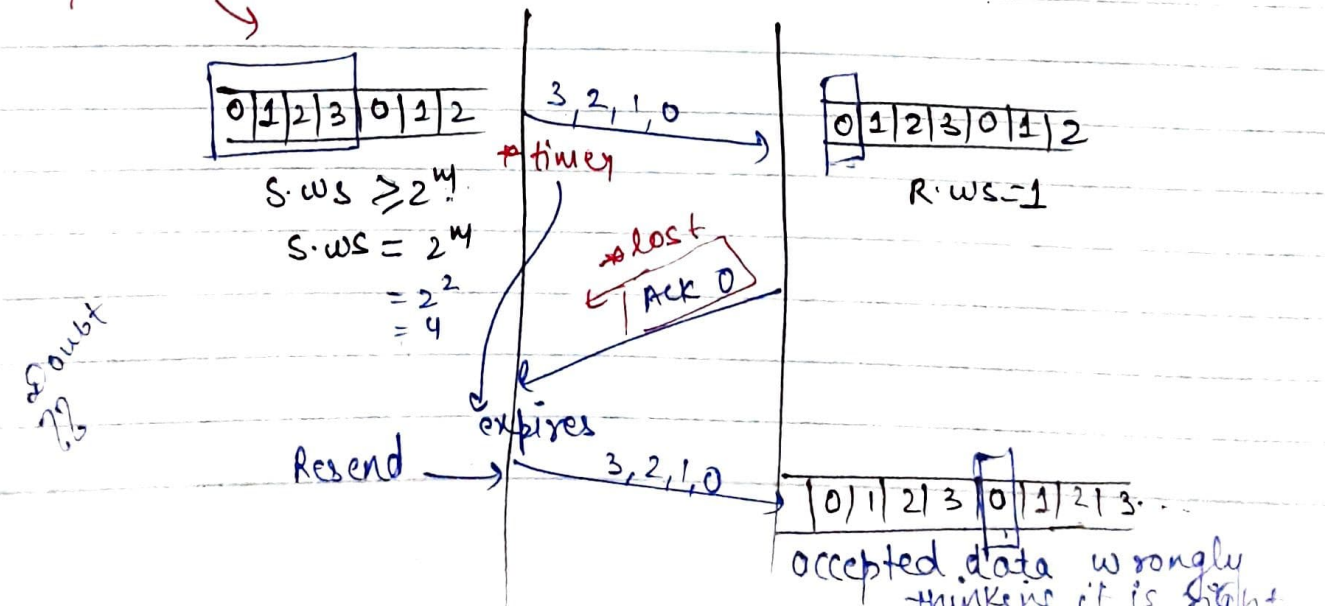
$$\text{ans} = \frac{1}{1-(1-p)} = \frac{1}{p} \text{ Ans}$$

Q3:- Probability of frame reaching safely = 0.1
and mean no. of transmission of a frame = 10
10 times we transmit the same frame
9 times → fail
10th time → Pass (Success)

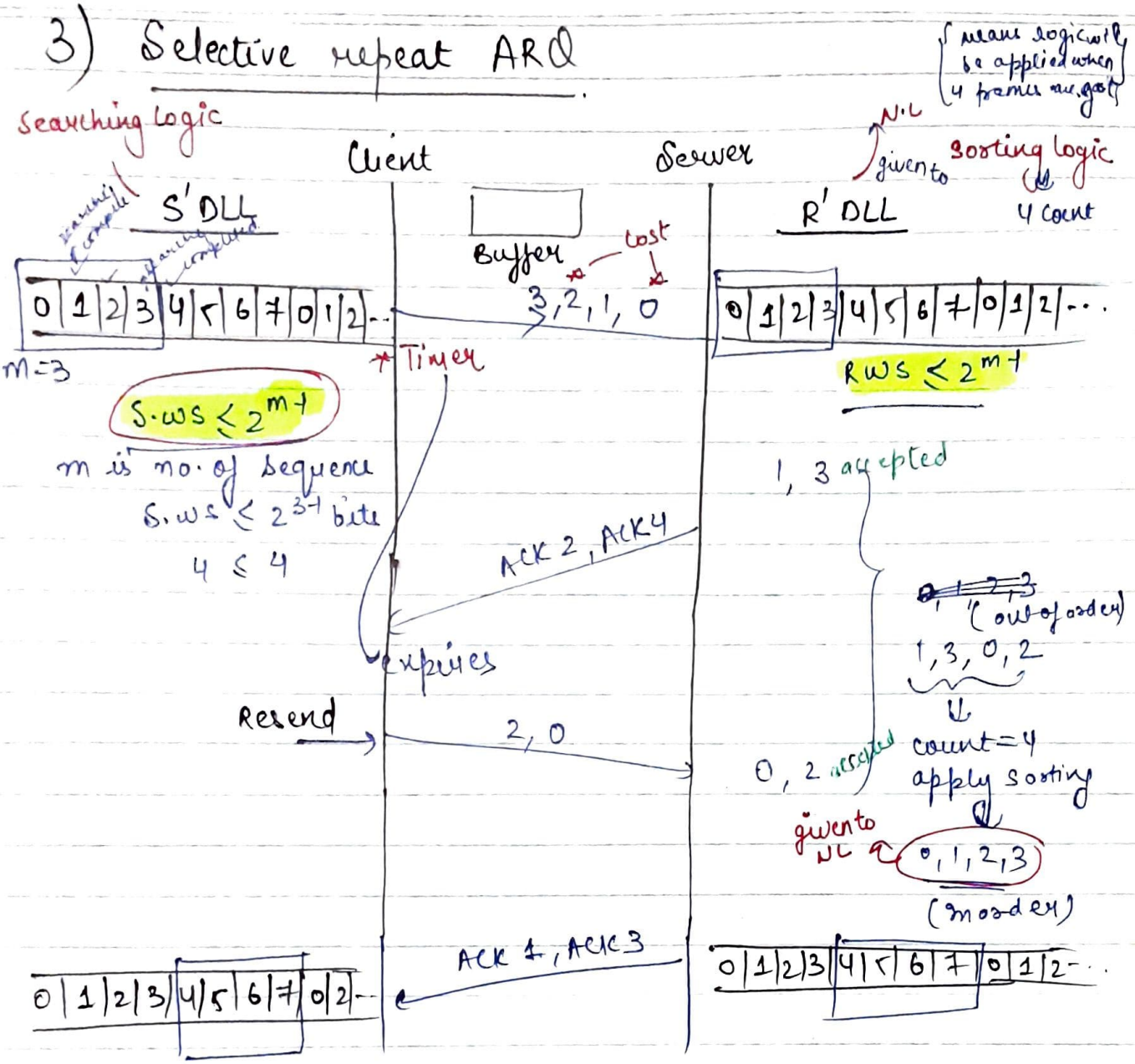
$$\therefore \frac{1}{9} = \underline{0.1}$$



Comparison



3) Selective repeat ARQ



» In selective repeat ARQ, sender requires searching logic and receiver requires sorting logic

Selective repeat ARQ supports only individual ACK's

Q:- 5 bit sequence number is used

SWS ≤ 2^(m-1)

		S.WS	R.WS
1)	Selective Repeat ARQ	16	16
2)	Go Back N	31	1

(96)

Sender

Q:- Maximum window size in Selective repeat ARQ = 4
no. of sequence bits = ?

⇓

$S.WS \leq 2^{m-1}$

$S.WS_{max} = 2^{m-1}$

$S.WS_{max} = \frac{2^m}{2}$

$m = \log_2 (2 * S.WS_{max})$

$\therefore \quad m = \log_2 (2 * 4)$

$m = \log_2 8$

$\boxed{m = 3}$

Q:- Maximum Sender window size in Selective repeat ARQ = Q

$\boxed{\text{no. of sequence bits} = \log_2 (2 * Q)}$

Q:- Maximum sequence no. in selective repeat ARQ=7
max size of Sender window=

⇓

$\frac{7+1}{2} = 4$

Way of the window

0	1	2	3	0	1	2	3	. . .

2 ↘ now ⇒ $\frac{3+1}{2} = 2$ Ans

generalized

Q:- Maximum Sequence no. in Selective repeat ARQ = "N"

$$\frac{\text{no. of sequence bits}}{\text{max size of sender window}} = \frac{N+1}{2}$$

Q:- BW = 100 Mbps
RTT = 50 μsec
Frame size = 50 bits
Calculate the window size?
and no. of sequence bits required in Selective repeat ARQ

Window size = no. of frames in R.T.T

1 sec = 10^8 bits
RTT → 50 μsec = $50 \times 10^{-6} \times 10^8$ bits
no. of bits in RTT = 5000 bits

∴ window size = $\frac{5000 \text{ bits}}{50}$

= 100

For (ii) part we will go to trial and error method.

	Selective repeat ARQ		Go Back N ARQ	
	S.WS	RWS	S.WS	RWS
7 bits ($2^7=128$)	64	64	7 bits $2^7 - 1 = 127$	1
8 bits ($2^8=256$)	128	128	~~8 bits~~	

(128 satisfy window size = 100)

$S.WS \leq 2^{N-1}$

» For maintaining same window size, Selective repeat ARQ require more bits compare to Go Back N ARQ.

⇒ Buffer size = 3 bits

2^3 = 8 Sequence no.

	Stop & wait ARQ	GO Back N ARQ	Selective Repeat ARQ
Sender maximum window size	1	7	4
Buffer Requirement	low	high	moderate

⇒ Buffer Requirement is low in Stop and wait ARQ whereas it is high in GO Back N ARQ and moderate in selective repeat ARQ.

When the Bandwidth is limited, Selective repeat ARQ will be better compared to GO Back N ARQ

Q:→

Bandwidth = 20Kbps

Using PT = 400 msec

frame size = 100 bytes = $\frac{100 \text{ bits}}{8}$

Transmission time = $\frac{100^{bits}}{8} / 20 \times 10^3 \text{ bits/sec}$

= ~~40 bits/sec~~ 40 msec

PT = 400 msec

$a = \frac{PT}{TT} = \frac{400 \text{ msec}}{40 \text{ msec}} = 10 \text{ msec}$

Throughput = Efficiency x BW

$= \frac{10}{21} \times 20$

$= \frac{200}{21} = 10 \text{Kbps}$

w = window size

Efficiency of GBN = $\frac{w}{1+2a} = \frac{10}{1+2\times10} = \frac{10}{21}$

Error Control policies of Data link layer :-

Hamming code (Error Correction policy)

Data + Parity bits = Codeword

Data = 10011010

$$2^r \geq m + r + 1$$

r = Parity bits
m = message bits

$\Rightarrow$ r = 3 ✗

$2^3 \geq 8 + 3 + 1$

$8 \geq 12$ (F) so

$\Rightarrow$ r = 4 =

$2^4 \geq 8 + 4 + 1$

$16 \geq 13$ (T) so

→ Parity bits placed in power of 2 positions

1	2	3	4	5	6	7	8	9	10	11	12
P_1 (2^0)	P_2 (2^1)	1	P_3 (2^2)	0	0	1	P_4 (2^3)	1	0	1	0

P1 :- Take one no, leave 1 no.

Even Parity → so even no. of 1's

So, 1, 3, 5, 7, 9, 11

0, 1, 0, 1, 1, 1 ∴ $P_1 = 0$

~~P2 :- 2, 4, 6, 8, 10, 12~~

P2 :- Take 2 Consecutive, leave 2 ~~bits~~ consecutive

So, 2, 3, 6, 7, 10, 11

1, 1, 0, 1, 0, 1 ∴ $P_2 = 1$

P_8 :- Take 8 consecutive no., leave 8 consecutive no.

So, 8, 9, 10, 11, 12
0, 1, 0, 1, 0

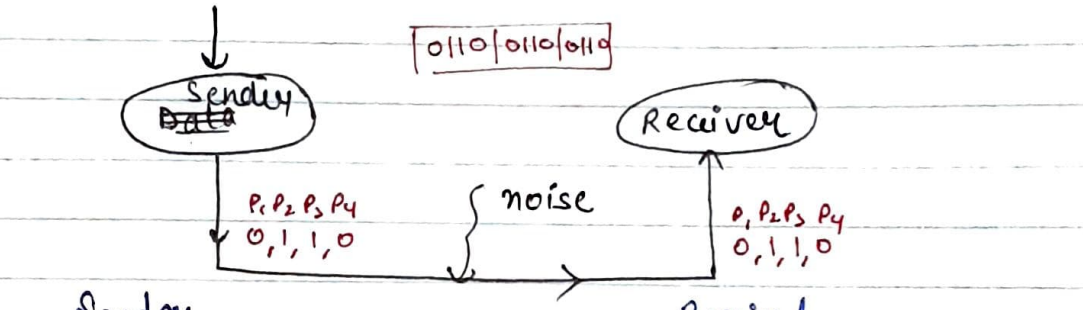
$\therefore P_8 = 0$

P_4 :- Take 4 consecutive no., leave 4 consecutive no.

So, 4, 5, 6, 7, 12
1, 0, 0, 1, 0

$\therefore P_4 = 1$

Data : 10011010



Sender
Codeword = 011100101010

Received
Codeword = 011100101110

noise has modified the data

Received Codeword = 011100101110
$P_1 P_2 1 P_4 00 P_8 1110$

Here ($P_1 = 0$, $P_2 = 1$, $P_4 = 1$, $P_8 = 0$)

↳ Received Parity in received codeword.

Received Codeword = $P_1\ P_2\ 1\ P_4\ 0\ 0\ 1\ P_8\ 1\ 1\ 1\ 0$
(positions 1 2 3 4 5 6 7 8 9 10 11 12)

P_1 :- 1, 3, 5, 7, 9, 11
0 1 0 1 1 1
So, $P_1 = 0$ ✓ calculated parity

P_2 :- 2, 3, 6, 7, 10, 11
0, 1, 0, 1, 1, 1
So, $P_2 = 0$ ✗ not matching

P_4 :- 4 5 6 7 12
1 0 0 1 0
So, $P_4 = 1$ ✓

P_8 :- 8 9 10 11 12
1 1 1 1 0
So, $P_8 = 1$ ✗ not matching

0+2 = 10

» So, there is an error at 10th position in the Received codeword., actually the bit at 10th position is modified

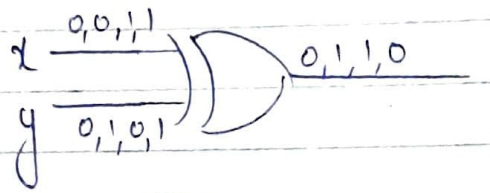
Only ~~two~~ ~~change occurs~~

» If noise modifies parity bits copy, it will be known immediately by comparing with reliable copy

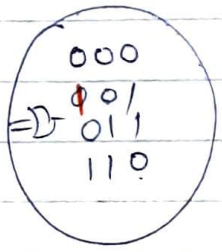
» The drawback of hamming code, it will correct only single bit errors.

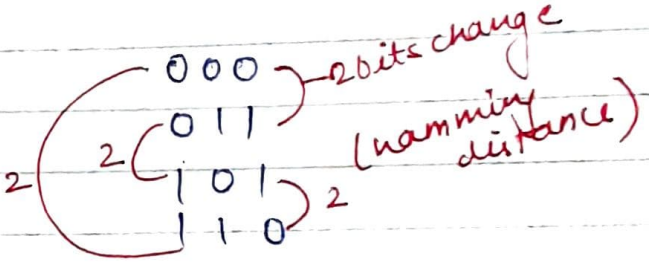
Data + Parity ⇒ Codeword

x	y	o/p ⇒ even parity
0	0	0
0	1	1
1	0	1
1	1	0



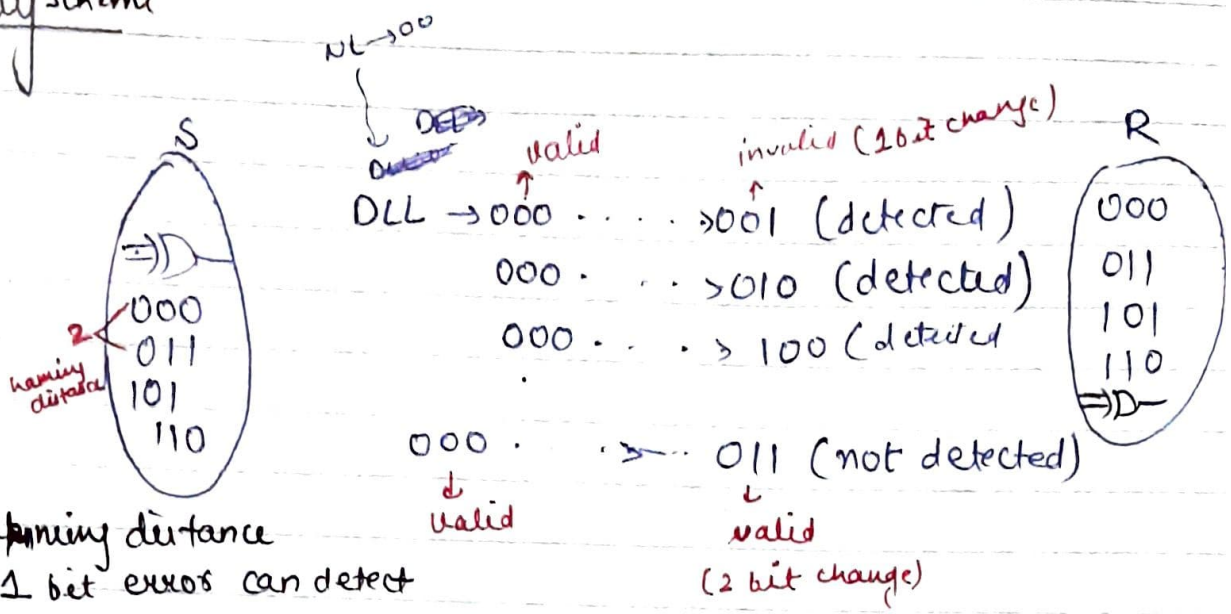
D.LL





- The no. of bits that differ by each other between two codewords is known as Hamming distance
- To detect "d" errors, the minimum hamming distance is d+1
- To correct "d" errors, the minimum hamming distance is 2d+1
- Codewords generated by the circuit is a valid codeword
- Codewords which are generated by from the circuit is known as valid codeword and remaining all are invalid codeword.

Parity scheme



(2) → hamming distance

2-1 → 1 bit errors can detect

- It will detect only odd no. of errors. (disadvantage)
- A valid codeword if it is converted into an invalid codeword then errors can be detected
- A valid codeword if it is converted into another valid codeword then errors can not be detected.
- The drawback of parity scheme is it will not only work for odd no. parities.

xor gate CKT generates ⇒ valid codewords

Noise generates ⇒ invalid codewords

If 3 = hamming distance

then 3 - 1 = 2 bit error can detect

Checksum :⇒

Data + Checksum bits = Codeword.

1

Sender [Data bits are modified] Receiver

Case (1)

7013 22 93 - - - - -> 7114 22 93

data checksum

error also detected

Received checksum

→ 70
13
22
105

→ 5
+1
6

→ 99
−6
93 ⇒ checksum

add checksum with data

{noise modify the data bits}

→ 71
14
22
107

→ 7
+1
8

→ 99
−8
91 calculated checksum

not accepted

2

Sender Receiver

Case (2)

7013 22 93 - - - - -> 7013 22 89

Received checksum

{noise modify the checksum bits}

→ 70
13
22
105

→ 5
+1
6

→ 99
−6
93

not accepted

Calculated checksum

bits are modified, ~~data~~ data not accepted

3

Sender — Receiver

case (3)

7013229 3 ---------> 7011 24 93

Received checksum

[noise modifies the data]

(Vertical bit errors)

70
13
22
105

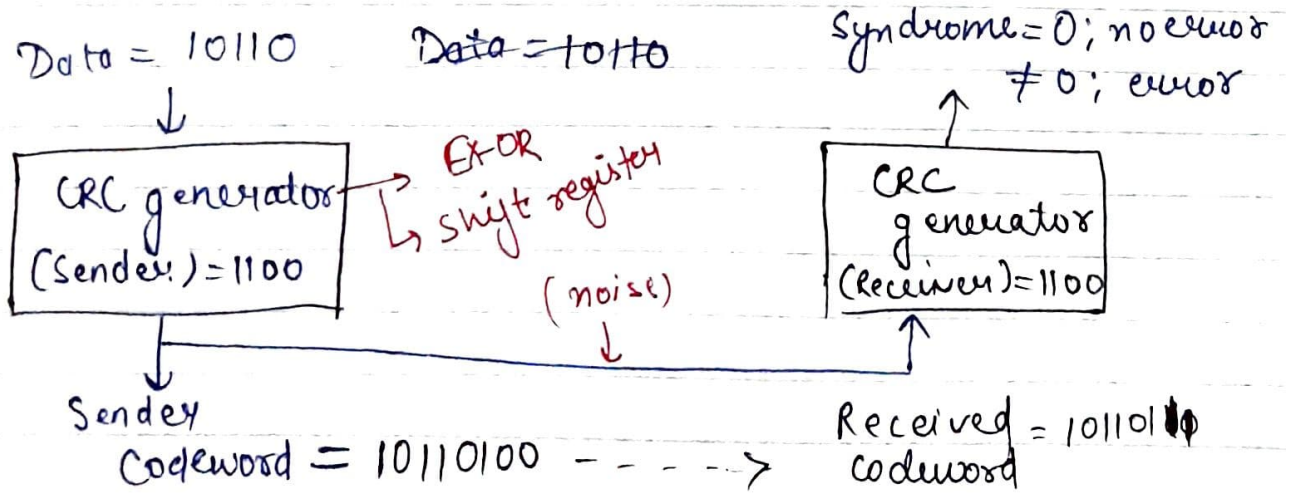
→ 70
11 -2
24 +2 → 99
105
-6
93
Calculated checksum

→ 5
+1
6

>> If noise modifies the data in such a way that the vertical placed bits cancel each other then the calculated checksum will be equal to the received checksum. This type of error is known as cannot be detected.

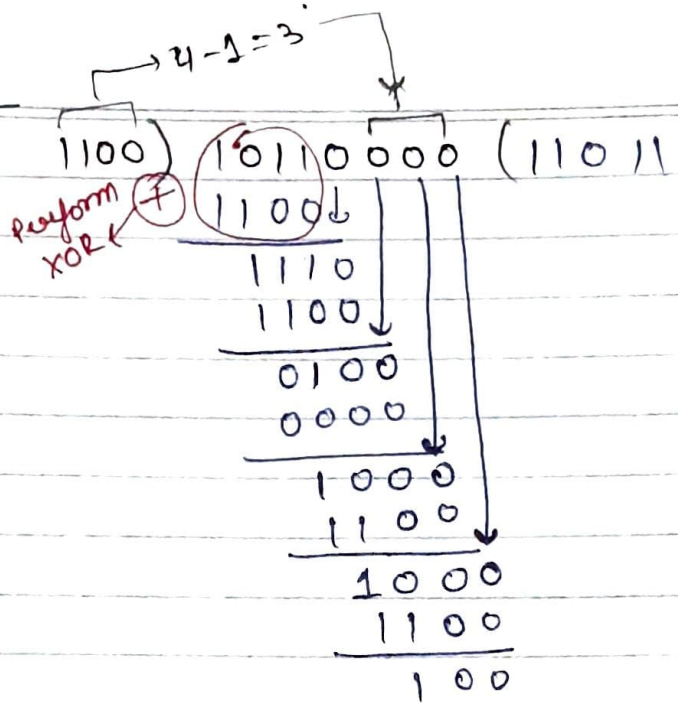
CRC (cyclic Redundancy Check)

Data + CRC bits = Codeword



(06)

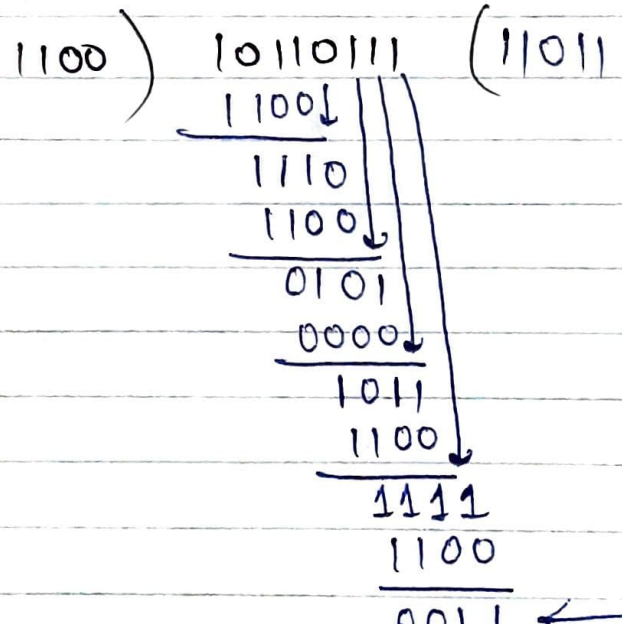
Sender



Sender Codeword = 10110100

Receiver

Received codeword = 10110111 (having error)



← Syndrome ≠ 0

∴ error is detect

CRC generator ⇒ $x^3 x^2 x^1 x^0$ ⇒ 1100

CRC generator polynomial ⇒ $x^3 + x^2$

⇒ 1100

Proof of why CRC generator should not contain 'x'.

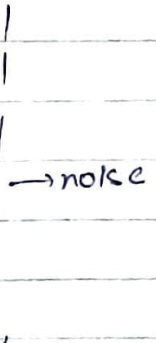
>> Data = 1011

CRC generator = $x = 1 \cdot x^1 + 0 \cdot x^0$

$= 10$

```
10) 10110 (1011
    10
    --
    01
    00
    --
    11
    10
    --
    10
    10
    --
    00
```

Sender Codeword = 10110



Received Codeword ⇒ 10100

```
10) 10100 (1010
    10
    --
    01
    00
    --
    10
    10
    --
    00
    00
    --
    0
```

→ syndrome = 0

∴ no error

But error is present ∴ not detected

∴ "x is a bad generator"

Rules for finding CRC generator

(i) CRC generator should not contain "x".
(Previous Page)

(ii) If x+1 is generator, it can detect odd no. of errors.

Proof

Data = 1011

CRC generator = x+1
$= 1 \cdot x^1 + 1 \cdot x^0 = 11$

Case 1 :- 1 bit modified

```
11) 10110 ( 1101
    11↓
    ---
     11
     11↓
     ---
      01
      00
      ---
       10
       11
       --
        1
```

noise { 1 bit is modified

Sender Codeword = 10111 — case (i) → Received Codeword 10110

```
11) 10110 (1101
    11↓
    ---
     11
     11↓
     ---
      01
      00
      ---
       10
       11
       --
        1
```

Syndrome ≠ 0 ⇐ 1

∴ error detected

Case 2 :- 2 bits are modified

Sender Codeword = 10111 — noise → Received Codeword 10100

```
11) 10100 (110
    11↓
    ---
     11
     11↓
     ---
      00
      00
      --
       00
```

Syndrome = 0 ⇐ 00

∴ error not detected though present

Case 3:- 3 bits are modified

Sender Codeword → (noise) → Received Codeword

10111 → 10000

```
11 ) 10000 ( 1111
     11
     ---
      10
      11
      --
       10
       11
       --
        10
        11
        --
         1
```

Syndrome ≠ 0 ⇒ 1

∴ error detected.

CRC-32 is a standard for detecting all types of errors in the LAN network.

(140)

Framing :->

Dividing large amount of data into small parts so that errors can be detected easily is known as framing.

-> The efficiency of any error detection scheme decreases as the length of data increases

(i) ~~Character Count~~

Sender — noise — Receiver

(1) 1000 - - - - - -> 1001

0001
0110
1011
1000

$^4C_1 = 4$

(2) 1000 . . . . . -> . . 1011

$^4C_2 = 6$

(3) 9999 bits —-> 2 bits by noise

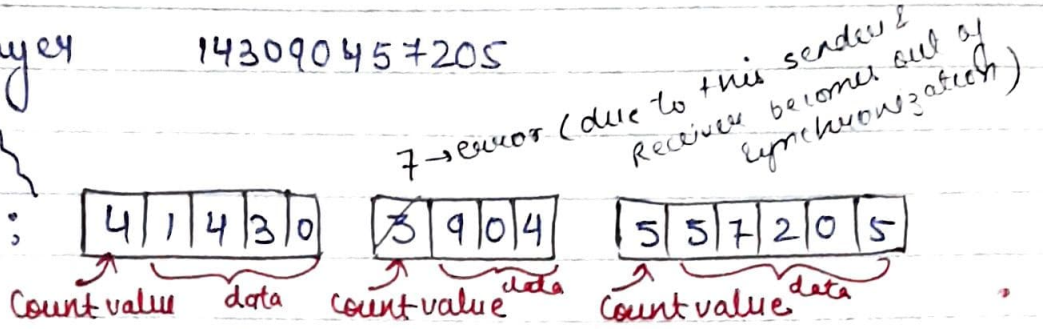
then

$^{9999}C_2$ ✓ High

So divide the $^{9999}C_2$ into small small parts so that errors can be easily detected by CRC

(i) Character Count

Network Layer 1430904 57205



- In character count technique, count value indicates the size of the frame
- If noise modifies data CRC will protect the data
- If noise modifies the count value both sender and receiver are out of synchronization. (drawback)

(ii) Character stuffing

Case 1

N·L : A Z
S' DLL : FLAG A Z FLAG ...

NL; A Z
R'DLL: FLAG A Z FLAG

Case 2

NL; A FLAG K
S'DLL: FLAG A FLAG K FLAG...
(starting flag, Data flag, ending flag)

NL: A ←
R'DLL: FLAG A FLAG K FLAG
(assume it wrong that it is an ending flag)

Case 3

NL: A FLAG K
S'DLL: FLAG A ESC FLAG K FLAG
(with esc it becomes clear that it is data flag)

NL: A FLAG K
R'DLL: FLAG A ESC FLAG K FLAG

Case :→ N·L: A ESC FLAG P

Data at D·LL after Character Stuffing :- FLAG A (ESC) ESC (ESC) FLAG P FLAG

• The drawback of character stuffing is that every flag occurs in the data there is "ESC" character is added so overhead size increases

(iii) Bit stuffing

N·L :- A Flag B

Data at Data link layer :- FLAG A (ESC) FLAG B FLAG (in Character stuffing)

after bit stuffing 01111110 01000001 01111101 01000010 01111110

FLAG = 01111110 , A(65) = 01000001 , B(66) = 01000010

For ESC in Bit Stuffing what we do is we add 0 after 5 1's. and this trick vary with flag. [see other eg's]

Q:- Data at NL ⇒ 01111101111110

FLAG ⇒ 01111110

Data at DLL ⇒ 01111110 01111101011111000 01111110

(stuff a 0 at these places after 5 consecutive 1's)

after bit stuffing — Flag — Flag

Q:- Data at N·L ⇒ 011111011110

Flag ⇒ 01111110

Data at DLL after bit stuffing ⇒ 01111110 01111010111100 01111110

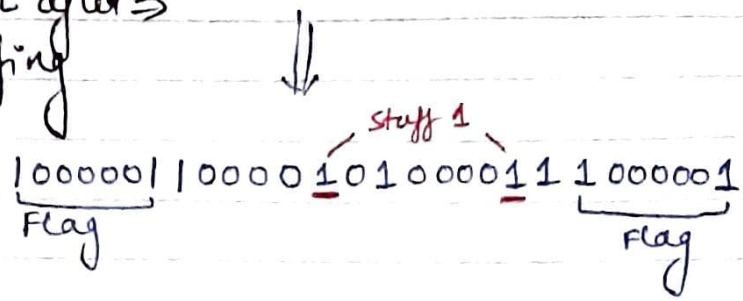
(stuff a 0 here) — Flag — Flag

Here we have stuffed 0 after 4 1's cos Flag has total 5 1's

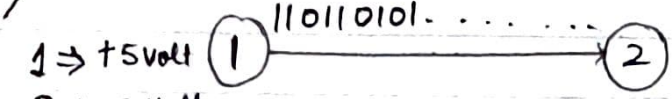
Band x n

Q: Data at N.L ⇒ 1000001 00001 , Flag = 1000001

Data at DLL after bit stuffing ⇒

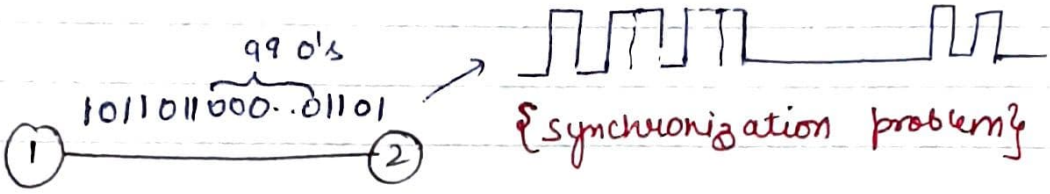


⇒



{ v = 0 channel is idle }

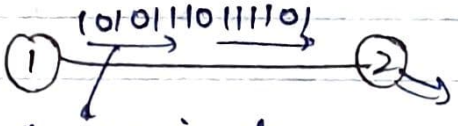
(i)



{synchronization problem}

Here it get confused whether this 0 indicates that channel is idle or it is a part of data.

(ii)



High BW signals

dc current is high due to more no. of 1's

{ our motive is reduce this dc current }

eg:- when we play game our mobile phone heats up and it is due to this reason.

⇒ **Bit rate** **Baud rate**

Here Bit rate = Baud rate

Bit rate = 1 1 ⇒ → Here 1 symbol → Baud rate = 1

no. of bits that you transmit

Bit rate = 2 10 ⇒ 0 → Here also 1 symbol → Baud rate = 1

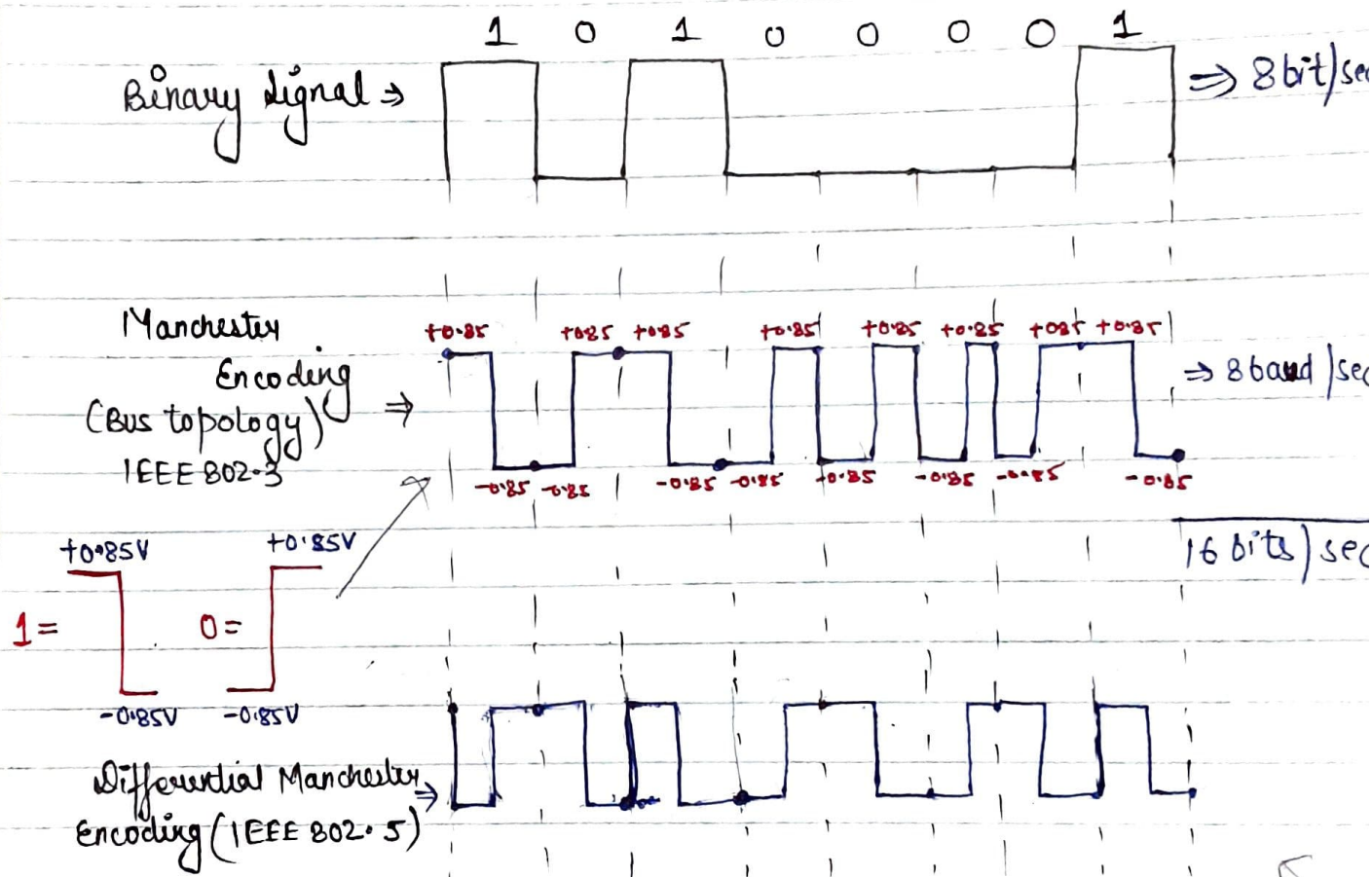
Here Bit rate ≠ Baud rate

⇒ Bit rate is no. of bits that are transmitted

⇒ Baud rate is a symbol rate or rate at which signals are transmitted / modulated

Encoding :-

Manchester Encoding :-



⇒ The advantage of Manchester Encoding is it provide synchronization and it eliminates high DC Component value

In Differential manchester 1 = transition (change)

0 = no transition (No change)

Here change means change the level

If you are at 1 go to 0 and vice versa

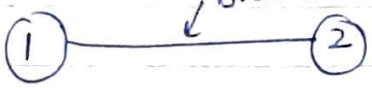
advantage of Differential Manchester :-

1. It provides synchronization
2. It eliminates high DC component value

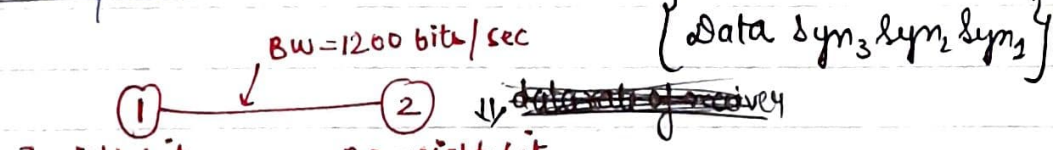
Serial data transfer

(i) Synchronous Serial Transfer
(ii) Asynchronous Serial transfer

Synchronous Serial transfer



Q: In synchronous serial transmission, a 3-eight bit sync characters are included in 30-eight bit information character then what is the data rate of receiver if the bandwidth of channel is 1200 bits/sec



3-eight bit sync characters
$3 \times 8 = 24$ bits Syn

30-eight bit Info characters
240 Info bits

24 Sync bits ⟶ 240 Info bits

1200 bits ⟶ $\frac{24 * 1200}{240}$ bits

= 120 Sync bits

240 info bits → 24 sync bits

1 info bit → $\frac{24}{240}$

1200 bits → $\frac{24 \times 1200}{240}$

data rate of receiver = (1200 − 120) bits/sec (subtracting Syc bits)

= 1080 bits/sec

= $\frac{1080}{8}$ char/sec

= 135 char/sec

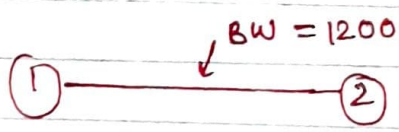
NOTE :⇒ In Synchronous Serial transmission Sync bits are added for group of characters

⇒ Sync bits are not taken by the receiver. These bits are only to alert the receiver that data is coming

Asynchronous Serial Transfer

Q:- In Asynchronous Serial transmission 1-start bit, 2 parity bit, 1 stop bit are added for character and the bandwidth of the channel is 1200 bits/sec then what is the data rate of receiver?

Soln



1 start bit + 1 char + 2 Parity bit + 1 stop bit

+ 1 char bit

data rate of receiver = 1200 bits/sec

$= \frac{1200}{(1+8+2+1)}$ char/sec

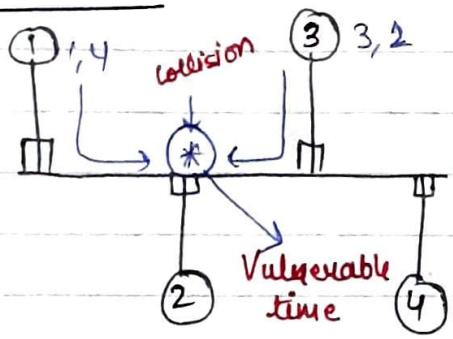
$= 100$ char/sec Ans

NOTE ⇒ In asynchronous Serial transmission the extra bits are treated as part of data.

⇒ In asynchronous Serial transmission the extra bits are added for every character. and that's they can't be removed and ∴ receiver considers them as a part of data

Data link layer
- → LLC Sublayer (Logic link control Sublayer) ⇒ flow control, error control
- → MAC Sublayer (Medium access control Sublayer) ⇒ To overcome collisions (interact with NIC, MAC address)
  - → Shared channel

(i) Pure Aloha :→

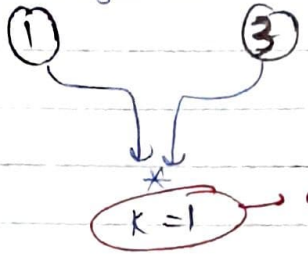


Rule of Pure aloha

1) Any System is having a data, it can transmit immediately
2) If two or more systems transmits the data at the same time then there is a possibility of collision
3) ~~If~~ ~~two~~ The time at which collision occurs is known as Vulnerable time

Exponential Back off Algorithm

Here systems wait for a random amount of time.



$WT_1 = (0 \text{ to } 2^K - 1) * P.T$

$= (0, 1) * P.T$

$WT_3 = (0 \text{ to } 2^K - 1) * P.T$

$= (0, 1) * P.T$

Q:- Systems 1 and 3 have transmitted their data for 1st time, collided and waited a random amount of time. Using exponential Back off Algorithm then what is the probability that System 1 will re-transmit before system 3

WT_1	WT_3
0	0
P.T	P.T

(0,0) (0, PT), (PT, 0), (PT, PT) ← at the same time

(0,0): at the same time

(0, PT): System 1 retransmit before 3

(PT, 0): System 3 retransmit before 1

$$\text{Probability} = \frac{\text{favourable}}{\text{total}}$$

$$= \frac{1}{4}$$

$$\left[\frac{1}{4} + \frac{1}{4} + \frac{2}{4} = 1 \right]$$

$WT_1 = (0, 1) * PT$ $\qquad$ $WT_3 = (0, 1) * PT$

$k = 2$ → data collided at 2nd time

$WT_1 = (0, 1, 2, 3) * PT$ $\qquad$ $WT_3 = (0, 1, 2, 3) * PT$

Q:- If Systems 1 and 3 have transmitted their data for 2nd time, collided ~~and that~~ then what is the probability that system 1 will retransmit before system 3.

WT_1	WT_3
0	0
PT	PT
2PT	2PT
3PT	3PT

$$\text{Probability} = \frac{\text{favourable}}{\text{total}}$$

$$\text{system 3 retransmit before system 1} = \frac{3+2+1}{16} = \frac{6}{16}$$

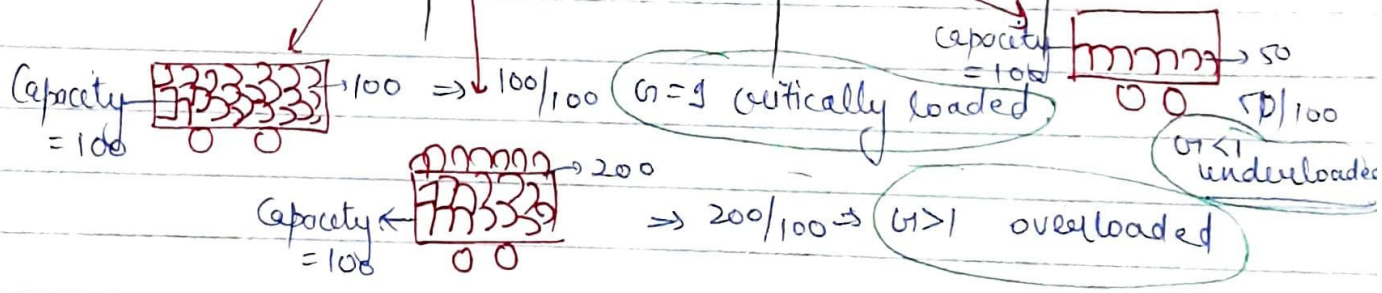
system 1 retransmit before system 3 $\left[\frac{6}{16} + \frac{6}{16} + \frac{4}{16} = 1\right]$ → Total probability

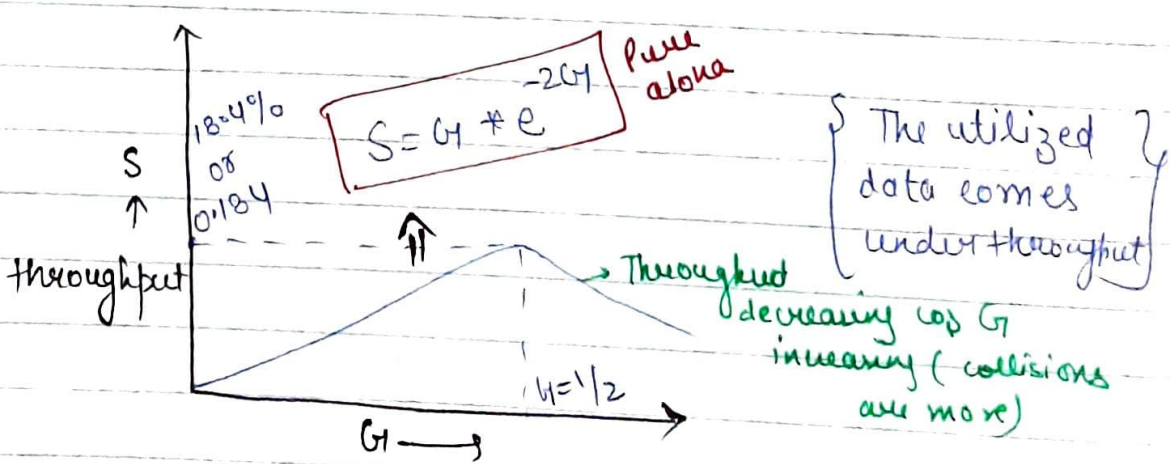
(Both at the same time)

» In exponential backoff algorithm as the k value increases, the possibility of collision occurence is decreasing

Pure aloha channel is a non-deterministic channel because every event is an independent event and ∴ applying Poisson distribution

no. of stations in LAN	no. of stations ready with data	collisions	data reached safely
100 stations	50 ⇒ 50/100 (underloaded)	20	30
100 stations	100 ⇒ 100/100 (critically loaded)	70	30
100 stations	25 ⇒ 25/100 (under overloaded)	5	20





Throughput in shared Channel: (Channel load)

The rate at which the user transmits the data and data should safely reached the destination

$$S = G * e^{-2G}$$

$$\frac{dS}{dG} = 0$$

$$G * (-2) * e^{-2G} + e^{-2G} * 1 = 0$$

$$e^{-2G} [-2G + 1] = 0$$

$$G = \frac{1}{2}, \; S_{max}$$

$$S = G * e^{-2G}$$

$$S_{max} = \frac{1}{2} * e^{-2 \times \frac{1}{2}}$$

$$S_{max} = \frac{1}{2e}$$

$$S_{max} = 0.184$$

$$\boxed{S_{max} = 18.4\%}$$

In Pure aloha out of 100 frames that are transmitted then only maximum 18.4 frames will safely reach the destination

Q:-

B.W = 50kbps

Maximum throughput = ?
of pure aloha

Maximum throughput of pure aloha = 18.4% of B.W

$$= \frac{18.4}{100} * 50\text{kbps}$$

$$= \frac{18.4}{100} \times 50\text{ kbps}$$

$$= 9.2\text{ Kbps}$$

The bandwidth which suffers from collision = 50 − 9.2 = 40.8 kbps

Throughput of pure aloha at G=1

$$S = G * e^{-2G}$$

$$S = 1 * e^{-2}$$

$$S = 0.135$$

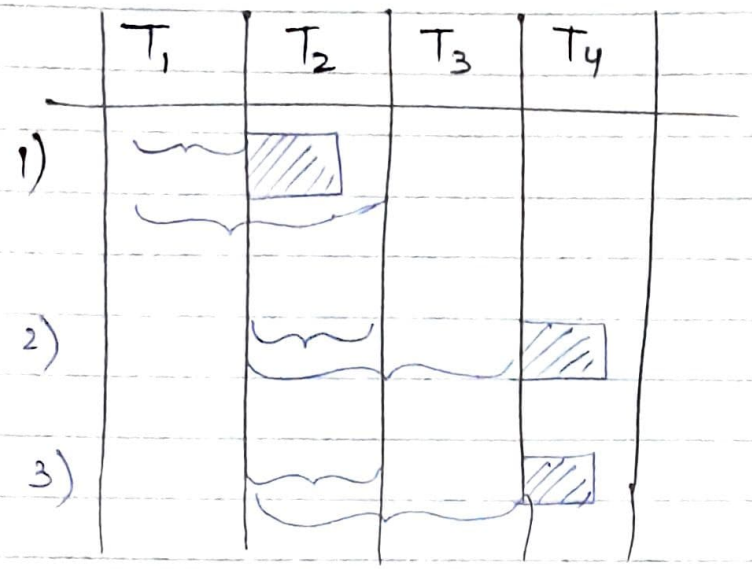
$$S = 13.5\%$$

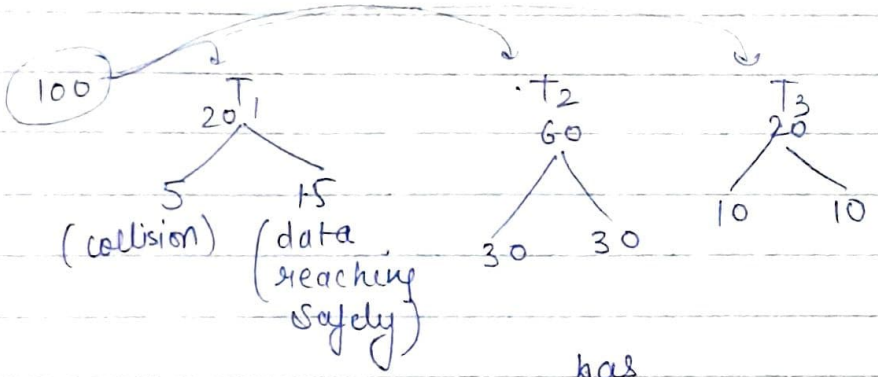
Throughput of pure aloha at G=1 ⇒ 13.5% of BW

$$= \frac{13.5}{100} \times 50 \text{ kbps}$$

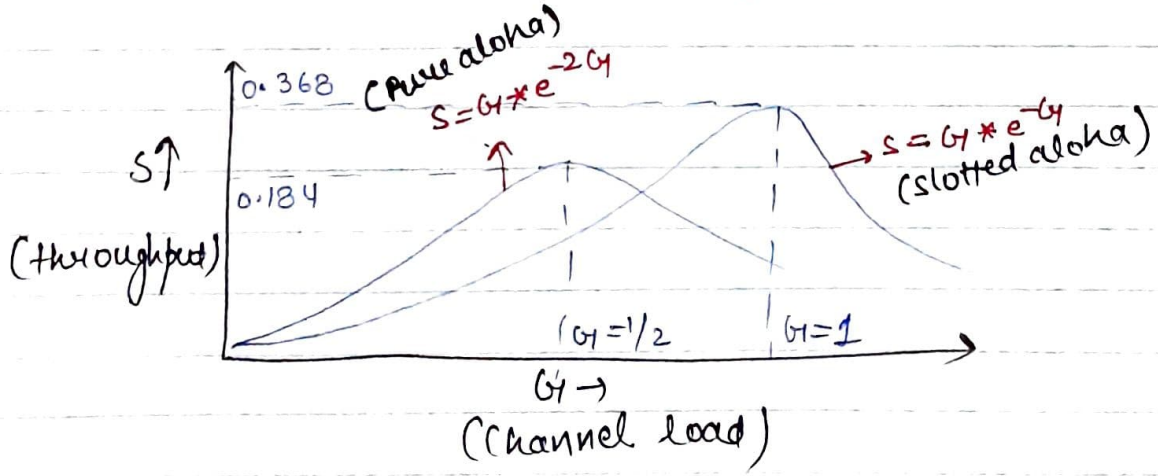
$$= 6.75 \text{ Kbps}$$

(ii) Slotted Aloha :→





∴ Slotted aloha has non deterministic channel



$S = G * e^{-G}$

$$\frac{dS}{dG} = 0$$

$$G*(-1)*e^{-G} + 1*e^{-G} = 0$$

$$e^{-G}[-G+1] = 0$$

$G = 1$, S_{max}

$S_{max} = 1 * e^{-1}$

$S_{max} = \frac{1}{e}$

$S_{max} = 0.368$

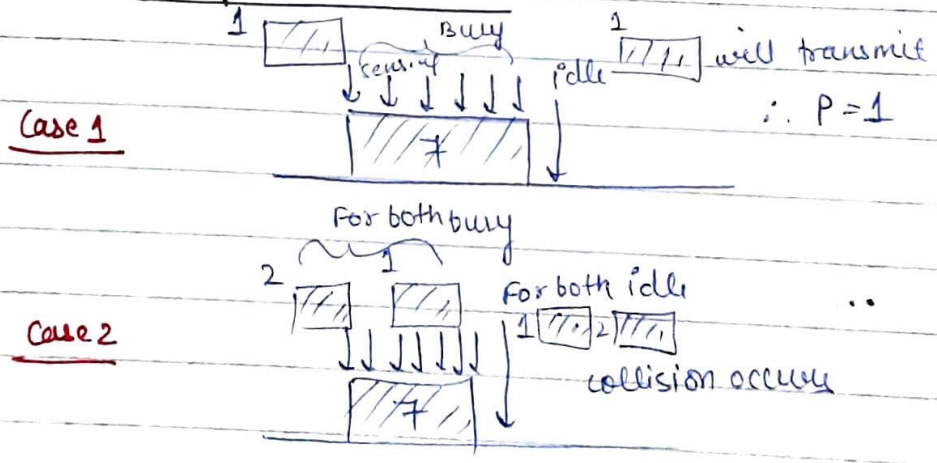
$S_{max} = 36.8\%$

{ throughput of slotted aloha is double that of pure aloha }

CSMA ⇒ Carrier Sense Multiple access

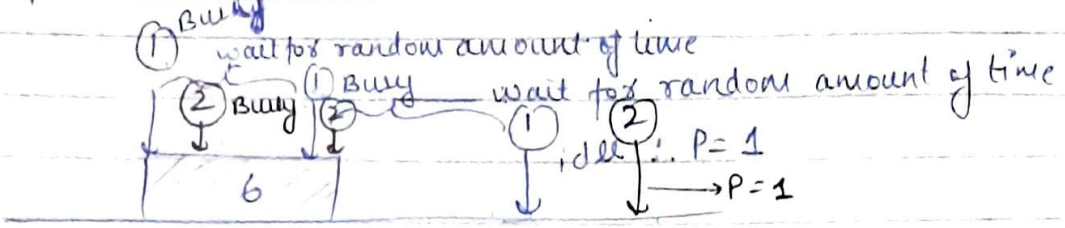
- When the energy is less, channel is idle
- When the energy is moderate, Channel is Busy
- When the energy is high, there is a collision on the network

(i) 1-persistent CSMA



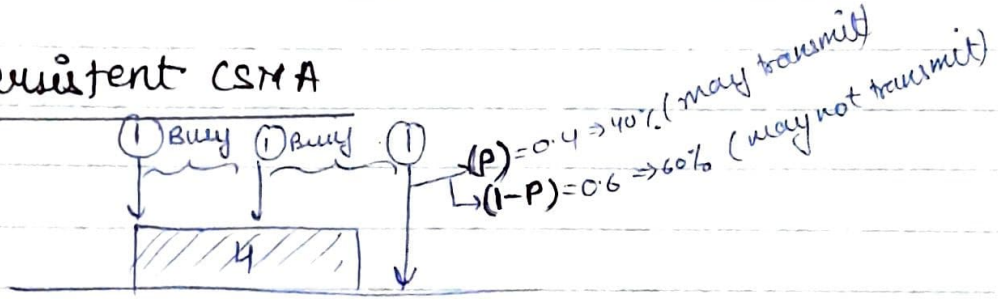
- In 1-persistent CSMA, stations will continuously sense the channel, once it is idle it will transmit with the probability P=1
- If two or more systems transmits the data at the same time then there is a possibility of collision

(ii) Non-persistent CSMA



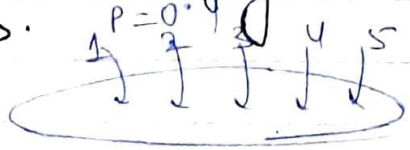
» In non-persistent CSMA, stations finding the channels (idleness) at the same place chance is less, so the possibility of collisions are less

(iii) p-persistent CSMA



» In p-persistent CSMA, once the channel is idle, it may transmit with ~~prop~~ probability p or it may not transmit with a probability 1-p

Q:- There are 5 stations in a channel. The probability of transmitting the data is 0.4. Only one station should transmit then what is the probability that only one station will transmit in the slot.



$\Rightarrow 1*(0.4)^1*(1-0.4)^4 + 1*(0.4)^1+(1-0.4)^4 + \ldots$ 5 stations

$\Rightarrow 5 * (0.4)^1 * (1-0.4)^{5-1}$

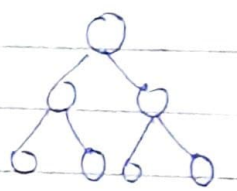
$\Rightarrow 5_4 * (0.4)^1 * (1-0.4)^{5-1}$

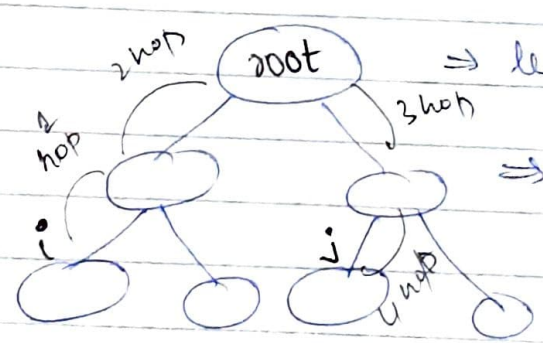
$$= {}^{n}C_1 * p^1 * (1-p)^{n-1}$$ Binomial

Q:→ A group of $(2^n - 1)$ routers are interconnected in centralized binary tree. Router i transmits the data to router j passing through the root router. Calculate the mean (avg.) number of hops a router makes for large n ~~long~~ value.

Ans :-

levels	no. of routers
1	$\Rightarrow 2^1 - 1 \Rightarrow 1$
2	$\Rightarrow 2^2 - 1 = 3$
3	$\Rightarrow 2^3 - 1 = 7$
⋮	
100	$\Rightarrow 2^{100} - 1$





$\Rightarrow$ level 1

$\Rightarrow$ level 2

$\Rightarrow$ level 3 $= n$ (let)

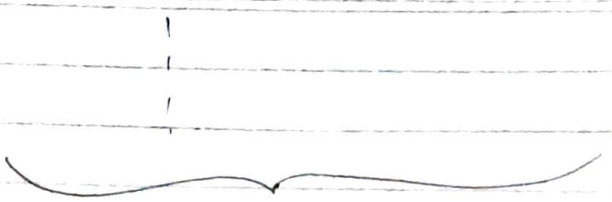
~~at level n~~

$$2^n - 1 \neq 2^n$$

at n^{th} level $\Rightarrow$ no. of routers $\Rightarrow \frac{1}{2} *$ total routers (2^n)

at $n-1^{th}$ level = no. of routers $= \frac{1}{4} * 2^n$

at $n-2^{th}$ level = no. of routers $= \frac{1}{8} * 2^n$



At n^{th} level router, no. of hops from router to root router = $(n-1)$ hops

At $n-1^{th}$ level router, no. of hops from router to root router = $(n-2)$ hops

Total no. of hops from router to root router = $\frac{1}{2} * 2^n * (n-1)$

$= \frac{1}{2} * 2^n * (n-1) + \frac{1}{4} * 2^n * (n-2) + \frac{1}{8} * 2^n * (n-3) + \ldots$

Average no. of hops $= \frac{\frac{1}{2} * 2^n * (n-1) + \frac{1}{4} * 2^n * (n-2) + \frac{1}{8} * 2^n * (n-3) + \ldots}{2^n}$

$= \frac{1}{2} * (n-1) + \frac{1}{4} * (n-2) + \frac{1}{8} * (n-3) + \ldots$

$= \frac{1}{2^1} * (n-1) + \frac{1}{2^2} * (n-2) + \frac{1}{2^3} * (n-3 + \ldots$

$= n\left[\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots\right] - \left[\frac{1}{2} + \frac{2}{4} + \frac{3}{8} + \ldots\right]$

$= \left(n * \frac{\frac{1}{2}}{1-\frac{1}{2}}\right) - \frac{1}{2}\left[1 + 2 * \left(\frac{1}{2}\right) + 3 * \left(\frac{1}{2}\right)^2 + \ldots\right]$

In cable after collision energy is back propogated

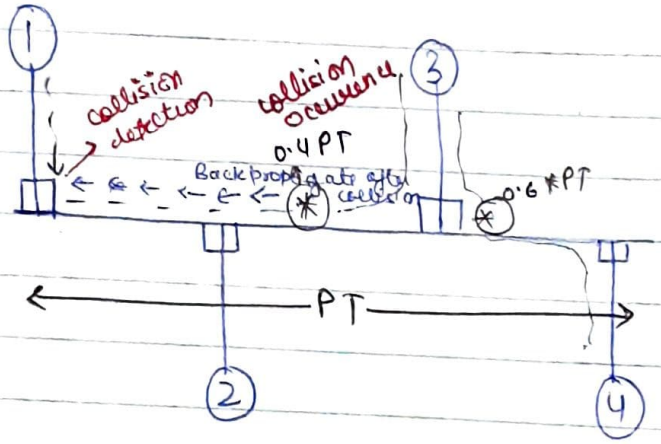
128

$$= n - \frac{1}{2}\left(1-\frac{1}{2}\right)^{-2}$$

$$= (n-2) \text{ hops}$$

Average no. of hops = 2(n-2) hops

CSMA/CD (Carrier Sense Multiple access / collision detection) {For wired}



PT: Propogation time.

Parallely
(i) transmits the data
(ii) Check for collisions

{ Collision occurs and then it back propogate so collision detection will take same time again so 0.4PT + 0.4PT = 0.2PT }

	Collision occurence	Collision detection
Best Case	0	0
	⋮	⋮
	0.4 * PT	0.8 * PT
	0.6 * PT	1.2 * PT
	⋮	⋮
Worst Case	1 * PT	2 * PT

- The range of collision occurence is [0 to PT]
- The range of collision detection is [0 to 2PT]

- If Collision has been detected at less than 2PT or at 2PT then station will stop transmitting the data and applies Exponential Backoff algorithm

- If Collision is not detected at less than 2PT or at 2PT then at 2PT, station acquires the channel or get control over the channel.

- The maximum time of which collision can be detected is $2 * PT$
- The minimum time to get control over the channel is $2 * PT$

Q:- In CSMA/CD

B.W = 10 Mbps

l = ~~100 Mbps~~ 200 m

v = $2 * 10^8$ m/sec

Calculate min frame size in CSMA/CD (Ethernet)

$T.T = 2 * PT$

$\frac{\text{frame size}}{BW} = 2 * \frac{100}{2 \times 10^8}$

$\frac{\text{frame size}}{10^6 \text{ bits/sec}} = 100 \times 10^{-8} \Rightarrow 10^{-6}$

$$\frac{\text{frame size}}{B.W} = 2 * \frac{l}{v}$$

$$\frac{x}{10^7 \text{ bits/sec}} = \frac{2 \times 200 \text{ m}}{2 * 10^8 \text{ m/sec}}$$

$$x = 20 \text{ bits}$$

Q2:- If 10base5 cable is used $v = 2*10^8$ m/sec. maximum frame size to detect collisions?

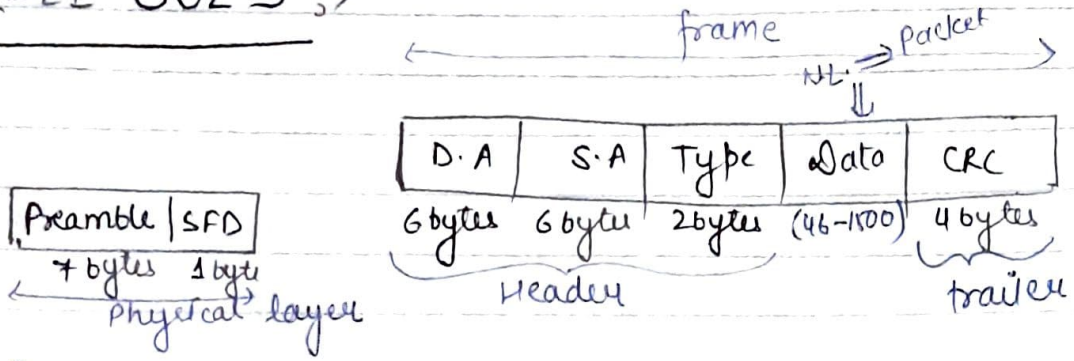
$$T.T. = 2 * PT$$

$$\frac{x}{10^7 \text{ bits/sec}} = \frac{2 * 500 \text{ m}}{2 \times 10^8 \text{ m/sec}}$$

$$x = 50 \text{ bits}$$

- If collision is detected at less than $2*PT$ then upto $2*PT$, jamming signal is transmitted in order to inform all stations about the collision.

IEEE 802.3 :→



- ⇒ Preamble and SFD are used to provide synchronization b/w Sender and Receiver ie. to alert the receiver that the data is coming.

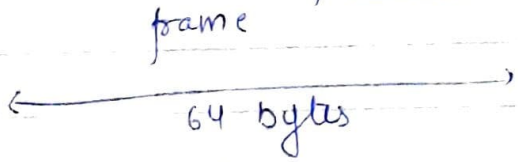
- ⇒ CRC calculation and data transmission can be done together coz CRC calculation is done inside the cable and transmission inside the cable.

- ⇒ Data link layer along with header, trailer is also added.

$$TT = 2 * PT$$

$$\frac{\text{frame size}}{\text{B.W} \Rightarrow \text{constant}} = 2 * \left(\frac{l}{v}\right) + \text{constant}$$

frame size = 64 Bytes (constant)



⇓ min frame size ⇒ to support (CSMA/D)

$$64 = 6 + 6 + 2 + x + 4$$

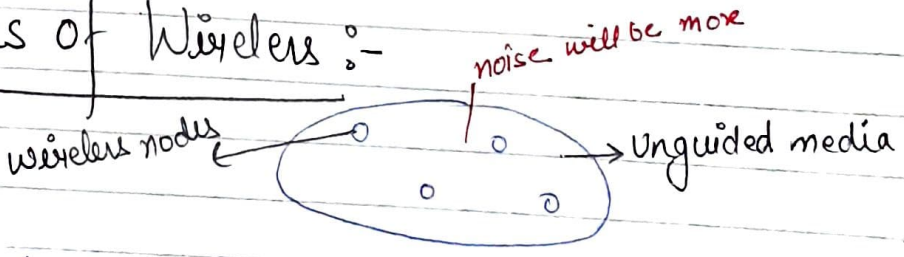
$$x = 46 \text{ Bytes}$$

- The minimum frame size in IEEE 802.3 is 64 bytes to support CSMA/CD
- The minimum payload or data in IEEE 802.3 is 46 bytes
- If the data coming from the network layer is less than 46 bytes then upto 46 bytes padding bits are added.
- The maximum frame size in IEEE 802.3 is 1518 bytes
- The maximum payload value or data in IEEE 802.3 is 1500 bytes
  This restriction is to give fair and equal chance to all systems in the network.

6+6+2+1500+4 = 1518 bytes

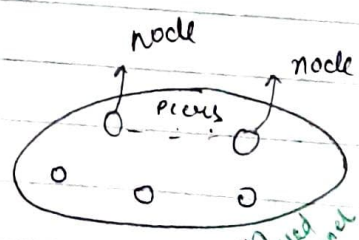
- Type field is going to indicate whether the frame is a data frame or control frame.

Basics of Wireless :-

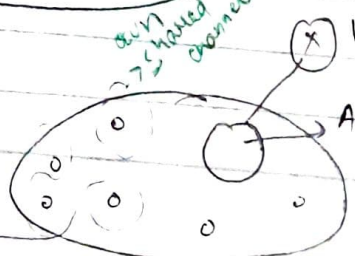


- Effects of noise will be more in wireless media

(i) Adhoc mode



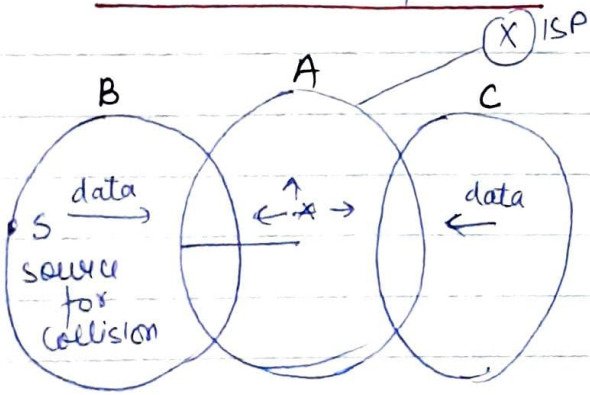
(ii) Infrastructure mode



→ In Bus topology all nodes will have same shared channel.
→ In wireless communication, every node will have its own shared channel.
→ In adhoc mode of transmission, every node can be transmitted to every other node and there is no centralized server
→ In infrastructure mode every node will get the servid of access point when they are in access range of access point.

Q:- Why we cannot apply CSMA/CD in wireless medium

Ans:- due to hidden node problem.



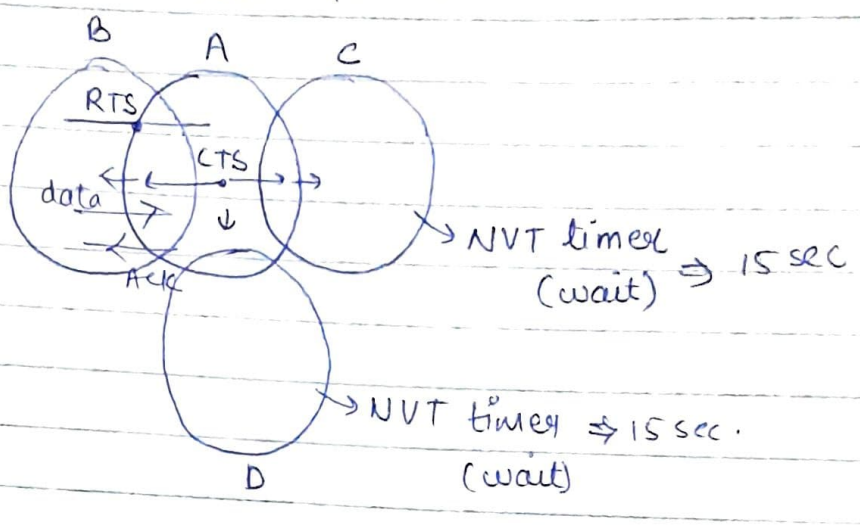
When nodes B, A, C are in a planar region, when nodes B and C transmits the data at the same time then there is a collision at node A but this cannot be detected by nodes B and C.
For node B, C is hidden and for node C, B is hidden. This problem is known as hidden node problem

CSMA/CA (Carrier Sense multiple access / Collision Avoidance)

IEEE 802.11 {For wireless}

RTS ⇒ Request to send
CTS ⇒ Clear to send
NVT ⇒ Network vector timer

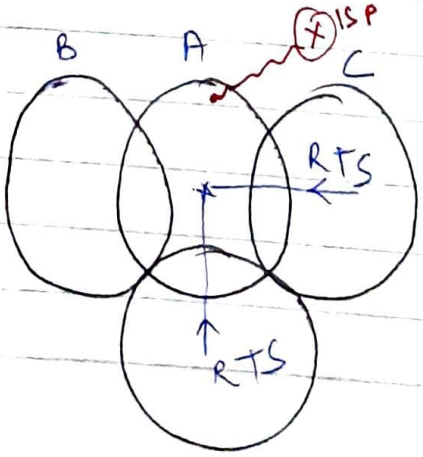
Case 1 :→



RTS, CTS (Control signals), data, Ack.

- Whenever the system wants to send the data, it will send RTS, if the channel is free, access point will reply CTS
- Node B can transmit the data parallely node C can start NVT timer
- Hidden node problem can be solved using CSMA/CA

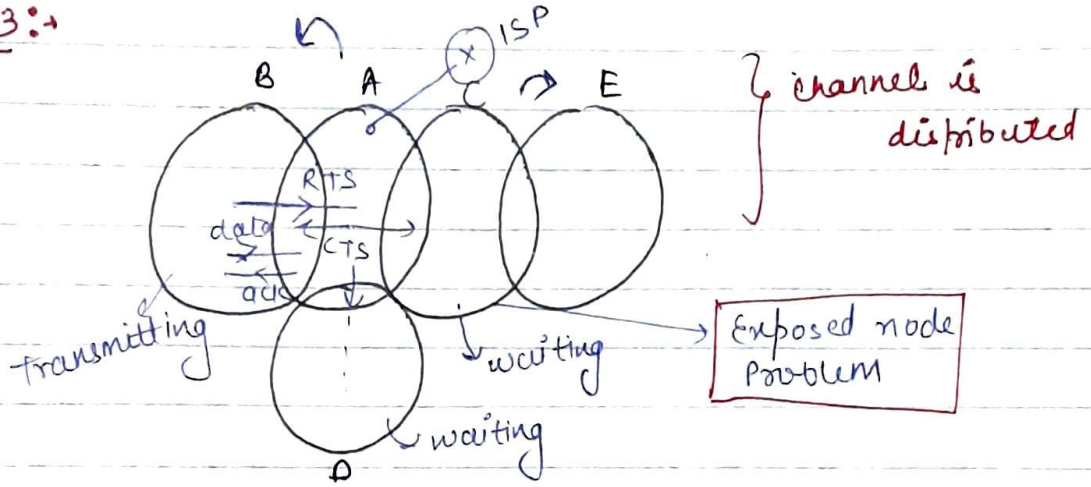
Case 2 :→



→ When more than 1 node sends RTS at the same time then there is a collision at the access node.

→ Not getting the CTS is the confirmation that there is a collision. Then those nodes will apply exponential Backoff algorithm.

Case 3 :-



→ At the cost of solving hidden node problem, there is an exposed node problem.

→ In CSMA/CD there is ack / no ack (~~ise~~)
because in this collision detection itself act as an acknowledgement

→ In IEEE 802.3 or CSMA/CD, there is no seperate acknowledgement collision detection itself will act as acknowledgement.

→ In CSMA/CA there is a seperate acknowledgement for the data.

→ In wireless, Retransmissions are more.

because node A can access node

•>> When node A wants to ~~send~~ transmit the data to node B, directly it can transmit the data.

Contention = collision (means)

•>> When nodes B, C and D tries to transmit to ~~node~~ access node A then ~~the~~ channel is contention channel.

•>> When node A wants to transmit the data to other nodes then the channel is a contentionless channel

•>> When access node has a data that should be given to multiple nodes then it would be given serially. This technique is known as Polling.

CSMA/CD → IEEE 802.3

CSMA/CA (wireless) → IEEE 802.11 → ~~ES~~ (wireless LAN)

⇒ IEEE 802.11 uses the 4 address.

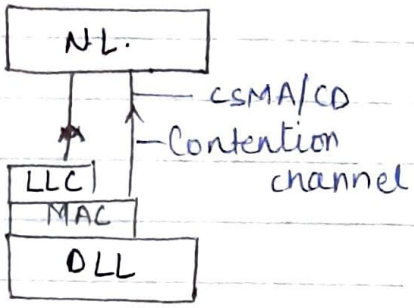
→ (i) DCF (distributed Coordination function)
(ii) PCF (Point Coordination ~~function~~ functio

✱ DCF (distributed Coordination function)

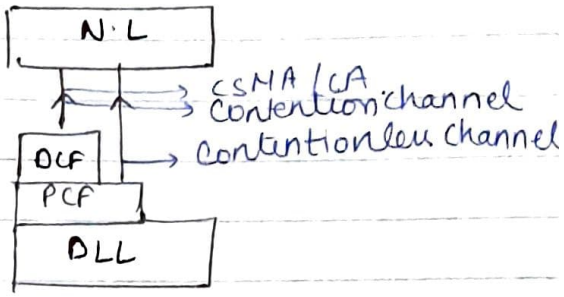
If (RTS, CTS, data, ack)
It is a ~~for~~ four handshaking

•> PCF will have more ~~to~~ priority than DCF

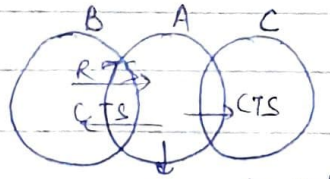
CSMA/CD → IEEE 802.3 → wired



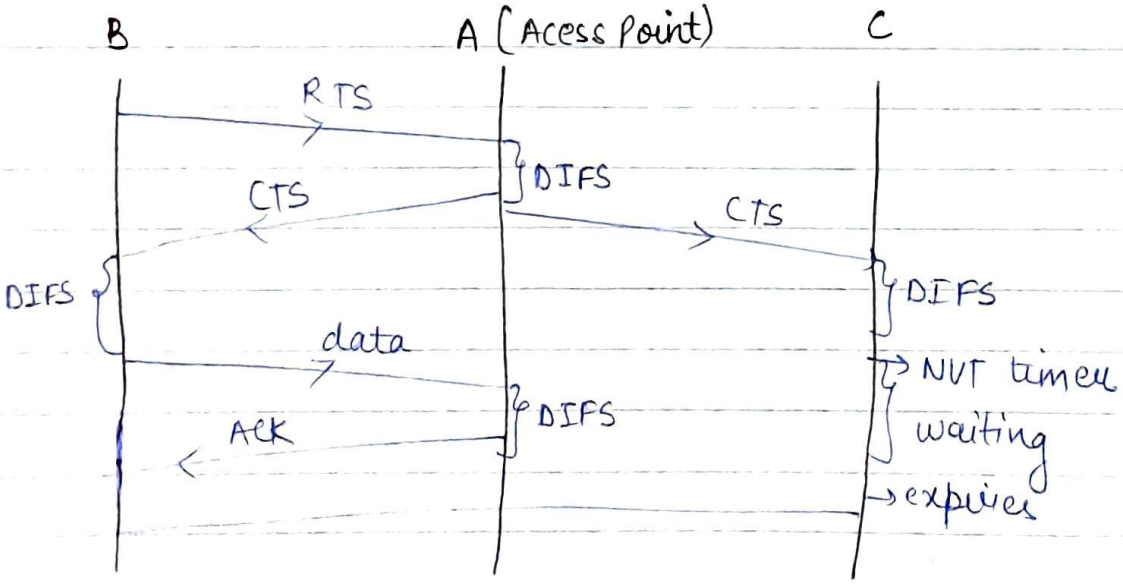
CSMA/CA → IEEE 802.11 → wireless



DCF function



1st Case



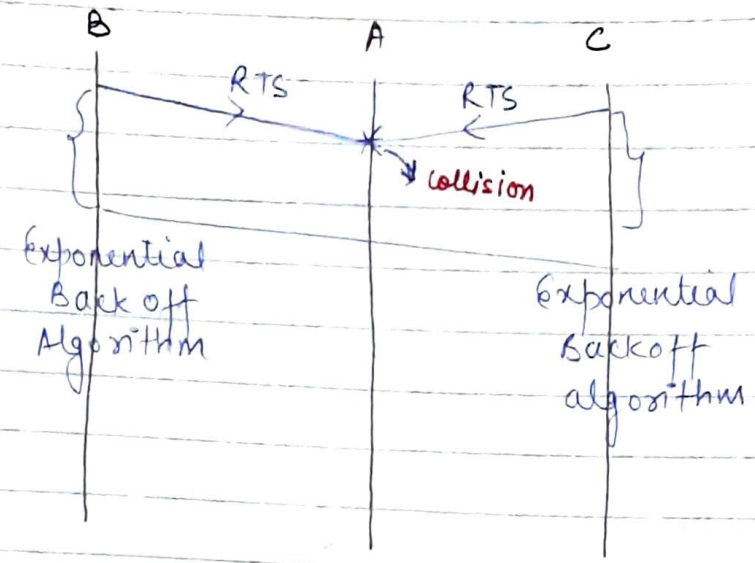
IFS ⇒ inter frame space

DIFS ⇒ It is a time gap b/w the two events

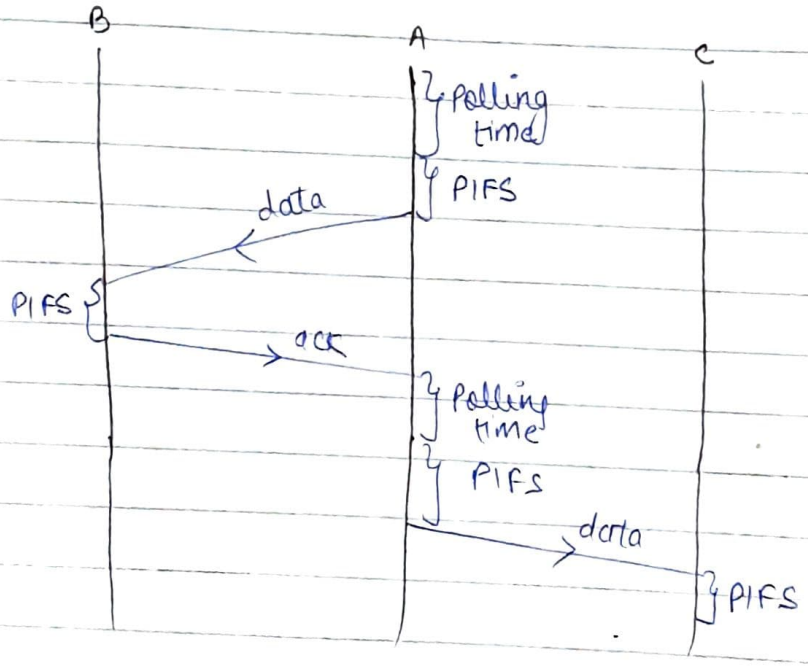
↓

Distributed

2nd Case



PCF function



⇒ Throughput of wireless LAN is less compared to throughput of wired LAN

Proof

In wireless throughput = $\frac{\text{Data Size}}{\text{RTS time} + \text{CTS time} + \text{Data time} + \text{Ack time}}$

denominator ⇒ is more ∴ throughput less

In wired throughput = $\frac{\text{Data size}}{\text{time to acquire channel} + \text{data transmission time}}$

denominator is not more ∴ throughput more

× PIFS > DIFS

= PIFS < DIFS

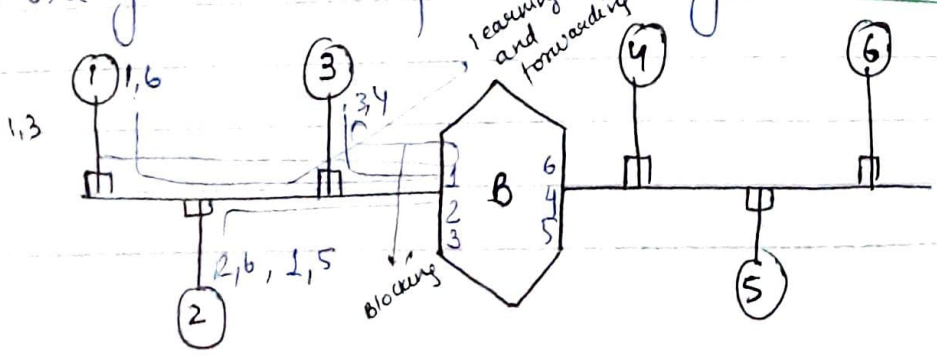
↳ when both node and AP node wants to transmit Access node has more priority than any other node

Networking devices :→

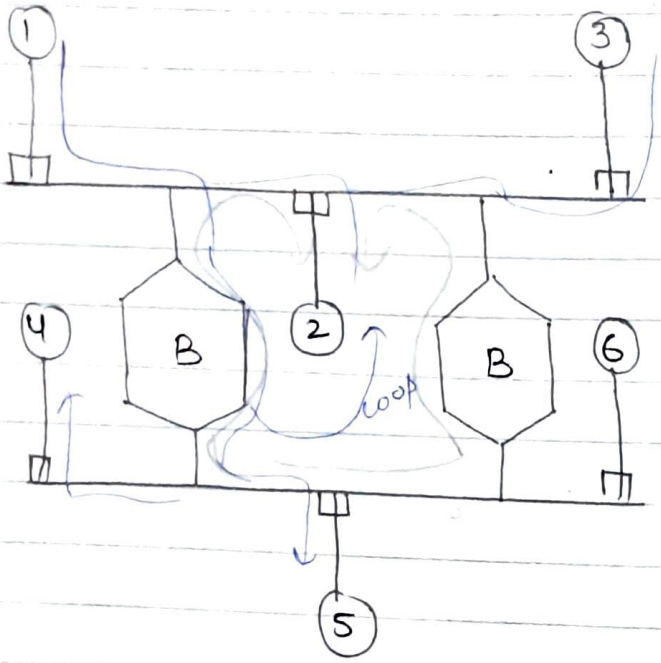
(i) Hub } Passive devices
(ii) Repeater }
(iii) Bridge } active devices
(iv) Router }
(v) Gateway }

Bridge :-

- Bridge is a LAN device and its operation is based on MAC address
- Bridge is used for connecting similar LAN networks



- Initially the Bridge table of the bridge is empty
- The functionality of Bridge is → forwarding
  → Blocking
  → learning
- Once complete information of the network known to the bridge then it is treated as converge and stable



Bridge is a Collision domain seperator but not broadcast domain seperator

- Between two similar LAN networks we connect more than one bridge to support fault tolerance
- When more than one Bridge is connected b/w similar LAN networks then there is a possibility of forming the loops b/w the bridges. (because bridge is not a broadcast domain seperator)

Spanning tree protocol (IEEE 802.1C) is used to eliminate loop by converting it into a tree

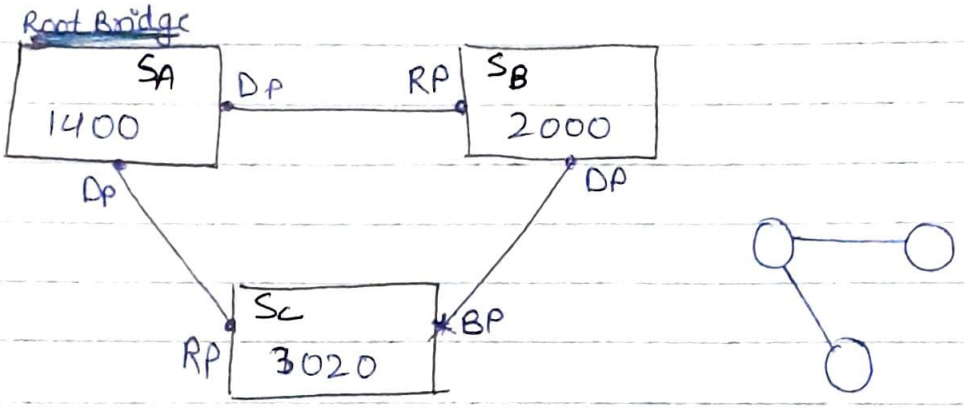
Root Bridge :→

The bridge which is having the least MAC address will become root bridge.

Root Port :→

Root Port is a port which is having the least cost path from non-root bridge to root bridge.

(1)



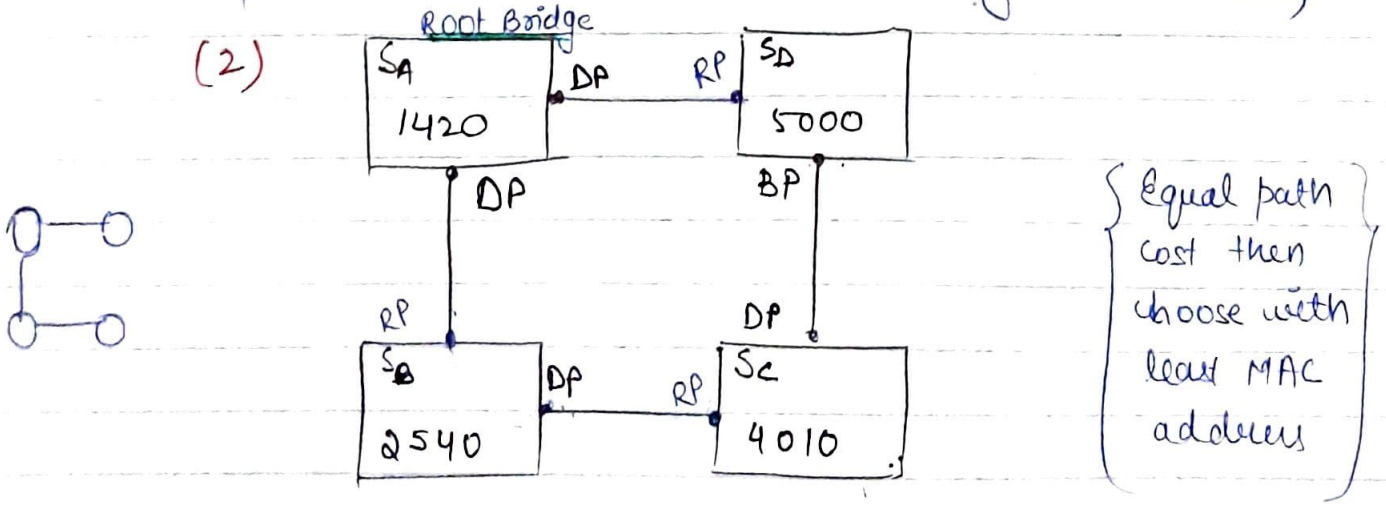
Designated Port :→

Designated Port is a Port having a least cost path from Root Bridge to non-root bridge node.

Blocked Port :→

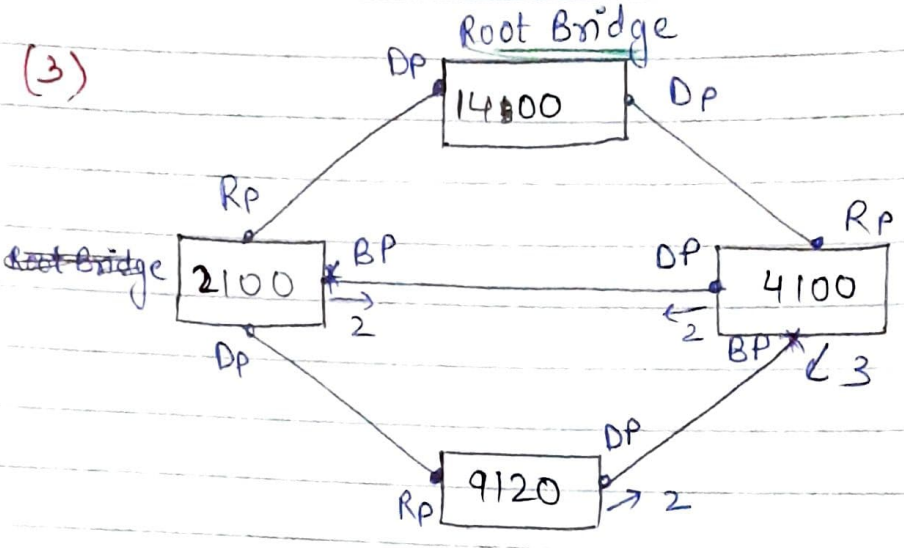
Blocked Port is a port which is having a highest cost path within the non-root bridges. (untouched link)

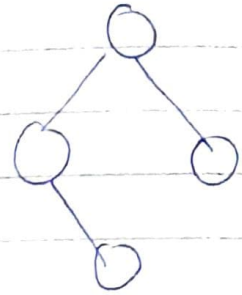
(2)



{ Equal path cost then choose with least MAC address

(3)

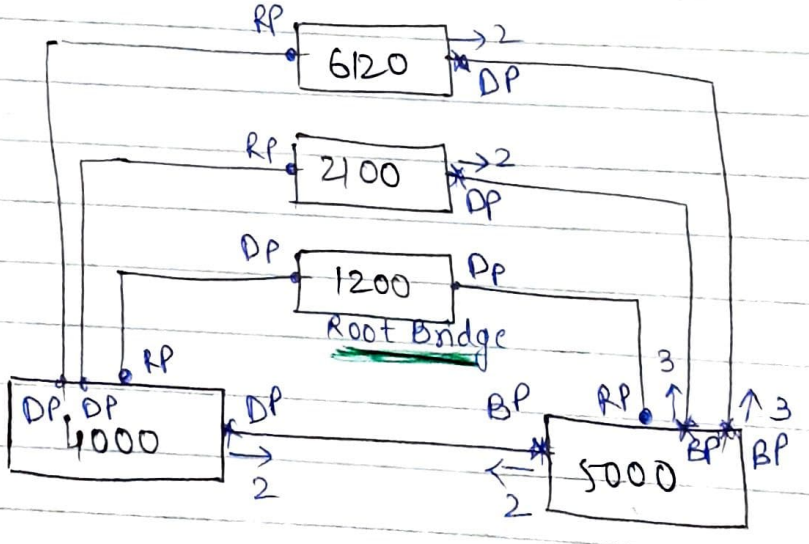


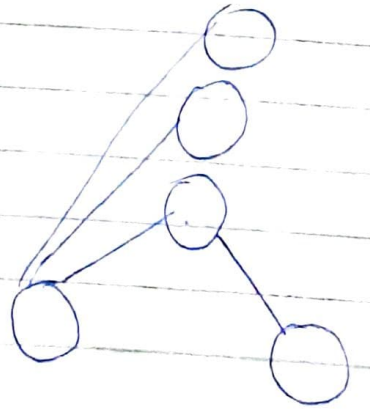


In Root Port if two equal path then go for the one with least MAC address out of the two is choosed.

In Blocked Port if two equal path cost come then the one with highest MAC address out of the two is choosed

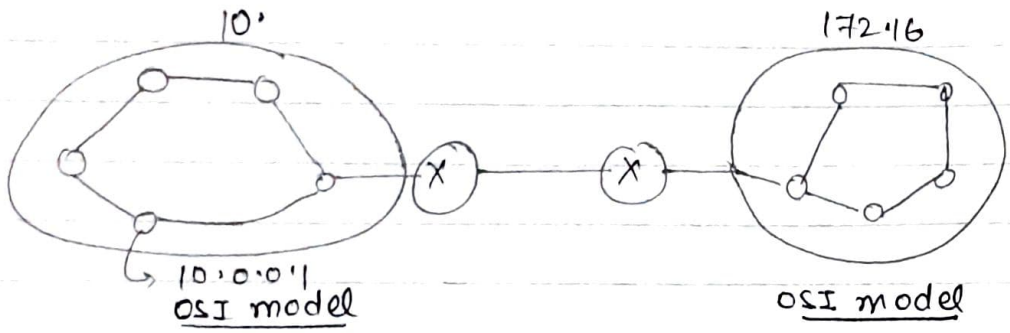
(4)





Router :-

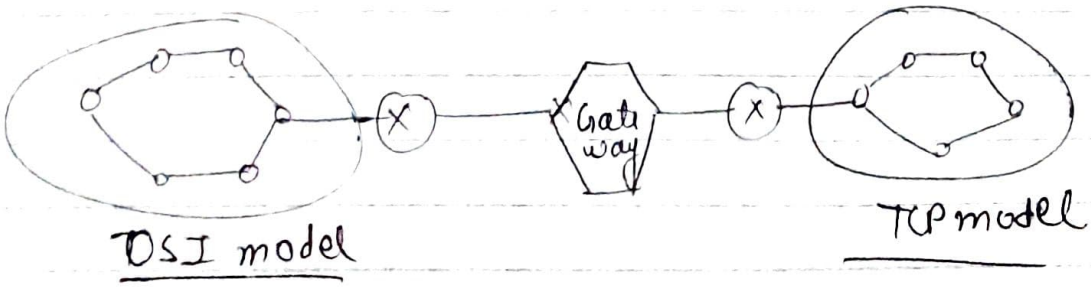
- By default router is a broadcast domain Seperator
- Router is a WAN device and its operation is based on IP address



- Router is used for connecting different networks
- By default router is a collision domain Seperator
- Router is not a multi-protocol converter because it cannot convert one model of packet into another model.

Gateway :-

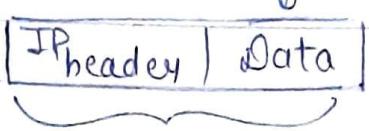
- Gateway is a multiprotocol converter because it can convert one model of packet into another model



NETWORK LAYER :->

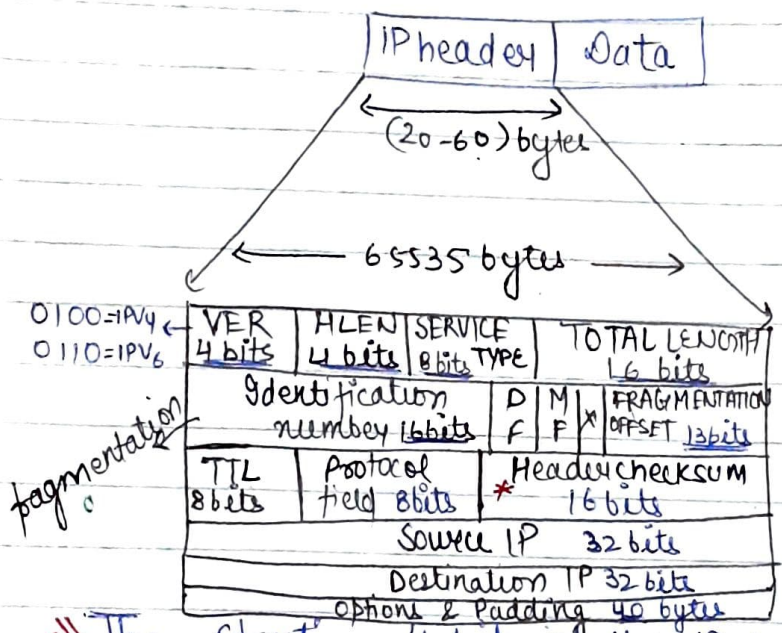
>IP Protocol

Transport ~~Application~~ Layer



TTL = time to live field value

MF = more fragment bit
= 1 {indicating I am not the last fragment}
= 0 {last fragment}



HLEN = 1010

Size of header = 10 rows * 4 bytes
= 40 bytes

DF = Do not fragment bit
= 1, Packet
= 0, fragment

» The starting 4-bits of the IP packet decides whether the packet is IPV4 or IPV6 (valid) and rest 14 are invalid conditions

HLEN

0000
0001
0010
0011
⇒ X

0100 → 4 rows * 4 = 16 ✗
0101 ⇒ 5 rows * 4 bytes = 20 bytes (min)
0110 ⇒ 6 rows
⋮
1111 ⇒ 15 rows * 4 bytes = 60 Bytes (max)

» Header length (HLEN) is going to indicate the size of header that is available in the packet

» SERVICE TYPE is going to indicate the type of service that is provided by router to the packet contain 3 bit → Precedence field, 1 bit Delay field, 1 bit Flags Throughput field, 1 bit Reliability and 2 unused bit

Q:- Total length bits are

00000000 11111111

Size of packet = 511

Q:- ⇒ HLEN = 1001

Size of header = 9 * 4

= 36 bytes

Packet size = header size + Payload (Data)

511 = 36 + x

x = 511 - 36

x = 475 bytes

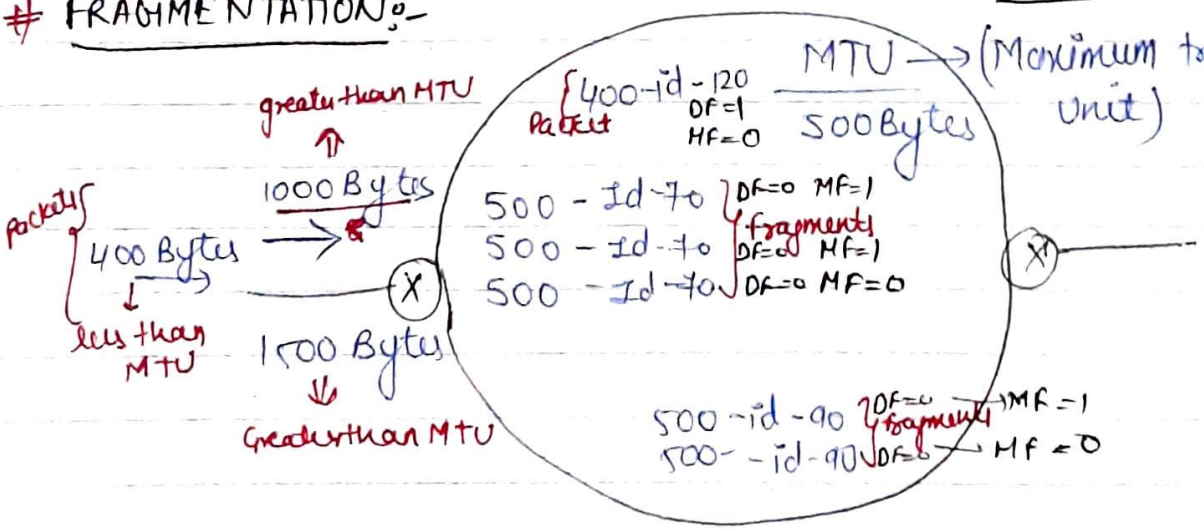
65535 bytes (20-60) bytes

» Both total length and header length bits are given. So, we can calculate the size of the data.

FRAGMENTATION:-

LAN

MTU → (Maximum transferable unit)

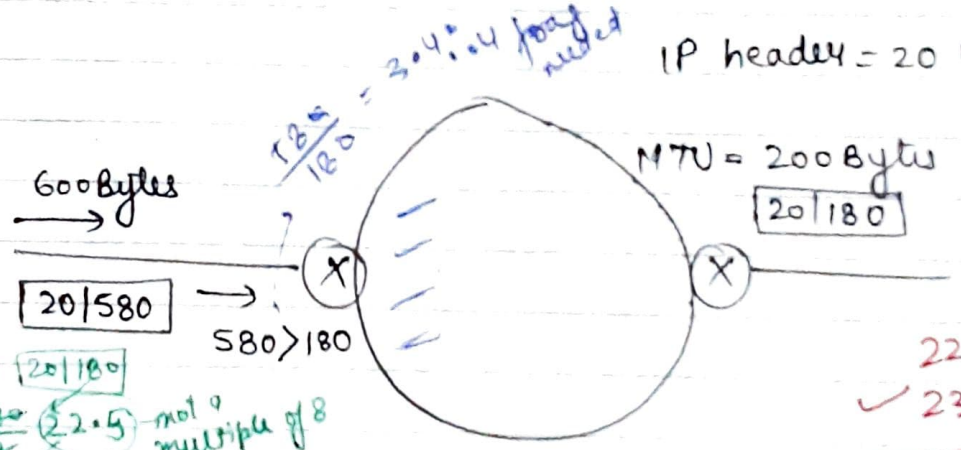


- Fragments belonging to same packets will given same identification number so that destination router can easily combine the fragments belonging to same packet.

- DF bit is going to indicate whether the content is packet or fragment. DF = 1 (Packet), DF = 0 (Fragment)

- For all intermediate fragments starting from 1st MF value is 1 especially for the last fragment MF value is 0

- Fragmentation offset is going to indicate the size of the fragment in the packet and the position of the fragment inside the packet



Q1

1) ⇒ MTU ⇒ 20|180

180/8 = 22.5 not a multiple of 8

Take 22 x 8 (176) multiple of 8

this 22 will be offset value.

22 x 8 = 176

23 x 8 = 184

580 − 3 x 176 = 52

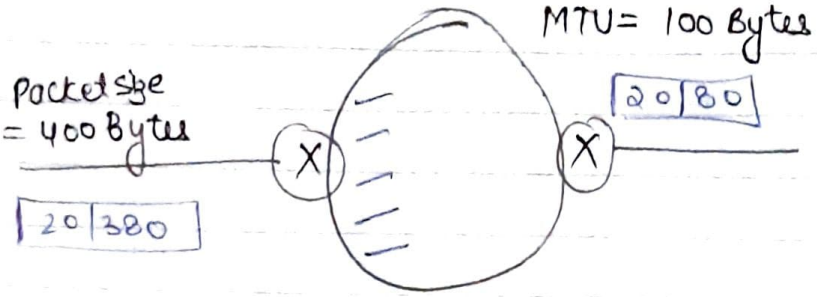
	1st frag	2nd frag	3rd frag	4th frag
id	90	90	90	90
DF	0	0	0	0
MF	1	1	1	0
fragment value	20|176	20|176	20|176	20|56
fragment offset	(0-21)	(22-43)	(44-65)	(66-72)

176/8 = 22 ⇒ fragment value

52 + 4 (Padding) = 56 (to get it multiple of 8)

(0, 22, 44, 66) ← offsets

Q2 IP header = 20 Bytes



	1st frag	2nd frag	3rd frag	4th frag	5th frag
fragment value	20|80	20|80	20|80	20|80	20|64
fragment offset	0-9	10-19	20-29	30-39	40-47

Padding: 60 + 4

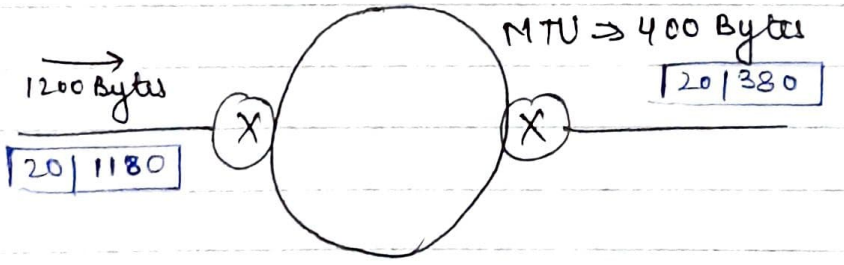
380 - 4×80
380 - 320
60

We add 4 as 60 is not a multiple of 8 but 64 is a multiple of 8

offsets = (0, 10, 20, 30, 40)

» If any padding bytes are added to the data that can be removed by identifying ~~bit~~ with MF bit as for last fragment MF = 0

Q3



47 - 5
1. 380
8
47 × 8 = 376

	1st frag	2nd frag	3rd frag	4th frag
fragment value	20|376	20|376	20|376	20|56
fragment offset	0-46	47-93	94-140	141-147

376 + 376 + 376 = 1128

1180 - 1128 = 52

not a multiple of 8

So, 52 + 4 = 56 → multiple of 8

offsets = (0, 47, 94, 141)

» The packet header is shared to all fragments with some change in value.

Q:- The fragment offsets are given as 0, 30, 60, 90 and all fragments are of equal size. IP header is of 20 bytes.

	frag 1	frag 2	frag 3	frag 4
fragment value	20 | 240	20 | 240	20 | 240	20 | 240
fragment offset	0 - 29	30 - 59	60 - 89	90 - 119

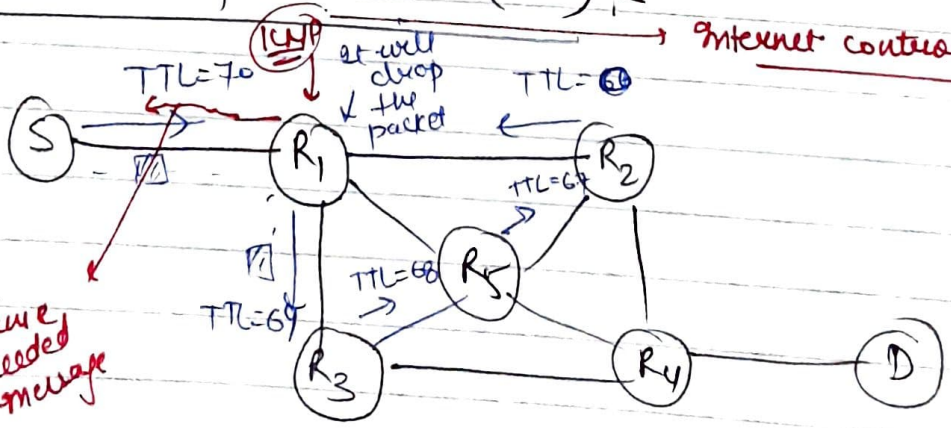
↳ coz they have mentioned that all are of same size

Packet size = 20 | 960

= 980

Time to live field value (TTL):-

Internet control message protocol



⇒ The purpose of TTL is to identify is there any loop exist for the packet or not

⇒ When the packet is forwarded in a wrong direction then there is a possibility of forming a loop for the packet then

⇒ At one point of time TTL value becomes 0 then the next router will drop the packet

⇒ The ICMP will take the source IP from the discarded packet and it informs to source by sending time exceeded message.

IP Protocol is connectionless, unreliable, best effort

IP Protocol

⇒ IP Protocol is a connectionless, unreliable (eg: router is forwarding to next router only), best effort delivery protocol.
IP doesn't have an error control so it depends on ICMP to provide error control

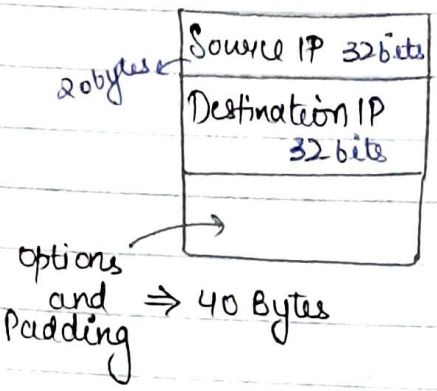
Protocol field is going to indicate the type of application of which the packet belongs to. (TCP, UDP etc)

Header checksum

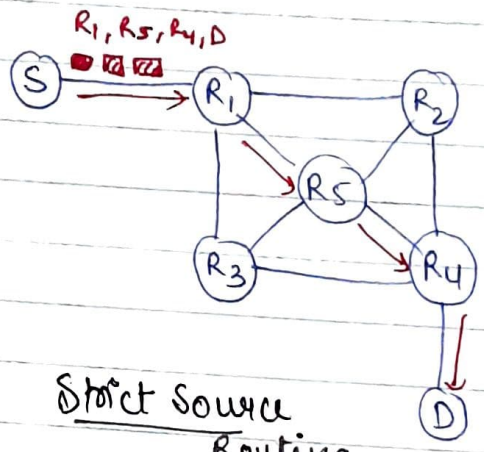
⇒ Checksum is provided only for the header because for the data it is already provided by TCP protocol at the transport layer

Checksum is provided only for the header so that the processing time is less, packet will be forwarded fastly

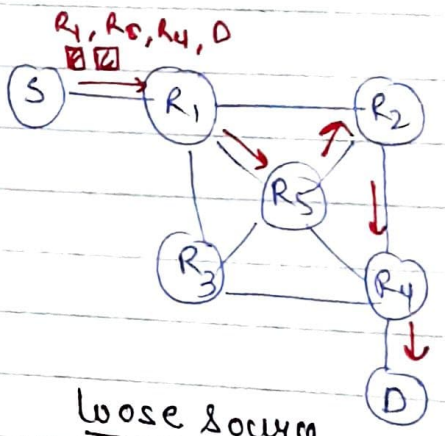
IP header is dynamic



(1) Source routing option :-



Strict Source Routing

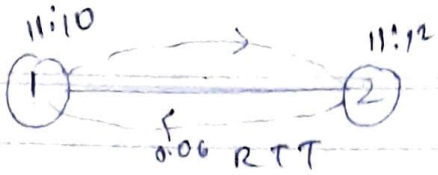


Wose Source Routing

- If the packets are strictly following the path that is specified by the source, it is known as Strict Source routing
- Along with the path that is specified by the source if some other paths are visited, it is known as loose source routing

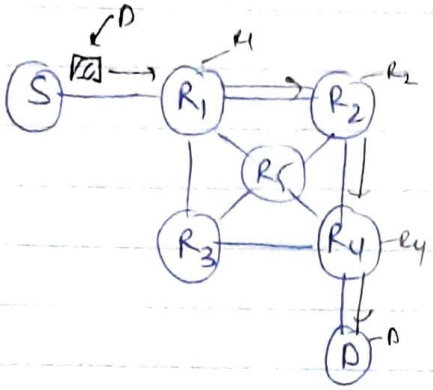
(2) timestamp option :-

It is used for calculating round trip time between two end systems



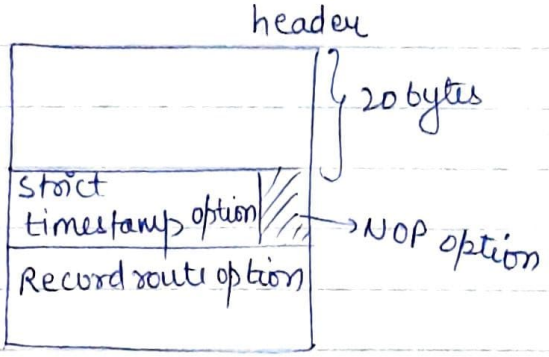
(3) Record route option :-

It is used for tracing the path



(4) NOP option :-

It is of 1 byte



NOP option is used to fill the gaps b/w options

(5) EOP option

↓ End of option

End of option is used as a seperator b/w header and data

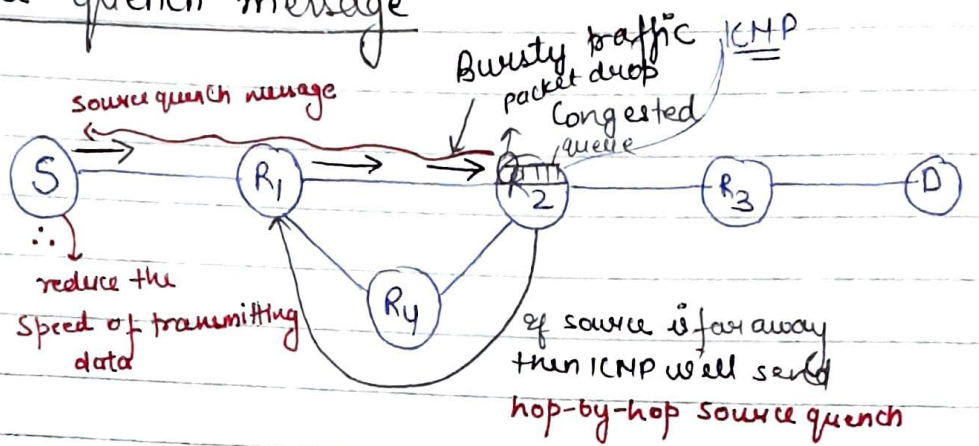
Whenever packet is dropped ICMP comes into picture

ICMP (Internet Control Message Protocol) :→

It is used for reporting errors and management queries.

ICMPv4
IPv4

(1) Source quench message



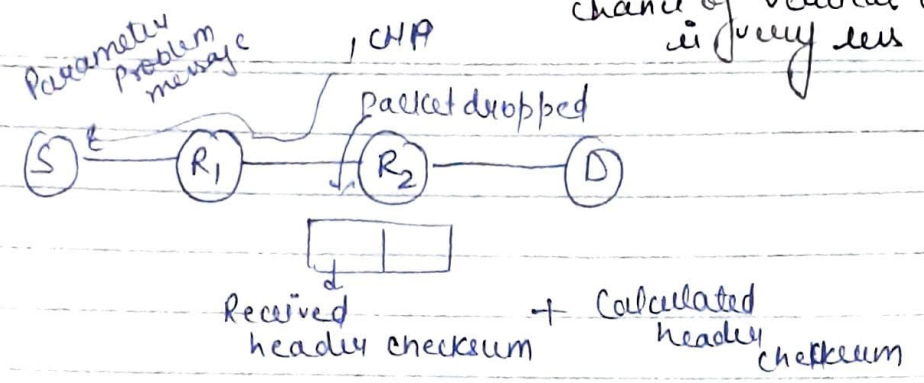
- Whenever a router is congested then some of the packet are dropped then ICMP will take the source IP from the dropped packet and informs to source by sending source quench message then the source will reduce the speed of transmission, so that congested router will free from congestion.
- When the congested router is far away from the source then ICMP will send hop-by-hop source quench messages then every router via that path reduce the speed of transmission

(2) Parameter Problem

IP header

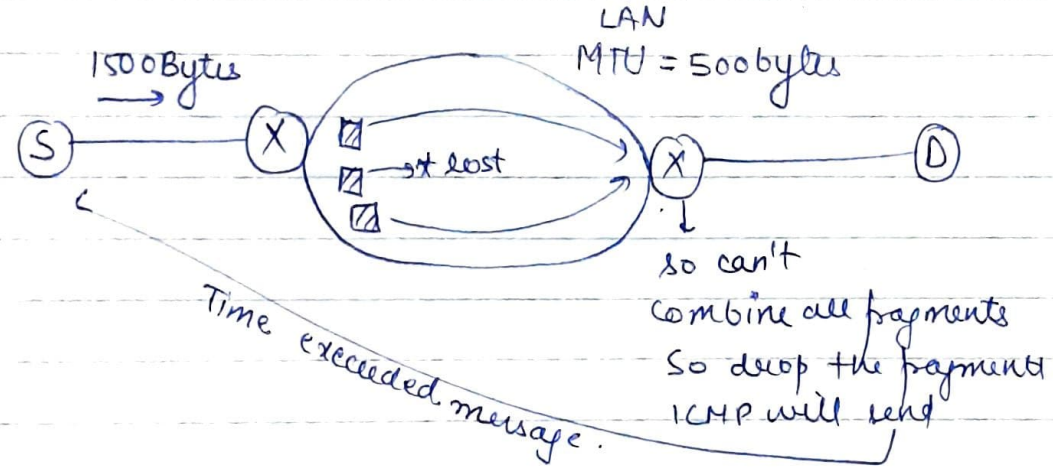
→ we can't use CRC coz header size is very large IP packet

→ we use header checksum coz chance of vertical bit errors is very less



Whenever a packet comes to a router, the calculated header checksum will not be equal to received header checksum when noise modified header checksum bits then ICMP will send parameter problem message

(3) Time-exceeded message

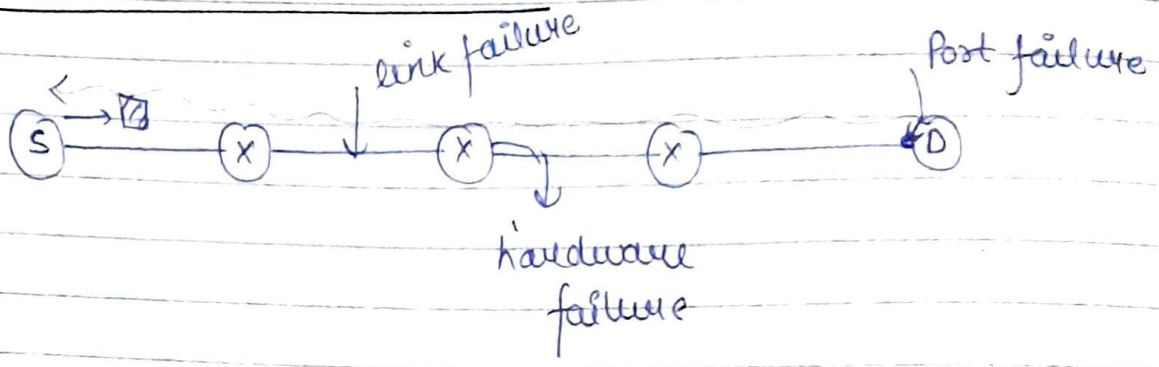


When some fragments are lost in the network then the holding fragments at the router are dropped.

Then ICMP will take source IP and informs to source by sending time exceeded message.

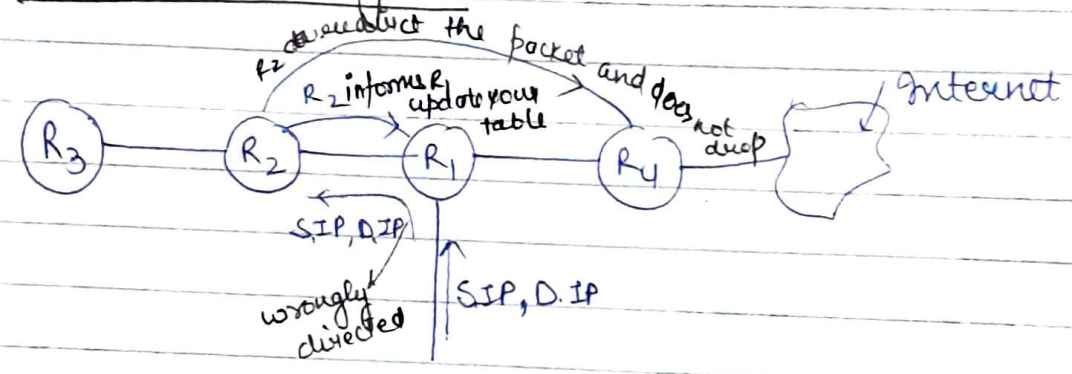
Ping is working with ICMP

(4) Destination unreachable



ICMP error messages are transmitted not only by the intermediate routers but also by destination host.

(5) Redirection Message



When a packet is directed in a wrong direction and later it is redirected in right direction then ICMP will send redirection message to update with correct entries.

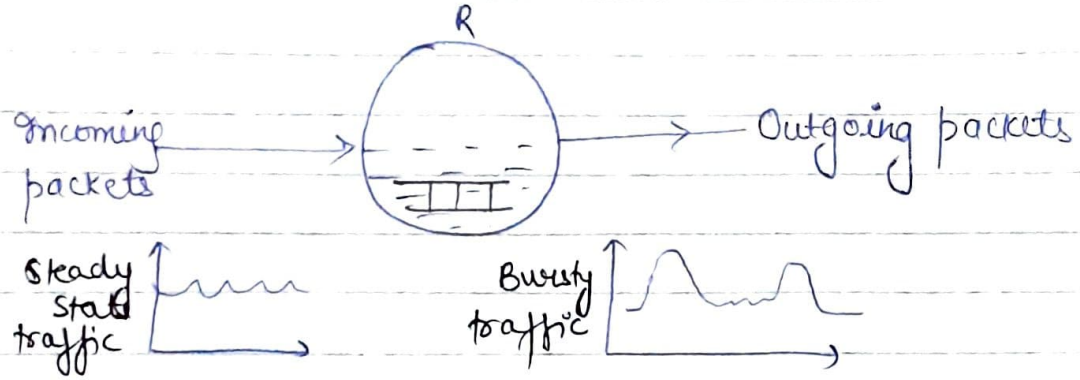
IP ensures there is an error control by using ICMP

- IP does not provide error control.
- IP ensures that there is a error control.

ICMPv6 (NDP) ⇒ Neighbour Discovery Protocol

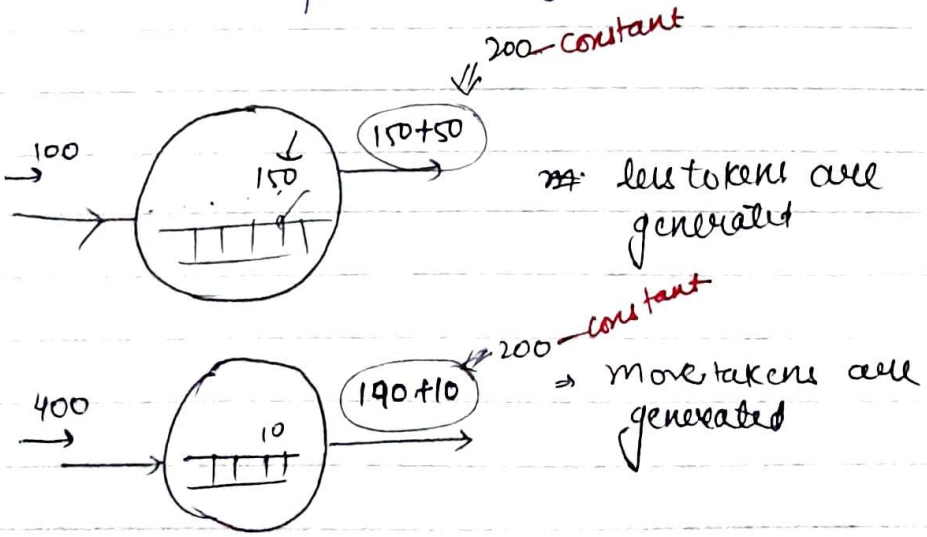
(6) Neighbour Solicitation Message.
(7) Router Solicitation Message.

Traffic Shaping



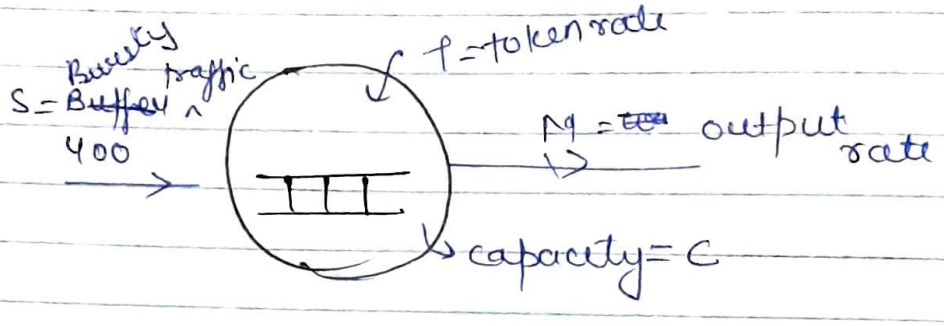
When there is a sudden increase in the traffic then it is known as bursty traffic.

When a o/p traffic state is steady state or steady, if the output rate is maintained at constant then it is known as Traffic shaping



whenever the packets are coming to the router, initial capacity is less then more tokens are generated, then more amounts of ~~money~~ data is transmitted.

If the packets are coming to the router, initial capacity is more, then less tokens are generated, then less amount of data is transmitted.



$$C + \rho S = MS$$

$2 + 998 = 1000$

$900 + 110 = 1000$

Q1:- Capacity = 1 Mbits

token rate = 6 Mbps

Output rate = 8 Mbps

Calculate Busty traffic time = ?

$$C + \rho S = MS$$

10^6 bits $+ 6 \times 10^6$ bits/sec $* S = 8 \times 10^6 *$

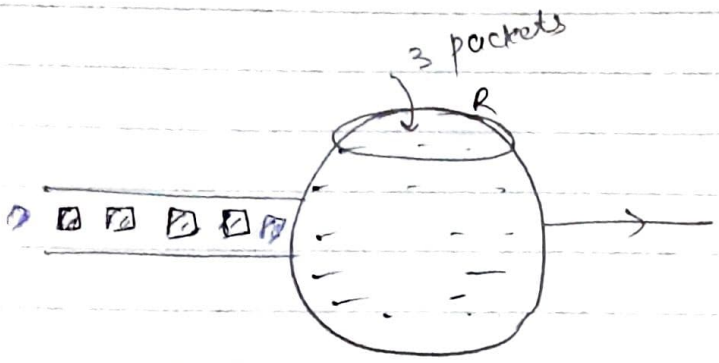
$10^6 [1 + 6] * S = 10^6 * 8S$

$2S = 1$

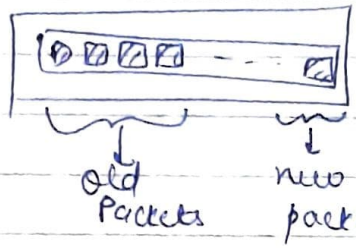
$S = \frac{1}{2}$

$S = 0.5$ sec

Load shedding :-

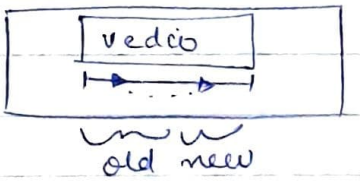


FTP



In FTP old packets are given more preference

Multimedia (vedio)

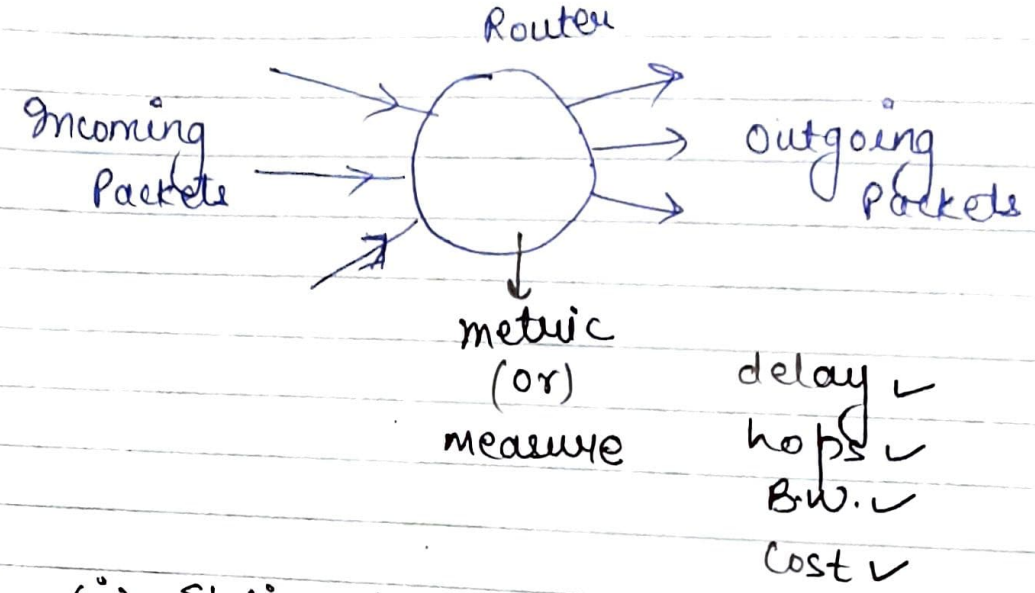


In multimedia new packets are given more preference.

Also known as MILK and WINE ; — old wine is given more preference
new milk is given more preference

- Load shedding is a way of loosing packets when the packets cannot be handled by routers
- Applications like FTP, preference is given to old packets
- Applications like Multimedia, preference is given to new packet

Routing Algorithms



(i) Static algorithms :-

- It doesn't consider any load on network.
- These algorithms can be called as non-adaptive algorithm
- eg:- Flooding algorithm

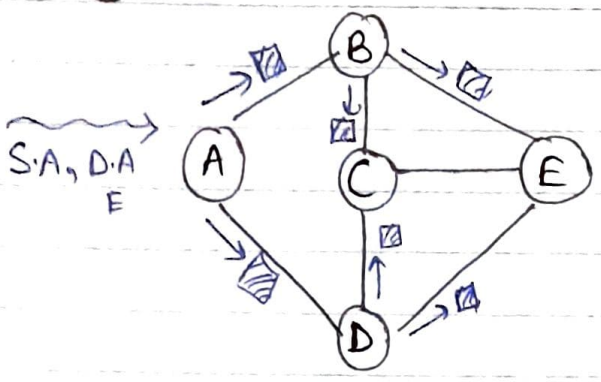
(ii) Dynamic algorithms :-

- It consider the load on network
- These algorithms can be called as adaptive algorithm
- eg:- (1) Distance vector routing algorithm
  (2) Link state routing algorithm
  (3) Path vector routing algorithm

one router to another router is called 1 hop

Static Algorithms :→

1) Flooding algorithm



•> All the Flooding is defined as whenever the packet comes to a router, it is diverted in all directions except the point of origin.

Flooding creates redundant packets

Flooding is used to find out unknown destination ie. IP address is known but physical location doesn't known.

logical address

Algorithm :-

1) Calculate all possible paths from A to E using flooding and using hops as metric.

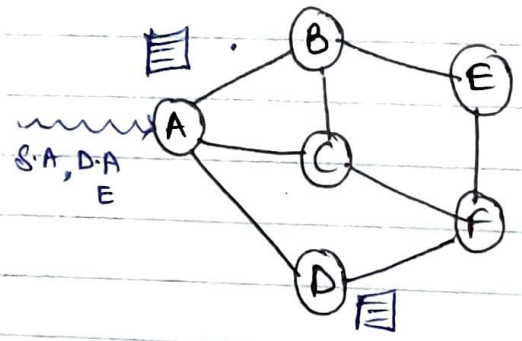
ABE = 2 hops	ADE = 2 hops
ABCE = 3 hops	ADCE = 3 hops
ABCDE = 4 hops	ADCBE = 4 hops

Flooding creates redundant packets which may lead to ~~conjunction~~ congestion of a router

The path of a packet will change even the destination address is same when new links are added or the existing links are broken

Dynamic algorithm :-

1) Distance vector routing :->



In distance vector routing whenever a packet comes to a router the neighbouring routers will give their vector tables then the new vector table is calculated for that node to forward the data.

It is also known as iterative algorithm because the output of the vector table is given as input for other routers for their calculations.

It is a distributed algorithm because routing tables are calculated for every node wherever the packet comes.

It is also known as Asynchronous algorithm because the routing tables given by the routers at different time interval

Vector table of B = (1, 0, 3, 2, 6, 5) (A B C D E F)
Vector table of C = (2, 4, 0, 1, 3, 4)
Vector table of D = (3, 1, 5, 0, 1, 2)

measured delay of A to B, C, D are 3, 2, 4

⇒ Vector table of A via B = (4, 3, 6, 5, 9, 8) (A B C D E F)

AA = AB + BA = 3 + 1 = 4
AB = AB + BB = 3 + 0 = 3
AC = AB + BC = 3 + 3 = 6

AD = AB + BD = 3 + 2 = 5
AE = AB + BE = 3 + 6 = 9
AF = AB + BF = 3 + 5 = 8

{ we are adding A delay in B vector table } → Trick

⇒ Vector table of A via C = (4, 6, 2, 3, 5, 6) (A B C D E F)

⇒ Vector table of A via D = (7, 5, 9, 4, 5, 6) (A B C D E F)

∴ Vector table of A = (0, 3, 2, 3, 5, 6) (A B C D E F)

{ A via B, C, D out of these take minimum }

⇓ via

(-, B, C, C, D, C)

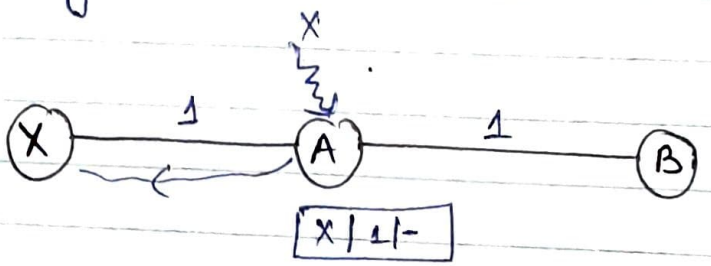
1) Distance vector routing works fine when there are no breakage of links
2) whenever there is a breakage of a link then there is a count to infinity problem.

⇒ Count to infinity problem :→

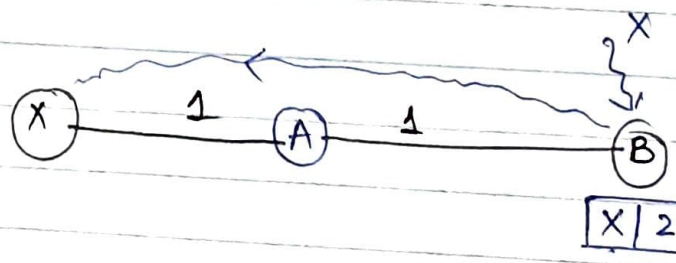
Initially the routing table of a router is empty

Every router will be knowing the directly connected routers without applying any routing algorithm.

Case 1

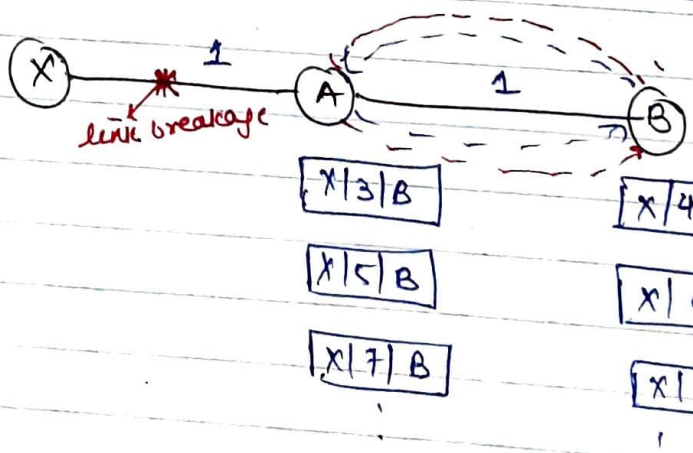


Case 2



upto here table is correct coz there is no link breakage

Case 3

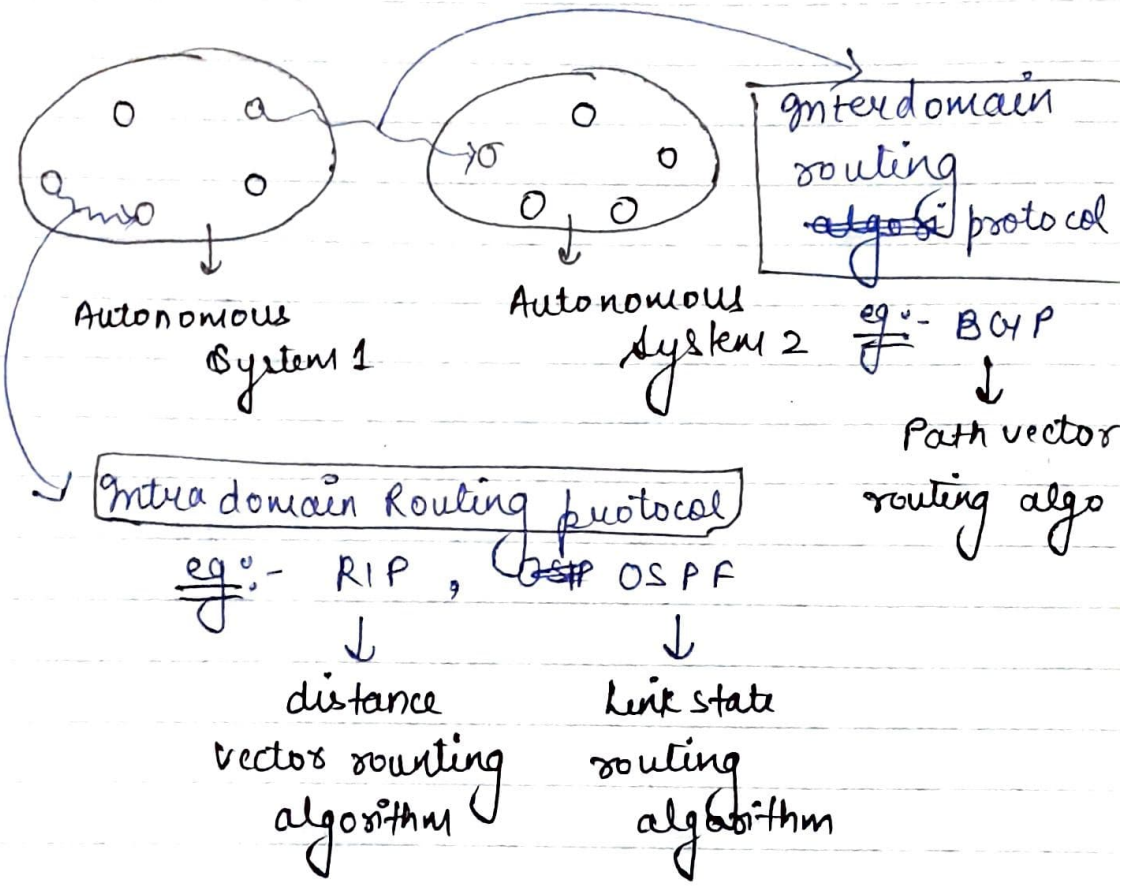


Here distance vector routing fails coz there is a link break as neighbours are given wrong information

Definition

1) Whenever there is a broken link the neighbouring routers are given a false information that they know how to reach a broken link

2. This information is given to other routers then that routers are also filled with wrong entries finally the network will collapse. This problem is known as Count to infinity problem



RIP :- Rating Information Protocol
OSPF :- open shortest path forwarding
BGP :- Border Gateway protocol.

If the packets are routed from router in one autonomous system to a router in same autonomous system it is known as Intradomain routing protocol

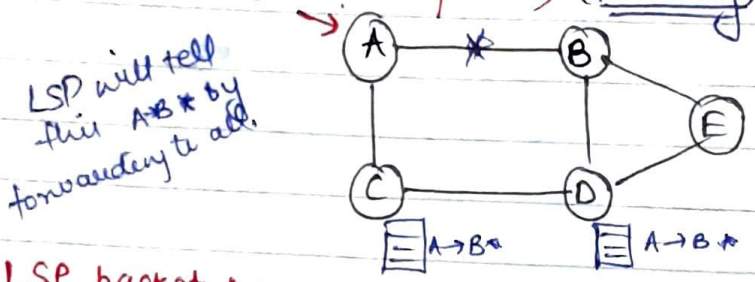
If the packets are routed from router in one autonomous system to a router in another autonomous system, it is known as Inter domain routing protocol

2. Link State routing algorithm :-

1. In distance vector routing, the algorithm is applied directly on data packets whereas in link state routing, the algorithm is applied on control packets (LSP packets)

link state packet

LSP (Link state packet) (Flooding)



LSP packet :→

LSP packet contains complete information of the ~~packet~~ network i.e. no. of routers, no. of links, UP and DOWN links (working & not working), LAN networks that are connected.

{ Flooding cause redundancy and due to which congestion occur so before flooding LSP apply shortest path tree algorithm. }

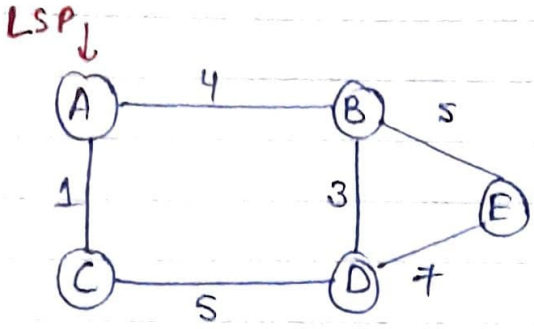
LSP packet should be generated periodically with the latest information.

LSP packet should be given to all the routers using flooding algorithm

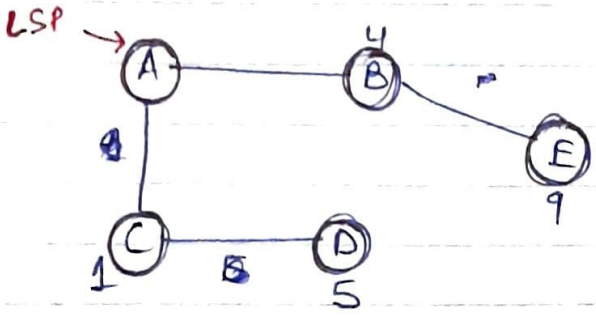
Before applying flooding graph should be converted into tree using shortest path tree algorithm (Dijikstra's algo)

Shortest Path tree

1)

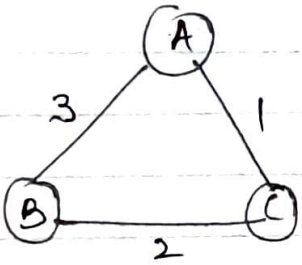


Here we may find loop or congestion problem

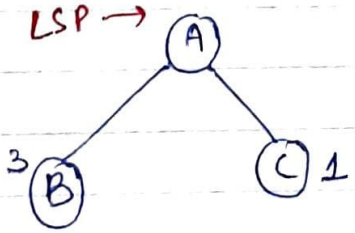


But here there will be no cycle and so no congestion problem

2)



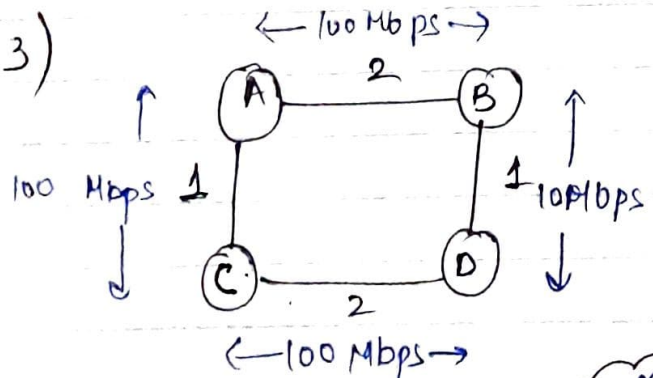
⇒ Convert this graph into tree.

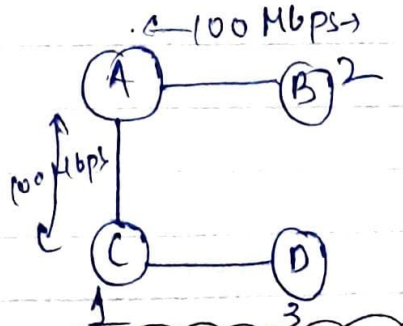


Here delay fails so go for hop metric

If I go A → C → B then 2 hop
If I go A → B then 1 hop.

3)

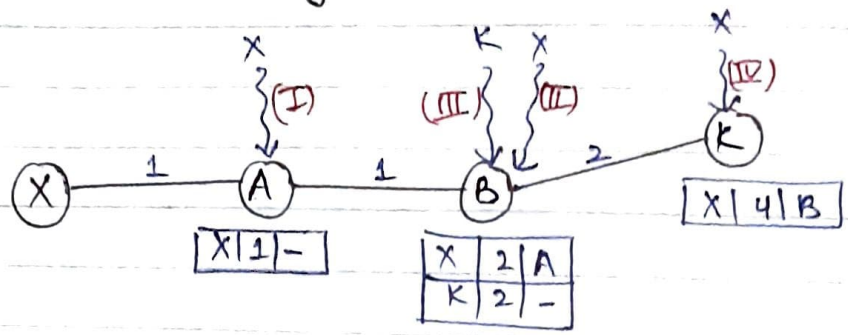


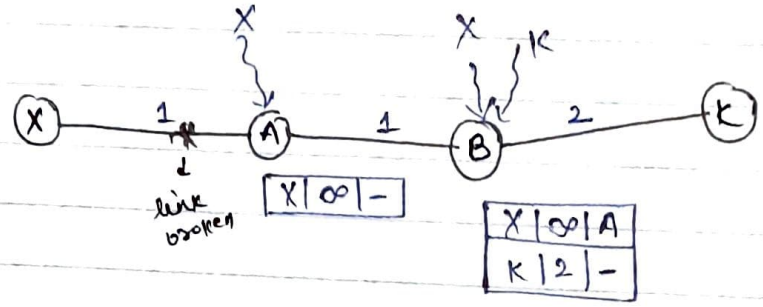


Here delay fails, hop fails
∴ So BW will work more BW will be taken

Special Case :→

* # Distance vector routing with split horizon :→





In 1st iteration A will know that X can not be reached as A is directly connected and not other routers will know this In order to inform all routers about this (link broken) it will take O(n) time.

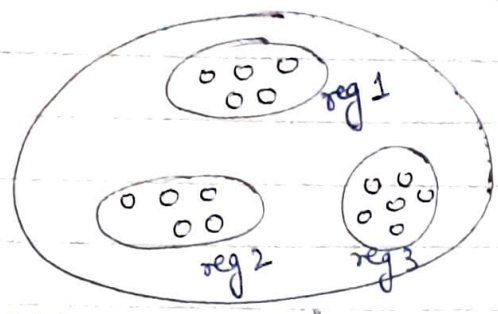
Using distance vector there is a count to infinity Problem

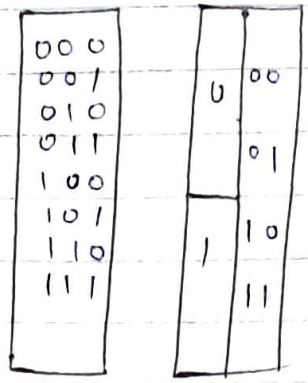
Using distance vector with split horizon there is no count to infinity problem.

Distance vector is a slow conversions algorithm because when a link is broken it will take O(n) time to know by all routers

Link state routing is a fast conversions algorithm because when a link is broken it will take O(1) time to know by all routers using LSP.

* Hierarchial routing





select any one

Case (1) 16 Comparisons

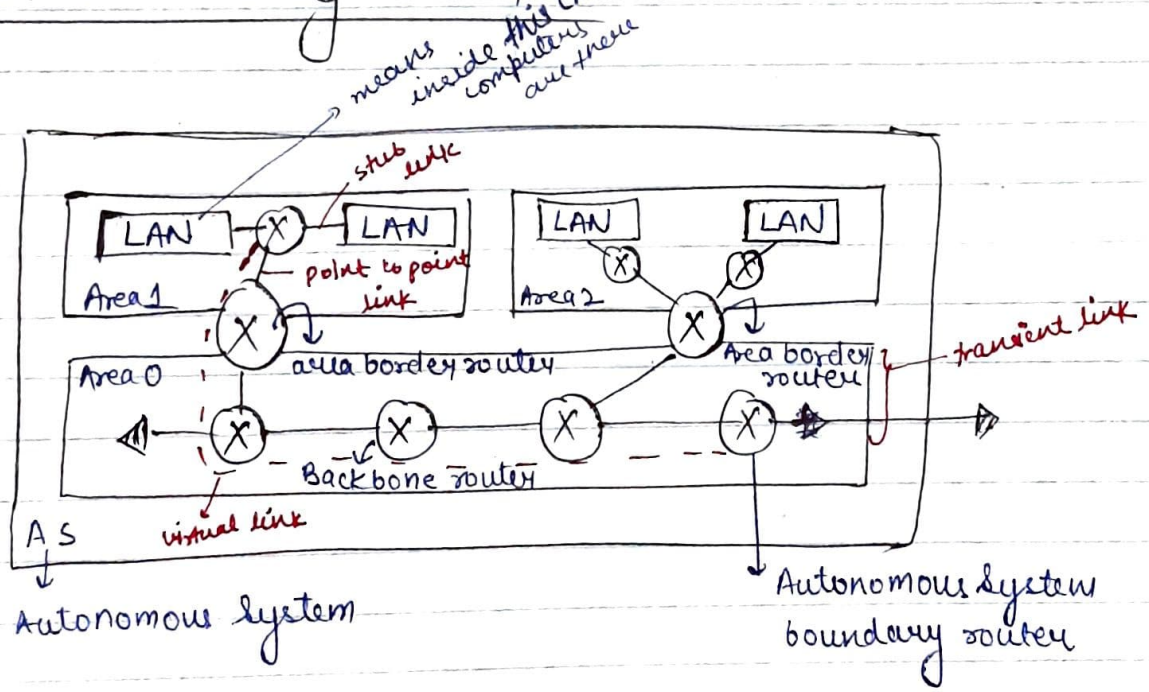
Case (2) 1 + 6 = 7 Comparison

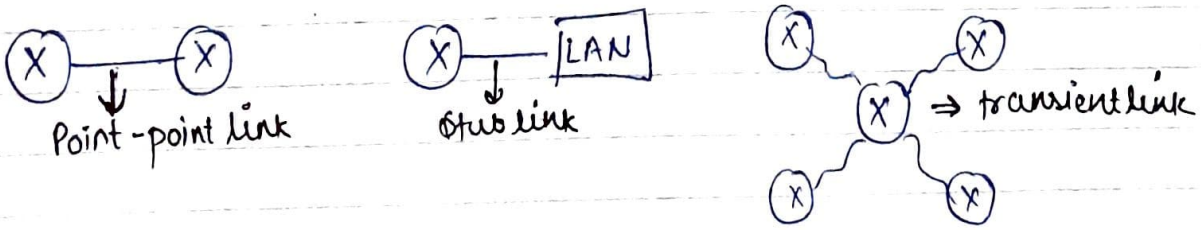
Case 1 — 8 comp

Case 2 — 2+4 = 6 comparison

* Using hierarchial routing logically the table size is reduced so that searching time is less and the packet can be forwarded fastly

Intradomain routing Problem

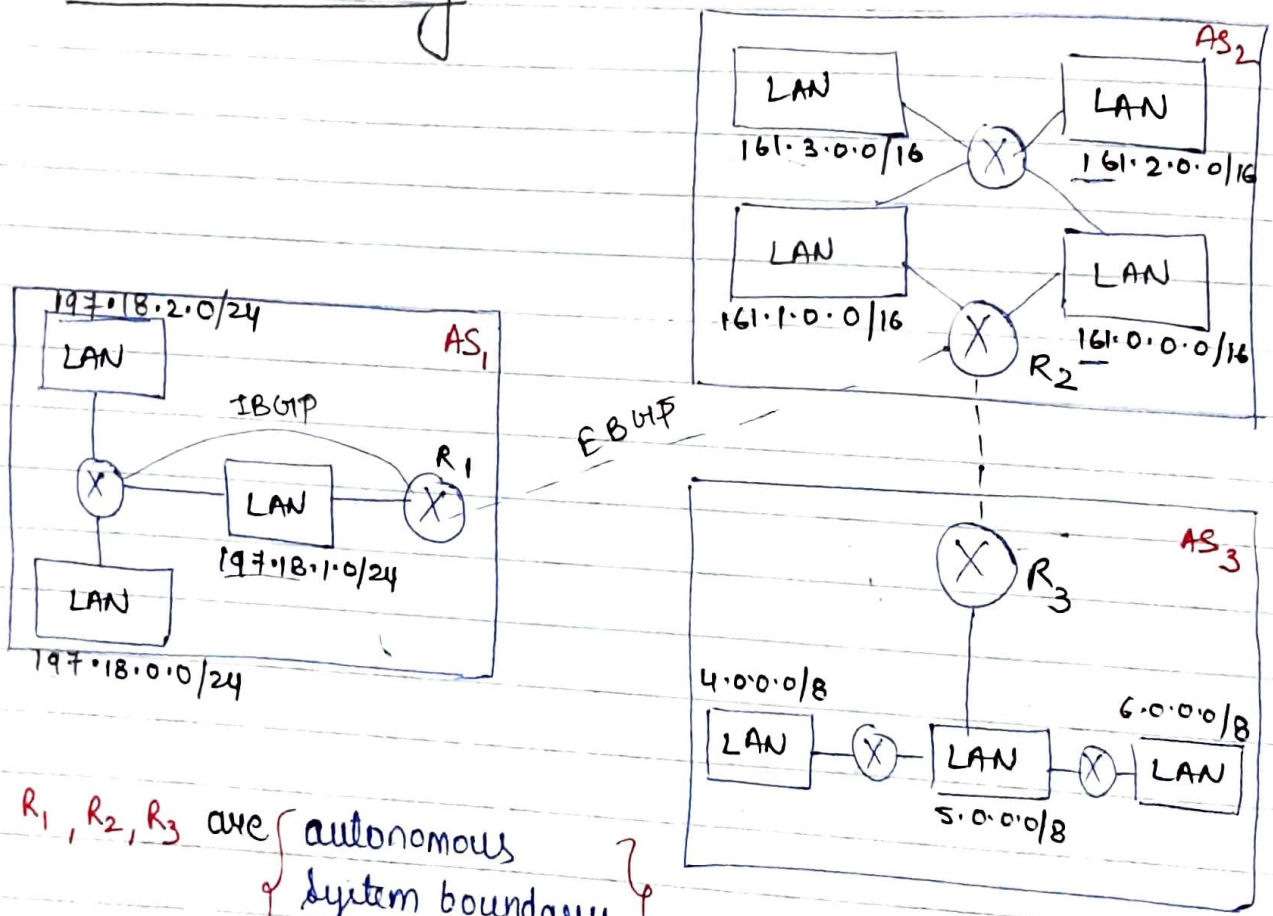




167 Virtual link is the (Physical) actual link but its purpose is to provide fault tolerance. (In case of link failure)

- Area border router is used for connecting area 0 with other areas
- Autonomous System boundary router is used for connecting different autonomous system.
- Whenever a link fails, data will be directed via virtual link

Path Vector Routing



R_1, R_2, R_3 are { autonomous system boundary router (or) External routers }

Border Gateway Protocol

BGP

IBGP EBGP

R1

Network	Path
197.18.0.0/24	AS_1
197.18.1.0/24	AS_1
197.18.2.0/24	AS_1
161.0.0.0/16	$AS_1 \rightarrow AS_2$
161.1.0.0/16	$AS_1 \rightarrow AS_2$
161.2.0.0/16	$AS_1 \rightarrow AS_2$
16.3.0.0/16	$AS_1 \rightarrow AS_2$
4.0.0.0/8	$AS_1 \rightarrow AS_2 \rightarrow AS_3$
5.0.0.0/8	$AS_1 \rightarrow AS_2 \rightarrow AS_3$
6.0.0.0/8	$AS_1 \rightarrow AS_2 \rightarrow AS_3$

Subnet mask

Supernet mask

Network	Path
197.18.0.0/22	AS_1
161.0.0.0/14	$AS_1 \rightarrow AS_2$
4.0.0.0/6	$AS_1 \rightarrow AS_2 \rightarrow AS_3$

197.18.0.0/24 $\Rightarrow AS_1$

0.0 = 00000000.00000000 } 2^8 (H)
00000000.11111111

1.0 = 00000001.00000000 } 2^8
00000001.11111111

2.0 = 00000010.00000000 } 2^8
00000010.11111111

$2^{32-22} \leftarrow 2^{10} \leftarrow 4 \times 2^8 \leftarrow (3) * 2^8$

Supernet mask

But this should be in power of 2

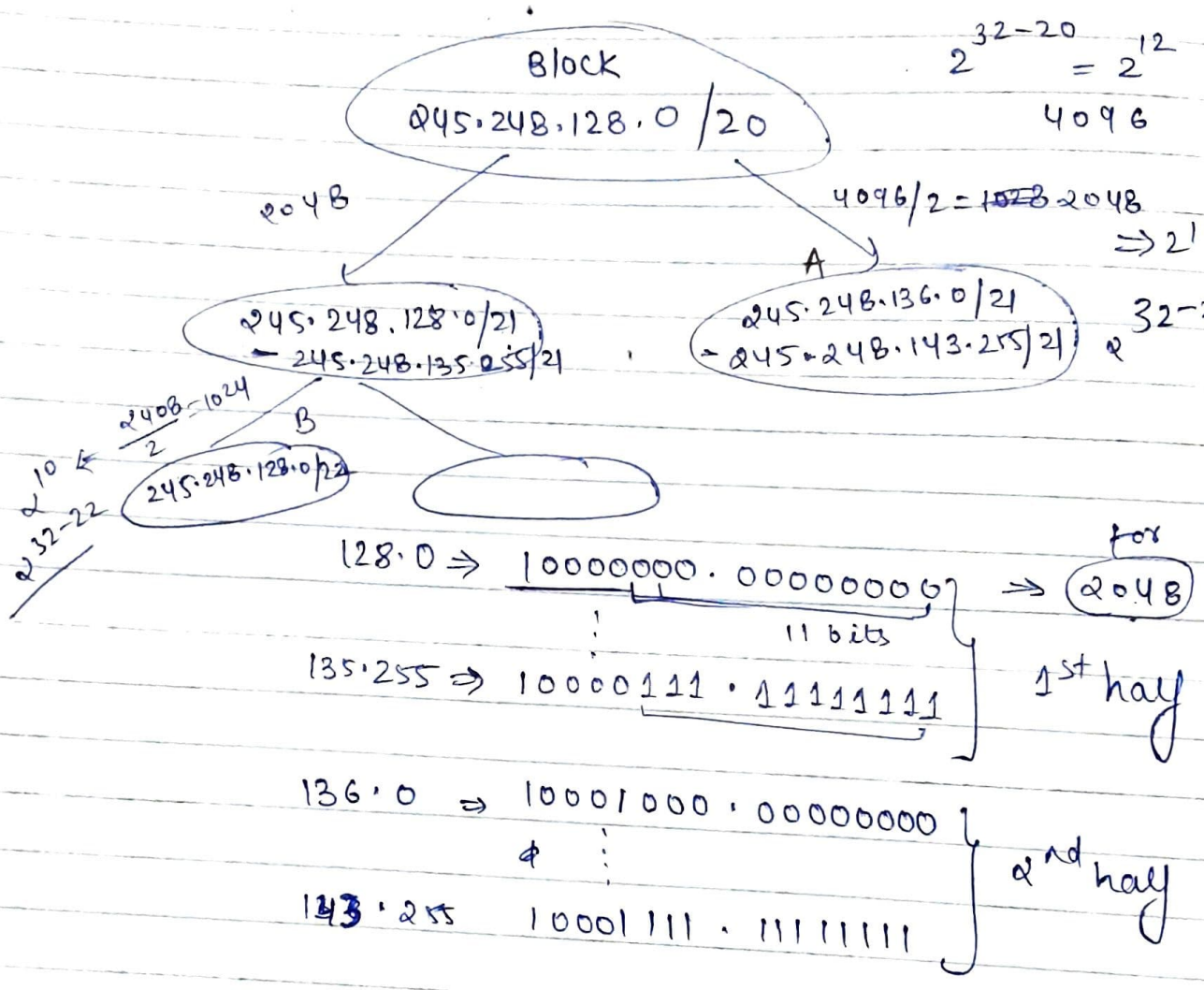
External router will get the information about its own n/w with the help of internal router

External router will get the information about other autonomous systems with the help of other external routers

Workbook

IP addressing (Chapter-1)

TG:→

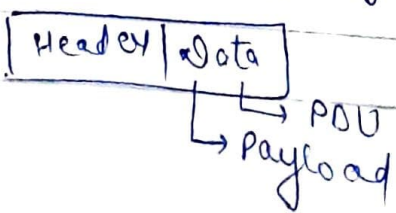


Data link layer:-

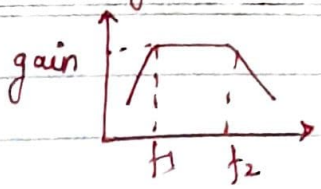
(1) DLL → LLC
DLL → MAC ↳ (NIC card)

∴ option (c)

(2) LLC sublayer (or) any layer will have ∴ option (c



Bandwidth = Range of frequency over which gain is constant



Q3:-

$BW = 20\ Hz$

$BW = f_2 - f_1$

i.e. BW = Upper frequency − lower frequency

$20\ Hz = 60\ Hz - x$

$x = 60\ Hz - 20\ Hz$

$\boxed{x = 40\ Hz}$

Q4:-

Data ⇒ 1010111011110011

	row parity
1010	0
1110	1
1111	0
0011	0
Column Parity 1000	1

Write down the entire data row wise

1010011101111000110000

Parity for this data | Parity | Parity | Parity | Parity for entire data at the end

So this is two-dimensional parity Check because we are calculating row parity and column parity.

∴ option (b)

Q5:-

$l = 3000\ km$

propagation speed = $6\mu sec/km$

(T_1) B.W ⇒ 1.544 Mbps

frame size = 64 bytes

$1\ km = 6\mu sec$

$3000\ km \Rightarrow 18$ millisec

$Pt \Rightarrow 18$ millisec

$RTT \Rightarrow 36$ millisec

From BW → 1 sec ⇒ 1.544×10^6 bits

From RTT 36 millisec ⇒ $36 * 10^{-3} * 1.544 * 10^6$ bits

no. of bits in RTT ⇒ $(36 * 1544)$ bits

Window size = no. of frames in RTT

$$= \frac{36 * 1544 \text{ bits}}{64 * 8 \text{ bits}}$$

$$= 108.56$$

$$= 109$$

∴ option (C)

Q6: GO Back N ARQ

$SWS < 2^m$

	SWS	RWS
6 bits ⇒ $2^6 = 64$	63 ✗	1
7 bits ⇒ $2^7 = 128$	127 ✓	1

∴ option (C)

Q7: average transmission rate

$$\text{Throughput} = \frac{\text{Data Size}}{TT + 2 * PT}$$

RTT = 2 seconds

BW = 10^5 bits/sec

Transmission time (TT) = $\frac{\text{Data Size}}{BW}$

$= \frac{100 \text{ bits}}{10^5 \text{ bits/sec}}$

$(TT) = 10^{-3} \text{ sec}$

Throughput $= \frac{100 \text{ bits}}{10^{-3}\text{sec} + 2 \text{ sec}}$ → RTT = 2×PT

$= \frac{100 \text{ Bits}}{2.001 \text{ sec}}$

$= 49.97 \text{ bits/sec}$

∴ option (b)

Q8:→

Link Utilization = $\frac{\text{throughput}}{BW}$

$= \frac{49.97}{10^5}$

$= 0.0005$

∴ option (a)

Q9:- Data size = 53 bytes

RTT = 60 millisec

BW = 155 Mbps

↳ 1 sec = $155 * 10^6$ bits

RTT → $60 * 10^{-3}$ sec ⇒ $60 * 10^{-3} * 155 \times 10^6$ bits

no. of bits in RTT ⇒ $(60 \times 155 \times 10^3)$ bits

$$\text{Window size} = \frac{60 * 155 * 10^3}{53 * 8}$$

$$= 21,934$$

option (d)

Q10:-

For maintaining same window size selective repeat ARQ requires more sequence bits compared to Go Back N

Window size = 30

Go back N ARQ

no. of sequence bits = 5 bits

$= 2^5 = 32$

→ Selective repeat ARQ = 6 bits

6 bits $= 2^6 = 64$

$SWS \leq 2^{m-1}$

SWS / 32 — RWS / 32

option (d)

64-1=8

Q11:- option (a)

Q4:-

Capacity = 6 bits/sec

frame size = 1 bits

RTT = R sec $\Rightarrow 2 * PT$

$$U = \frac{TT}{\text{Total time}} \quad \text{or} \quad = \frac{TT}{TT + 2PT}$$

$$\text{Total time} = \frac{\text{frame size}}{\text{Capacity}} = \frac{1}{b}$$

$$U = \frac{1/b}{1/b + R}$$

LAN → PT = $\frac{l}{v}$ → small

∴

TT ∝ PT

TT >>> PT

TT ↓ high, PT ↓ less

WAN

PT = $\frac{l}{v}$ → large

TT <<< PT

∴ l ↓ less, l ↓ more

In LAN

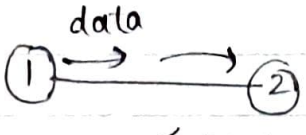
Window size = no. of frames in RTT

This area is small ∴ TT large, PT small.

means you are transmitting upto the value of RTT

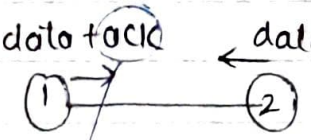
In WAN

Here area large ∴ TT small, PT more.



(data + ack)

↳ half duplex piggybacking



This is an ack for the previous data send by (2)

full duplex with piggybacking

$1 * \frac{TT}{TT+2*PT}$ → stop and wait ARQ

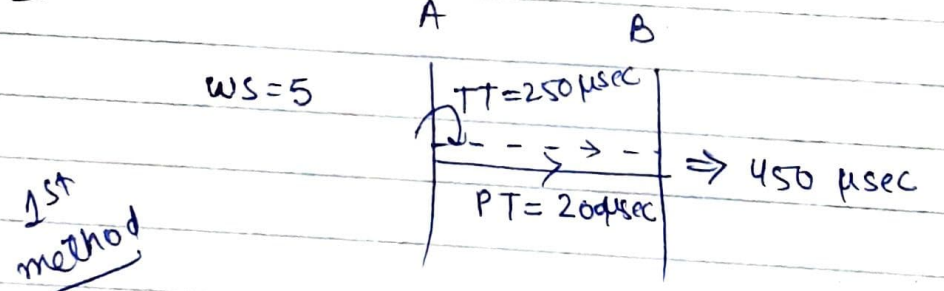
$N * \frac{TT}{TT+2*PT}$ → Go Back N ARQ

Piggybacking

Sending the data along with acknowledgement is known as piggybacking.

The advantage of piggybacking is effective channel utilization.

Q15:-



1st method

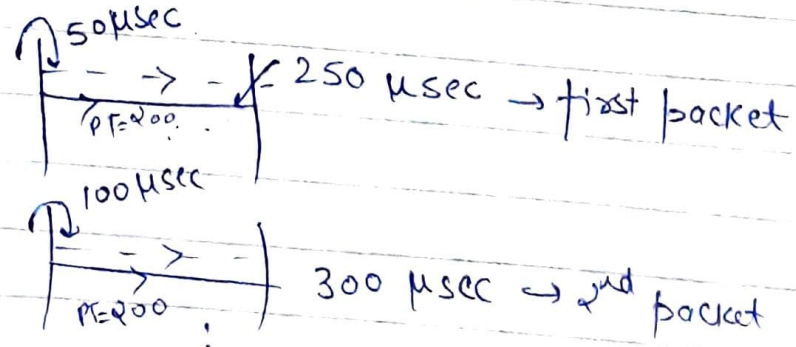
TT of one packet = 50 μsec

TT of 5 packet = 5*50 μsec

= 250 μsec

∴ option (d)

2nd method



16 maximum throughput = $\frac{\text{Data size}}{\text{Total time}}$

$= \frac{5 * 1000 \text{ bytes}}{450 \mu\text{sec}}$

∴ option(b) $= \frac{5000}{450}$ $11.11 * 10^6$ bytes/sec

17:-

$G(x) = x^4 + x + 1$

$= 1 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x^1 + 1 \cdot x^0$

$= 10011$

∴ option (b)

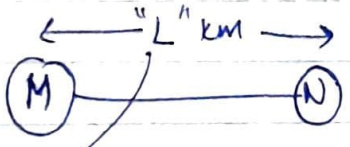
$M(x) = x^7 + x^6 + x^4 + x^2 + x$

$= 1 \cdot x^7 + 1 \cdot x^6 + 0 \cdot x^5 + 1 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x^1 + 0 \cdot x^0$

$= 11010110$

18 (C)

Q19:-



frame size = K bits

P.d = "t" sec/km

B.W = "R" bits/sec

1 km = "t" sec

L km ⇒ (Lt) sec

P.t ⇒ (Lt) sec

RTT = (2Lt) sec

From BW: 1 sec = "R" bits

From RTT: (2Lt) sec ⇒ (2LtR) bits

no. of bits in RTT ⇒ (2LtR) bits

$$\text{Window size} = \left(\frac{2LtR}{K}\right)$$

$$\text{no. of Sequence bits} = \log_2(1+Q)$$

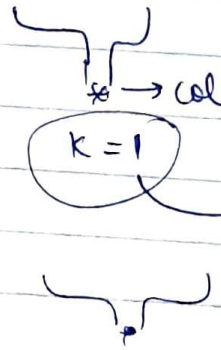
Q: window size

$$= \log_2\left(1 + \frac{2LtR}{K}\right)$$

∴ option (c)

$$= \log_2\left(\frac{K + 2LtR}{K}\right)$$

Q20:



at what time collision is occurring

1

min (n, 10)

= 1

min (2, 10)

= 2

min (n, 10) = (1, 2, 3, 4, 5, 6, 7, 8, 9)

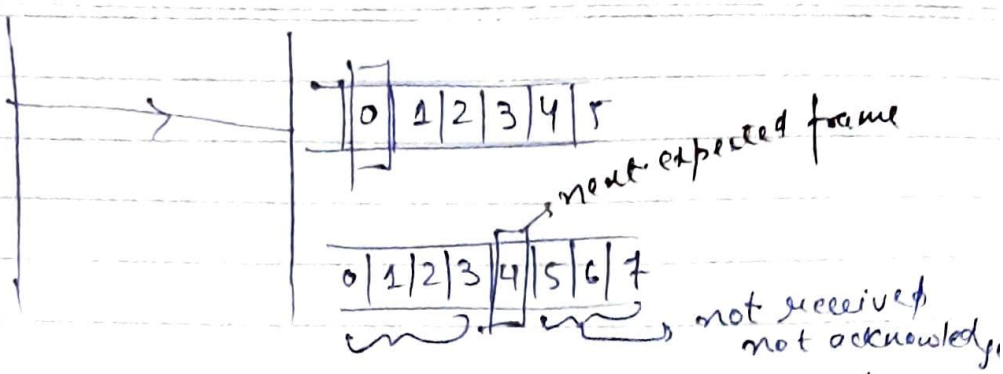
max (n, 10) = (10, 10, 10 ... ∞)

Every time 10 we are applying but this is not so

∴ option (b)

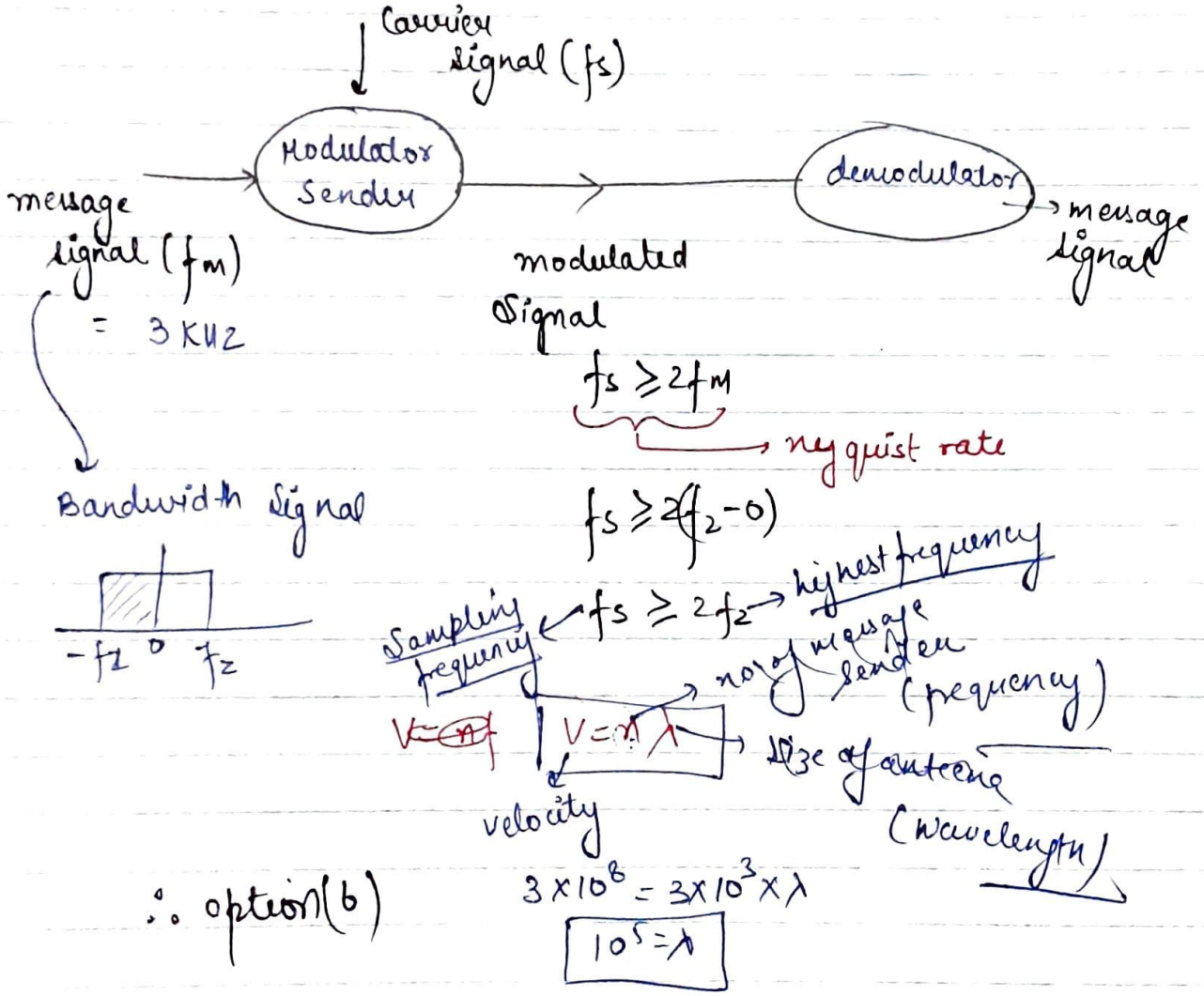
Q21:- option (d)

Q22



∴ option (b)

Q23 :→ Communication &



∴ option (b)

Q24 :→ option (a)

Q25 :- option (c)

Q26 :- option (a)

Q27 :→

$$TT = \frac{\text{frame size}}{BW}$$

$$= \frac{16\ Kb}{100\ Mbps}$$

$$= \frac{16 \times 10^3 \text{ bits}}{100 \times 10^6 \text{ bits/sec}}$$

$$= \frac{16 \times 10^3}{10^8}$$

$$= 16 * 10^{-5} \text{ sec}$$

$$T.T. = 160 \mu sec$$

$$P.T = \frac{l}{v} = \frac{24 * 10^3 \text{ m}}{3 * 10^8 \text{ m/sec}}$$

$$= 8 * 10^{-5} \text{ sec}$$

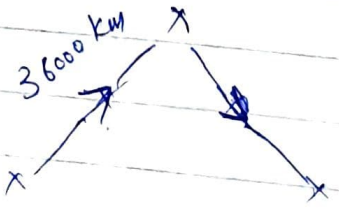
$$PT = 80 \mu sec$$

Since $TT = 2 * PT$

$\therefore$ LU = 50% (this we know

$\therefore$ option (b)

Q28 :→



$$PT = \frac{2 * l}{v}$$

$$PT = 2 * \frac{36000 * 10^3}{12000} \text{ m}$$

$PT = 24 * 10^{-2}$ sec

% LU = 50%

$$50 = N * \frac{TT}{TT + 2*PT} \times 100\%$$

$N \downarrow 100$

$$\frac{1}{50} = 100 * \frac{TT}{TT + 2*PT} \times \frac{2}{100}$$

$$TT + 2*PT = 200\,TT$$

$$2*PT = 199\,TT$$

$$2 * 24 * 10^{-2} = 199 * \frac{\text{Data size}}{10^7 \text{ bits/sec}}$$

$$\text{Data size} = \frac{2 * 24 * 10^{-2} * 10^7}{199}$$

$$= 24.1 * 10^3 \text{ bits}$$

$$= 24.1 \text{ Kbits}$$

$$= \frac{24.1}{8} \text{ bytes}$$

$$= 3 \text{ bytes}$$

∴ option (b)

Q29 :- option (d)

Q30 :- option (c)

Q31 :- option (d)

Q32:→ Selective Repeat ARQ = 7 bits

$2^7 \Rightarrow 128$

$\frac{S.WS}{64}$ $\frac{RWS}{64}$

∴ 64

Q33:→

$$TT = \frac{\text{Data size}}{BW}$$

$$= \frac{5000 \text{ bits}}{9000 \text{ bps}} = \frac{5}{9}$$

$$P.T = \frac{l}{v} = \frac{2000 \text{ km}}{2 \times 10^5 \text{ km/sec}}$$

$$= 10^{-2} \text{ sec}$$

$$\% \text{ LU} = \frac{TT}{TT + 2*PT} \times 100\%$$

$$= \frac{5/9}{5/9 + 2*10^{-2}} * 100\%$$

$$= 96.5\%$$

$$= 97\%$$

Q34:→

Data size = 32 bytes

RTT = 80 millisec

B.W = 128 Kbps

1 sec = $128 * 10^3$ bits

80 millisec ⇒ $80 * 10^{-3} * 128 * 10^3$ bits

no. of bits in RTT ⇒ (80×128) bits

window size $\Rightarrow \frac{80 \times 128}{32 \times 8}$

$\Rightarrow 40$

Q35 :→

BW = 3KHz

Signal to noise ratio = 20 dB

$20\ dB = 10 \log_{10}\left(\frac{S}{N}\right)$

$\left(\frac{S}{N}\right) = 10^2 = 100$

max data rate $= B \log_2\left(1+\frac{S}{N}\right)$

$= 3 \times 10^3 * \log_2 (1+100)$

$= 3 * 10^3 * \frac{\log_2(101)}{\log(2)}$

~~$= 3 * 10^3 * 19.9$~~

$= 19.97$ K bits

Q36 :→

BW = 4 kbps

Pd = 20 millisec

↳ %LU = 50%.

↳ TT = 2 * PT

TT = 2 * 20 millisec

TT = $2 * 20 \times 10^{-3}$ sec

TT = 40×10^{-3} sec

$\frac{\text{frame size}}{BW} = 40 * 10^{-3}$ sec

$\frac{x}{4 \times 10^5 \text{ bits/sec}} = 40 * 10^{-3}$ sec

frame size = 160 bits

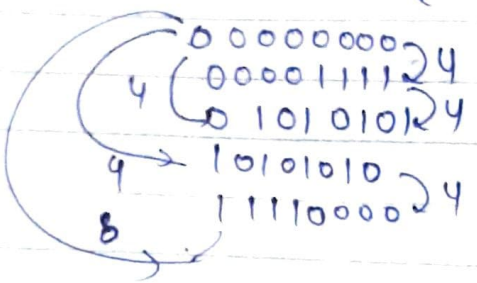
37 To correct "d" errors, the min hamming distance is (2d+1)

$2d+1 = 4$

$d = \frac{3}{2}$

$= 1.5$

$\simeq 1$ Ans



38 :-

B.W = 400 Hz

Signal to noise ratio = 7dB

$7 = 10 \log_{10}\left(\frac{S}{N}\right)$

$\frac{S}{N} = 10^{0.7}$

$\boxed{\frac{S}{N} = 5.011}$

Maximum data rate = $B \log_2\left(1 + \frac{S}{N}\right)$

S = 800 if Manchester is used

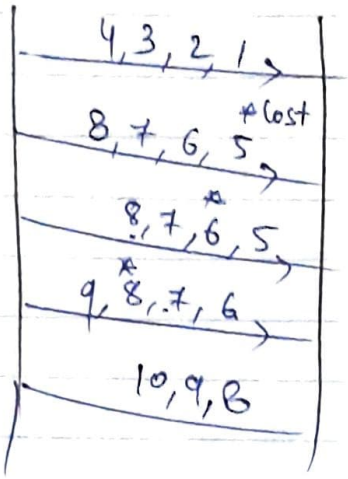
$= 400 * \log_2(1+5.0$

$= 400 * \frac{\log(5.011)}{}$

T3 :- 10 packets

Go Back N ARQ

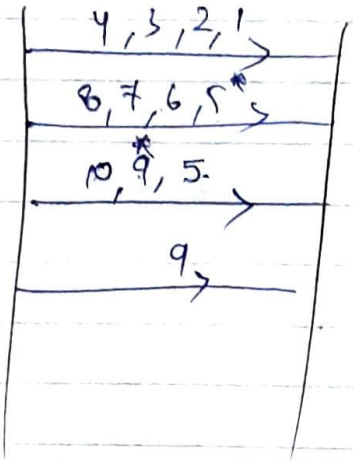
ws = 4



$x = 19$

Selective repeat ARQ

ws = 4



$y = 12$

$x + y = 19 + 12 = 31$ Ans

RARP, BOOTP, DHCP

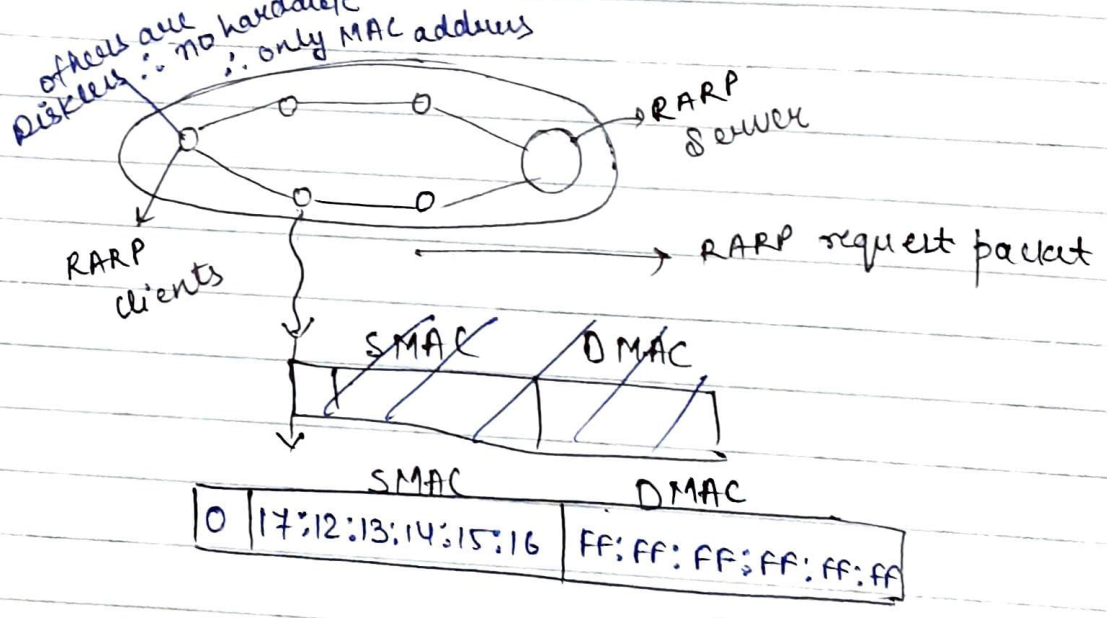
RARP (Reverse address Resolution protocol) :→

(i) diskless station ⇒ IP address, MAC address
(ii) disk station (harddisk) ⇒ IP address, MAC address

MAC address of a computer is stored on ROM chip.

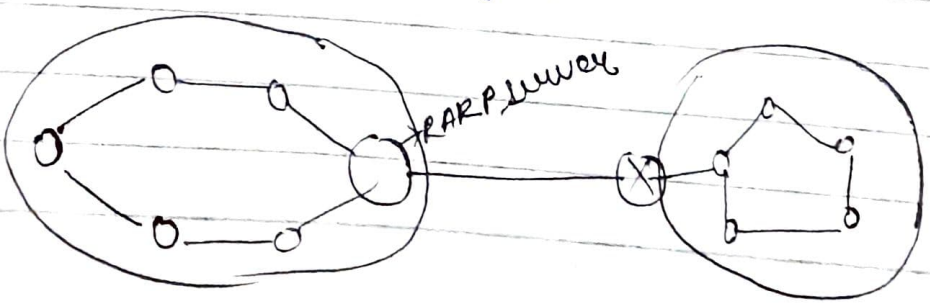
IP address is stored on hard disk.

diskless station is called RARP clients
disk station is called RARP server



↑ MAC Broadcast address

RARP request packet is broadcast
RARP reply packet is unicast.

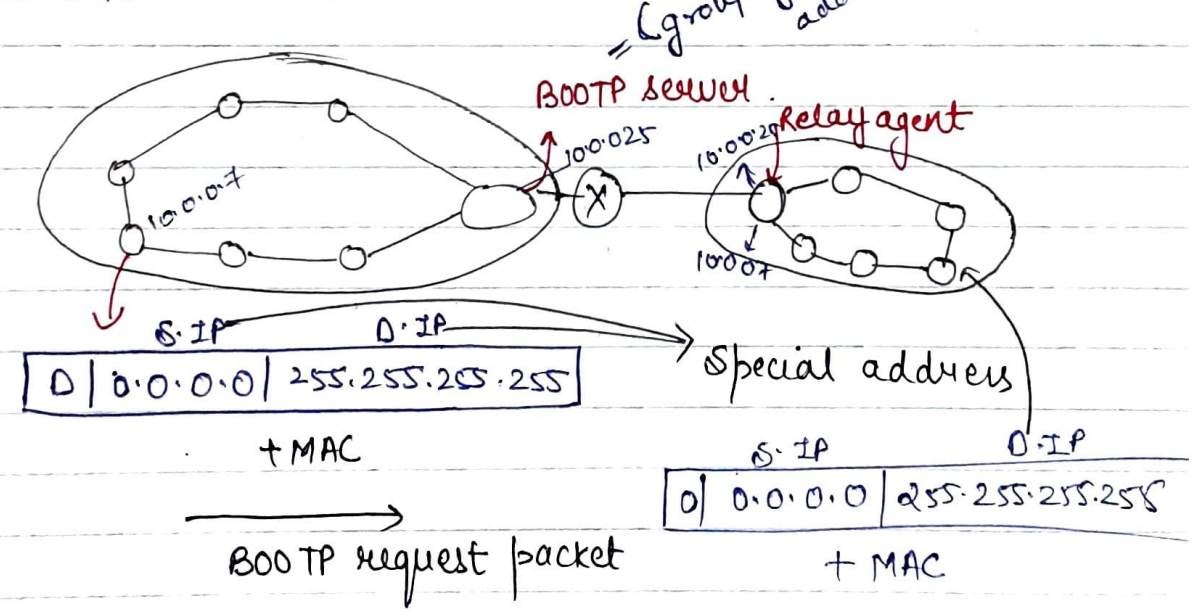


RARP request packet is a broadcast whereas RARP reply is unicast containing the IP address.

NOTE:→ Even the computers are not having any hard disk still we can assign IP addresses to the computer at run time

Drawback of RARP protocol is for N LAN networks N RARP servers are required (coz Router will accept IP address and by using RARP server those MAC addresses are converted into IP addresses) N-RARP servers are required so cost is high. RARP clients are called Thin clients

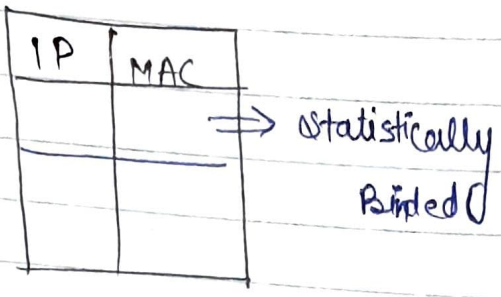
→ BOOTP (application software)



→ Using BOOTP protocol we can assign IP addresses at run time in different LAN networks so cost is less compared to RARP.

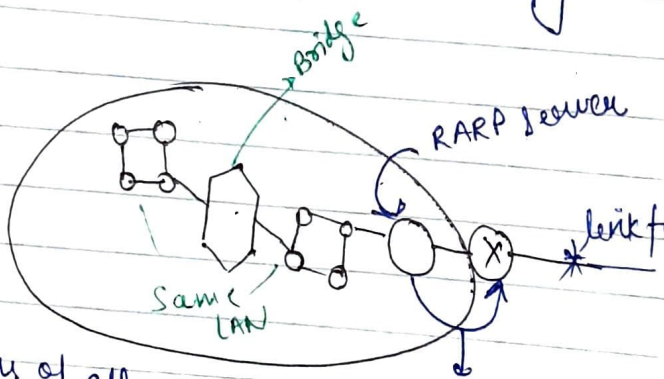
7)

The relay agent will convert a limited broadcast packet into a unicast packet so that router will allow packet into other LAN where BOOTP server resides.



DHCP

- Both static and dynamic IP's can be assigned using DHCP protocol.
- It is not statistically Bind
- RARP Protocol is used for rebooting the machines or router



MAC address of all system taken from bridge

RARP

IP address.

Rebooting the router when router link fails

Applying RARP protocol on those MAC addresses we get IP addresses which are forwarded to external router. This process is called Rebooting

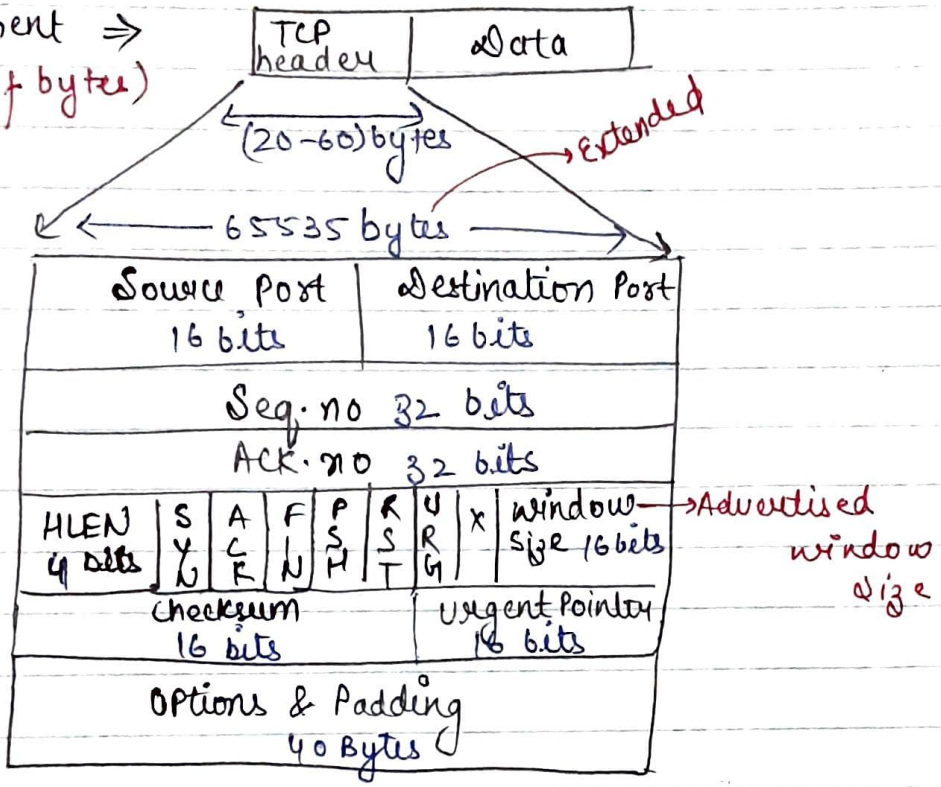
TRANSPORT LAYER :->

⇒ Provide flow control

TCP ⇒ Transport Control Protocol

↓

Segment ⇒ (group of bytes)

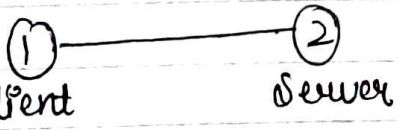


IANA

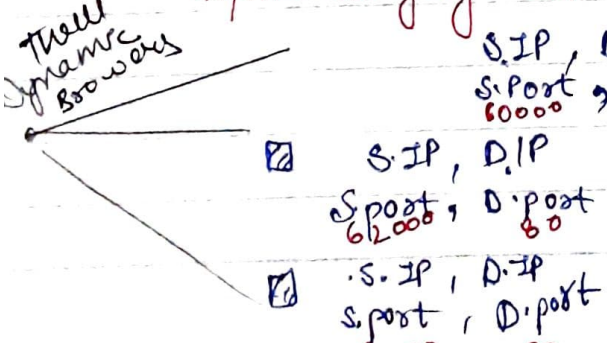
↳ 0 to $2^{16}-1$

0 to 65535 port address

server



http:// www.google.com



http ⇒ 80 | SMTP ⇒ 25
ftp = 21, 20 | Telnet ⇒ 23

Division of Port addresses by IANA :-

1) 0 – 1023 ⇒ Predefined ports, universal ports, fixed port

2) 1024 – 49151 ⇒ Registered ports

3) 49152 to 655375 ⇒ dynamic ports, ephemeral ports

Predefined Ports are the ports which are used for some pre-defined applications like Http, ftp, SMTP etc

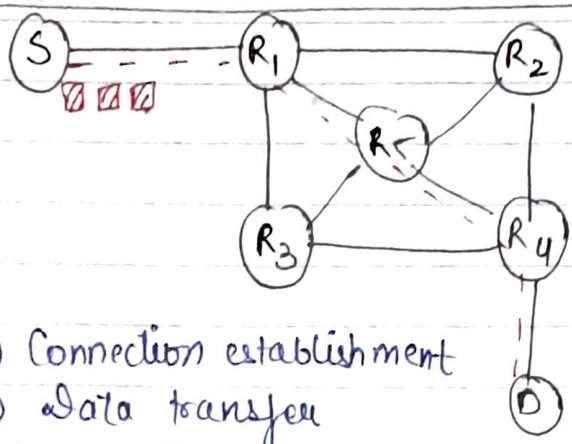
Registered Ports are the ports which are used by the companies to test networking softwares.

Dynamic ports are the ports which are used to distinguish different process in the n/w environment.

Rule :-

- If source port is a dynamic port and destination port is a static port (fixed port) then the data is moving from client to server
- If source port is a fixed port and the destination port is a dynamic port then the data is moving from server to client

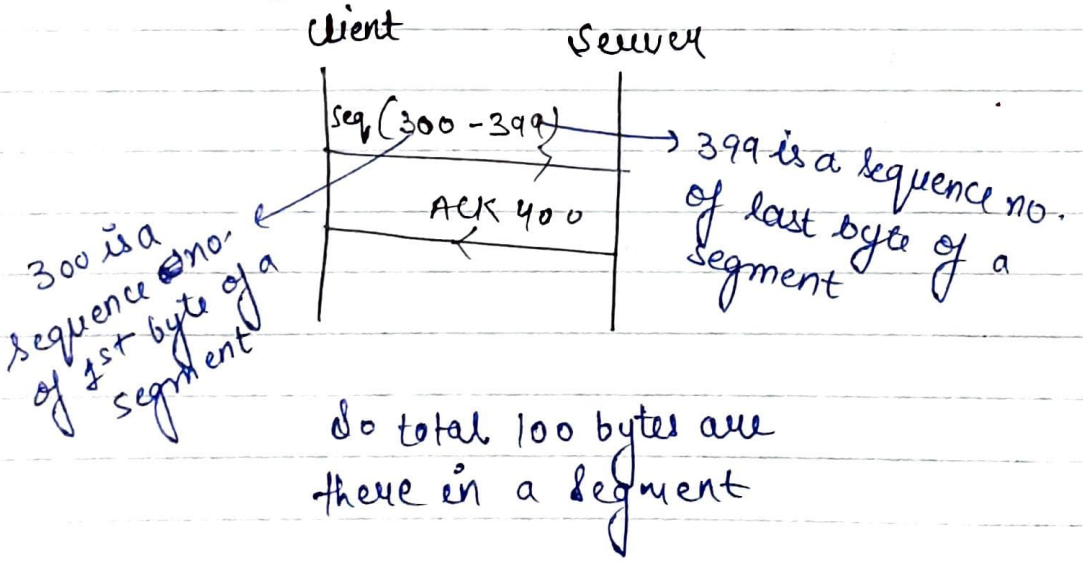
TCP is a connection-oriented Protocol



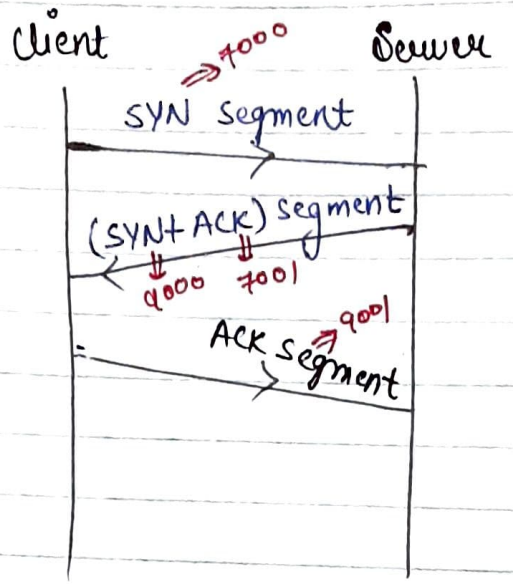
(i) Connection establishment
(ii) Data transfer
(iii) Connection Release

In data link layer, Sequence nos are given for every frame whereas in TCP, sequence no's are given for every byte in the segment.

The initial sequence no. in TCP is a random no. to provide Security.



1) Connection Establishment



Connection Establishment requires 3-way handshaking

SYN Segment does not carry data, it carries only one Sequence no.

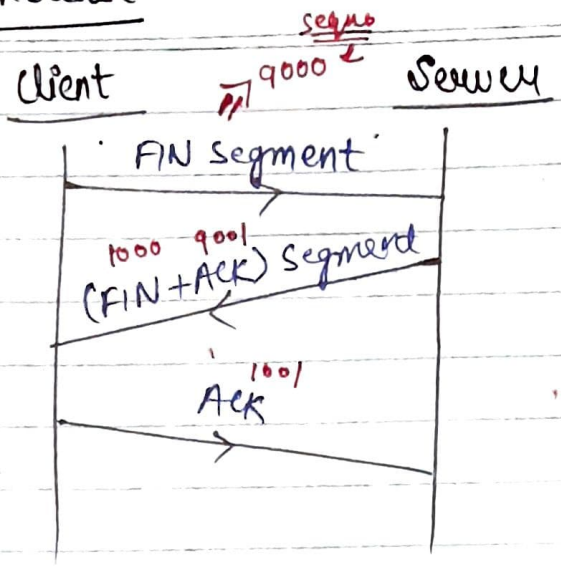
TCP supports full duplex operation as other side i.e. Server side also send (SYN+ACK) Segment, server is also requesting and wants to transmit the data and hence has sent SYN segment.

» For Complete connection establishment 3-way handshaking is required

» SYN segment doesn't carry any data but it consumes one sequence number

» TCP supports full duplex operation

3) Connection Release



* For complete connection release 3-way handshaking is required

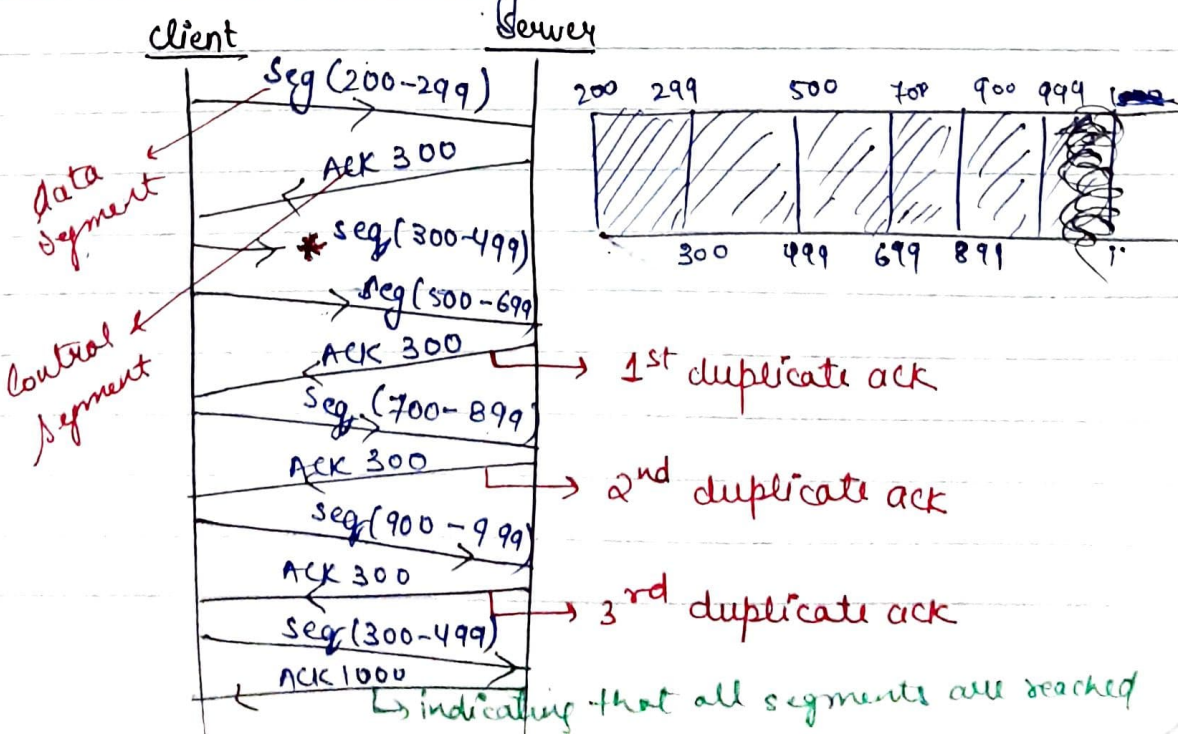
2) ~~Data transfer~~ :→

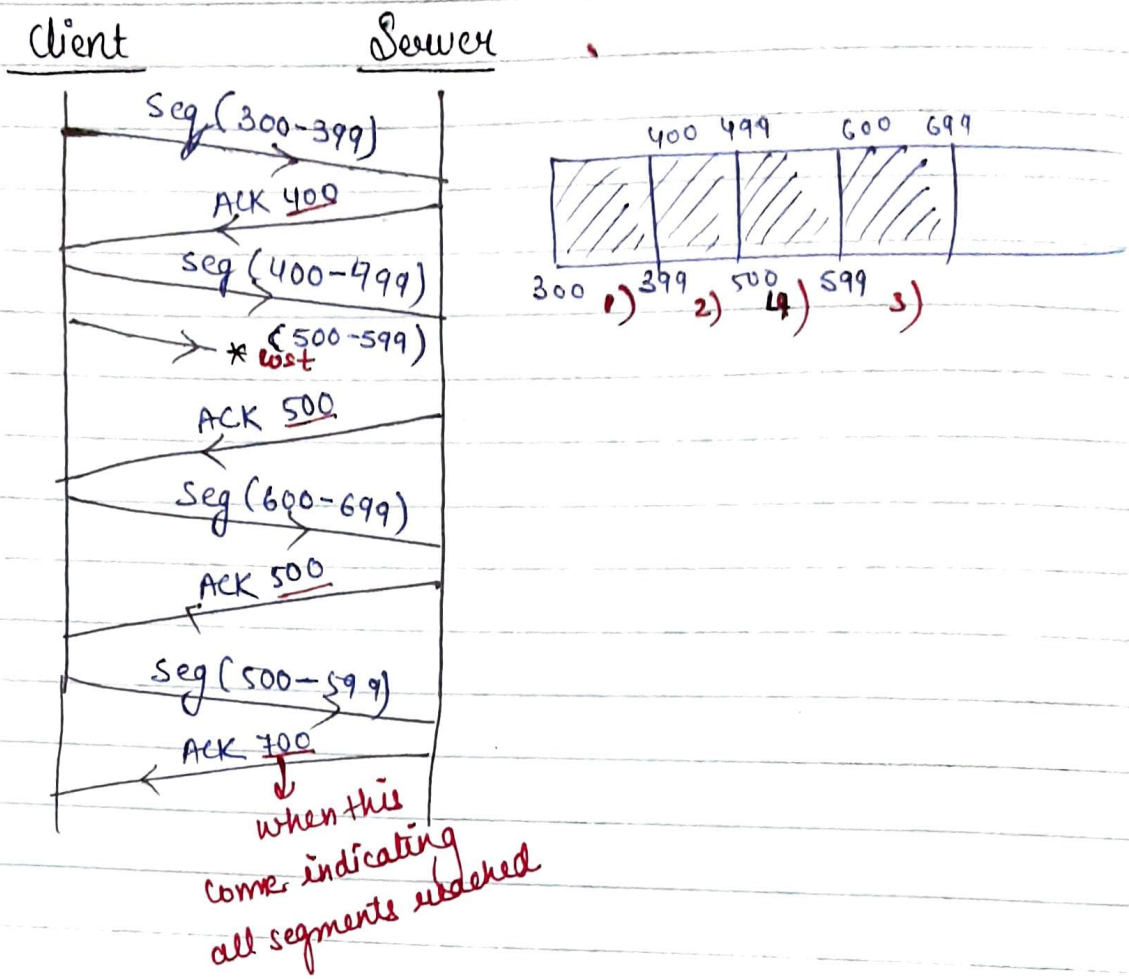
On connection establishment and connection release control segments are transmitted whereas during data transfer phase, data segments are transmitted

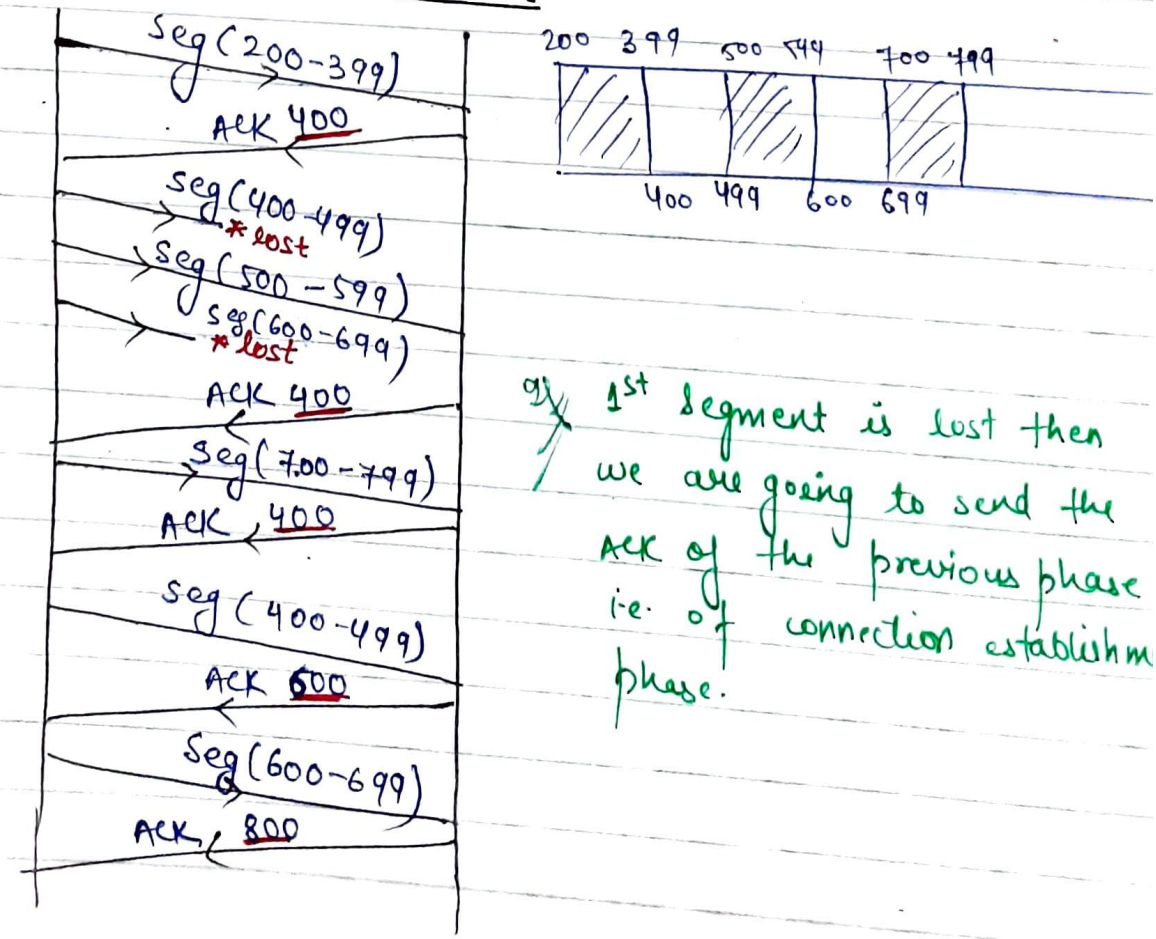
2) DATA TRANSFER:-

#Flow Control policies of TCP

TCP can accept out of order segments but always sends inorder acknowledgement.

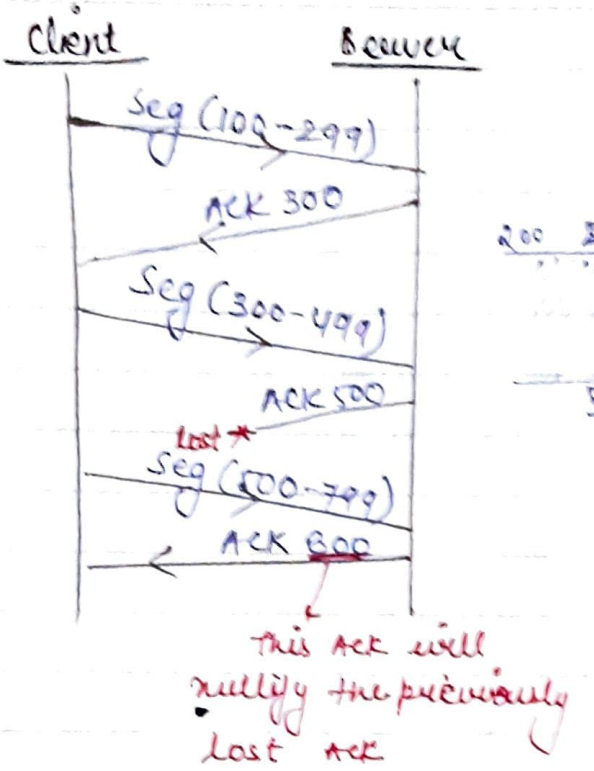


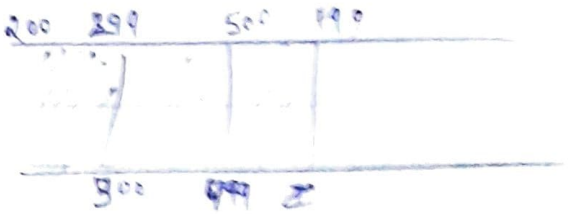




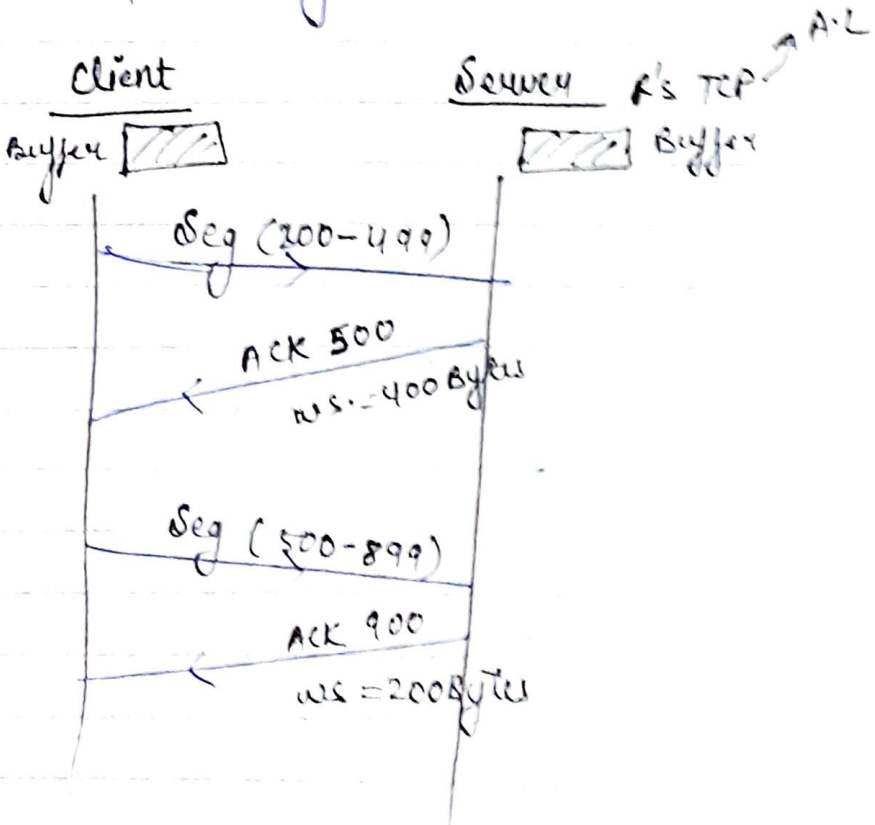
Q) 1st segment is lost then we are going to send the ACK of the previous phase i.e. of connection establishment phase.

ACK Segment is lost

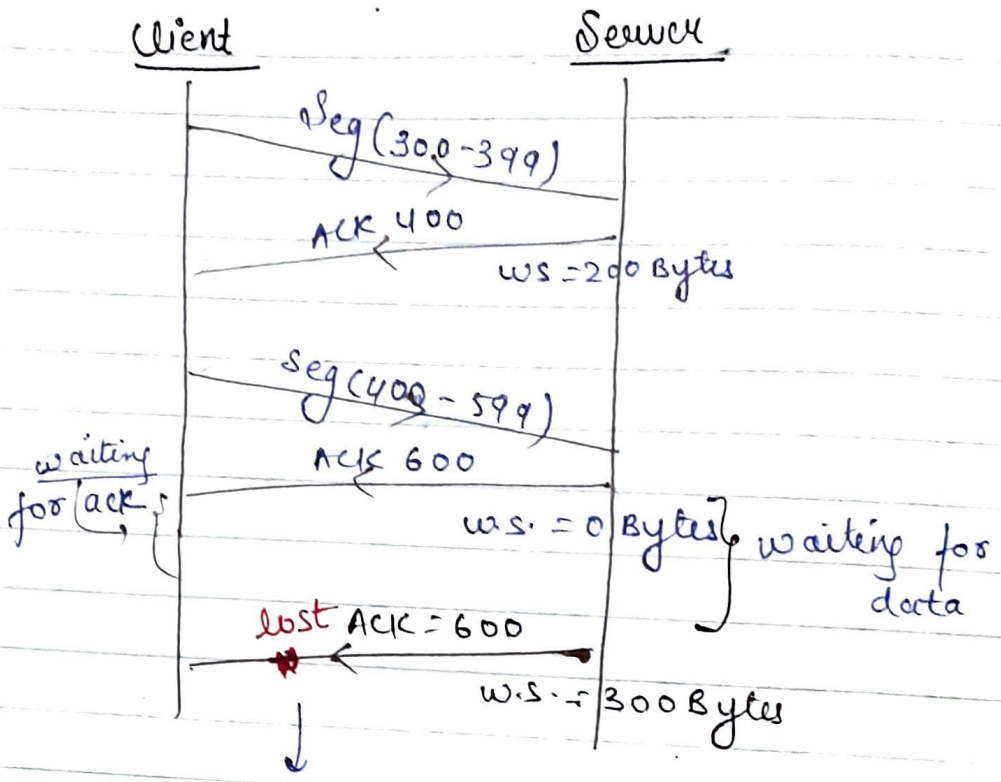




Once ACK is lost, the next upcoming ACK will nullify the previously lost ACK.

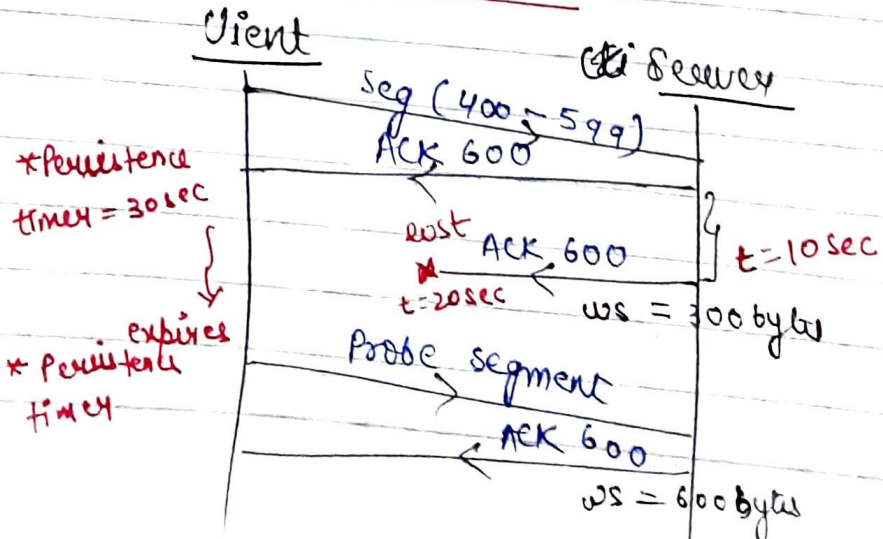


Window size is used for synchronization b/w sender and receiver.

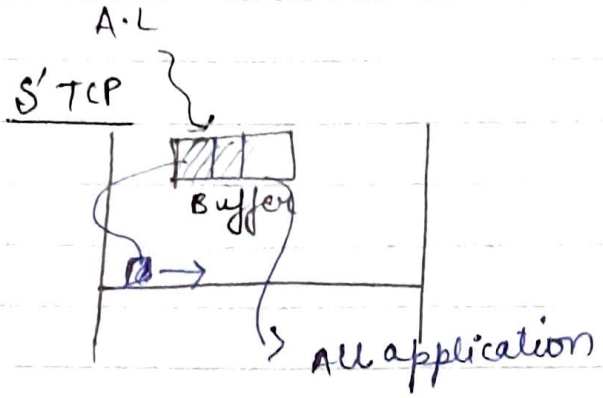


∴ Both are waiting and this condition is called deadlock

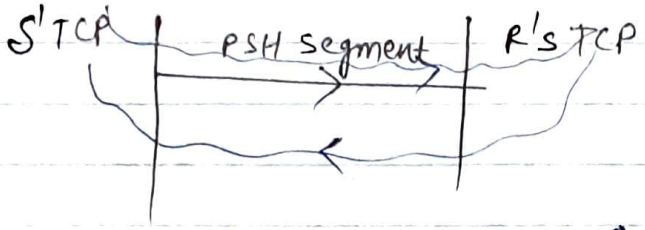
⇒ Once the ack containing window size 0 reaches to client and if the next ACK is lost then sender is waiting for ACK and receiver is waiting for data. This condition is known as deadlock



The problem of deadlock is resolved using persistence timers.



Interactive application (those give response immediately)
↳ TCP



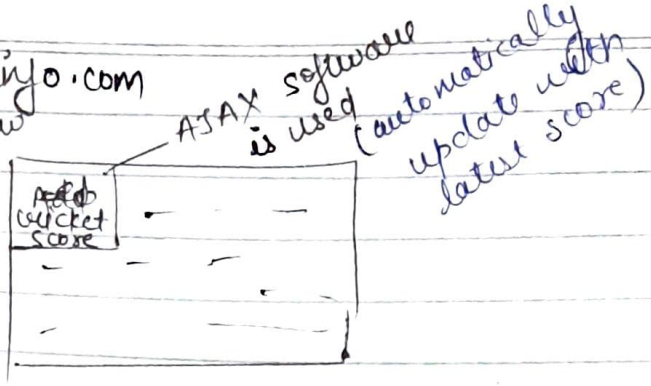
If PSH=1 ⇒ this indicates that it is an interactive data so response is immediate, data will not be buffered.

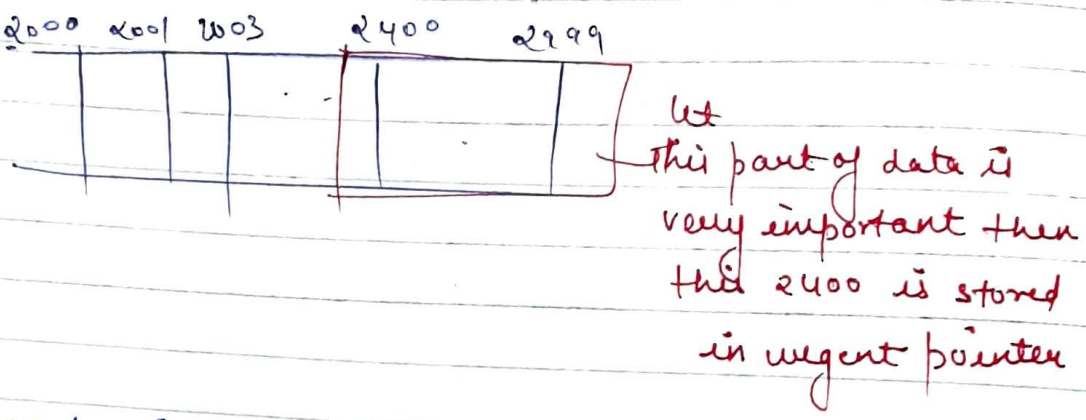
⇒ When you sign out you are sending FIN
⇒ without sign out if you close the window and again open it within the timer duration then that time you are sending RST segment

RST is used for suddenly closing the connection and reestablishing the connection.

URG :→

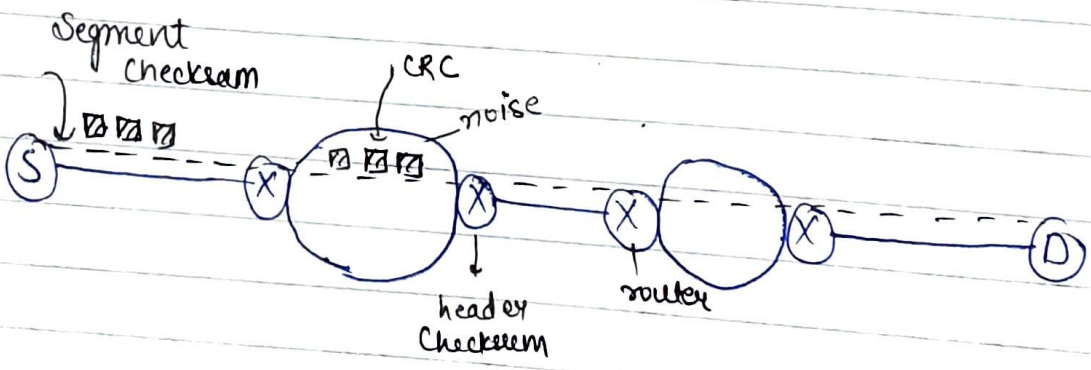
www.cricinfo.com window





If URG = 1, it indicates that it is an urgent data and the address of urgent data is available in urgent pointer.

Checksum :→



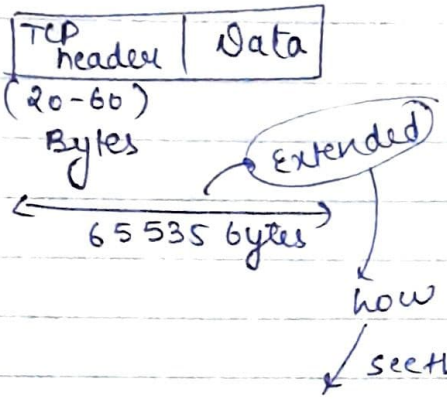
* TCP has its own error control because of potential errors at the routers.

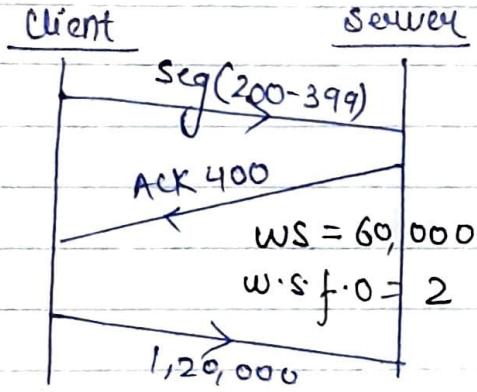
* TCP provides error control because of potential error at receiver's side (∵ noise can modify any thing

OPTIONS & PADDING :→

(1) Window scaling factor option (w.s.f.o)

TCP Segment





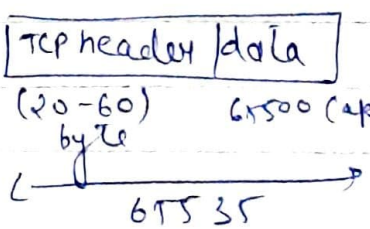
Max Segment size = any size.

How can we insert bigger data but ~~the~~ size of ~~window~~ Packet can be max 65535 so by segmentation we can do this.

$$\Rightarrow 2^{16} * 2^{14}$$

2^{16} ↓ ws, 2^{14} ↓ w.s.fo

max packet size possible is 65535 bytes

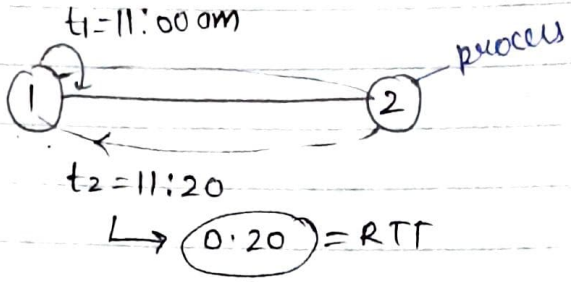


So, if bigger data come divide in small small parts called segmentation

:⇒ TCP has its own error control so it does not depend upon ICMP

* Maximum Segment Size is of any size

(2) Timestamp option :→



{ In N/w layer, Timestamp option is for b/w two end systems }

Timestamp option is used for calculating RTT b/w two end process

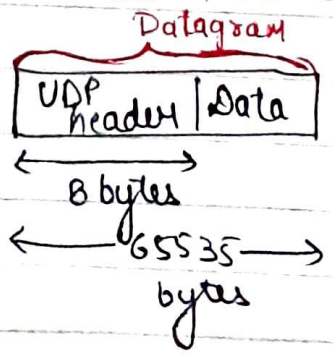
(3) NOP option:-
It is used to fill the gaps b/w the options

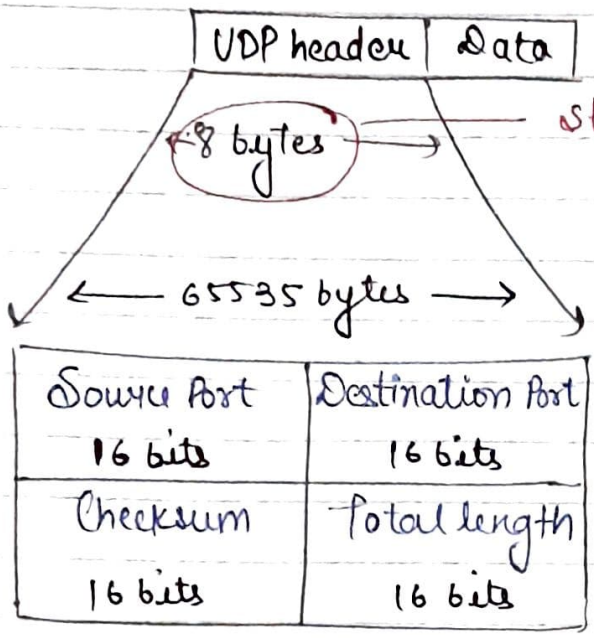
(4) EOP option :- It is used as a seperator b/w data and header

TCP doesn't depend on ICMP because TCP has its own error control.

UDP Protocol (User Datagram Protocol)

⇒ It is unreliable, fast, and it can be used if you want to transmit the small data.





(1) Total length bits of UDP header

⇓

Solution | 00000001 11111111 |

↳ Size of datagram = 511 bytes

Header + data = datagram

~~8 bytes + 511 bytes~~ =

8 bytes + x = 511 bytes

x = (511 − 8) bytes

x = 503 bytes

"Packet encapsulate datagram"

(2) UDP header is $(FF\,F0\,00\,50\,FF\,FE\,FF\,FE)_{16}$

Calculate (1) Source Port =

(2) Destination Port =

(3) Size of datagram =

(4) Size of Payload value =

(5) Is the datagram travelling from client to server or vice versa

200

Solution (1) Source Port = $FFF0_{16^3\,16^2\,16^1\,16^0}$ (Dynamic Port)

or

(FFFF − 000F)

= (65535 − 15)

= 65520

(2) Destination port = $0050_{16^3\,16^2\,16^1\,16^0}$ (static or fixed Port)

= 80

(3) Size of datagram = FFFF

= 65534 bytes

(4) Size of payload value = 65534 − 8

= 65526 Bytes

(5) It is client to server

TCP	UDP
1) header is Dynamic (20-60) Bytes	1) Header is fixed (8 bytes)
2) TCP has flow control	2) UDP has no flow control (no, seq and ack option) in udp header
3) Checksum is mandatory	3) Checksum is option
4) It has error control	4) It has no error control
5) It doesn't depend upon ICMP	5) It depends on ICMP
6) TCP+IP is connection-oriented service	6) UDP+IP is a connection-less service
7) TCP doesn't support multicasting and broadcasting	7) It supports multicasting and broadcasting

Datagrams travel in different direction so some data can be dropped.

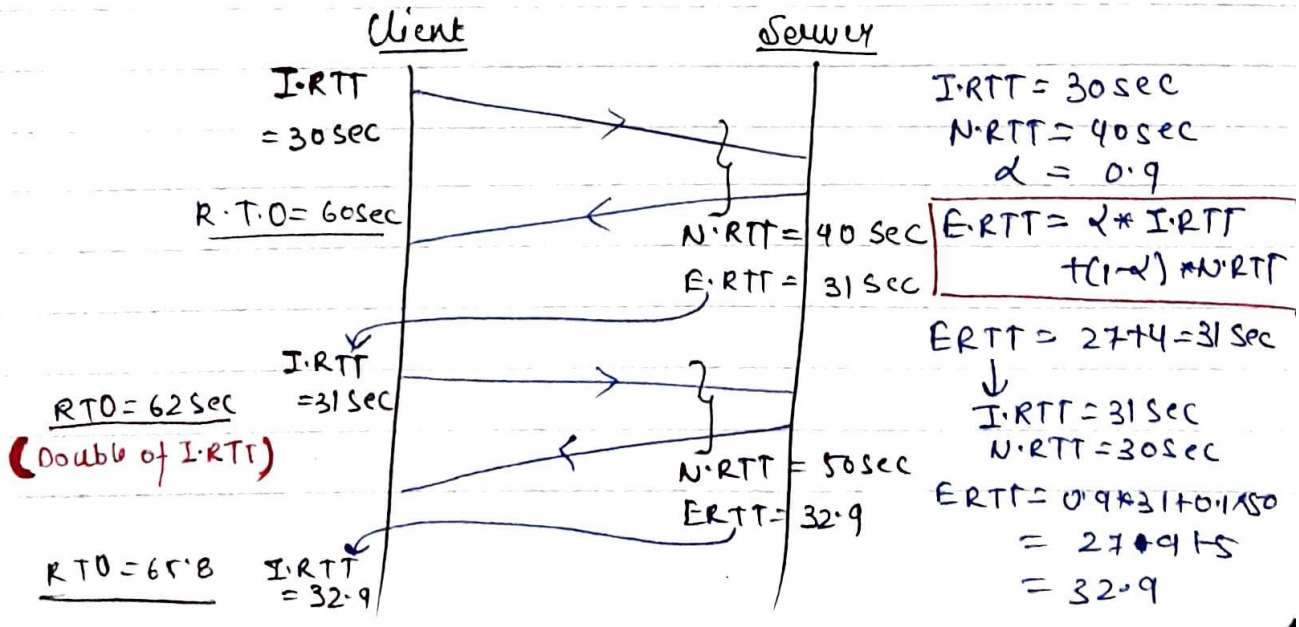
In TCP path is reserved so no packet will be dropped.

TCP + IP ⇒ provide connection-oriented service
UDP + IP ⇒ Connectionless.

UDP depends upon ICMP because UDP has no error control

TCP	UDP
8) Http, ftp, SMTP, Telnet	8) DNS, TFTP, SNMP etc.
for 7th point It doesn't support multicasting and broadcasting because path is connected	for 7th point It supports because datagram packet travel in different path.

RTO Timer (Retransmission after time-out timer) :→



→ 1st I.RTT is an assumption
NRTT is New RTT depends upon the traffic

→ RTO timer depends on load on the network
→ ERTT is Calculated by using formula
→ IRTT is equivalent to ERTT
Initial RTT
→ RTO is double of IRTT calculated.
Estimated RTT

Q:- For what value of α estimated RTT will be the average of initial RTT and New RTT

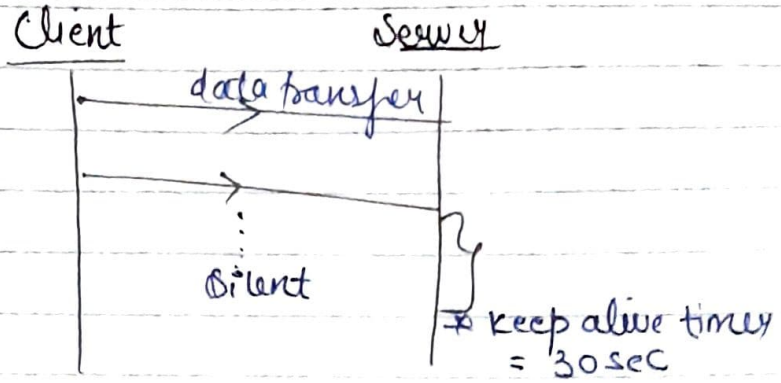
$$ERTT = 0.5 * IRTT + 0.5 * NRTT$$

$$= \frac{IRTT}{2} + \frac{NRTT}{2}$$

$$= \frac{IRTT + NRTT}{2}$$

Keep alive timer (Server)

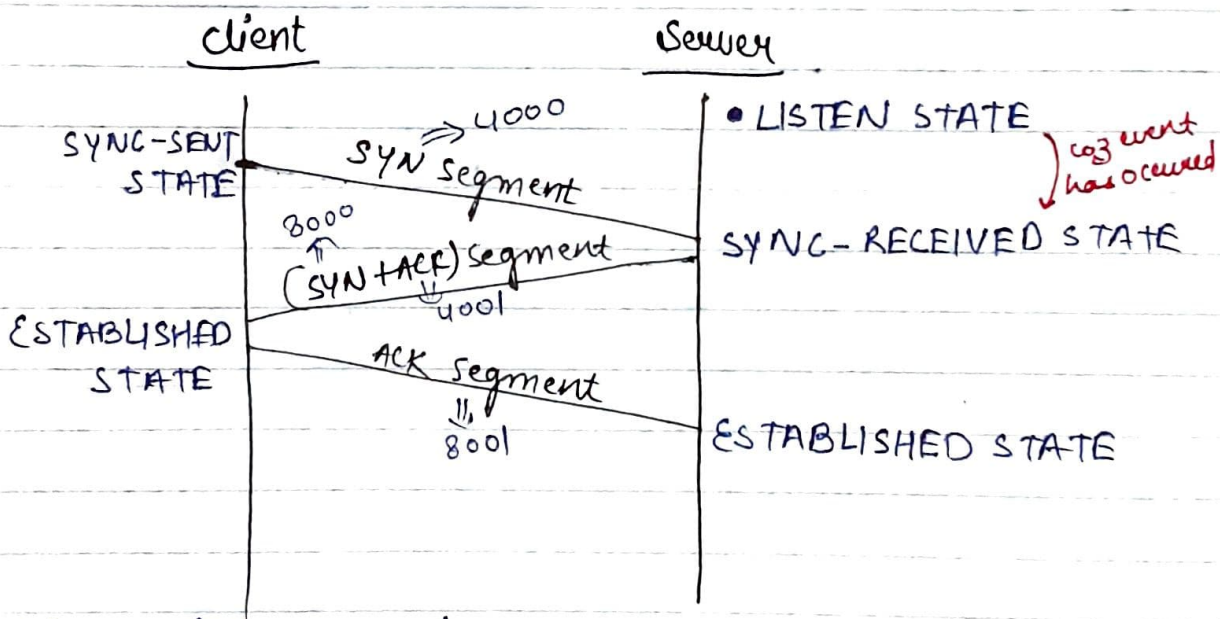
* If client is transmitting data to Server and suddenly become silent then server will wait for sometime, then it start keep alive timer, if in a meanwhile client send data it will take data and stop timer. But once the timer expires server will stop and ~~del~~ deallocate so it will give that service to some other client.



* When the client is transmitting the data and suddenly it is silent then Server will start keep alive timer.

* Once the timer expires multiple time the server will suddenly close the connection.

State transitions of TCP :→

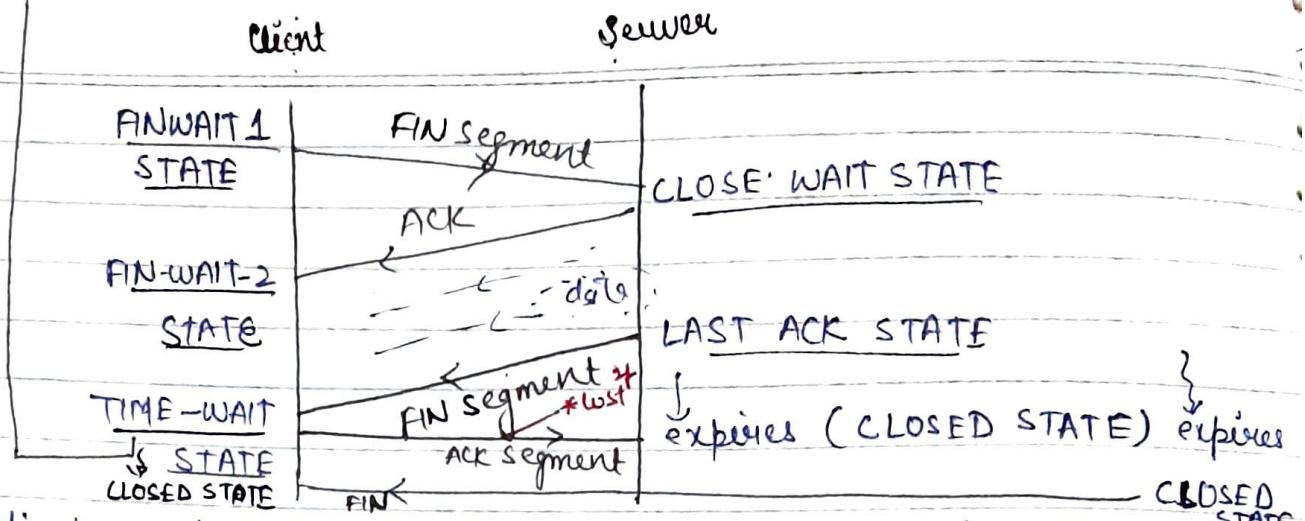


Client will move from SYNC-SENT STATE to ESTABLISHED STATE when it gets (SYN + ACK) Segment

Server will move from SYNC-RECEIVED to ESTABLISHED STATE when it gets (ACK) segment

Maximum Segment lifetime

Q09 (2 * MSL)

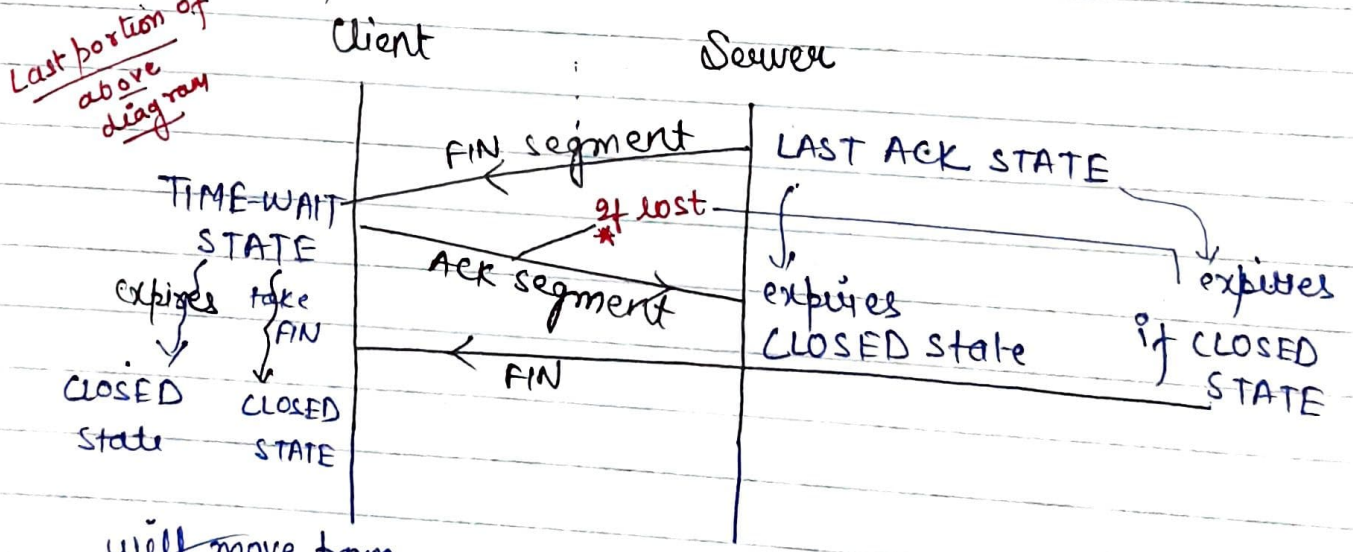


Client sent FIN when he wants to finish or close the connection

Client was expecting (FIN+ACK) coz he may think server also want to stop but on receiving only ACK it understant that there still more data to come

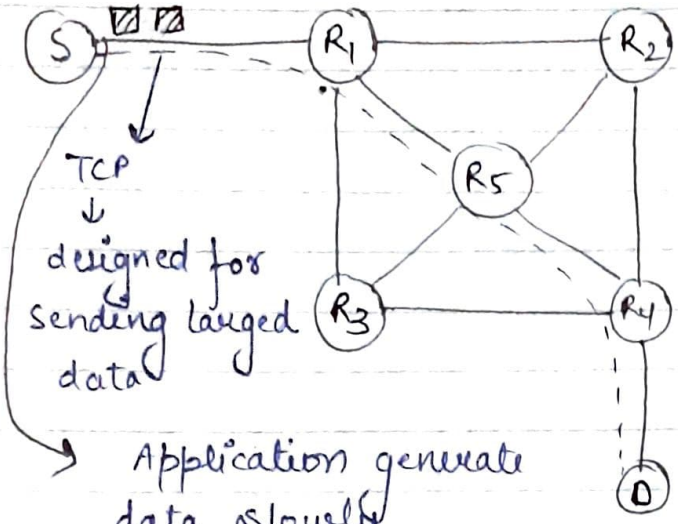
During FIN-WAIT 1 and FIN-WAIT 2 client cannot send any data to the server but it receives the data from server.

Last portion of above diagram



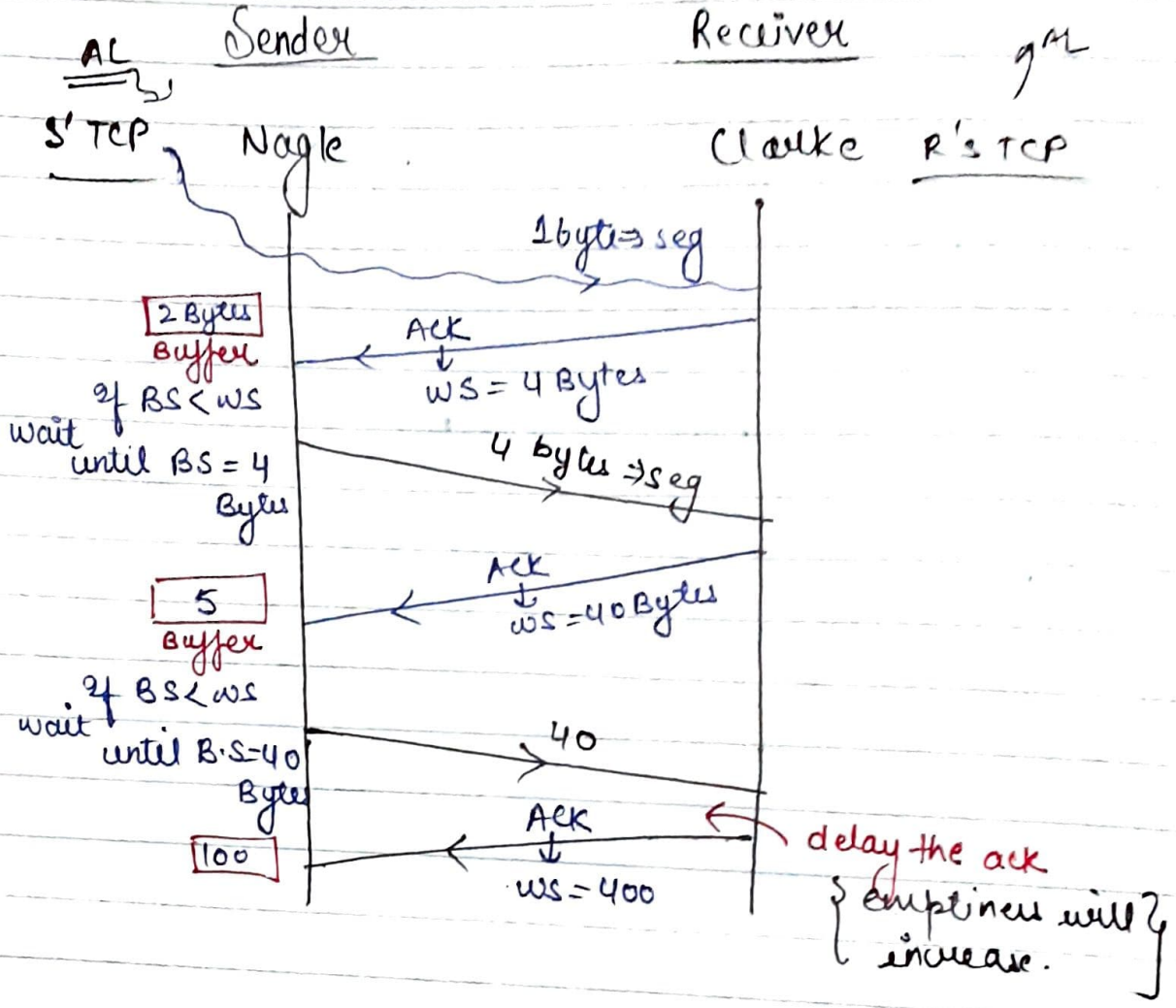
~~will move from~~ CLIENT ~~A FIN-WAIT-1~~ will directly go to

CLIENT will move from FIN-WAIT 1 state to TIME-WAIT state when it gets FIN+ACK from the server



Window size → no. of frames in RTT (no LL)
no. of bytes that you transmit in a segment and that too in propogation time (no TL)

When the application is generating data slowly then the window size will be small then this problem is known as Silly window Syndrome



Nagle suggested that whenever ACK segment comes to the client compared the Buffer size with window size.

If BS < W.S then wait at the sender side until the buffer size = Window size.

Clarke suggested that delay the acknowledgement so that parallely window size will increase along with buffering of data. So that, Silly window syndrome problem will be solved.

Workbook

MAC - Sublayer

1) a)

2) a)

3) Ethernet station

Utilization is in terms of time but here it is in terms of slots

Utilization of Ethernet Shared channel $= \frac{5}{5 + \frac{N}{2}}$

5 → transmits, 2 → acquiring channel

$= \frac{10}{10 + N}$

∴ option (b)

4) Latency = 50 millisec

BW = 45 Mbps

1 sec ⇒ 45×10^6 bits

50 millisec ⇒ $50 \times 10^{-3} \times 45 \times 10^6$ bits

⇒ 2250×10^3 bits

⇒ 2.25×10^6 bits

∴ option (b)

5) a)

6) $T.T = \frac{\text{Data Size}}{BW} = \frac{2 \times 10^3 \times 8 \text{ bits}}{10^6 \text{ bits/sec}}$

$= 16 * 10^{-3}$ sec

$= 16$ millisec

∴ option (a)

7) Max data rate $= B \cdot \log_2\left(1+\frac{S}{N}\right)$

$$1.544 \times 10^6 \text{ bits/sec} = 50\times10^3 * \log_2\left(1+\frac{S}{N}\right)$$

$$\log_2\left(1+\frac{S}{N}\right) = \frac{1.544 * 10^6}{50 * 10^3}$$

$$\log_2\left(1+\frac{S}{N}\right) = 30.8$$

$$1+\frac{S}{N} = 2^{30.8}$$

$$\frac{S}{N} = 2^{30.8} - 1$$

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

$$= 10\log_{10}\left(2^{30.8}\right)$$

$$= 10 \log_{10} 2^{30.8}$$

$$= 308 \log_{10} 2$$

$$= 308 * 0.3010$$

$$= 92.9 \text{ dB}$$

∴ option c

8) a)

9) $TT = 2 * PT$

$$\frac{\text{frame size}}{BW} = 2 * \frac{l}{v}$$

$$\frac{x}{10^9 \text{ bits/sec}} = \frac{x * 10^3 m}{2\times10^8 m/sec}$$

$x = 10^4$ bits

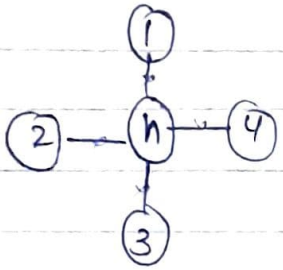
$x = 10,000$ bits

∴ option (a)

10)

802.3 ⇒ R
802.11 ⇒ P
802.15 ⇒ O
802.16 ⇒ S ∴ option (a)

11) (a)



hub is a passive device and data is forwarded in all direction so there is a chance of collision

12) (b)

13) CSMA/CD

↓

$TT = 2 * PT$

$$\frac{\text{Data size}}{BW} = 2 * \frac{l}{v}$$

$$\frac{1500 * 8 \text{ bits}}{10^7 \text{ bits/sec}} = 2 * \frac{l}{10^9 \text{ m/sec}}$$

$l = 600$ km

Q14:- Signal to noise ratio = 7 dB

$$7\ dB = 10 \log_{10}\left(\frac{S}{N}\right)$$

$$\Rightarrow \frac{S}{N} = 10^{0.7}$$

$$\Rightarrow \frac{S}{N} = 5.011$$

$$\text{max data rate} = B \log_2\left(1 + \frac{S}{N}\right)$$

$$= 400 * \log_2 (1 + 5.011)$$

$$= 400 * \frac{\log (6.011)}{\log 2}$$

$$= 1035$$

Q15 :- Each station transmits = $\frac{500 \text{ bits}}{5000 \text{ millisec}}$

$$= \frac{500 \text{ bits}}{5 \text{ sec}}$$

$$= 100 \text{ bits/sec}$$

N stations $\Rightarrow$ N * 100 bits/sec

↓

no collisions

↓

throughput of slotted aloha = 0.368

$\therefore$ 0.368 * 50 kbps = N * 100

$0.368 * 50 * 10^3$ bits/sec $= N * 100$ bits/sec

184 stations $= N$

16) no. of requests = 70 requests/sec

1 slot = 50 milliseconds

1 slot = 50×10^{-3} sec

$$\frac{1}{50 \times 10^{-3}} = 1 \text{ sec}$$

no. of slots = 20 slots/sec

Slots are less people came more.

$$G = \frac{70}{20} = 3.5$$

$(G > 1) \rightarrow$ overloaded

17) $$T.T = \frac{50 \text{ bits}}{200 \text{ bits/sec}}$$

$$T.T = \left(\frac{1}{4}\right) = 0.25 \text{ sec}$$

↑ time taken by 1 frame in pipelining

18) $${}^{n}C_1 * p^1 * (1-p)^{n-1}$$

$$n * (0.2)^1 * (0.8)^{n-1}$$

1 is transmitting ∴ no collision and ∴ it is called throughput

Throughput in slotted aloha $= 0.16 * n$

(212)

$$0.16 * n = n \times (0.2) * (0.8)^{n-1}$$

$0.16 * n$: 0.8 ; $n \times (0.2) * (0.8)^{n-1}$: throughput

$$(0.8)^1 = (0.8)^{n-1}$$

$$n-1 = 1$$

$$n = 2$$

or

$$N * 0.16 \leq 0.368$$

$$N \leq 2.3$$

$$\therefore N = 2$$

19) Length of One time slot = time to transmit 100 bits + end to end propagation delay

$$= \frac{100 \text{ bits}}{10 \text{ Mbps}} + \frac{1 \text{ km } (d)}{2 \times 10^8 \text{ m/sec } (v)}$$

$$= \frac{100 \text{ bits}}{10^7 \text{ bits/sec}} + \frac{10^3 \text{ m}}{2 \times 10^8 \text{ m/sec}}$$

$$= 10 \mu\text{sec} + 5 \mu\text{sec}$$

length of 1 time slot value = $15 \mu\text{sec}$

$$\text{Total Throughput} = \frac{\text{Data size}}{\text{Total time}}$$

$$= \frac{100 \text{ bits}}{15 \mu\text{sec}}$$

$= 20$ 20 Mbps

Throughput of one station = $\frac{2}{3} \times N$ Mbps

$N = 10$

20) Ethernet
↳ CSMA/CD

$TT = 2 * PT$

$TT = RTT$

$\frac{\text{frame size}}{BW} = RTT$

$\frac{x}{10^8 \text{ bits/sec}} = 64 \text{ millisec}$

frame size = $64 \times 10^{-3} \times 10^8$ bits
= 6400000 bits

If RTT = 64 μsec

then frame size = $64 \times 10^{-6} * 10^8$ bits
= 6400 bits
= 800 bytes

⇒ When collision is detected in less than PT then there is a jam signal
⇒ when we apply = there is no jam signal

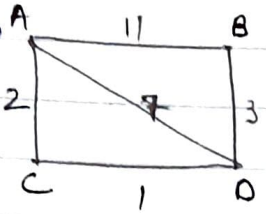
(2.14)

Network layer

(1) d

(2) b

(3) (B)



A → B = 11 units

D → B = 3 units

C → B = 4 units

C is telling A that I know how to reach B in 4 + 2 = 6 units

D says in 3 + 7 = 10 units

A → B = 11 units

∴ Smallest is 6 units

∴ option (C)

(4) a) is true as circuit switch follow same path ∴ they arrive in-order

b) True as they follow routing tables

c) False.

WAN

Packet-switching → table changing

↓

∴ path change

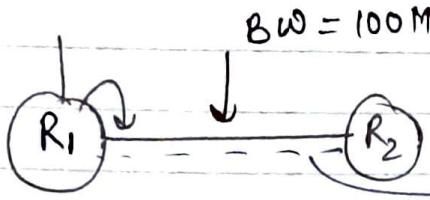
5) a) True → many packets from many source are allowed in the queue

b) False.

c) True as every packet enter in the queue checksum and is done in packet

but less in circuit switching

Q6:-



$PT \cong 0$ {wired speed, forwarding}

Data size = 84 bytes

$$TT = \frac{\text{data size}}{BW}$$

$$TT = \frac{\text{frame size}}{BW} = \frac{84 * 8 \text{ bits}}{10^8 \text{ bits/sec}}$$

$$TT = 6.72 \mu\text{sec}$$

∴ option (C)

Q7:-

$$4\begin{pmatrix} 0101011 \\ 1001101 \\ 1110001 \end{pmatrix}4$$

If in (I) 0010111

Include this in above 3 code if hamming distance is maintained then it will also be a code word.

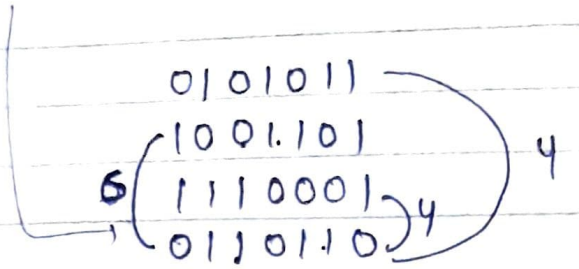
c.

$$4\begin{pmatrix} 0101011 \\ 1001101 \\ 1110001 \\ 0010111 \end{pmatrix}4$$

∴ Yes (I)

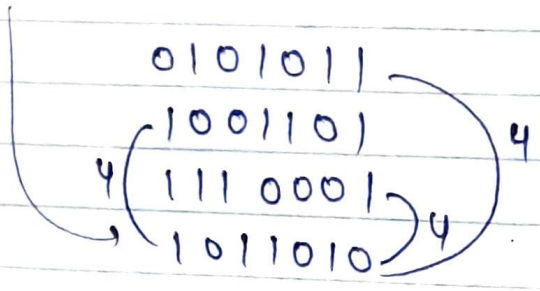
206

II 0110110



∴ II also Yes

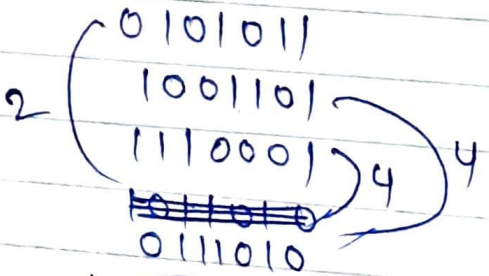
III 1011010



∴ III also Yes

option

IV 0111010



∴ IV is No

∴ option (b)

8) (a)

9)

9) 199.202.0.0
199.202.1.0
199.202.2.0
199.202.3.0

Class C subnet mask is 255.255.255.0

= 11111111.11111111.11111111.00000000

N | super | host

= 255.255.252.0

∴ option (a)

10) option (c)

11) option (a)

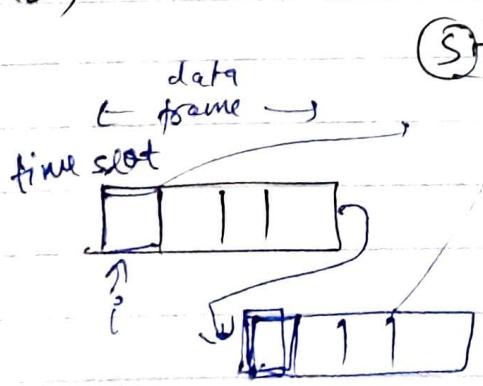
12) S1 and S4 are true.

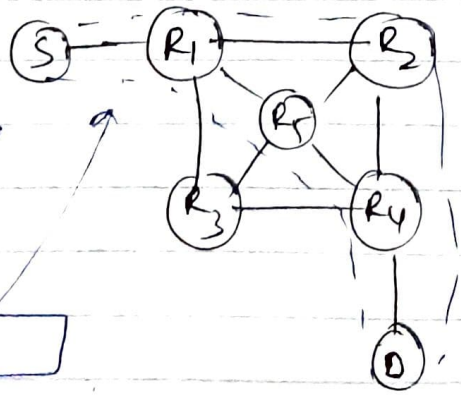
↓

cos when you have to inform to all routers large packets are send whereas in DV we inform only neighbours ∴ less packets

∴ option (d)

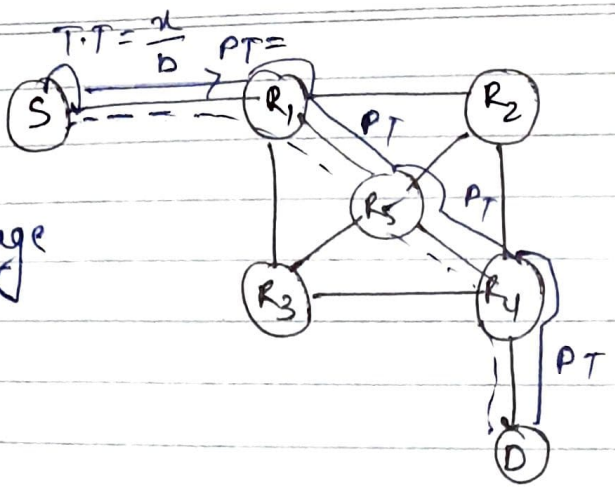
13) TCP





In TCP session multiple paths are possible whereas in TCP connection multiple paths are not possible there is only 1 single path

14



x-bit message

So the entire path there is only PT and no TT as they are by-passing and storing forwarding

Circuit Setup time = "s" seconds

P.d = "d" sec/hop

1 hop = d sec

K hop = (kd) sec

transmission time

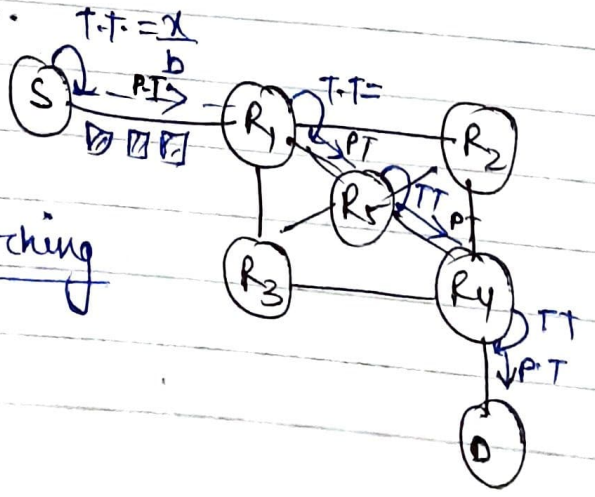
Propogation time

Setup time + TT + ~~hop~~ time

T.T. ⇒ $s + \frac{x}{b} + kd$ — (1)

∴ option (c)

15



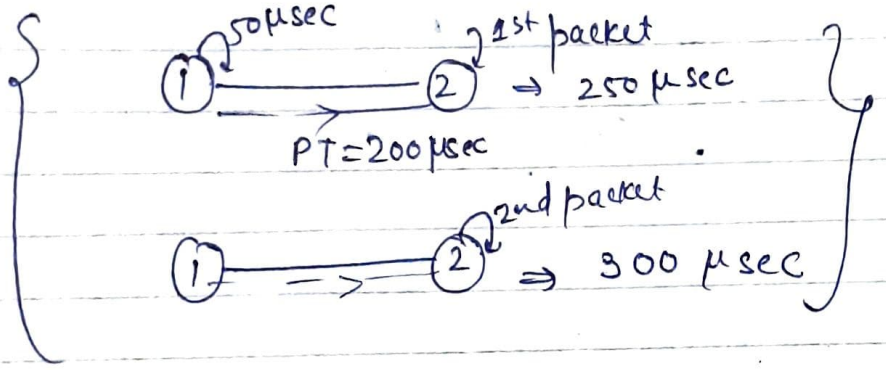
Packet Switching

Propagation time = kd

transmission time of router and not System = $\frac{P}{b}(k-1)$

Total time TCT = Setup time + PT + T.T.

$$= \frac{x}{b} + kd + \frac{P}{b}(k+1) \quad \text{---(2)}$$



Relation ship b/w (1) and (2)

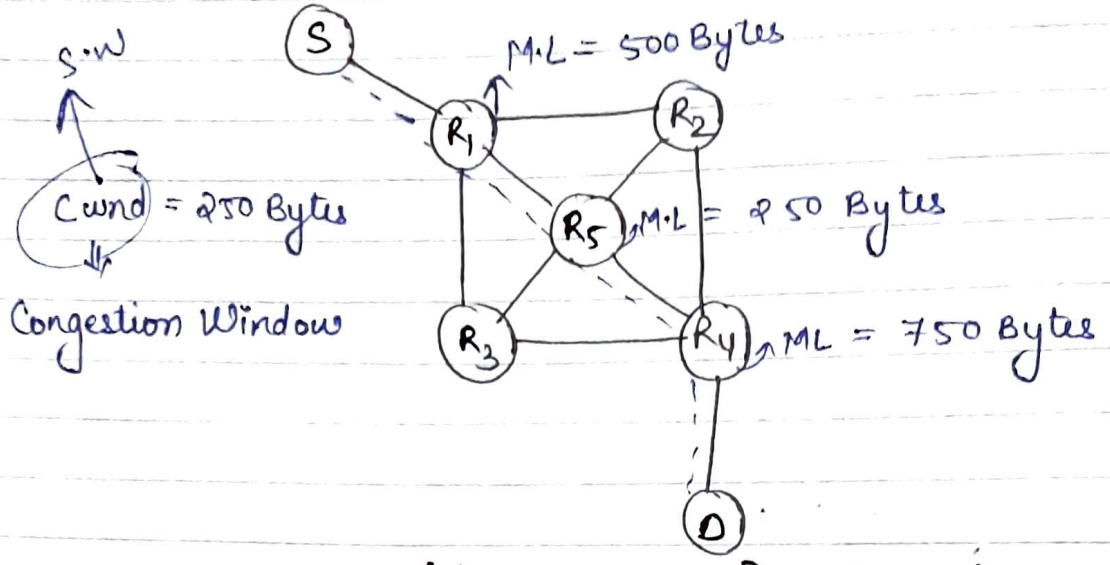
$$S + \frac{x}{b} + kd = \frac{x}{b} + kd + \frac{P}{b}(k+1)$$

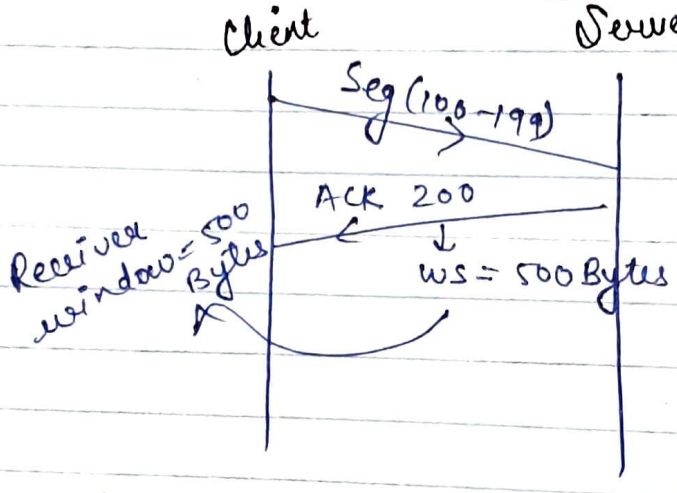
$$S > (k+1)\frac{P}{b}$$

∴ Packet switching is faster than circuit switching

∴ option (b)

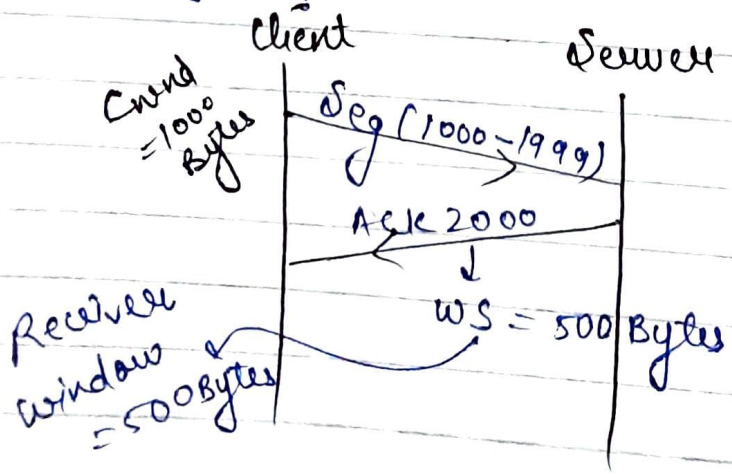
Congestion Policies of TCP:→





S.W = (Cwnd, Rwnd)

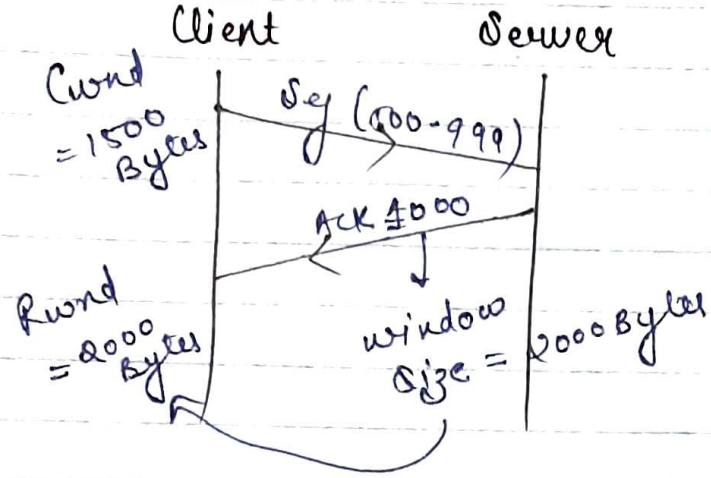
Congestion window will be known to sender during connection establishment phase.
Receiver window will be known to sender during data transfer phase.



If Rwnd << Cwnd

S.W = Rwind

{ Flow control policies of TCP }



If Cwnd << Rwnd

S.W = Cwnd

(Congestion policies of TCP)

Congestion Policies of TCP

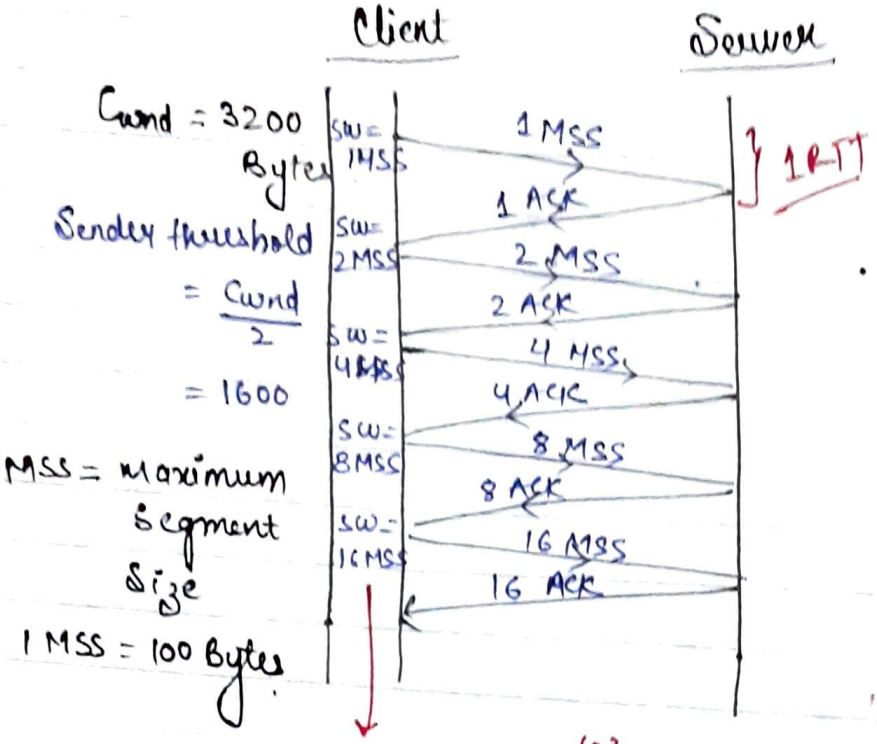
(1) Slow start algorithm
(2) Congestion Avoidance
(3) Congestion detection

} Cwnd << Rwnd

Slow Start Algorithm →

* Slow start mechanism deals with both Congestion and flow control.
* TCP handles both congestion and flow control
* UDP does not have any flow control or Congestion Control.
* Fast retransmit deals with congestion and not with flow control.

Slow Start Algorithm :- {Exponential Algorithm}



Here we stop (as) we have reached sender threshold value = 16 MSS ⇒ 16 × 100 ⇒ 1600 Bytes.

Initially S.W = 2^0 MSS

After 1 RTT → SW = 2^1 MSS

After 2 RTT → SW = 2^2 MSS

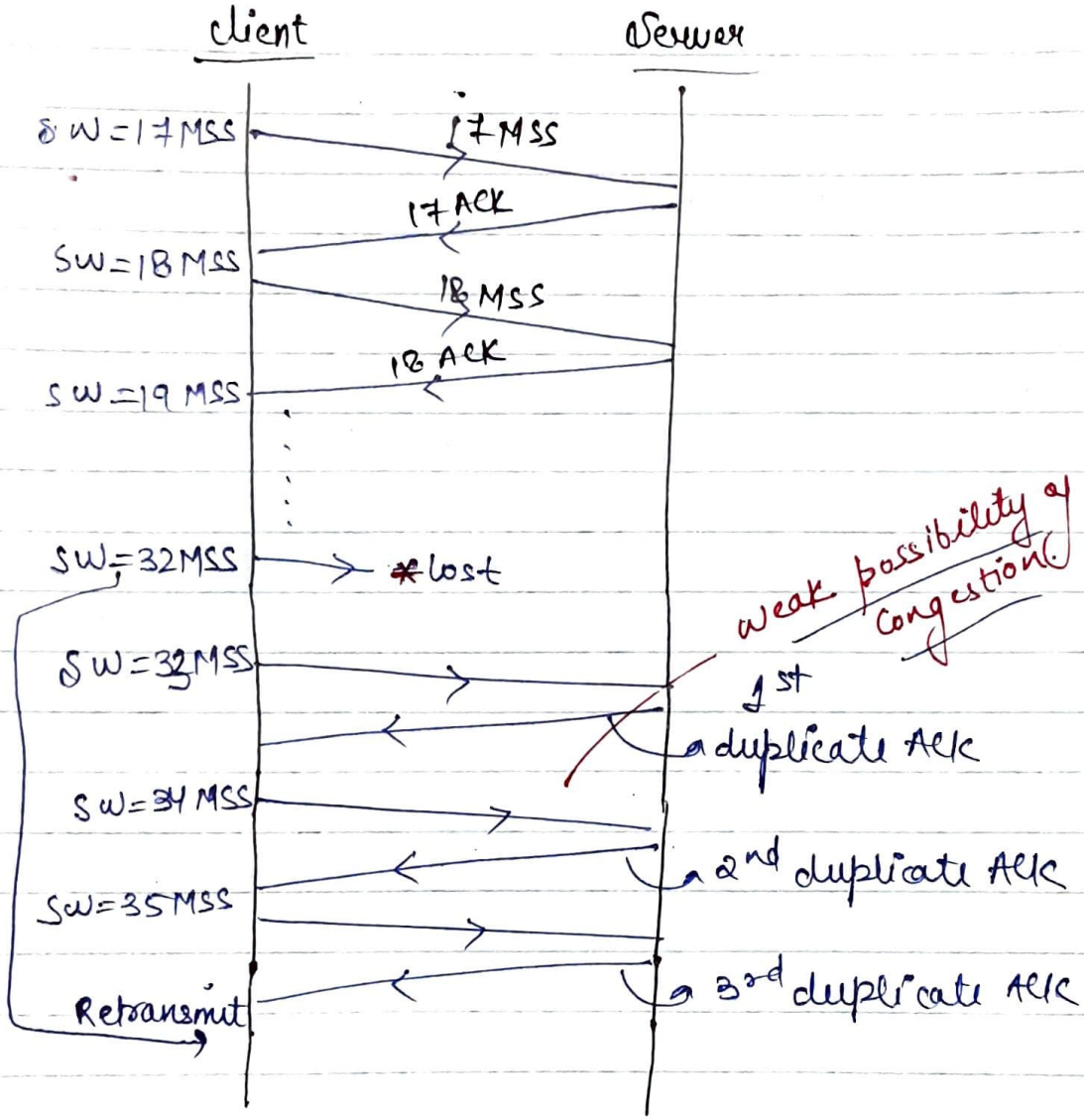
⋮

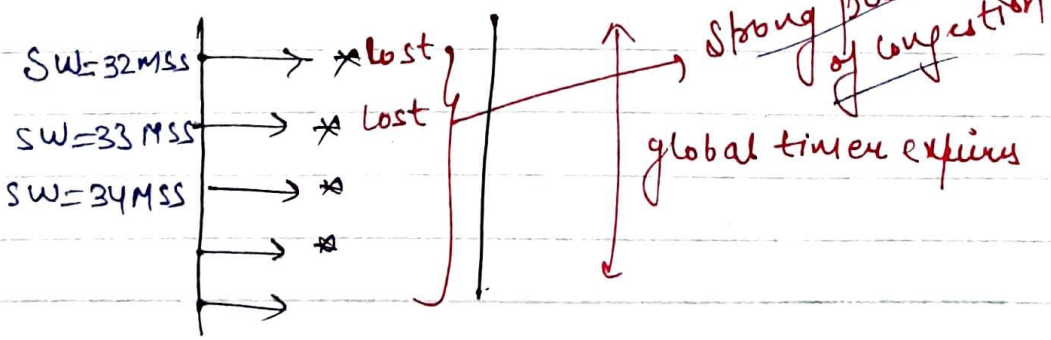
After n RTT → SW = 2^n MSS

- In slow start Algorithm, the increase of sender window size is based on Acknowledgement
- In slow start Algorithm, the ~~increase of~~ Sender

window size ~~it based on~~ increases exponentially upto slow start threshold.

Congestion Avoidance :→ {Additive increase algorithm}





- In Congestion avoidance algorithm, the increase of Senders window size is based on RTT.
- Once the data is lost and after 3 duplicate acknowledgements if the data is accepted then it is known as weak possibility of Congestion
- If the data is lost continuously until the global timer expires it is known as strong possibility of Congestion.

Congestion detection :-> {Multiplicative decreasing algorithm}

Congestion detection

Three duplicate acknowledgement
(weak possibility of Congestion)

$SWI = \frac{1}{2} * (\text{window size})$ ↓ lost

Again apply Congestion avoidance algorithm

Global timer Expires
(Strong possibility of Congestion)

SW = 1 MSS

threshold = $\frac{1}{2} * (\text{window size})$ ↑ lost

Apply Slow start algorithm

Sender threshold = 800

Congestion

Congestion avoidance

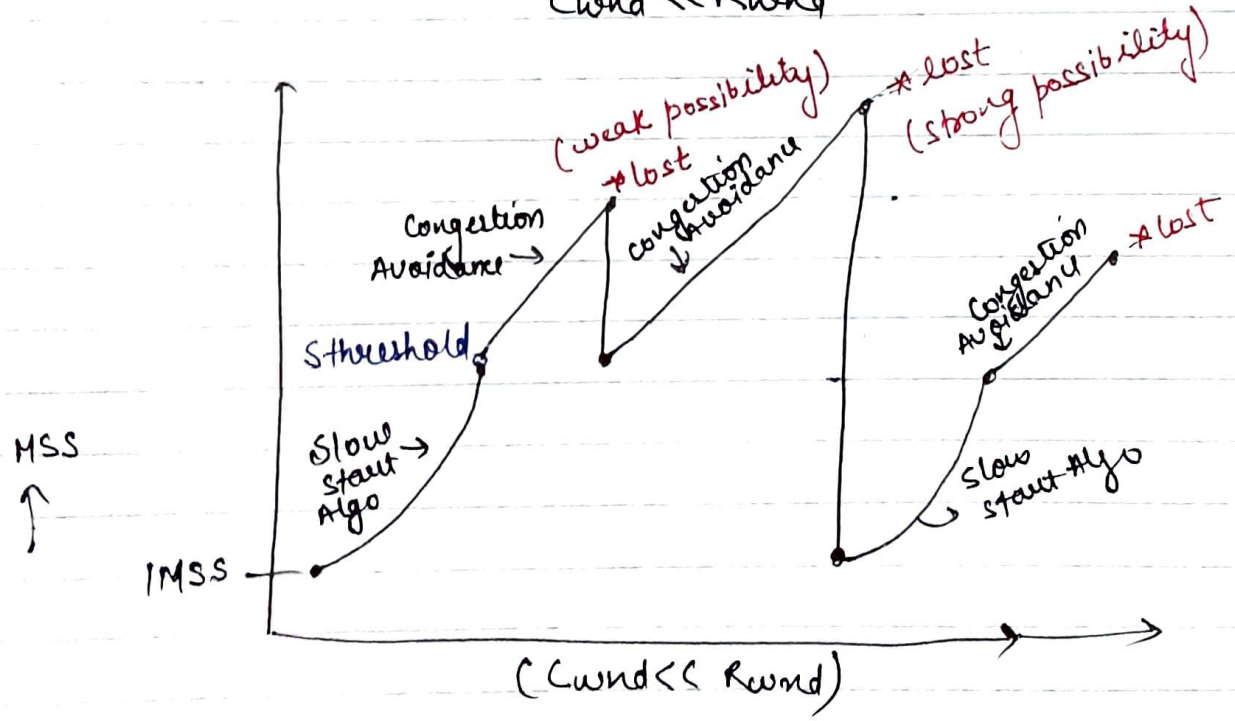
SW = 100 Bytes ← Slow start
200
400
800
1600
1700 ← Congestion Avoidance
1800
1900
2000
2100
2200 * lost
(weak possibility)

1100
1200
1300
1400
1500
1600 * lost
(global timer expires)

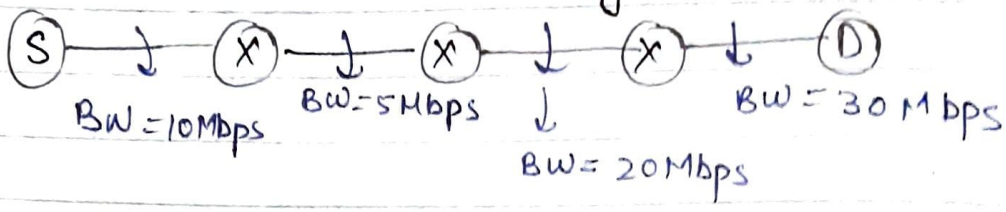
SW = 100 ← Slow start
200
400
800
900 ← Congestion Avoidance
1000
1100
1200 * lost
(weak possibility)

SW = 600 ← Congestion window

Cwnd << Rwnd



Q:- What is the maximum data rate which sender will transmit and that data will go to destination



Ans 5Mbps because all will allow.

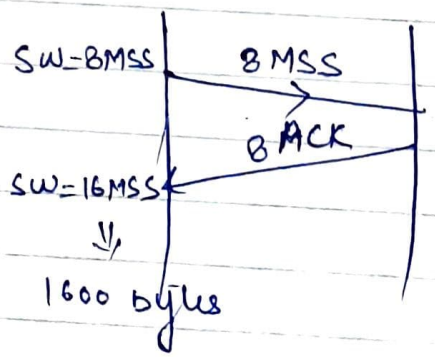
If D < 2Mbps then 2Mbps because all will allow

So, We will take min (Rwnd, Cwnd)

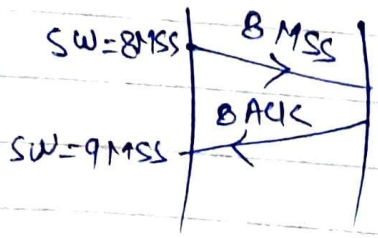
Q:→ MSS = 100 Bytes

Present Window = 800 Bytes

(1) What is the next Window size in slow start algorithm = 1600 Bytes



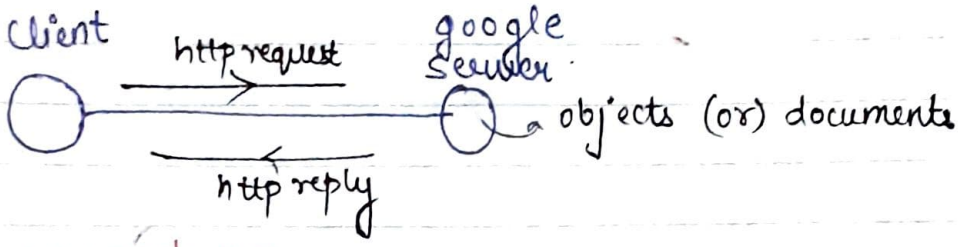
(2) In above problem if congestion avoidance is used sender window = 900 Bytes



APPLICATION LAYER

http protocol (hypertext transfer protocol)

(1) Client - Server Protocol



http://www.google.com
hostname
URL ⇒ uniform resource locator

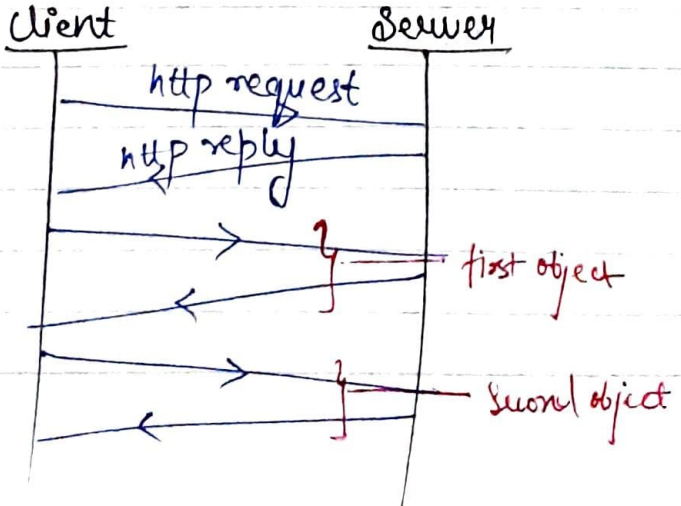
(2) Synchronous Protocol

(3) http
- Persistent http Connection
- Non persistent http connection

(4) Port 80 ≅

(5) Persistent http connection

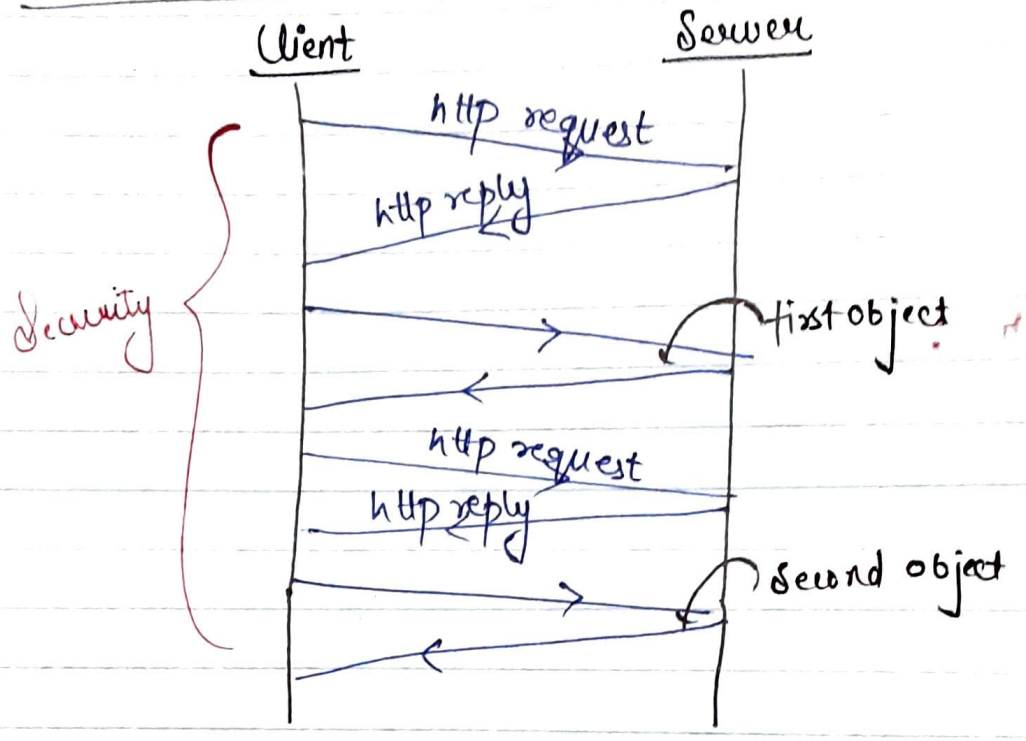
user friendly



(vi) Non-Persistent http:

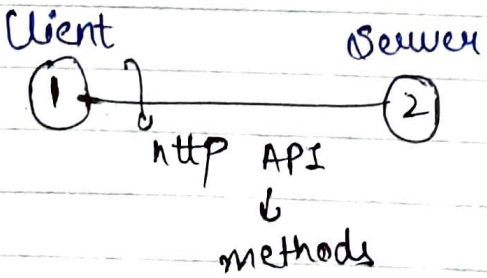
In Persistent http connection, connection will be there only until the objects the accessed.

(vi) Non-Persistent http :-



In non-persistent http, a seperate connection will be established for every individual object to be transferred. So the requirement is to support Security

(vii)



To retrieve document ← get()

Update the modified doc ← Post()

modify the content of doc ← Put()

head() → To get info about the docum

connect() → http → https: → TCP as TL

trace()

Cookies

get() ⇒ It is used to retrieve the document

put() ⇒ It is used to modify the document

post() ⇒ It is used to place the updated document in Server

Connect() ⇒ When connect() method is used data will go via secure channel and that too in encrypted form

trace() ⇒ It is used for debugging the network

listen() ⇒ It converts unconnected active TCP socket into Passive Socket

(viii) http is a stateless protocol.

These days :

1) It is a stateless protocol because it doesn't store any information about the server, the client browser.

2) Cookie is a piece of code that is transmitted from the server to the client browser.

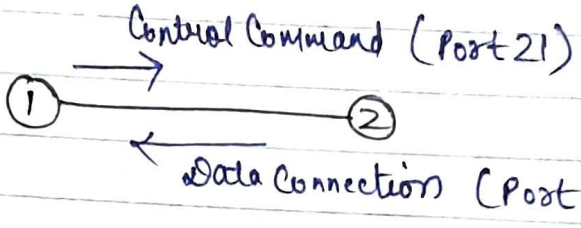
3) The advantage of cookies is faster response and the other one is authentication.

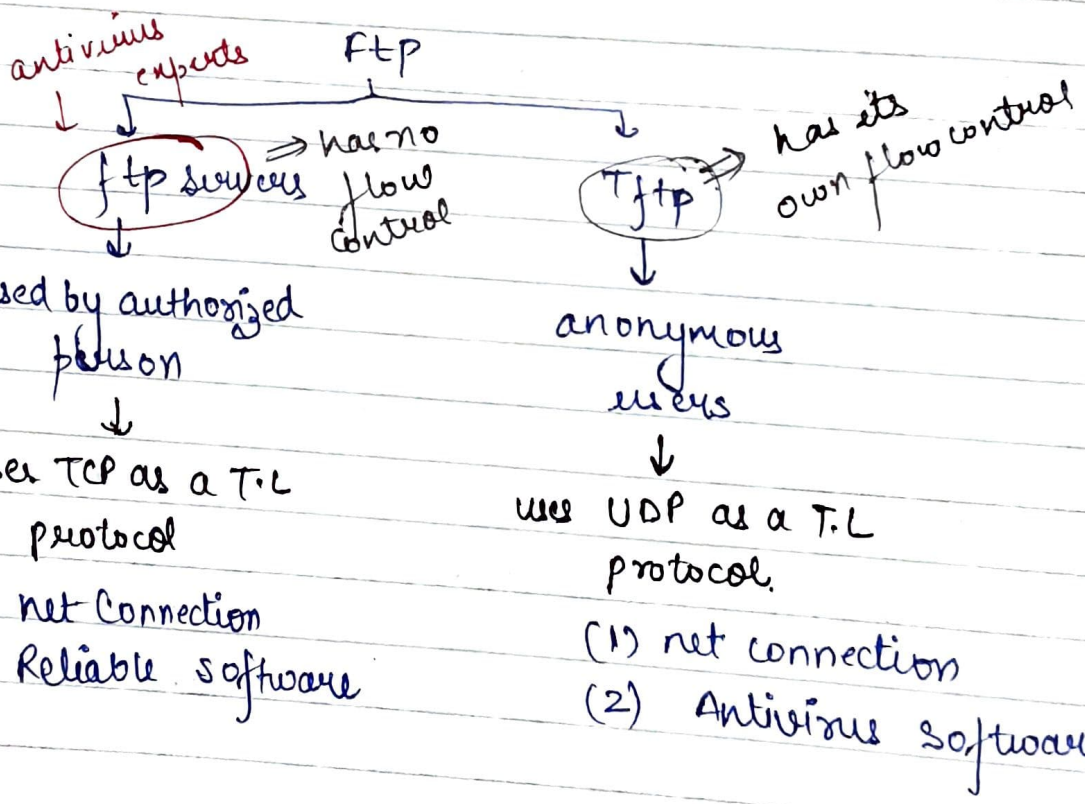
FTP (File Transfer Protocol) :→

FTP ⇒ downloading a file

(i) Port 21 ⇒ Control Connection
Port 20 ⇒ Data Connection

» Synchronous protocol



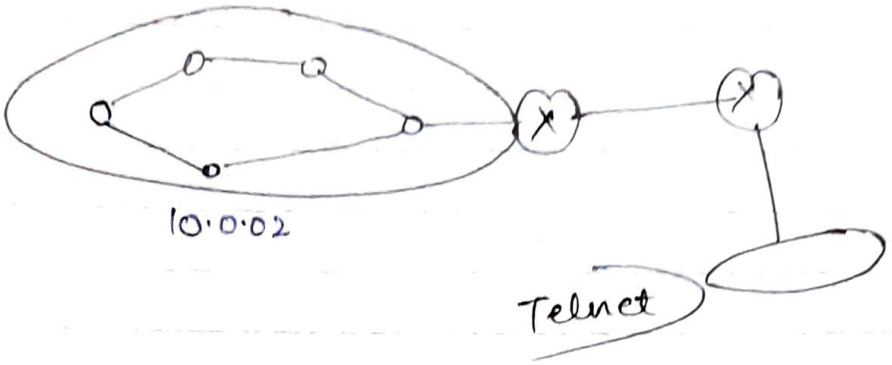


FTP has no flow control

FTP uses control connection to send control comment and once the data is about to download a seperate

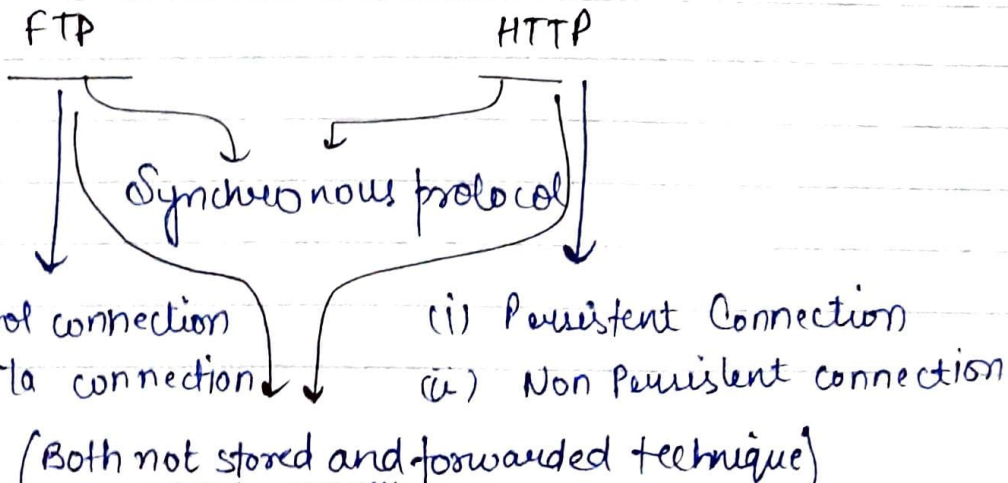
data connection is established

ftp uses tcp as a transport layer protocol because it has no internal flow control



FTP	Telnet
(i) downloading file	(i) Chat operation
(ii) Port 21 ⇒ Control Connection Port 20 ⇒ data Connection	(ii) (Exchange of words) Common connection ↳ Port 23

TCP as Transport layer.



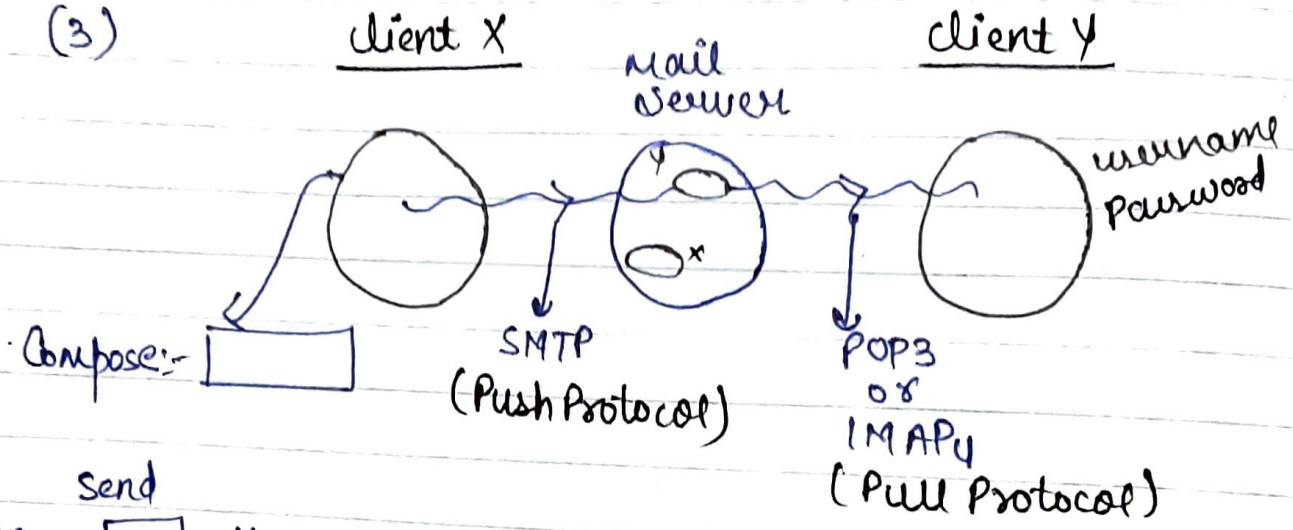
SMTP : Simple Mail Transfer Protocol :-

(1) Port 25
(2) text - based protocol

MIME ⇒ Multimedia Internet Mail Extension

SMTP is a text based protocol but we can send graphical data with the help of MIME extension

(3)



Send
when clicked on ↗ the SMTP agent gets activated.

SMTP is a Push protocol because it is used for sending the mail to the mail server.

POP3 = Post office Protocol
IMAP4 = Internet message access protocol

POP3 or IMAP4 are known as pull protocols because they are used for retrieving the mails from mail server

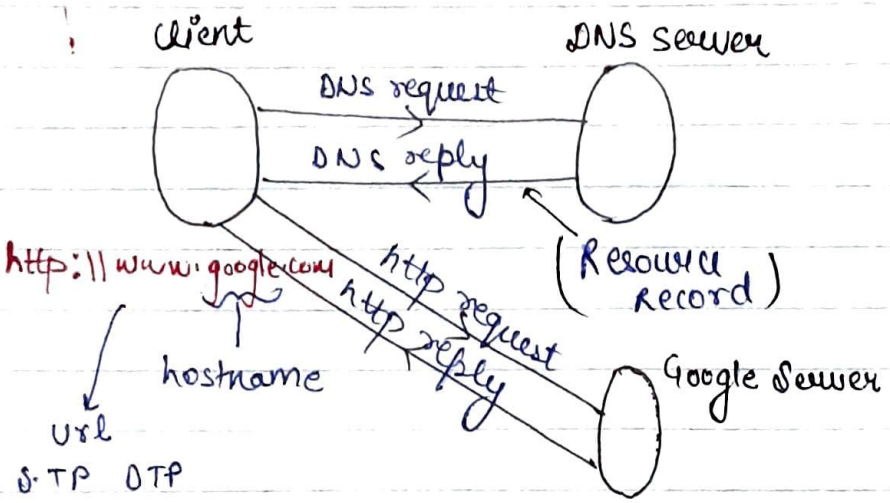
SMTP combine with POP3 or IMAP4 are known as client - to - client protocol with the mediation done by mail server

SMTP combine with POP3 is a store and forward technique with the mediation done by mail server.

IMAP4 is more secure than POP3 because it will scan for viruses before the files gets downloaded

Mails can be kept in hierarchy in case of IMAP4 but whereas in POP3 all mails are equal.

DNS (Domain Name Service) :→



DNS Server contains IP addresses of different Servers. It is used for mapping hostname to IP addresses or vice versa

Design of DNS Server

1. DNS Server should be placed in hierarchy (Searching time is less and uniform)

2. DNS Server should be placed in different geographical locations. (Propogation time is less and uniform)

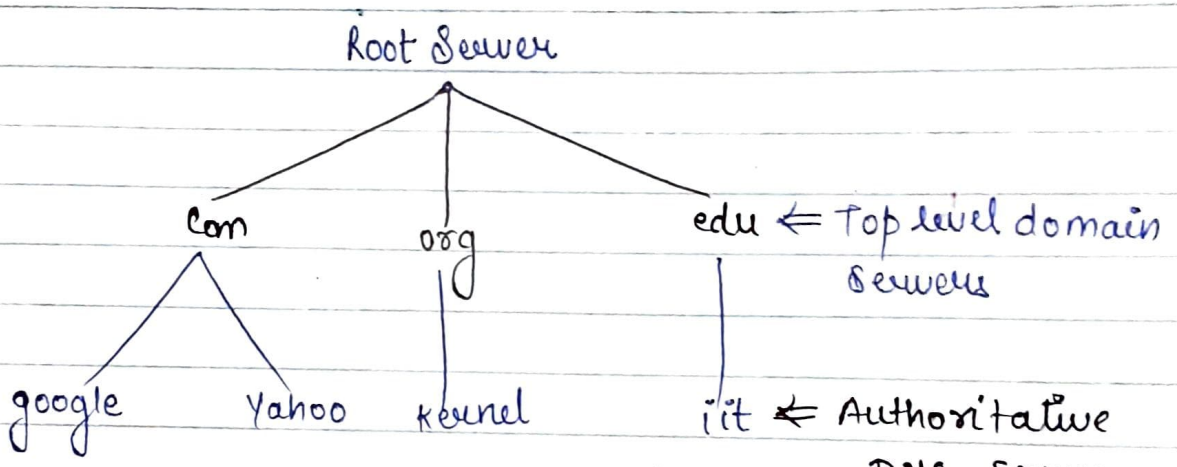
234

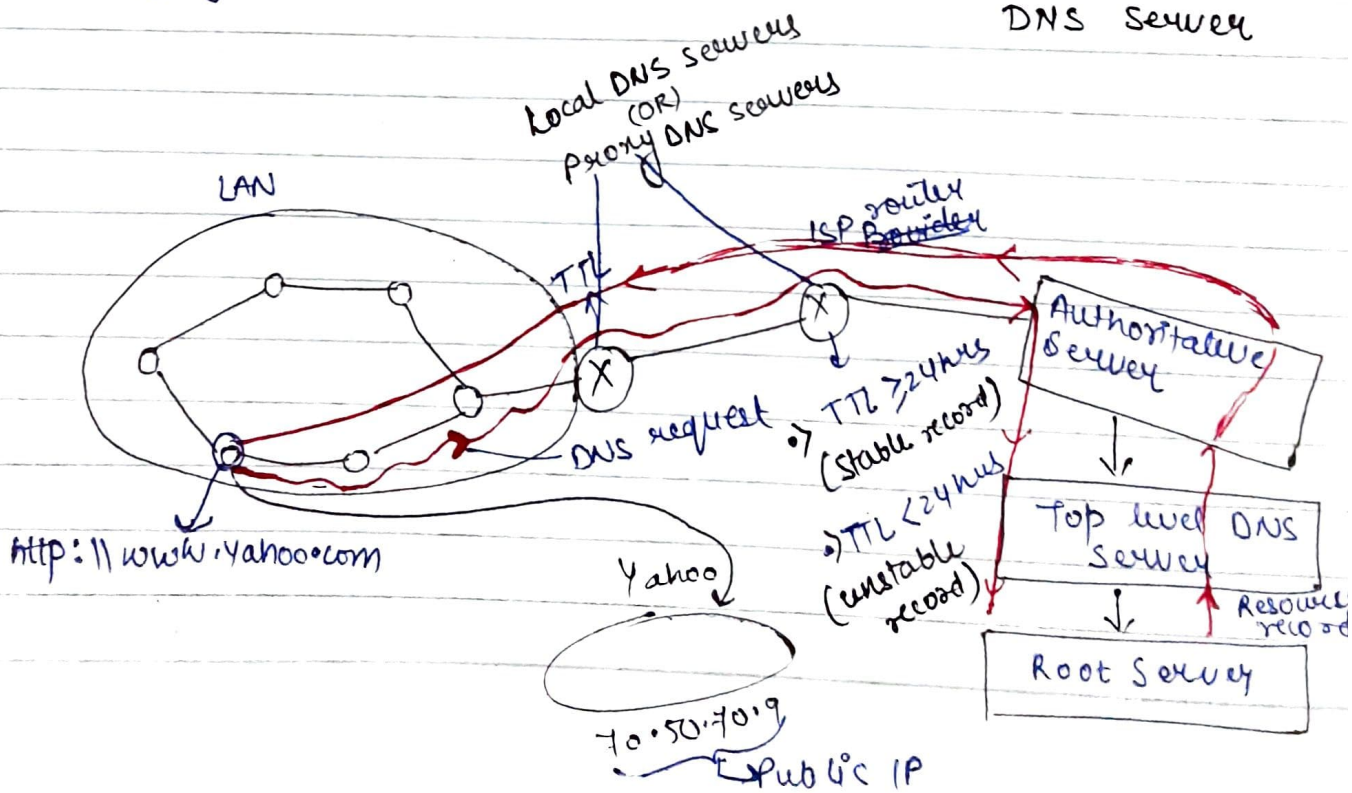
DNS Server :→

(i) Root Server
(ii) Top level domain Server
(iii) Authoritative Server
(iv) Local DNS Server

DNS query
127 levels

www.google.com
www.yahoo.com
www.kernel.org
www.iit.edu





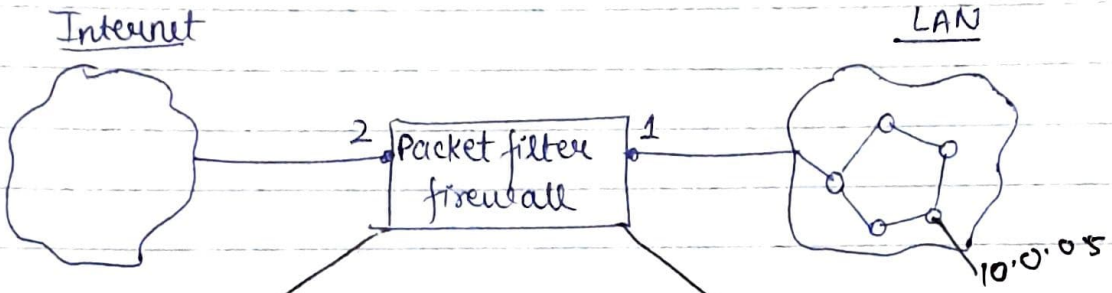
DNS uses UDP as Transport layer

⇒ DNS query < 512 bytes ⟶ UDP as TL

⇒ DNS query ≥ 512 bytes ⟶ TCP as T.L

FIREWALL :-

-> Packet filter firewall (stateless firewall)



Interface	SIP	DIP	S.Port	D.Port
2	141.1.0.0	*	*	*
2	*	10.0.0.5	*	*
2	*	*	*	23
1	*	*	*	80

Packet coming from Lo and Lo n/w should be blocked

* ⇒ all, any

Incoming

- Packets coming from a particular net ID should be blocked
- Packets destinated to 10.0.0.5 are blocked because this system is used for internal LAN only.
- If Port 23 is blocked then telnet service is blocked i.e. no outside system can contact internal system directly.

Layer 4 - Firewall block TCP traffic from specific user on a multi-user system during 9:pm to 5am.

⇒ If Port 80 is blocked then almost all websites can not be used

Definition

Packet filter firewall is a firewall which forwards or block the data by comparing ~~the~~ with network layer and transport layer header.

⇒ If a virus or malicious software is placed in the application layer data then packet filter firewall cannot be detected.

⇒ In stateless firewall every packet or datagram should be checked independently because there is no connection state.

⇒ In stateful firewall group of packets can be checked at the same time because of connection state or sequence number.

Work book

Network layer

16) d

17) c

18) b or d

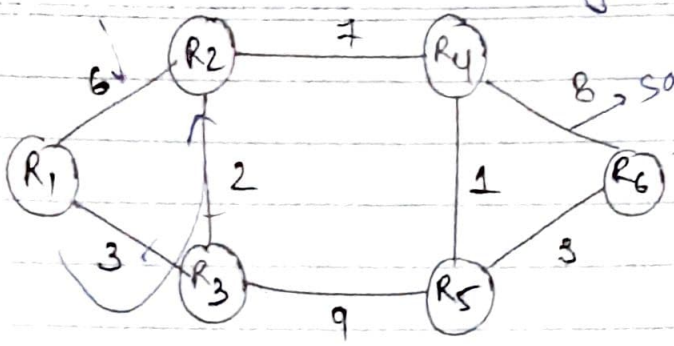
~~b~~ not possible as there is high transmission delay due to store and forwarding

19) b

20) d

21) 9

22)

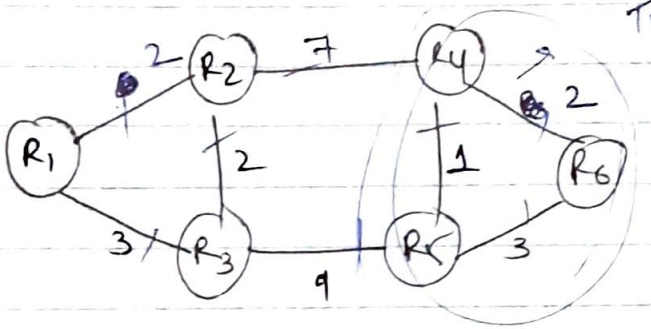


So, in total 2 links will never be used by the Router.

$R_1 \leftrightarrow R_2$ and $R_4 \leftrightarrow R_6$

∴ option - C

23)



To reach R6 path 3 is only either go R5-R4-R6 or R5→R6 so go for no. of hops. (less no of hops we will consider)

∴ 0. and that's why option (a)

24)

BW = 10^7 bps

propagation speed = 200 m/μsec

→ 1 μsec = 200 m

→ 1 sec = 10^7 bits

1 bit delay ⇒ 10^{-7} sec

1 bit delay ⇒ 10^{-7} sec ⇒ 20 m of cable

25)

C + PS = MS

C = 8 megabits

237

$f = 1\,Mbps$

$N = 6\,Mbps$

$$8 * 10^6 + 1 * 10^6 * S = 6 * 10^6 * S$$

$$10^6 [8 + S] = 6S * 10^6$$

$$8 = 5S$$

$$S = \frac{8}{5}$$

$$\boxed{S = 1.6\,sec}$$

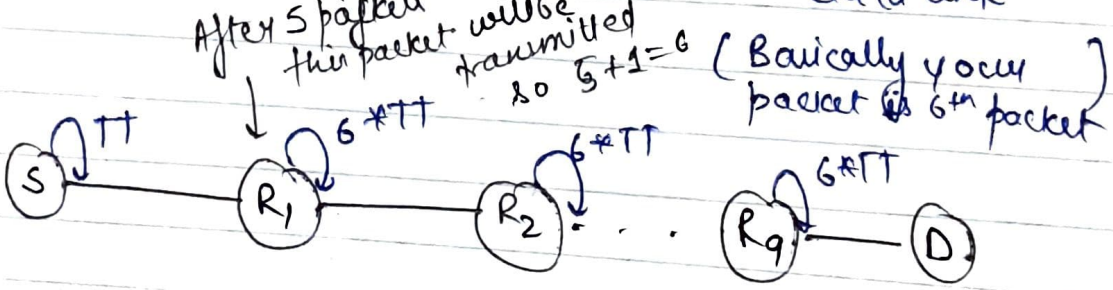
Q26

OSI → 7 layers

TCP/IP → 5 layers

X.25 network → 3 layers ⇒ Physical network data link

Is



$$= TT + 9 * 6 * TT$$

$$= 17.18 + 54 * 17.18 \text{ millisec}$$

$$= 945.3 \text{ millisec}$$

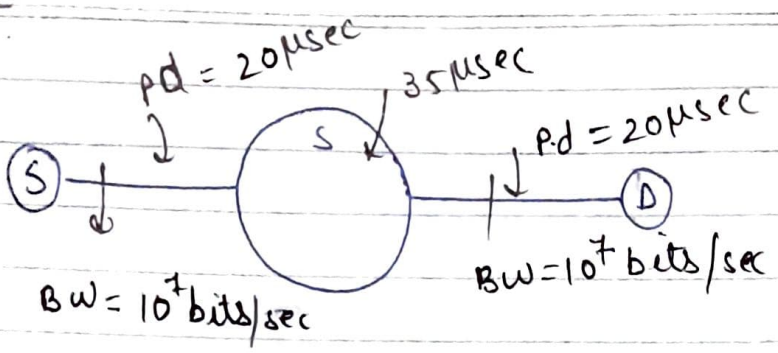
$$TT = \frac{1100 \text{ bits}}{64 \text{ Kbps}}$$

$$TT = \frac{1100 \text{ bits}}{64 \times 10^3 \text{ bps}}$$

$$= 17.18 \text{ millisec}$$

Chapter - 6

T2



10000 bits

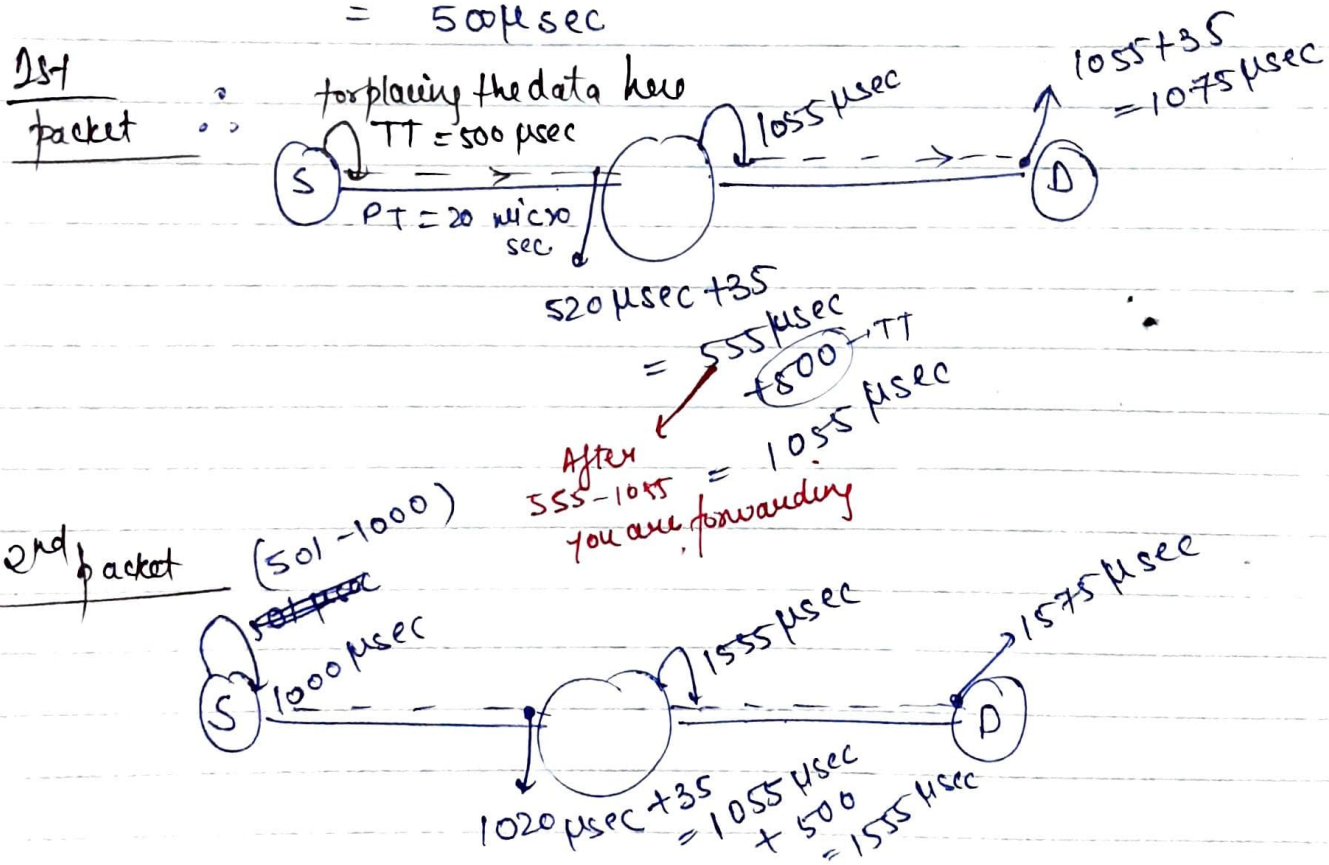
↓

two packets

Each packet size 5000 bits

$$T.T = \frac{5000 \text{ bits}}{10^7 \text{ bits/sec}}$$

$$= 500 \mu sec$$



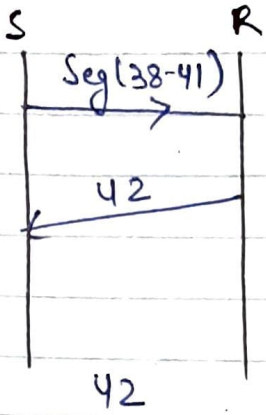
* By the time of 1055 2nd packet is ready for transmission and 1st packet complete the transmission that's why it is store and forward.

240

1) d)

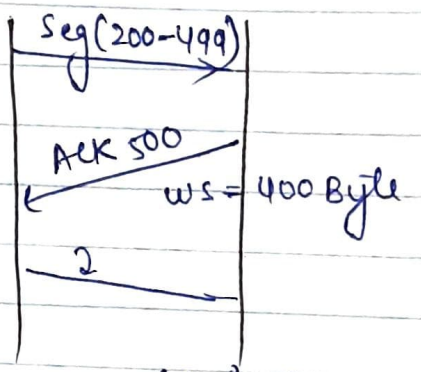
2) a)

3)

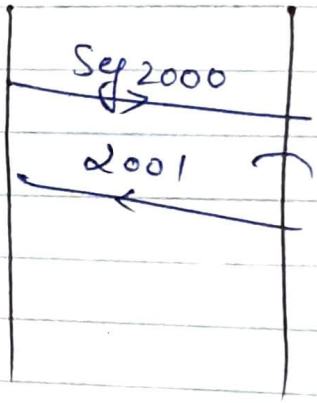


∴ option C

4)



S1 is true



only one Ack when Segment size is only 1 byte

So option (a)

5) d)

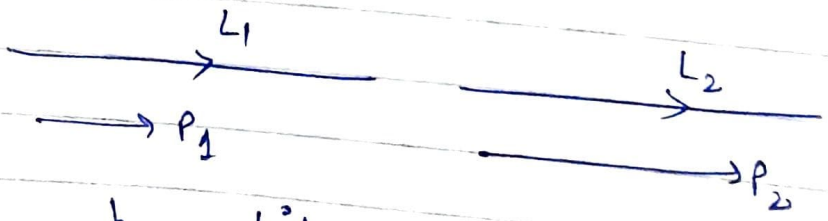
6) IP ensures means take the help of ICMP

∴ option (d)

7) TCP is designed for maximum communication rat

∴ option a)

8)



b_1 = bit error probability

b_2 = bit error probabili

$(1-b_1)$ → no error for 1 bit

$[(1-b_1) * (b1-b_1) * \ldots L]$

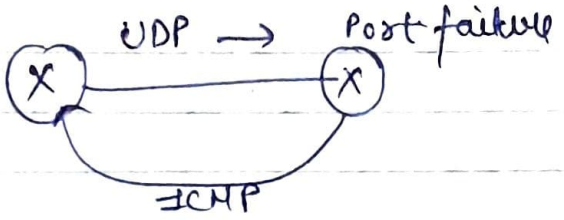
$(1-b_1)^L \Rightarrow$ no error

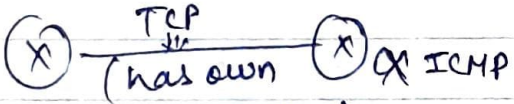
b_2 bit error probability $(1-b_2)^L$

$$P(L_1 \cup L_2) = P(L_1) + P(L_2) - P(L_1 \cap L_2)$$
$$= P_1 * (1-b_1)^L + P_2 * (1-b_2)^L$$

∴ option (a)

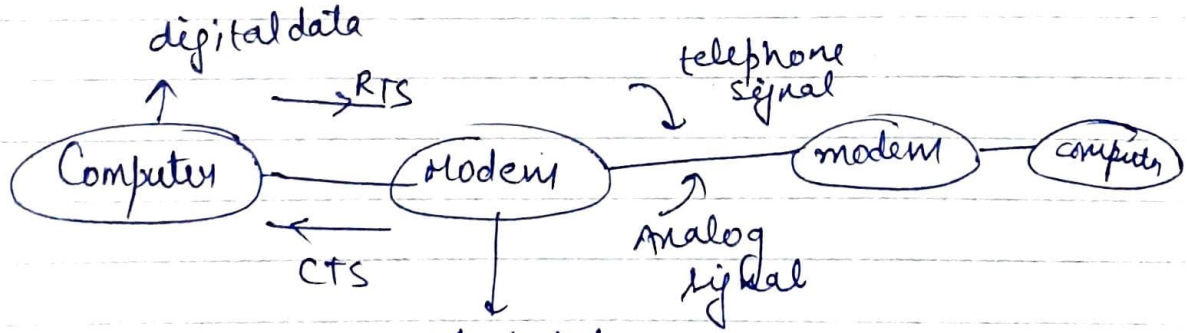
9)





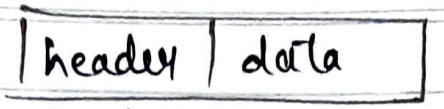
∴ option (a)

10)

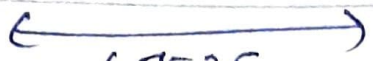


∴ option (a)

11)



20-600



{ If data is max header is min. }

$20 + x = 65535$

$x = 65535 - 20$

$x = 65515$ Byte

12) d)

13)

∴ option (b)

14) d)

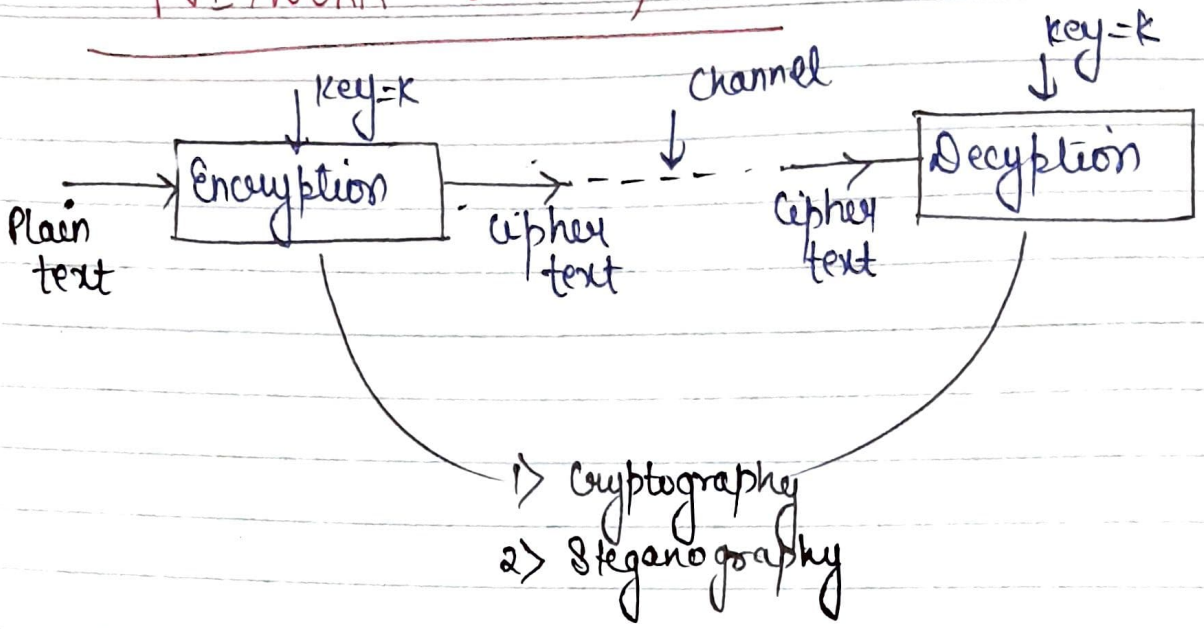
LLC is a data link layer

15) a)

When on the local n/w then use ARP to get the physical address of the station and send packet directly

Or on any other n/w then send packet to gateway specified in the routing table

NETWORK SECURITY



Cryptography :-

Cryptography is a Science of Converting one form of data into another form to provide Security to the data is known as cryptography

Steganography :-

Steganography is a Science of hiding the data behind an image or video

=> Key
- Public key
- Private key

Public key

If the key is transmitted on the channel it is known as Public key

Private key

If the key is not transmitted on the channel it is known Private key

Cryptography

- Symmetric key Cryptography
  - eg:- Diffie hellman key exchange
- Asymmetric key Cryptography
  - eg:- RSA algorithm

- For encryption and decryption if same key is used it is known as Symmetric key cryptography
- For encryption and decryption if different keys are used it is known as Asymmetric key cryptography

Functions of Cryptography :-

1) To provide Confidentiality :-
   Providing secrecy to the data is known as Confidentiality

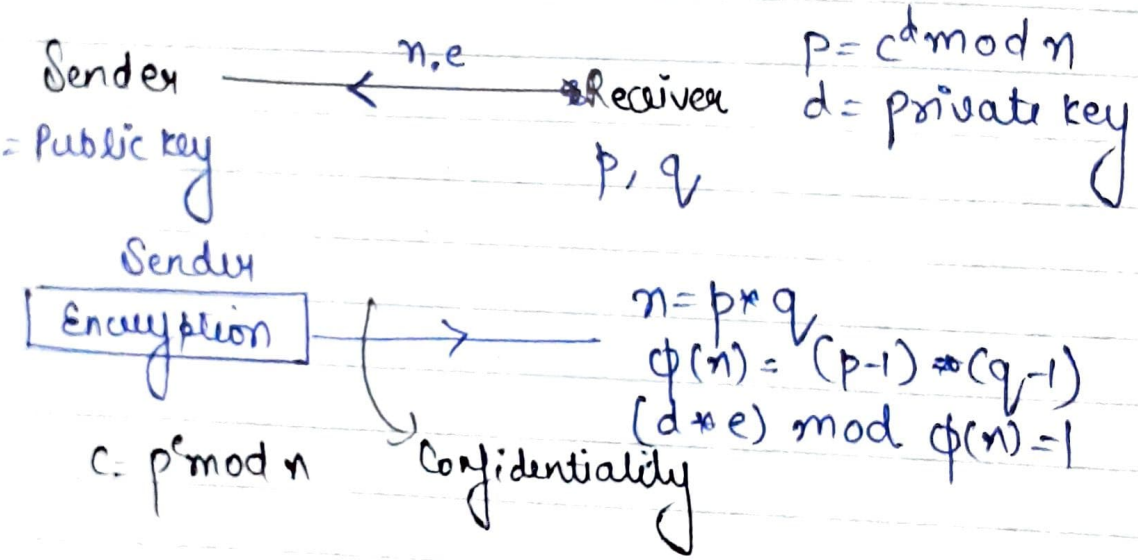
2) To provide authentication
   - Authentication of user
   - Authentication of data

- Providing integrity of user and proving user identity is known as authentication of user
- Providing integrity to the data is known as authentication of data

Key features of Cryptography :-

1) Prime numbers
2) Random numbers (challenge)
3) time stamp
4) Key → Private key
   Key → Public key.

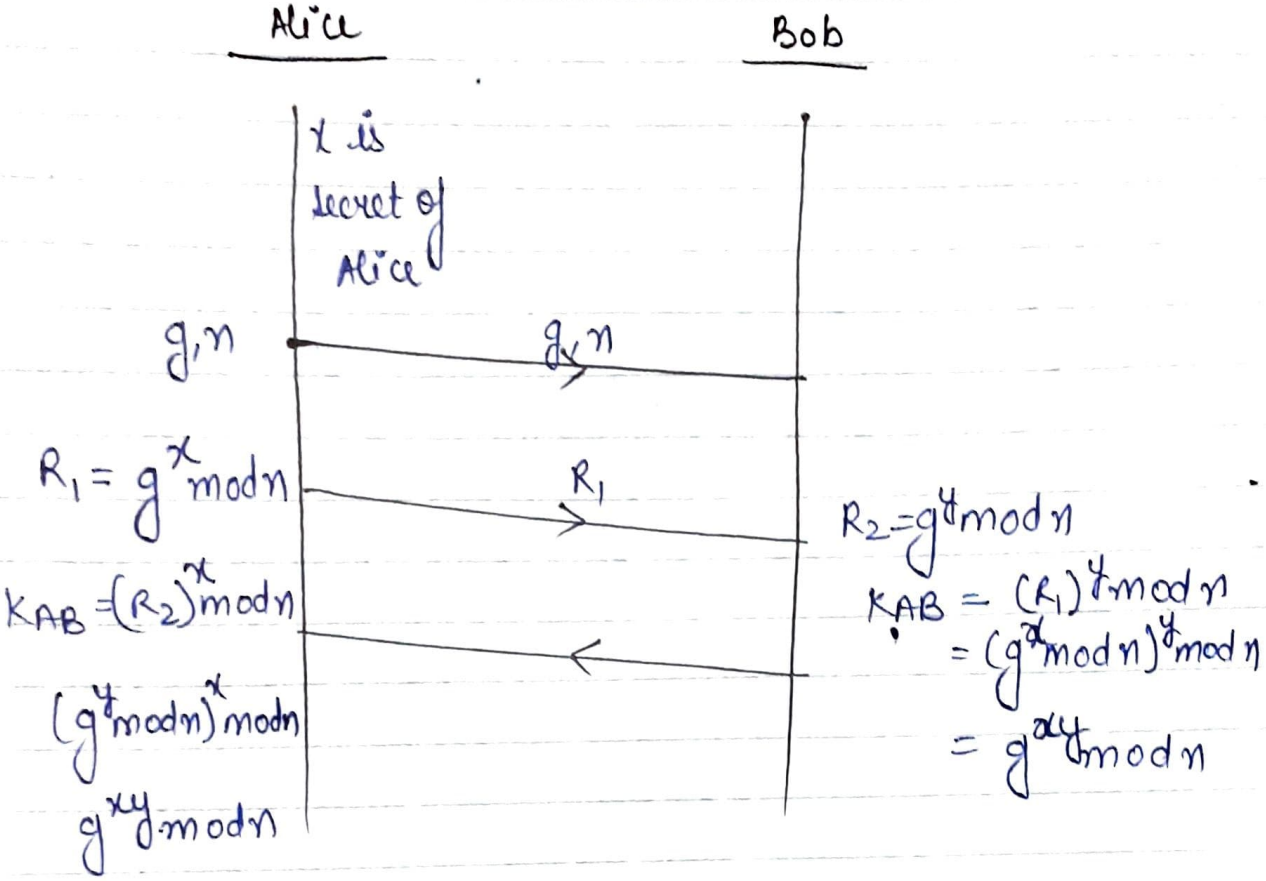
RSA Algorithm :-



→ Initially RSA algorithm is used to provide confidentiality

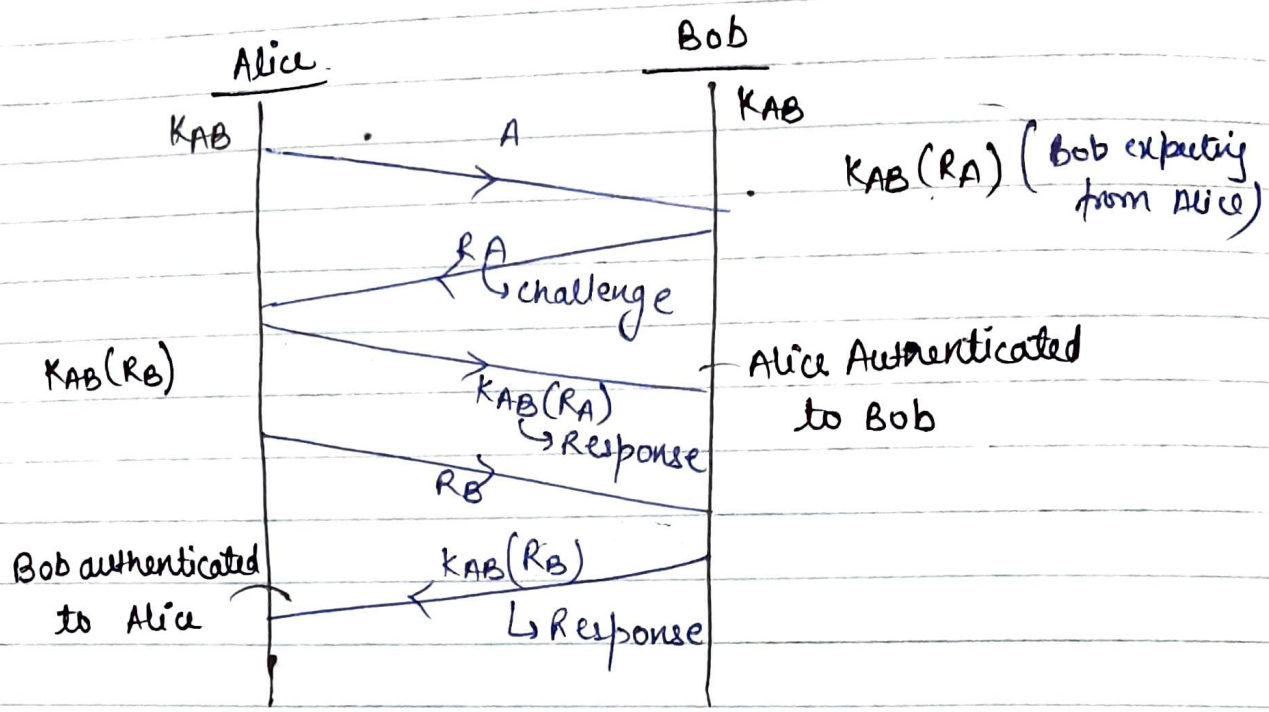
→ If the Sender is encrypting the data with receivers public key data is decrypted with receivers private key, it is used to provide Confidentiality

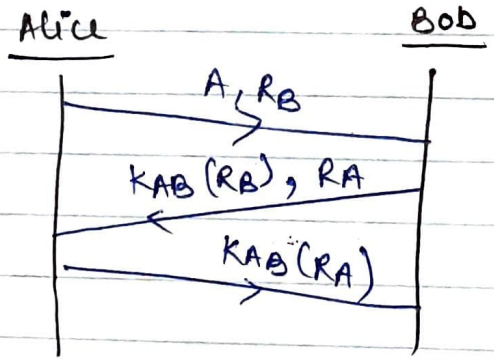
Diffie Hellman Key Exchange :-



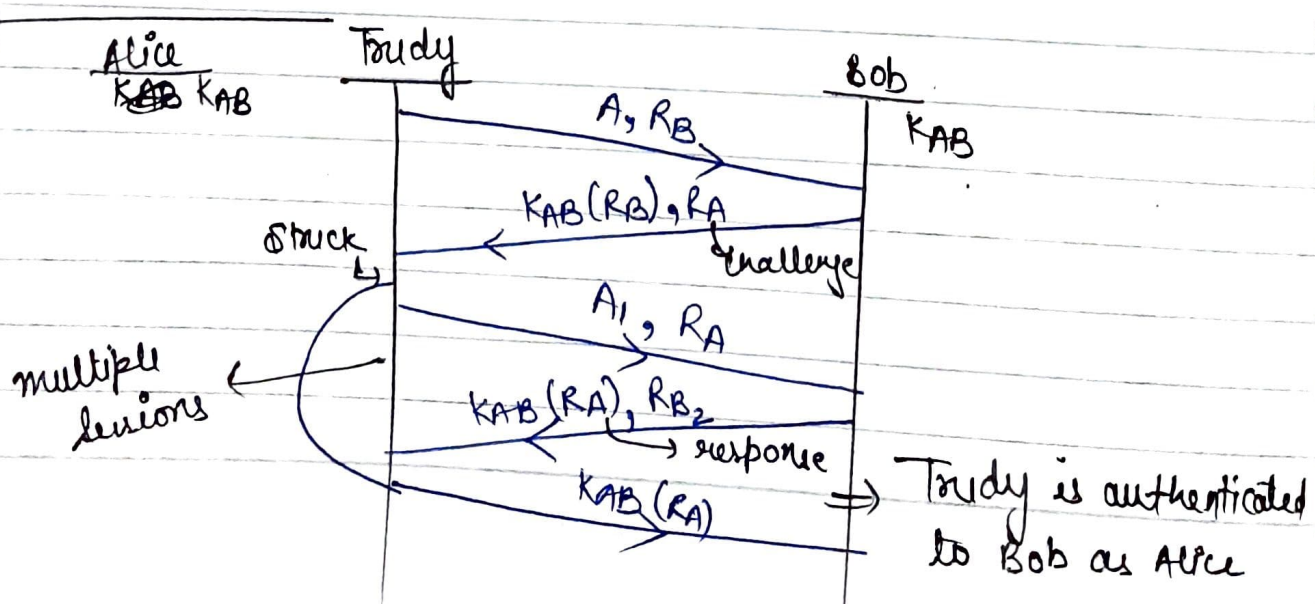
Diffie Hellman key algorithm is also called as symmetric key cryptography or (secret key cryptography).

Mutual authentication using Diffie Hellman key Exchange



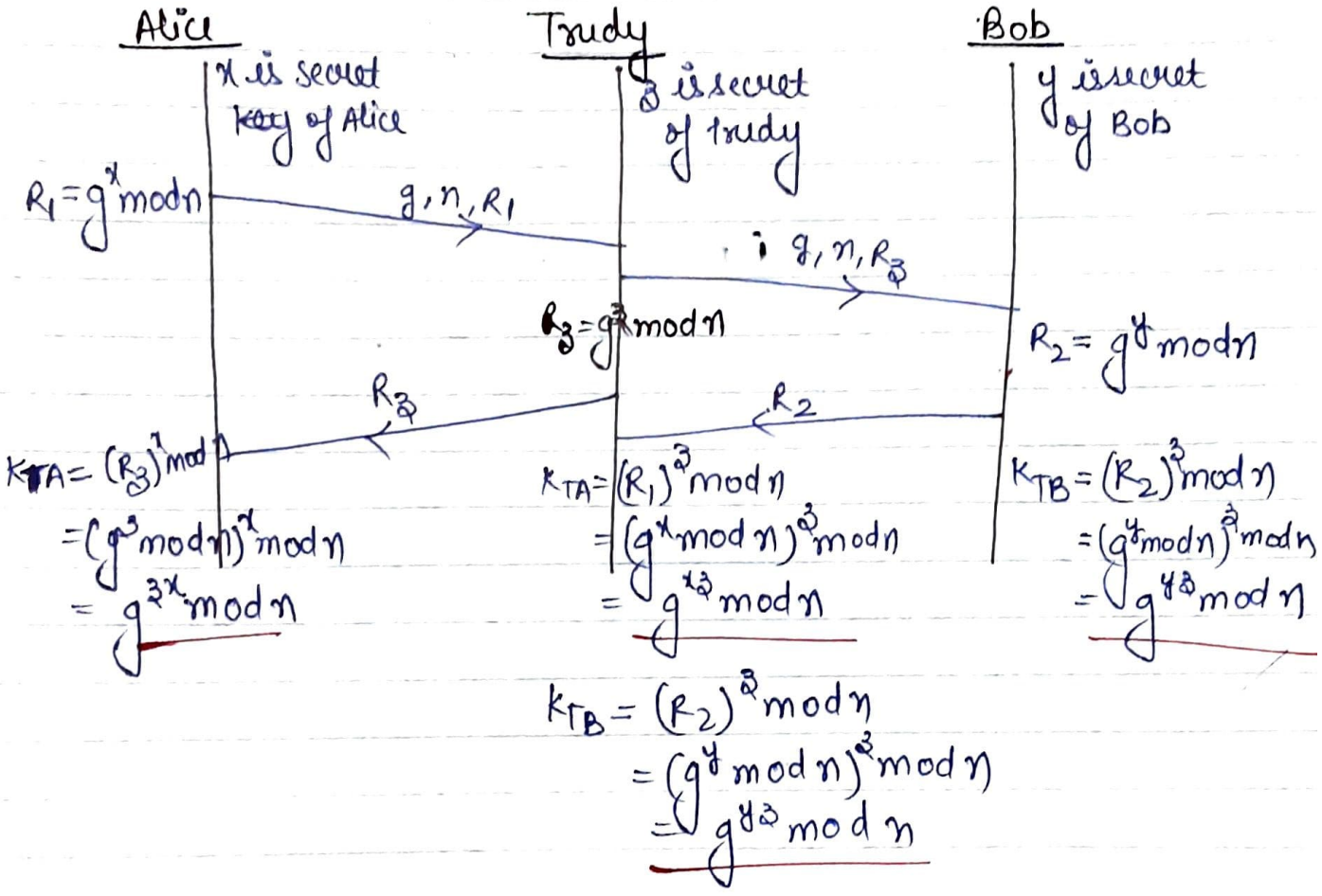


Reflection attack



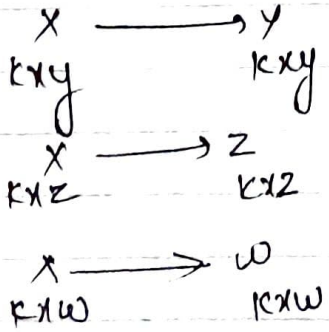
⇒ Mutual authentication can be broken using an attack called reflection attack

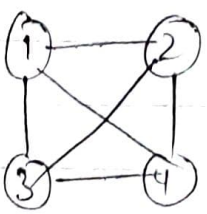
Man in the middle attack



$K_{TB} = (R_2)^z \bmod n$
$= (g^y \bmod n)^z \bmod n$
$= g^{yz} \bmod n$

⇒ If the systems are connected in mesh topology with n no. of systems then total nC_2 cables/keys are required

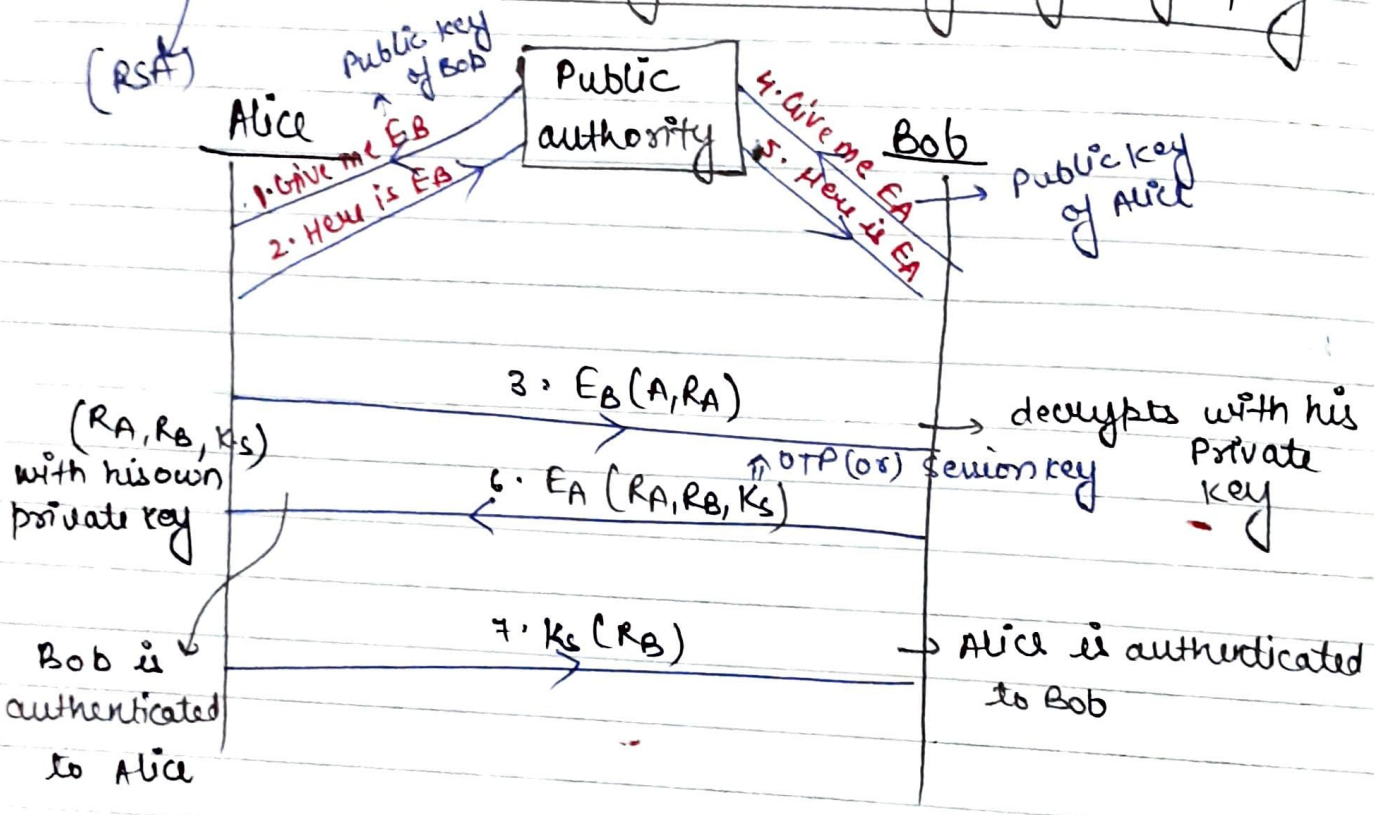




$= nC_2$ keys

•> The drawback of Diffie Hellman key is remembering all the key values or maintaining the database of all key values is difficult so the burden of key value is taken care by Public Authority or third party agencies.

Mutual authentication using Public key Cryptography

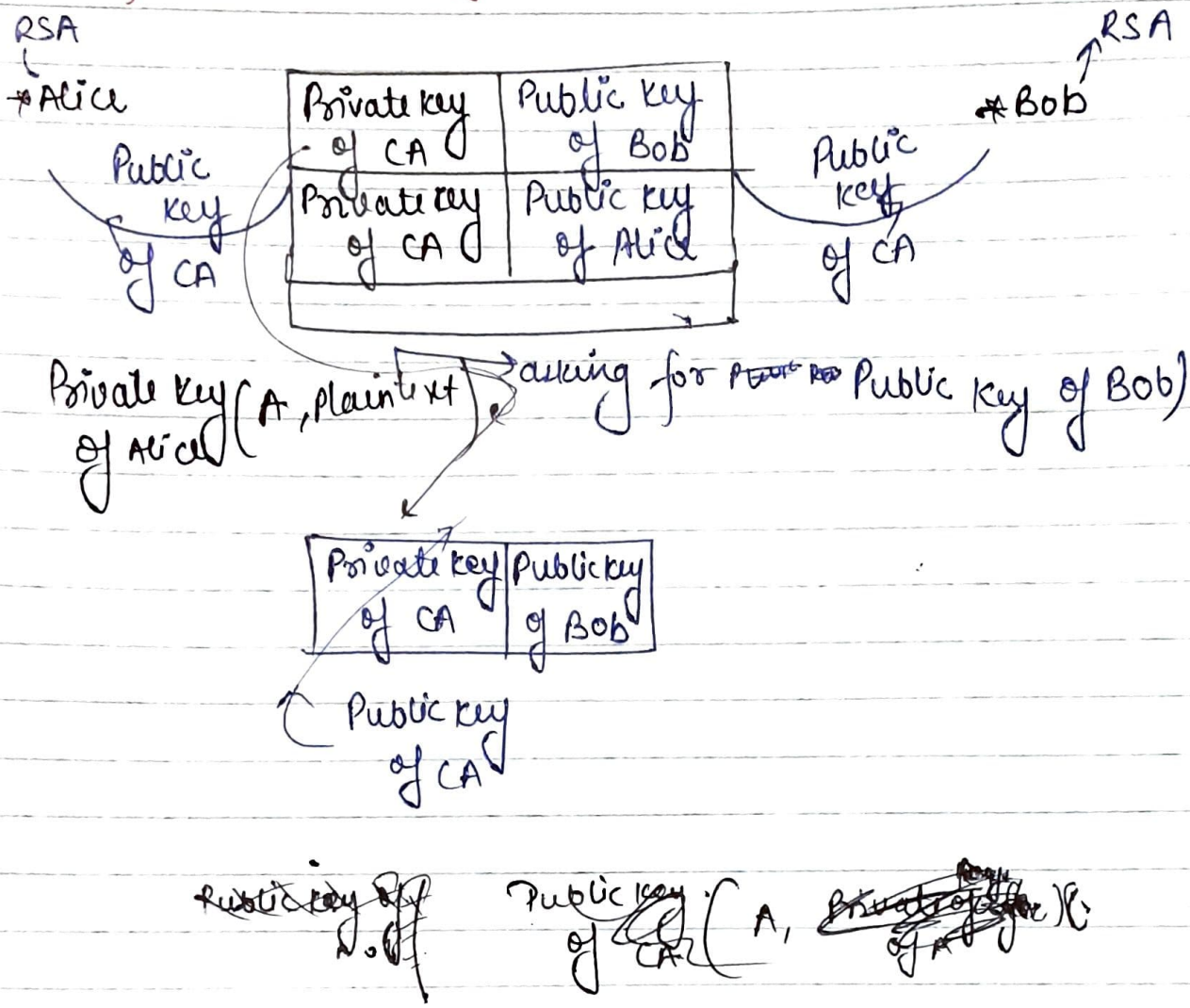


It is slow because here encryption is done and encryption take some time.

•> Mutual authentication using RSA is better than mutual authentication using Diffie hellman key in terms of Security

•> Mutual authentication using diffie hellman key is better than mutual authentication using RSA in terms of speed.

Certification Authority :→ (Public Authority)



⇒ If sender is encrypting with his own private key and receiver is decrypting with sender's Public key it is used to provide authentication.

⇒ If the sender is encrypting with receiver's Public key and receiver is decrypting with his own private key it is used to provide Confidentiality

Public key of CA (A, Private key of Alice (A, Plain text))

decrypt ↓ Private key of CA

↓ decrypt with Public key of CA

Authentication of Data :-

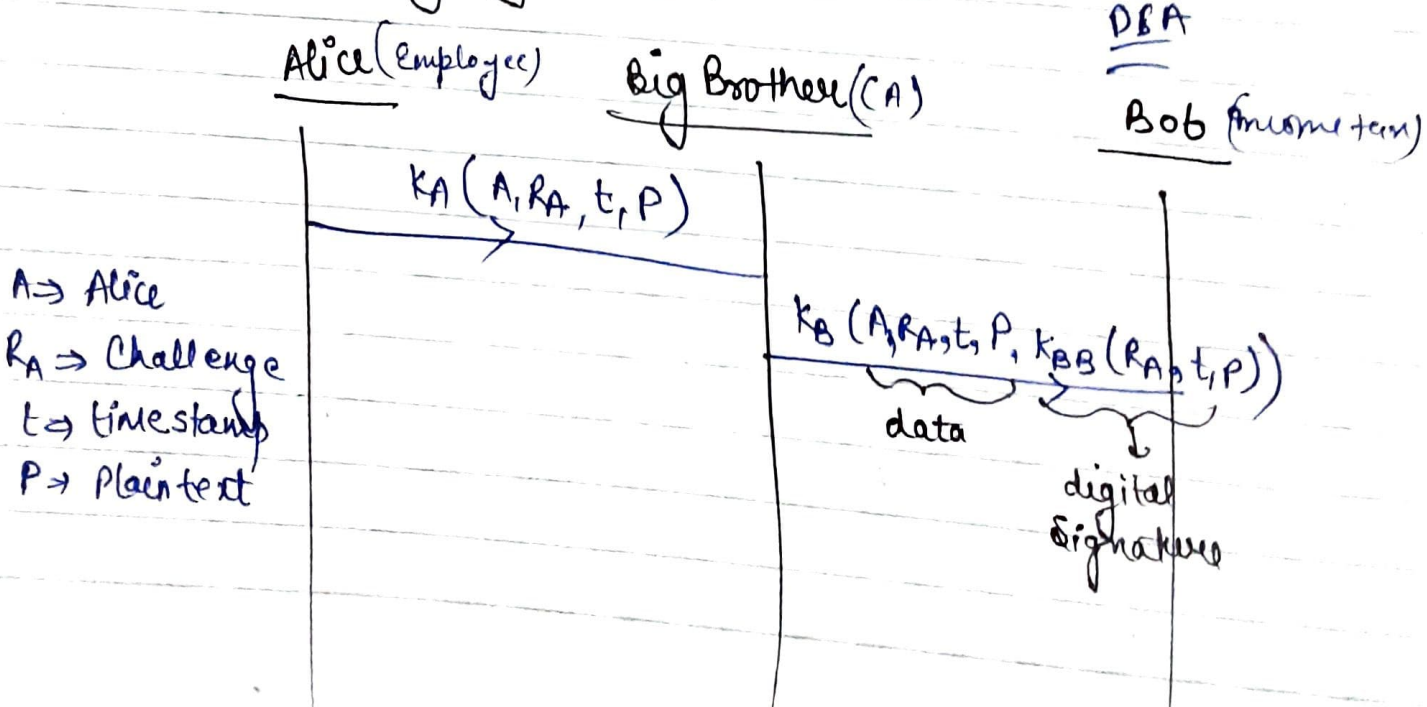
→ Digital Signature

- In Conventional Signature for all types of data same signature is used. whereas in digital Signature for every individual data a seperate signature is created.
- In a Conventional Signature both data and Signature cannot be seperated whereas in digital Signature both data and digital Signature can be seperated.

Digital Signature

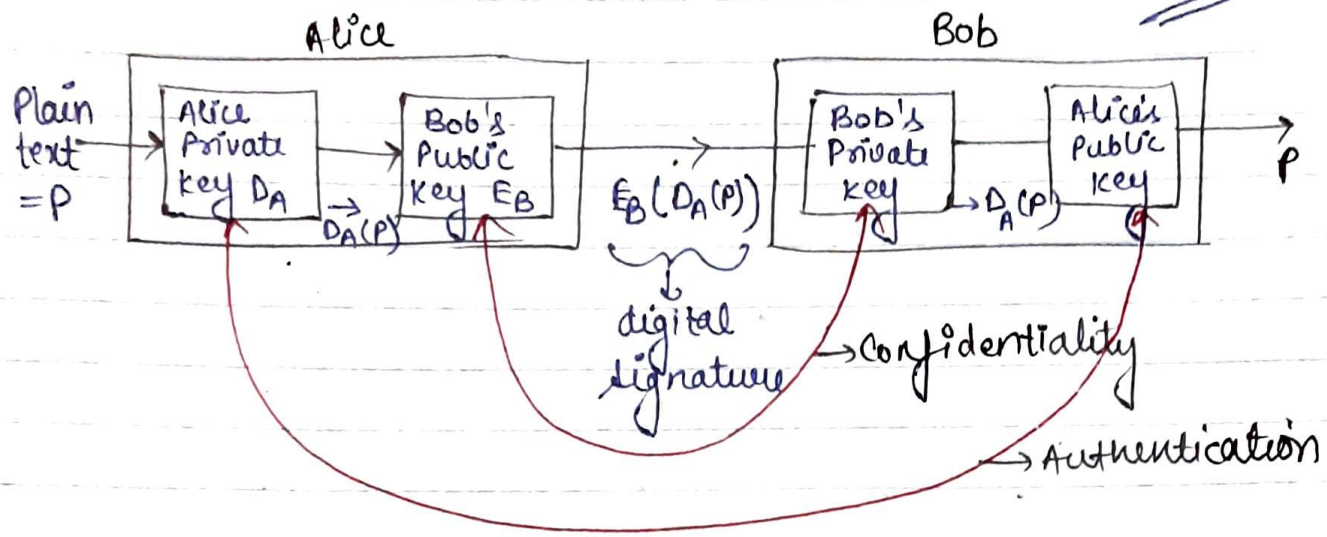
- Symmetric key Signature
- Asymmetric key Signature

Symmetric key Signature



Asymmetric key Signature

RSA



Drawback of Symmetric key Signature

The drawback is that entire algorithm is based on big brother

Getting a public key is easy once you get the private key that's why in Asymmetric key signature if we swap in Alice then $D_A(E_B(A))$ is not correct as D_A is private key, once the hacker gets this he/she can easily guess public key So its better to have public key outside

- Asymmetric key signature is better than Symmetric key signature in terms of Security
- Symmetric key signature is better than asymmetric key signature in terms of speed

Message digest

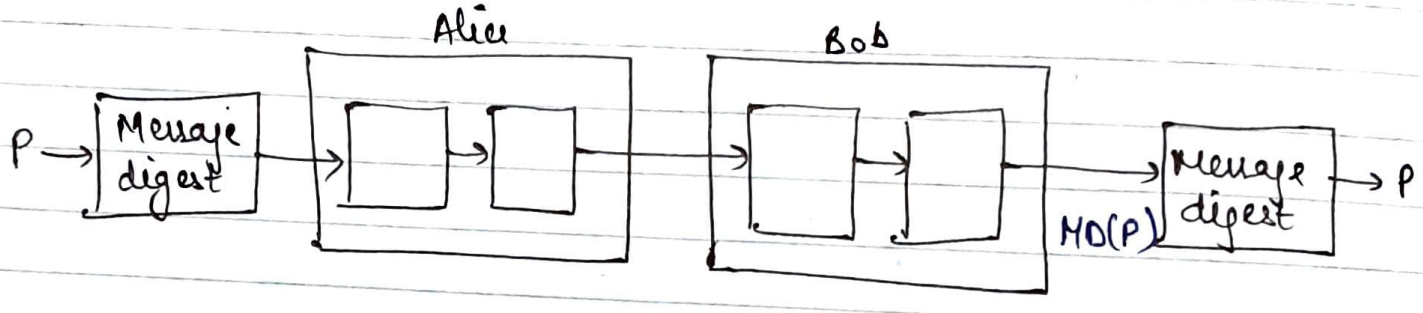
Plaintext = (15170193019501906030 4)

mod function (100)

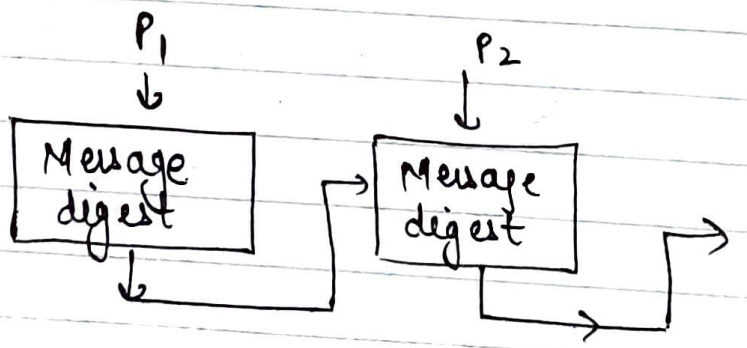
$MD(P) = P \bmod n$

$= (15170193019501906030 4) \bmod 100$

$= 4$



Plaintext = ($\overbrace{15}^{P_1}\overbrace{17}^{P_2}\overbrace{01}^{P_3}\overbrace{93}^{P_4}\overbrace{01}^{P_5}\overbrace{95}^{P_6}\overbrace{01}^{P_7}\overbrace{90}^{P_8}\overbrace{60}^{P_9}\overbrace{30}^{P_{10}}\overbrace{4}^{P_{11}}$)



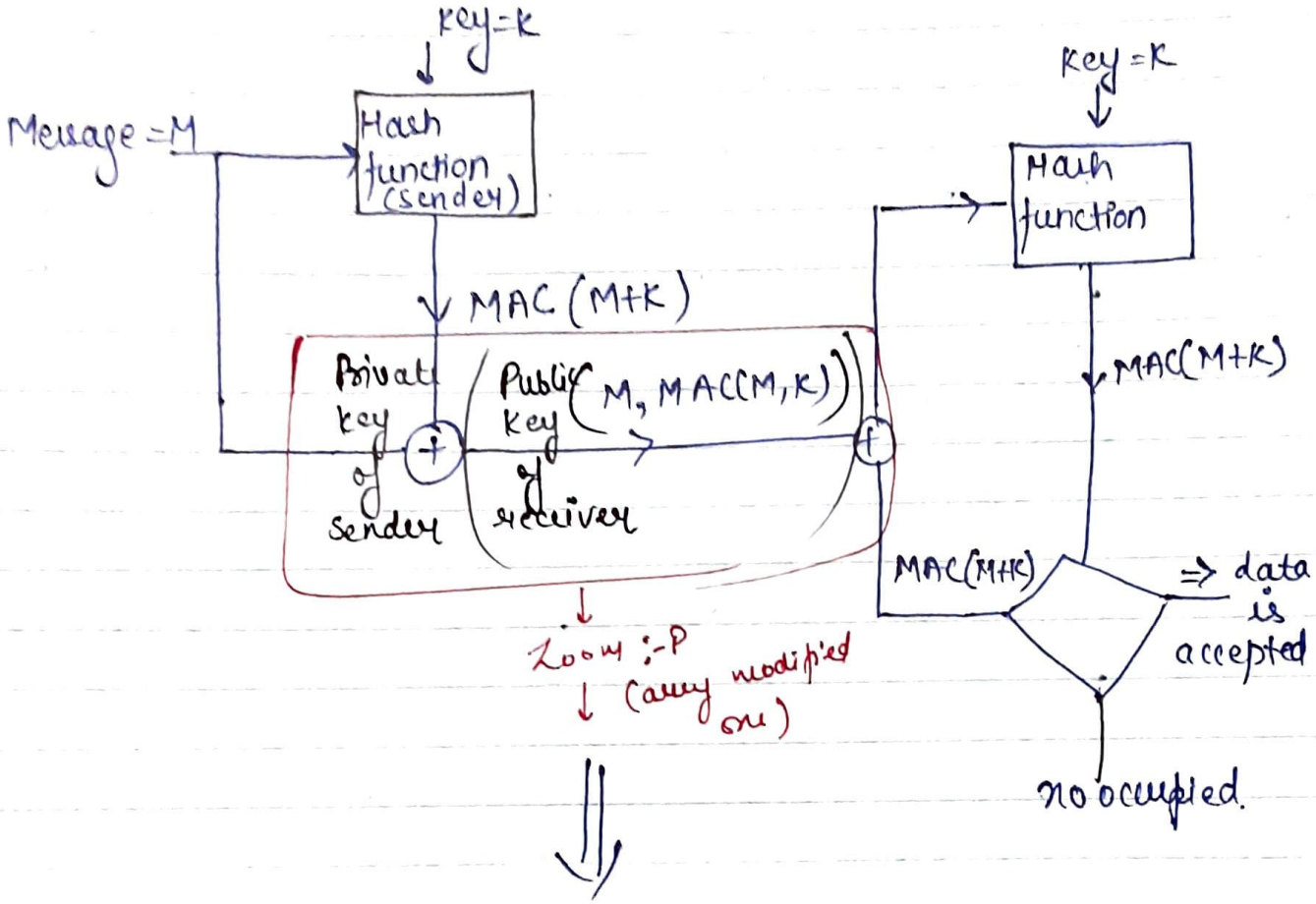
- (i) Given P, any one can calculate MD(P)
- (ii) Given MD(P), it is difficult to calculate P' such that $MD(P') = MD(P)$

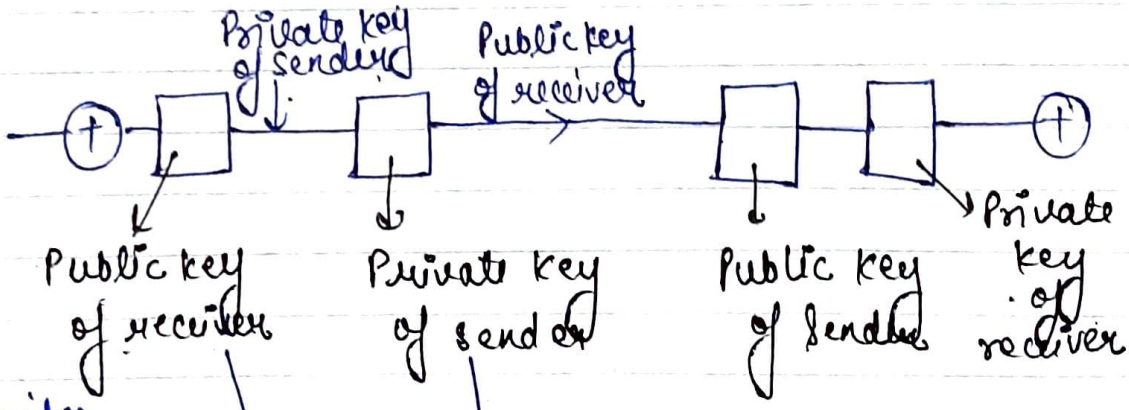
Digital Signature

↓ application

→ Message authentication

~~Ethernet~~ (chained hash function)





It provides

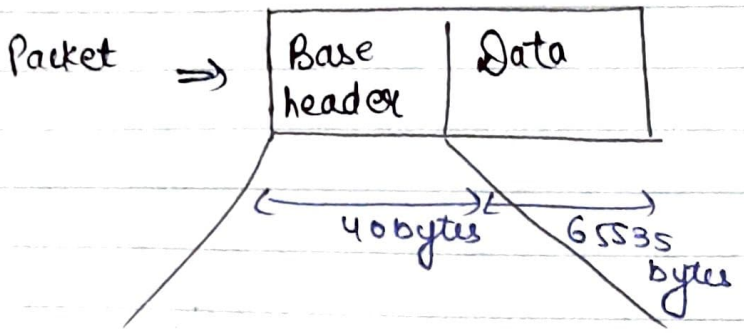
→ authentication of user

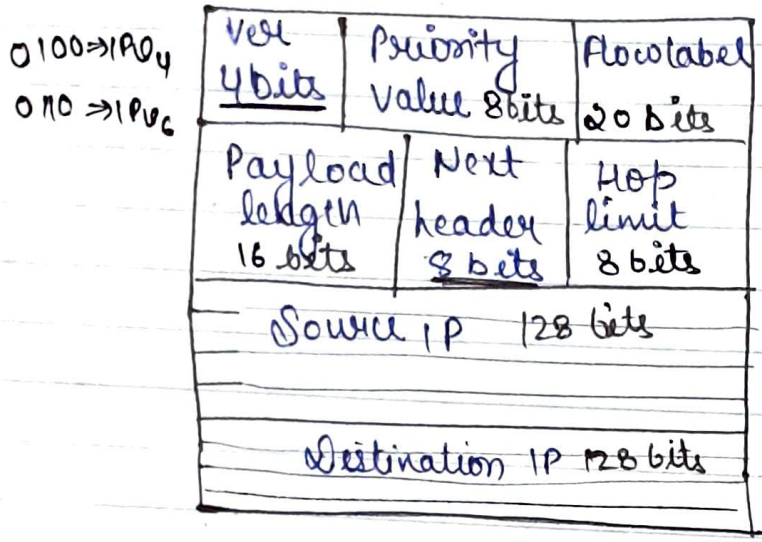
→ Confidentiality

→ authentication of data

25.5

IPV6



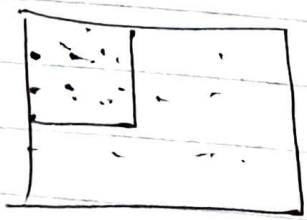


32*4 = 128 bits

* FTP is having more priority then SMTP
* Foreground packet is having more priority than background packet

FTP , SMTP

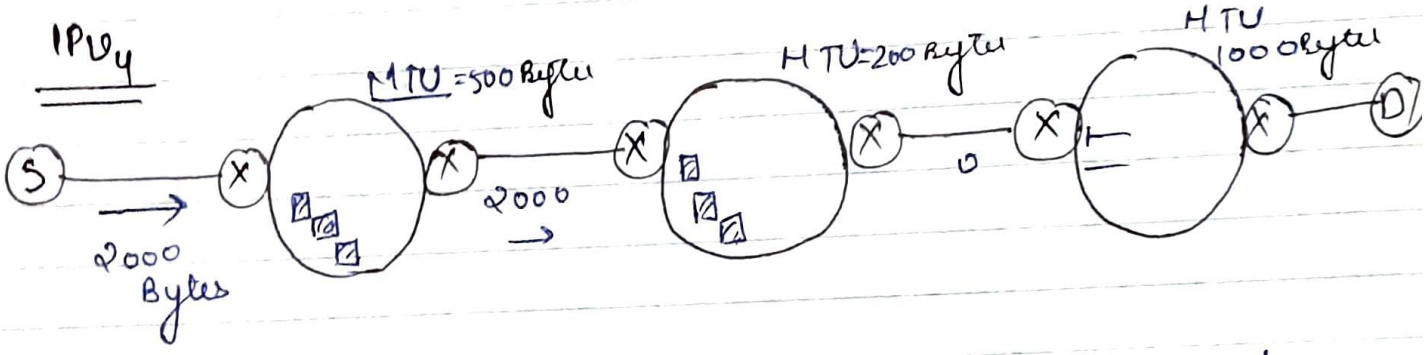
foreground packet , Background Packet



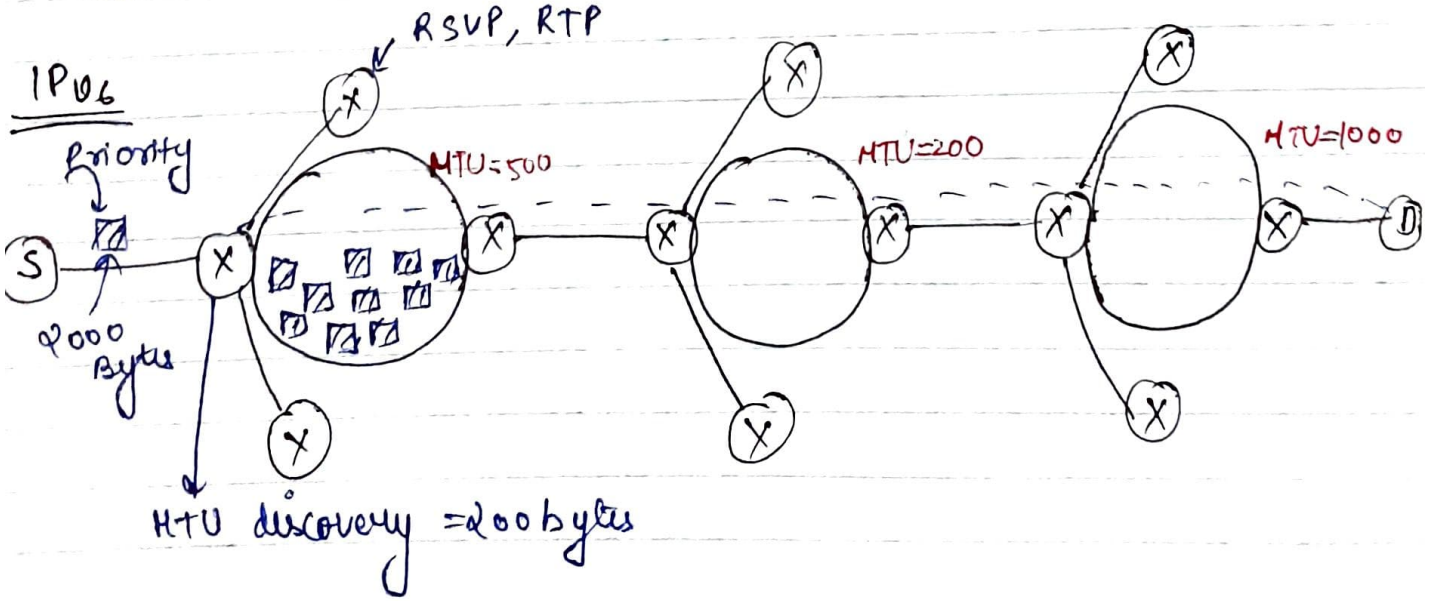
www.cuciyfo.com

* Control Packets have highest priority out of all packet

- In IPv6 packets are forwarded based on priority and the flow label numbers.
- In IPv6, each packet can be uniquely distinguish with a priority value combine with flow label number.
- Total length in IPv4 indicates the size of the packet whereas payload length in IPv6 indicates size of the data.



In IPv4 fragmentation and defragmentation are done by the intermediate routers



257

⇒ Every LAN has its own MTU. It is not fixed.

⇒ In IPv6, fragmentation is done only at the source and defragmentation is done at the destination and that too it is an option.

⇒ The purpose of hop limit is to identify if any loop will exist for the packet

⇒ IPv6 is fast as compared to IPv4

Q:- In standard Ethernet cable if "l" is the length of cable. What would be the length of cable if:

(1) fast Ethernet (100 Mbps) is used $\overset{As}{=} l/10$

(2) if Gigabit Ethernet (1000 Mbps) is used in order to maintain same frame size in CSMA/CD of standard Ethernet cable? $\overset{As}{=} l/100$

IEEE 802.3

↓ CSMA/CD

$TT = 2 * P.T$

↳ acquiring the channel

→ Standard Ethernet ⇒ BW = 10 Mbps

→ $\frac{\text{data size}}{BW} = 2 * \frac{l}{v}$

$\frac{\text{data size}}{10 \text{ Mbps}} = 2 * \frac{l}{v}$

(1) $\frac{x}{100 Mbps} = 2 * \left(\frac{1/10}{v}\right)$ — this is a question

If cancelled then one zero of 100 Mbps will be

(2) $\frac{x}{1000 Mbps} = 2 * \left(\frac{1/100}{v}\right)$

Parallely Bandwidth increases
Channel utilization is less
length is decreased.

Workbook (Transport layer)

(1) Initial RTT = 35 millisec
New RTT = 32 millisec

$ERTT = \alpha * I.RTT + (1-\alpha) * NRTT$

$= 0.9 * 35 + 0.1 * 32$

$= 31.5 + 3.2$

$\boxed{ERTT = 34.7 \text{ Msec}}$

$IRTT = 34.7$
$NRTT = 40$ millisec

$ERTT = \alpha * IRTT + (1-\alpha) * NRTT$
$= 0.9 * 34.7 + 0.1 * 40$
$= 35.23$ ∴ option (4)

2) RTO = 2 * 35.23
= 70.46
∴ option (a)

3) S1 : true
SMTP uses TCP protocol ∴ S2 also true.

4) Assertion (A) is true.

S.W = min (Cwnd, Rwnd)

If Cwnd << Rwnd
SW = Cwnd ⇒ Congestion policies

If Rwnd << Cwnd
SW = Rwnd ⇒ flow control policies

∴ option (d)

5) option (c) same as 1st question

6) option (d)

7) option (d)

8) option (c)

9) option (b)

SMTP → 1
BGP → 4
TCP → 2
PPP → 3

10) (a) option

11) (d) option

12) Socket creates a logical part b/w TL and NL
(logical part → virtual circuit)

TL → Port address
NL → IP address

-> bind() → joining
when IP address and Port address are bind then the socket address is visible.

-> listen() → ready to provide service to the client.

-> Socket() → logical path at the client side

-> Connect() → Going to fail in this question coz socket address not visible.

1) Socket function will create a logical path b/w a transport layer and network layer

2) Bind() function will join port address and IP address :∴ option (c)

13) Public key cryptography → RSA
Secret message → Confidentiality

∴ option (a)
(c) option is for authentication

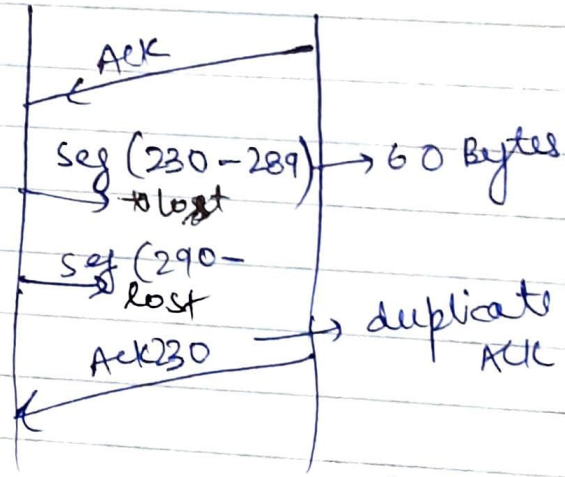
14) Cwnd = 4 KB
Rwnd = 6 KB

Cwnd. < Rwnd
then (congestion policy will be implemented)

s.w. = Cwnd
= 4096 bytes
∴ option (b)

If flow control policy is implemented
then s.w = 2048.

15)



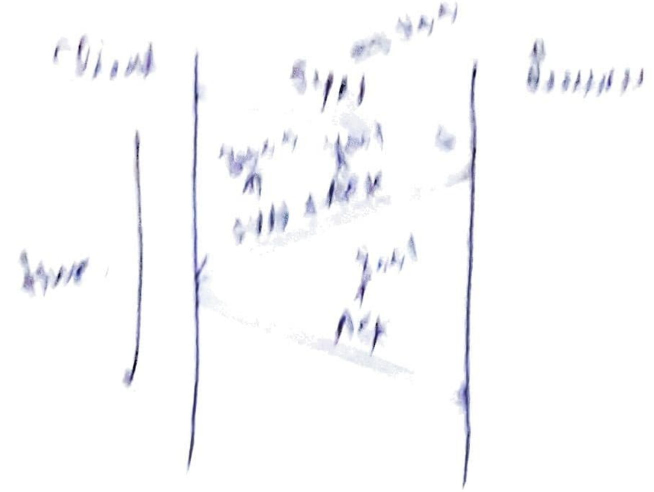
∴ option (d)

16) Telnet ⇒ 3
FTP ⇒ 2
NNTP (Network News transfer Protocol) ⇒ 4
DNS ⇒ 1

∴ option (c)

[illegible]

18.)



S_1 is true → as there is no connection b/w client & server
S_2 is false
S_3 is false
(SYN is at client side and not server side)
S_4 is true
∴ option (b)

18) option (c)

19) option (b)

20) NNTP → 3
SSH → 4
Daemon → 2
means background process
↓
process we cannot preempt
Append → 1
∴ option (b)

21) option a
22) option (d) as seq no is there that's stateful protocol
23) option (d)
24) option (c)

25:→ Wrap around time

- 3 bits then 0 → 7 → 1 wrap
- TCP → Sequence bit → 32 bits

$(0 \text{ to } 2^{32}-1)$

1 byte ← 1 sequence no. is assigned

2^{32} bytes ← 2^{32} sequence no.

(In TCP only the 1st segment is assigned a sequence no. and then followed by a window size segment) ↑ 1 wrap around

Here BW = 40GBps

1 sec = 40×10^9 bits

1 sec = 5×10^9 bytes

Logic

2^{32} bytes ← 2^{32} seq no ← wrap around time

$\left(\frac{2^{32}}{5 \times 10^9}\right)$ sec

1 sec = 5×10^9 bytes

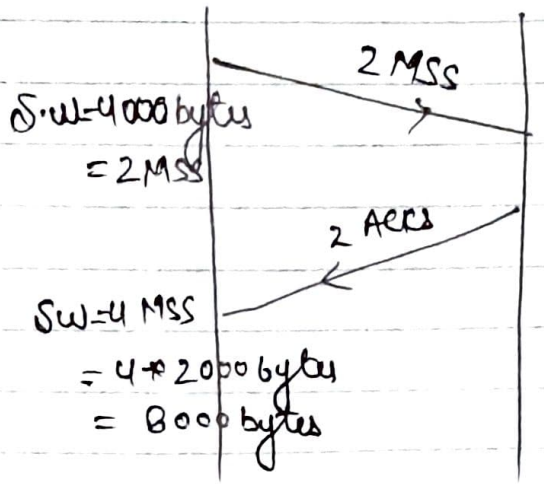
5×10^9 sec ← 1 byte

0.859 sec

In this time 1 wrap is almost completed

If they ask for 3 wrap around multiply by 3

Q26 :→



Q27 ⊢ $C + PS = MS$

Capacity (C) = 6 Mbps

Ans 2 sec

Q28 ⊢ $BW = 45$ Mbps

$\hookrightarrow 1 sec = 45 \times 10^6$ bits

$1 sec = \frac{45}{8} \times 10^6$ bytes

$= 2^{32}$ bytes ≤ wrap around

$$(\quad) \Leftarrow \frac{1 \times 2^{32}}{\left(\frac{45}{8} \times 10^6\right)} \Leftarrow$$

↓ for minutes divide by 60

Q29 :→ TTL ≥ 24 hrs

≥ 24 * 60 min

≥ 24 × 60 × 60 sec

≥ 86400

(stable record)

Network Security :→

1) $n = 23, \; g = 7$

$x = 3$

$R_1 = g^x \bmod n$

$R_1 = 7^3 \bmod 23$

$R_1 = 21$

∴ option c

2) $y = 6$

$R_2 = g^y \bmod n$

$= 7^6 \bmod 23$

$= 4$

∴ option (4)

3) (Session key) $k = g^{xy} \bmod n$

$= 7^{18} \bmod 23$

$= (7^3 \bmod 23)^6$

$= 21$

$(7^6 \bmod 23)^3$

$(4)^3$

$(4 \bmod 23)^3$

$4^3 \bmod 23$

$64 \bmod 23$

∴ option (d)

4) $p = 7$, $q = 11$
$e = 7$
$d = ?$

$n = p \times q = 7 \times 11 = 77$

$\phi(n) = (p-1) \times (q-1) = 6 \times 10 = 60$

$(d \times e) \bmod \phi(n) = 1$
$(d \times 7) \bmod 60 = 1$

Substitute the option and find out d.
$d = 43$
∴ option (d)

5) & P → plaintext $= 9$

$C = P^e \bmod n$
$C = 9^7 \bmod 77$
$C = 37$
C → ciphertext
∴ option (a)

6) $x = 3$, $g = 7$, $n = 23$

$R_1 = g^x \bmod n$
$R_1 = 7^3 \bmod 23$
$R_1 = 21$
∴ option (c)

7) $y = 5$

$R_2 = g^y \bmod n$

$= 7^5 \bmod 23$

$= 17$

$\therefore$ option (b)

8) Session key $(K) = g^{xy} \bmod n$

$= 7^{15} \bmod 23$

$= (7^5 \bmod 23)^3$

$= (17 \cdot \quad)^3$

$= (17 \bmod 23)^3$

$= 17^3 \bmod 23$

$= 14$

$\therefore$ option (a)

9) $n = 47$, $g = 3$, $x = 8$

$R_1 = g^x \bmod n$

$= 3^8 \bmod 47$

$= 28$

10) $y = 10$ $R_2 = g^y \bmod n$

$= 3^{10} \bmod 47$

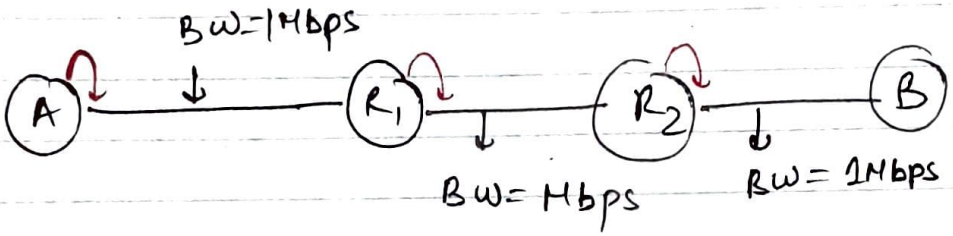
$= 17$

11) Session key $(K) = g^{xy} \bmod n$

$= 3^{80} \bmod 47$

$= 4$

Q:- The Bandwidth of each link is 10^6 bits per second = 1 Mbps. A User on host 'A' sends a file of size 10^3 bytes to host 'B'. In the 1st case single packet containing the complete file is transmitted from A to B.
In the 2nd case the file is split into 10 equal parts and these packets are transmitted from A to B.
In the 3rd case the file is split into 20 equal parts and these packets are send from A to B. In all these three cases each packet contains 100 bytes of header along with user data



1st case :-

Data size = 10^3 bytes

$$TT = \frac{\text{Data size}}{BW} = \frac{(1000 \text{ bytes} + \underset{\text{header}}{100 \text{ bytes}})}{10^6 \text{ bits/sec}}$$

$$= \frac{1100 * 8 \text{ bits}}{10^6 \text{ bits/sec}}$$

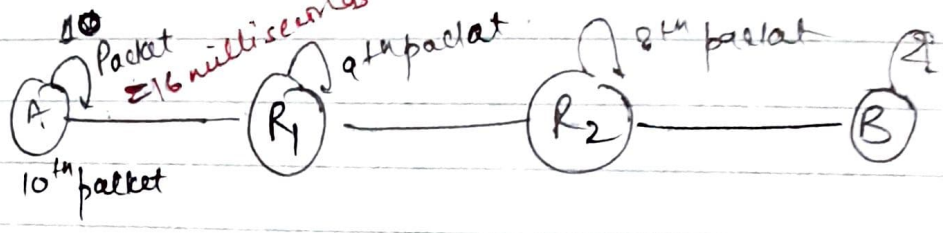
$$TT = 8.8 \text{ milliseconds}$$

269.

1100
÷ 10
110×8

Total time = 3 × 8.8
= 26.4 millisec

2nd Case :-



T.T of 1st packet = $\frac{(100 + 100)\text{ bytes}}{10^6 \text{ bits/sec}}$ (header)

= $\frac{200 \times 8 \text{ bits}}{10^6 \text{ bits/sec}}$

= 1.6 millisec.

Total TT of all 10 packet at A = ~~16 milli~~
= 1.6 × 10 millisecond

8th packet reach destination = 16 millisecond

Since there is no delay ∴ Synchronous it is
~~destination~~ 9th packet reach destination = 16 + 1.6
= 17.6 millisec

10th packet reach destination = 17.6 + 1.6
= 19.2 millisec

When 10th packet is placing at A, 9th will be at R1, 8th will reach B.

Transmission Delay

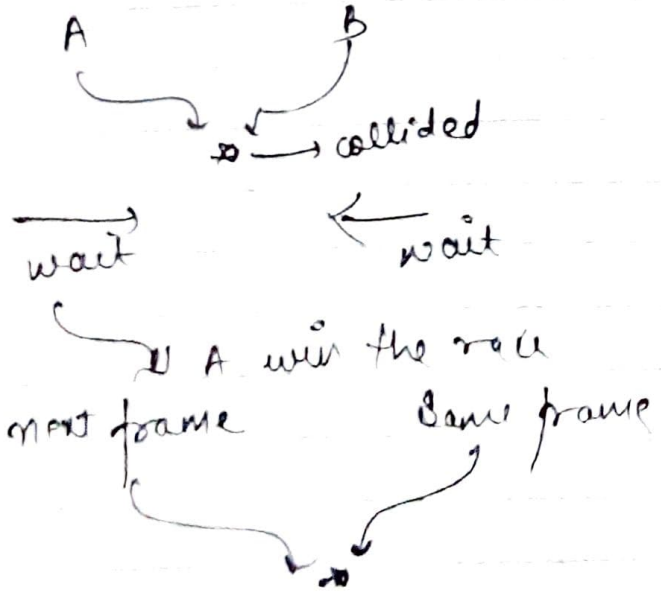
1st packet = 1.6 X 3
= 4.8 millisec

2nd packet = 4.8 + 1 * 1.6 milli sec

3rd packet = 4.8 + 2 * 1.6 millisec.

10th packet = 4.8 + 9 * 1.6
= 19.2 millisec.

Q:- A and B are only 2 stations on ethernet. Each has a steady queue of frames to send. Both A and B attempt to transmit a frame, collided and A wins the first back off race. At the end of successful transmission by A, both A and B attempt to transmit and collided. The probability that A wins the 2nd back off race is ?



9912389639
hankumar_satya@yahoo.com

K = 1
WT = (0,1) * PT

K = 2
WT = (0, 1, 2, 3) * PT

WT_A	WT_B
0	0
PT	PT
	2PT
	3PT

$$= \frac{3+2}{8} = \frac{5}{8} = 0.625$$

IP addressing → 2-4 marks (longest prefix matching, best path.)
fragmentation → 2 marks
flow and error control → 2marks
Application layer (theory) → 1marks question
ARP, RARP → 1 mark question
Stateful Stateless
what is extended MAC

Distance vector routing, link state routing

VLSM

IEEE 802.3 → always asked
↳ CSMA

On Wireless

Hidden node problem
Exponential Backoff.
CSMA/CD why there is no ACK.

Ref Circuit and Packet switching
TCP / UDP
Theoritical questions are asked of more.

NOTE:- In statistical TDM, the bandwidth is divided into slots each for a source if the source requires. There is no dedicated slot for each source in the bandwidth.
STDM do not reserve a time slot for each terminal, rather it assign a slot when the terminal is required the slot to send its data.

Multiplexer BW = 5000 bps

Eg
Calculate

$$\frac{5000}{1000} = 5$$

so if the no. of sources sending are greater than 5, no body can send and packets are backlogged.

∴ Avg no. of blocked logged packets are :-

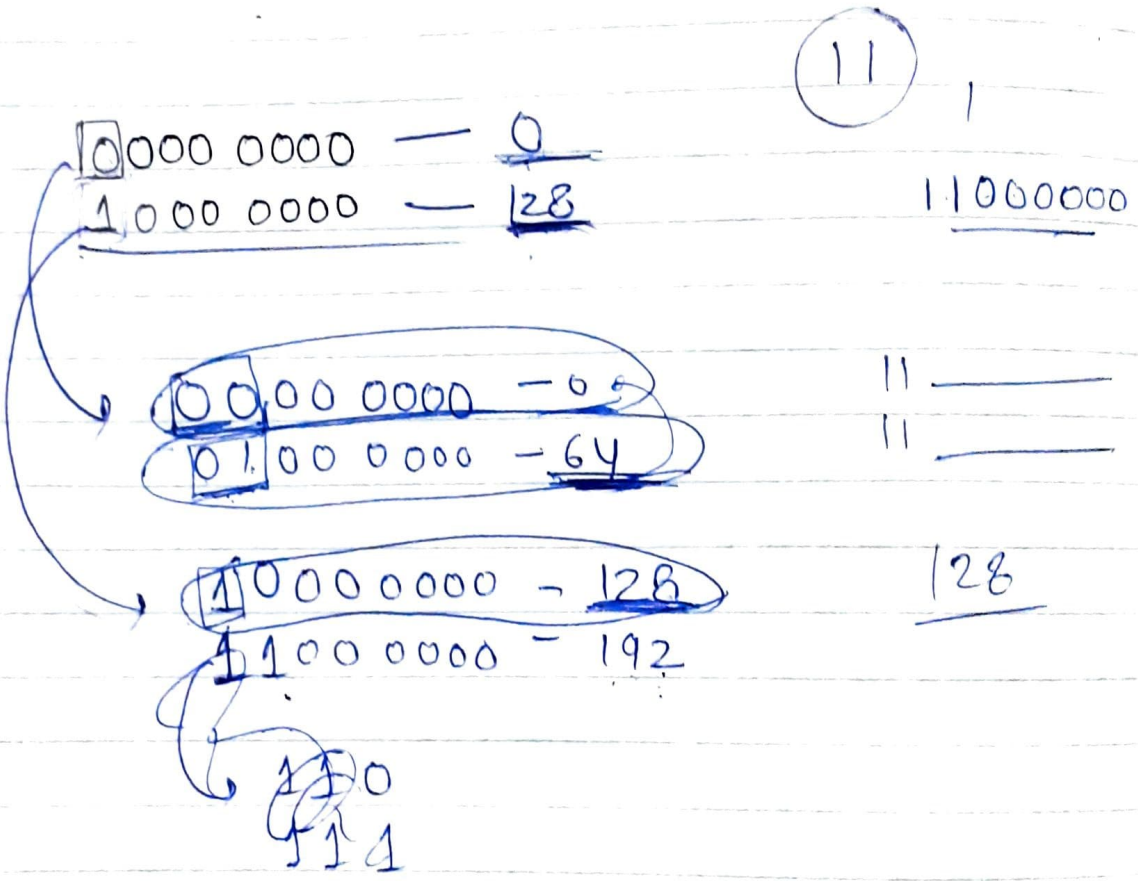
$$= \frac{6 + 9 + 7 + 6 + 10 + 7 + 8 + 9}{20}$$

$$= 3.4$$

* Current window size = Min (Congestion window, advertised Window)

* Ethernet uses a CRC algorithm to detect transmission errors.
The Internet Protocol (IP) and most higher layer protocol suite (ICMP, IGMP, UDP, UDP-lite, TCP) use a common checksum algorithm to validate the integrity of the packets that they exchange.

Gate 021



* Timeout value is set to twice the PT from sender to receiver in TCP

* Connect() system call returns an error.

- TTL changes from one hop to the next
- Checksum changes on each hop due to TTL change.
- Fragment offset may be computed again.

- the sequence no. of the subsequent segment depends on the no. of byte characters in the current segment.